Theoretical Computer Science 12 (1980) 19–37

CPO'S OF MEASURES FOR NONDETERMINISM

N. SAHEB-DJAHROMI
Faculty of Science, University of Tehran, Tehran, Iran

Communicated by R. Milner
Received December 1977
Revised June 1979

Abstract. In this approach to the semantics of nondeterminism, we introduce and study the complete partial order (cpo) of probability distributions on a domain. The approach avoids considering equivalent subsets, used in theory of powerdomains, which may lead to some unwelcome identifications. These results show that the class of probability distributions on a cpo is itself a cpo and that every probability distribution is the lub of an increasing sequence of 'finite' probability distributions. We introduce the probabilistic extensions of continuous functions in order to extend the 'usual' continuous functions on this new domain. On the other hand the structure of this cpo suggests introducing an operation called 'random selection', which is the counterpart of the 'OR' (or union) operation, commonly used in nondeterministic programs. The paper then studies the 'naturalness' of these extended notions and treats the question of continuity, which is of prime importance in the Scott theory of fixed point semantics.

1. Introduction

Different methods have been used by many authors to study semantics of nondeterministic programs. De Bakker [1], Hitchcock and Park [6] used a relational approach to handle a fixed point semantics. The method presents some difficulties as has been pointed out by Milner [11]. In a more recent paper, De Bakker [2] improved this approach by using another ordering (based on the Egli–Milner order, see below), which is computationally more meaningful than the inclusion ordering.

More fundamental studies have been carried out by Plotkin [13] and Smyth [19] who introduced the notion of powerdomains to model nondeterministic computations. The construction of strong powerdomains, introduced by Plotkin and studied also by Smyth, is based on the Egli–Milner order, which suggests that a non-empty subset A of states approximates another non-empty subset B if and only if every element of A approximates an element of B and every element of B is approximated by an element of A (the set of states is supposed to be a cpo partially ordered by 'approximation'). This 'ordering' on the class of subsets is a preorder, and in the case of non-flat cpo's is not a partial order (a cpo D is flat if $x, y \in D$ and $x \sqsubseteq y \Rightarrow x = y$ or $x = \perp$). The method of Plotkin and Smyth consists in identifying finite subsets which are equivalent with respect to this preorder. This is a powerful and elegant mathematical method. Nevertheless the equivalence may imply identifications on the class of finitely generable subsets which are not computationally meaningful.

Another approach based on category theory has been developed by Lehmann [7], who suggests that domains are categories, where every denumerable chain has a colimit.

In the present paper, we suppose that domains are cpo's and we then prove that the class of probability distributions on a domain is itself a domain. Here we intend to identify the set of possible states, together with their respective 'degrees of frequency', with a probability distribution on the domain of states. This should also enable us to take into account a statistical evaluation of possible outcomes.

At this point it will be suitable to consider the following informal example inspired by Lehmann's introductory one [7]. Suppose that the domain D is the set of non-negative integers enriched by ∞ and ordered as in Fig. 1. Consider now the following 'recursive nondeterministic program' on D

$$Y(\lambda x\,.\,p \to 0, q \to x+1)$$

where p and q are two non-negative real numbers such that $p+q=1$. This program might informally be denoted by the least fixed point (if it exists) of a 'random transformation' which assigns to any $x \in D$, 0 with probability p and $x+1$ with probability q. Operationally it may be interpreted as a 'probabilistic recursive procedure' which yields 0 with probability p, or with probability q adds 1 to the result which it hopefully—by repeating the whole procedure—yields. Note that in the cpo, D, an infinite computation does not necessarily correspond to 0 (the bottom element).

More formally, as we shall see, the above random transformation is a function ϕ on the set $\mathscr{P}_D$ of probability distributions on D. Here, a probability distribution P is dominated by another one P' (this will be denoted by $P \sqsubseteq_{\mathscr{P}} P'$) if and only if for any

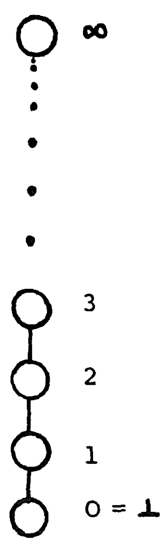


Fig. 1.

integer n, $P(\{x \in D \mid x \geqslant n\}) \leqslant P'(\{x \in D \mid x \geqslant n\})$, which informally means that P' is distributed on higher elements (in comparison with P). As we shall prove, $\mathcal{P}_D$ equipped with this ordering is a cpo and ϕ is continuous (for the definition of cpo and continuous functions on a cpo see [10]). Therefore ϕ has a least fixed point in $\mathcal{P}_D$, which is given by the well-known formula $\bigsqcup_n \phi^n(\bot_{\mathcal{P}})$, where $\bot_{\mathcal{P}}$ is the probability distribution concentrated on $\bot$. A computation, which is formally discussed at the end, yields

$$\bigsqcup_n \phi^n(\bot_{\mathcal{P}}) = \begin{cases} \{(i, pq^i) \mid i \in \mathbf{N}\}, & \text{if } p \neq 0, \\ \{(\infty, 1)\}, & \text{if } p = 0, \end{cases}$$

where the first one is a geometric probability distribution (i.e. the non-negative integer i has probability pq^i to appear) and the second one is the probability distribution concentrated on ∞.

When dealing with probability distributions, an important question is whether or not discrete probability distributions are adequate for our purpose, or in other words, can every probability distribution, involved here, be determined uniquely by its values on singletons. The following example provides a negative answer to this question and shows that the class of discrete probability distributions is not closed under lub. Let D be the set of all strings (finite and infinite) on $\{0, 1\}$, ordered as follows.

for $x, y \in D$, $x \sqsubseteq y$ iff x is a prefix of y.

Consider the sequence

$$\{(\bot, 1)\}, \{(0, \tfrac{1}{2}), (1, \tfrac{1}{2})\}, \{(00, \tfrac{1}{4}), (01, \tfrac{1}{4}), (10, \tfrac{1}{4}), (11, \tfrac{1}{4})\}, \ldots,$$

of probability distributions, where each element $(x, (\frac{1}{2})^{n-1})$, (i.e. x with probability $(\frac{1}{2})^{n-1}$) in the nth term is substituted by two elements $(x0, (\frac{1}{2})^n)$ and $(x1, (\frac{1}{2})^n)$, (i.e. $x0$ and $x1$ each one with probability $(\frac{1}{2})^n$) in the next term. This sequence corresponds roughly to the computation related to

while true do ($\frac{1}{2} \rightarrow$ print 0, $\frac{1}{2} \rightarrow$ print 1).

It is an increasing sequence of probability distributions in the sense that each term is the result of transmitting the previous term to higher elements. (Actually this notion remains to be formalized). In this case a pointwise probabilistic study of the limit outcome does not provide any interesting information, since the probability that it takes some fixed value is zero. Nevertheless, we do not believe that this really is a disadvantage and that we should consider this case as an unfavourable one: We only need to borrow more sophisticated tools from probability theory. In probability theory there exist many well-known distributions which are not uniquely determined by their values on singletons, and in the case of real random variables the class of intervals (more precisely the class of Borel sets) provides a measurable space for a formal study (see [8, Chapter III]). We have here Scott's topology [18], and the corresponding class of Borel sets (i.e. the σ-algebra generated by the class of open sets, see next section) should enable us to define a suitable measurable space. Although in this particular example (and in many similar ones), the probability that the random limit takes a given value is zero, there remain many non-obvious interesting questions about the probabilistic behaviour of finitary characteristics of the random outcome. For instance, one could put forward the following questions:

(a) what is the probability of having a prime number of occurrences of 1 before the first occurrence of 0 in the (random) outcome?

(b) what is the probability that, in every finite prefix of the outcome, the number of occurrences of 0 does not exceed that of 1?

The answers are $\sum_{n\text{ prime}} (\frac{1}{2})^{n+1}$ and 0 respectively, but what is important here is that the sets defining the above events (and all similarly defined) are Borel sets and can be defined in terms of open sets by using countable set operations. Therefore, in order to take these events into account, it will be suitable to define probability distributions, involved here, on the σ-algebra generated by the class of open sets (see next section).

The application of probability theory in programming and algorithms is not a new concept. Several authors, mainly Rabin [14] and Paz [12], have intensively studied the notions of probabilistic algorithms and probabilistic automata. However, to the author's knowledge, the present approach is a new one based on the Scott theory of fixed point semantics. It aims to provide a probabilistic foundation for nondeterministic computations.

2. Preliminaries and notations

We denote the non-empty set of states and its ordering by $(D, \sqsubseteq)$. We sometimes refer to D as a 'domain'. It is supposed to be algebraic with countable basis [19]. The least element will be denoted by $\perp$. We denote the basis of D by Q. Markowsky and Rosen [9] have discussed bases in full detail. We need only the following assertions about Q:

(a) Q is the set of isolated elements of D;

(b) Q is countable;

(c) Every $x \in D$ is the lub of some increasing sequence in Q.

By a continuous function on D we mean a ω-chain continuous function on D [10].

A topology $\mathcal{O}$ on D is defined in the following way. A subset U of D is open if and only if whenever $x \in U$ and $x \sqsubseteq y$, then $y \in U$ and whenever the lub of an increasing sequence (x_n) belongs to U, then $x_n \in U$, for some n. Scott [18] introduced a similar topology to study the limits in continuous lattices. The transformations of Scott's topology on lattices into the present one on cpo's is straightforward. The following results are standard [18]:

(d) $(D, \mathcal{O})$ is a T_0-space;

(e) $(D, \mathcal{O})$ is separable and $\{\{x \mid q \sqsubseteq x\} \mid q \in Q\}$ is a base of this topology;

(f) A function $f: D \to D$ is continuous if and only if it is $\mathcal{O}$-continuous;

(g) $q \in Q$ if and only if $\{x \mid q \sqsubseteq x\}$ is open.

A σ-algebra (see [5, p. 28]) or σ-field (see [8, p. 59]) $\mathcal{B}$ on a set E is a non-empty class of subsets of E closed under all countable set operations. Here, by the introductory discussion, we use the σ-algebra generated by $\mathcal{O}$ (i.e. minimal σ-algebra including $\mathcal{O}$) to define probability distributions. We denote this σ-algebra by $\mathcal{B}$. It is sometimes called the class of Borel sets in $(D, \mathcal{O})$. Therefore by a probability measure (or distribution) on D, we mean a σ-additive function $P: \mathcal{B} \to [0, 1]$ such that $P(D) = 1$. This class of Borel sets in $P\omega$ has been studied by Tang [20] for another purpose. Here we are not concerned with its detailed constructive study; all we need about $\mathcal{B}$ are the following assertions, which are easy consequences of its definition:

(h) $\mathcal{B}$ contains every singleton and consequently every countable subset of D. In particular any subset of Q belongs to $\mathcal{B}$;

(i) $\mathcal{B}$ coincides with the σ-algebra generated by the class $\{\{x \in D \mid q \sqsubseteq x\} \mid q \in Q\}$.

We denote the set of probability distributions on D by $\mathcal{P}_D$. If $P \in \mathcal{P}_D$ and $x \in D$, then we write $P(x)$ instead of $P(\{x\})$. We let $|P| = \{x \in D \mid P(x) > 0\}$. $|P|$ is countable and if P is such that $P(|P|) = 1$, then we may represent it by $\{(x, P(x)) \mid x \in |P|\}$. P is said to be *finite* if and only if $|P|$ is a finite subset of Q and $P(|P|) = 1$. The set of finite probability distributions is denoted by $\mathcal{F}_D$.

3. CPO of $\mathcal{P}_D$.

Definition 1. For $P, P' \in \mathcal{P}_D$, we let $P \sqsubseteq_{\mathcal{P}} P'$ (P is dominated in a probabilistic sense by P') if and only if, for $\forall U \in \mathcal{O}$, $P(U) \leq P'(U)$.

Theorem 1. *$(\mathcal{P}_D, \sqsubseteq_{\mathcal{P}})$ is poset with a least element.*

Proof. $\sqsubseteq_{\mathcal{P}}$ is clearly reflexive and transitive. In order to prove its antisymmetry, suppose $P \sqsubseteq_{\mathcal{P}} P'$ and $P' \sqsubseteq_{\mathcal{P}} P$. Then, by definition, P and P' are equal on $\mathcal{O}$. On the other hand $\mathcal{O}$ is closed under finite union and intersection operations and this implies $P = P'$ (see [3, p. 185, Theorem 2]). The least element is $\{(\perp, 1)\}$, i.e. the probability measure concentrated on $\perp$.

Theorem 2. *Suppose $P, P' \in \mathcal{F}_D$. Then $P \sqsubseteq_{\mathcal{P}} P'$ iff*

(i) $(\forall A \subset |P|, A \neq \emptyset)\ (\exists B \subset |P'|)\ (A \sqsubseteq_M B$ and $P(A) \leq P'(B))$, or iff

(ii) $(\forall A \subset |P'|, A \neq \emptyset)\ (\exists B \subset |P|)\ (B \sqsubseteq_M A$ and $P(B) \geq P'(A))$, where $\sqsubseteq_M$ is the Egli–Milner order, discussed previously.

(i) and (ii) reflect the intuitive idea that P' is the result of transmitting P to higher sets or P is the result of transmitting P' to lower sets (in the Egli–Milner sense).

Proof. We show only the equivalence of $P \sqsubseteq_{\mathcal{P}} P'$ with (i); the second part of the theorem may be proved similarly. Suppose $P \sqsubseteq_{\mathcal{P}} P'$ and consider any non-empty subset A of $|P|$. Then $B = \{y \in |P'| \mid \exists x \in A \text{ s.t. } x \sqsubseteq y\}$ satisfies (i). Assume now (i) and consider any open set U. Then there exists $B \subset |P'|$ such that $U \cap |P| \sqsubseteq_M B$ and

$P(U \cap |P|) \leqslant P'(B)$. Therefore we have $P(U) = P(U \cap |P|) \leqslant P'(B)$. On the other hand $U \cap |P| \sqsubseteq_M B$ implies $B \subset U$ and consequently $P'(B) \leqslant P'(U)$. This yields $P(U) \leqslant P'(U)$.

In order to prove that $\mathscr{P}_D$ is a cpo, we shall need the following definition.

Definition 2. A subset T of D is called a *crescent*, if and only if there exists two open sets U and V such that $V \subset U$ and $T = U \setminus V$. We denote the set of all crescents of $(D, \mathcal{O})$ by $\mathscr{S}$.

Lemma 1. (a) $\mathcal{O} \subset \mathscr{S}$;

(b) $T \in \mathscr{S}$ *if and only if there are some open set A and some closed set B such that* $T = A \cap B$;

(c) T *is a crescent if and only if*

(i) *if* $x, y \in T$ *and* $x \sqsubseteq z \sqsubseteq y$, *then* $z \in T$,

(ii) *whenever* (x_n) *is an increasing sequence in T, then* $\bigsqcup_n x_n \in T$, *and*

(iii) *whenever* (x_n) *is an increasing sequence such that* $\bigsqcup_n x_n \in T$, *then for some* n, $x_n \in T$;

(d) $\mathscr{S}$ *is a semi-ring (see [5, p. 22]) or semi-algebra (see [15, p. 224]);*

(e) *A function* $\mu : \mathscr{S} \to [0, 1]$ *is uniquely extensible to a probability measure on* $\mathscr{B}$ *if and only if it is finitely additive, σ-subadditive (i.e. countably subadditive) and* $\mu(D) = 1$.

Proof. (a), (b), (c) and (d) are easily checked. For (e) see [15, pp. 223–224].

Lemma 2. *Every increasing sequence in* $\mathscr{F}_D$ *has a lub in* $\mathscr{P}_D$.

Proof. Let (P_n) be an increasing sequence in $\mathscr{F}_D$. Then, for any $U \in \mathcal{O}$, we let $\mu(U) = \lim_{n\to\infty} P_n(U) = \sup_n P_n(U)$. Since $P_n(U)$ is increasing and bounded by 1, this limit exists. If the lub of (P_n) exists, then by definition, its restriction to $\mathcal{O}$ must be μ. On the other hand if μ is extensible to a probability measure, then the extension is unique. Therefore, by clause (e) of Lemma 1, it is sufficient to prove that μ is extensible to $\mathscr{S}$ and its extension satisfies the mentioned conditions in (e).

For any $T \in \mathscr{S}$ such that $T = U \setminus V$, where U, V$\in \mathcal{O}$ and $V \subset U$, let $\bar{\mu}(T) = \mu(U) - \mu(V)$. It is not difficult to check that this definition is unambiguous and $\bar{\mu} = \lim_{n\to\infty} P_n$. In addition the finite additivity $\bar{\mu}$ is an easy consequence of that of P_n. It remains, therefore to prove the σ-subadditivity of $\bar{\mu}$, since clearly $\bar{\mu}(D) = 1$. In order to prove this, let $(T_m) = (U_m \setminus V_m)$, $m = 1, 2, \ldots$, be a sequence of pairwise disjoint crescents such that $T = \bigcup_m T_m = (U \setminus V)$ is also a crescent. Then we have to prove $\bar{\mu}(T) \leqslant \sum_{m=1}^{n} \bar{\mu}(T_m)$. In order to prove this inequality, we assume that there is some $\alpha > 0$ such that for any positive integer p, $\bar{\mu}(T) - \sum_{1 \leqslant m \leqslant p} \bar{\mu}(T_m) \geqslant 2\alpha$ and derive a contradiction. Since $\bar{\mu}$ is the limit of (P_n), this relation may be carried on (P_n):

$$(\forall p)(\exists N)\left(n \geqslant N \Rightarrow P_n\left(\bigcup_{m>p} T_m\right) \geqslant \alpha\right). \tag{1}$$

Now we can define a sequence (A_n) of finite subsets of T and subsequence (P_{N_n}) of (P_n) such that

$$P_{N_n}(A_n) \geqslant \alpha/2^{n-1} \quad \text{and} \quad (\forall y \in A_{n+1})(\exists x \in A_n)(x \sqsubseteq y)$$

as follows.

Since $(P_n(U))$ is convergent, it is possible to choose N_1 such that $|P_{n'}(U^C) - P_{n''}(U^C)| \leqslant \frac{1}{2}\alpha$, (where U^C denotes the complement of U in D), whenever n', $n'' \geqslant N_1$. Let $A_1 = |P_{N_1}| \cap T$. Since A_1 is finite and $T = \bigcup_m T_m$, it is possible to choose p_2 such that $\cup_{m \leqslant p_2} T_m$ includes A_1.

Apply now (1) to p_2 in order to obtain $N_2' > N_1$ such that $P_n(\bigcup_{m>p_2} T_m) \geqslant \alpha$, whenever $n \geqslant N_2'$. Suppose that N_2'' is such that

$$\left|P_{n'}\left(\bigcup_{m \leqslant p_2} V_m^C\right) - P_{n''}\left(\bigcup\nolimits_{m \leqslant p_2} V_m^C\right)\right| \leqslant \tfrac{1}{4}\alpha,$$

whenever n', $n'' \geqslant N_2''$, and let $N_2 = \sup\{N_2', N_2''\}$. We can prove that the finite subset $A_2' = |P_{N_2}| \cap (\bigcup_{m>p_2} T_m)$ has a subset A_2 such that $P_{N_2}(A_2) \geqslant \frac{1}{2}\alpha$ and $(\forall y \in A)(\exists x \in A)(x \sqsubseteq y)$.

In order to prove this, let $B_2 = \{y \in A_2' \mid \forall x \in A_1, x \not\sqsubseteq y\}$ and then apply (ii) of Theorem 2 to P_{N_1}, P_{N_2} and $B_2 \cup U^C$ in order to prove $P_{N_2}(B) \leqslant \frac{1}{2}\alpha$, which yields $P_{N_2}(A_2' \backslash B) \geqslant \frac{1}{2}\alpha$.

We now choose p_3 such that $\bigcup_{m \leqslant p_3} T_m$ includes $|P_{N_2}| \cap T$ and apply (1) again to obtain $N_3' > N_2$ such that $P_n(\bigcup_{m>p_3} T_m) \leqslant \alpha$, whenever $n \geqslant N_3'$. Suppose again N_3'' is such that

$$\left|P_{n'}\left(\bigcup_{m \leqslant p_3} V_m^C\right) - P_{n''}\left(\bigcup_{m \leqslant p_3} V_m^C\right)\right| \leqslant \tfrac{1}{8}\alpha,$$

whenever n', $n'' \geqslant N_3''$, and let $N_3 = \sup\{N_3', N_3''\}$. Again the finite set $|P_{N_3}| \cap (\bigcup_{m>p_3} T_m)$ has a subset A_3 such that $P_{N_3}(A_3) \geqslant \frac{1}{4}\alpha$ and $(\forall y \in A_3)$ $(\exists x \in A_2)(x \sqsubseteq y)$. For the proof of this see below, the general case of N_i.

Suppose, in general, that N_i, A_i and $p_i (i \geqslant 2)$ are defined such that

$$P_{N_i}(A_i) \geqslant \alpha/2^{i-1}, \qquad (\forall y \in A_i)(\exists x \in A_{i-1})(x \sqsubseteq y),$$

$$B_i = \{y \in |P_{N_i}| \cap T \mid \forall x \in A_{i-1}, x \not\sqsubseteq y\}$$

with

$$P_{N_i}(B_i) \leqslant \alpha - \frac{\alpha}{2^{i-1}} \quad \text{and} \quad \left|P_{n'}\left(\bigcup_{m \leqslant p_i} V_m^C\right) - P_{n''}\left(\bigcup_{m \leqslant p_i} V_m^C\right)\right| \leqslant \frac{\alpha}{2^i},$$

whenever n', $n'' \geqslant N_i$. Then N_{i+1}, A_{i+1} and p_{i+1} will be defined as follows.

We choose p_{i+1} such that $\bigcup_{m\leqslant p_{i+1}} T_m$ includes $|P_{N_i}|\cap T$ and apply (1) to p_{i+1} in order to obtain $N'_{i+1}>N_i$ such that $P_n(\bigcup_{m>p_{i+1}} T_m)\geqslant\alpha$, whenever $n\geqslant N'_{i+1}$. Suppose N''_i is such that

$$\left|P_{n'}\left(\bigcup_{m<p_{i+1}} V_m^{\mathrm{C}}\right)-P_{n''}\left(\bigcup_{m<p_{i+1}} V_m^{\mathrm{C}}\right)\right|\leqslant\frac{\alpha}{2^{i+1}},$$

whenever n', $n''\geqslant N''_{i+1}$. Let $N_{i+1}=\sup\{N'_{i+1},N''_{i+1}\}$. Now let $A'_{i+1}=|P_{N_{i+1}}|\cap T$. Then we prove that A'_{i+1} has a subset A_{i+1}, such that $P_{n_{i+1}}(A_{i+1})\geqslant\alpha/2^i$ and $(\forall y\in A_{i+1})\ (\exists x\in A_i)\ (x\sqsubseteq y)$. To do this, let $B_{i+1}=\{y\in A'_{i+1}|\forall x\in A_i, x\not\sqsubseteq y\}$. If we apply (ii) of Theorem 2 to P_{N_i}, $P_{N_{i+1}}$ and $B_{i+1}\cup B_i\cup(\bigcup_{m\leqslant p_i} V_m^{\mathrm{C}})$, then by using the facts that the change of probability for $\bigcup_{m\leqslant p_i} V_m^{\mathrm{C}}$ is bounded by $\alpha/2^i$ and that $P_{N_i}(B_i)\leqslant\alpha-\alpha/2^{i-1}$, we obtain $P_{N_{i+1}}(B_{i+1})\leqslant\alpha-\alpha/2^i$, which yields $P_{N_{i+1}}(\{y|\exists x\in A_i, x\sqsubseteq y\})\geqslant\alpha/2^i$.

Now, we may apply König's infinity lemma (see e.g. [21, p. 40]) to the sequence (A_n) to obtain an increasing sequence (x_n), with $x_n\in A_n$ for any n. By clause (c, ii) of Lemma 1, $\bigsqcup_n x_n\in T$. Hence $\bigsqcup_n x_n\in T_{m_0}$, for some m_0. But then, by clause (c, iii) of Lemma 1, all but a finite number of x_n are in T_{m_0}. This is not possible, since by the construction of (A_n), if $x_n\in T_{m_0}$, then $x_{n+1}\notin T_{m_0}$.

For the sake of smoothness, we prove the following lemma. From now on for any $q\in Q$, we let $V_q=\{x\,|\,q\sqsubseteq x\}$.

Lemma 3. *Suppose $P\in\mathcal{P}_D$ and let U be any non-empty open set. Then, for any $\varepsilon>0$, there exists a finite subset $\{r_1,\ldots,r_m\}$ of $Q\cap U$ such that*

$$P\left(\bigcup_{1\leqslant i\leqslant m} V_{r_i}\right)\geqslant P(U)-\varepsilon.$$

Proof. It is not difficult to check that $U=\bigcup\{V_q\,|\,q\in Q\cap U\}$. On the other hand, there is a well-known result in measure theory, which asserts that if an increasing sequence (A_n), in a measure space $(D,\mathcal{B},P)$, converges from below to A, then $P(A_n)$ converges to $P(A)$ (See [5, p. 38] or [8, p. 85]). This proves the lemma.

Theorem 3. *Every element of $\mathcal{P}_D$ is the lub of some increasing sequence in $\mathcal{F}_D$.*

Proof. If Q is finite, then the theorem is obvious. Otherwise let $q_0(=\bot)$, $q_1,q_2,\ldots$ be an infinite enumeration of Q without repetitions. First we define a sequence $(\mathcal{A}_n)=((A_m^n)_{m=0,\ldots,k_n})_{n=0,1,2,\ldots}$ of finite partitions of D, where each term is a refinement of the previous one and each A_m^n has a least element b_m^n in Q. Then P_n is defined by letting $P_n(b_m^n)=P(A_m^n)$.

Consider any finite non-empty sequence $S = r_0, \ldots, r_l$ in Q such that $r_0 = \perp$. For S, we define a partition $\mathscr{A}_S = (A_i)_{i=0,\ldots,l}$ of D into $l+1$ crescents as follows:

$$A_i' = V_{r_i} \setminus (\bigcup \{A_j' \mid 0 \leq j < i, r_j \not\sqsubseteq r_i\}),$$

$$A_i = A_i' \setminus (\bigcup \{A_j' \mid 0 \leq j \leq l, A_j \subsetneq A_i'\}).$$

It is not difficult to see that $(A_i)_{i=0,\ldots,l}$ is a partition of D and that r_i is the least element of A_i. Also, if $S = r_0, \ldots, r_l$ and $S' = r_0, \ldots, r_l, r_{l+1}, \ldots, r_{l+k}$, then $\mathscr{A}_{S'}$ is a refinement of $\mathscr{A}_S$.

Let $S_0 = q_0$ and $\mathscr{A}_0 = \mathscr{A}_{S_0}$. If $\mathscr{A}_n$ is already defined, then $\mathscr{A}_{n+1}$, derived from S_{n+1}, is defined as follows. Suppose $q_{n+1} \in A_l^n$. Let $B_{n+1} = D \setminus A_l^n$ and $C_{n+1} = B_{n+1} \cap V_{q_{n+1}}$. It is not difficult to check that C_{n+1} is open. If $P(C_{n+1}) = 0$, then we let $S_{n+1} = S_n, q_{n+1}$. Otherwise, by Lemma 3, there exist $r_1, \ldots, r_h \in C_{n+1} \cap Q$ such that $P(\bigcup_{1 \leq i \leq h} V_{r_i}) \geq \frac{1}{2}P(C_{n+1})$ and we let $S_{n+1} = S_n, q_{n+1}, r_1, \ldots, r_h$. Let (P_n) be defined by $P_n(b_m^n) = P(A_m^n)$, $m = 0, 1, \ldots, k_n$.

Since $\sum_{0 \leq m \leq k} P(A_m^n) = 1$, the above equality determines uniquely P_n as an element of $\mathscr{F}_D$. We now prove the following assertions about (P_n):

(i) (P_n) is increasing. For any open set U, $P_n(U) = \sum P(b_m^n)$, where the summation is extended to all m for which $b_m^n \in U$. But then, by the definition of $P(b_m^n)$ and the fact that $b_m^n \in U$ if and only if $A_m^n \subset U$, we have $P_n(U) = \sum P(A_m^n)$, where the summation is extended to all m for which $A_m^n \subset U$. This equality, and the fact that $\mathscr{A}_{n+1}$ is a refinement of $\mathscr{A}_n$, imply $P_n(U) \leq P_{n+1}(U)$.

(ii) $P_n(U) \sqsubseteq_{\mathscr{P}} P(U)$. This is an immediate consequence of $P_n(U) = \sum P(A_m^n)$ mentioned above.

(iii) $\bigsqcup_n P_n = P$. To prove this, it is sufficient to show that, for any non-empty open set U, we have $\sup_n P_n(U) = P(U)$. To do this, since $P_n(U) = \sum P(A_m^n)$, where the summation is extended to all m for which $A_m^n \subset U$, we have only to prove that the probability (with respect to P) of $B_U^n = \{x \in U \mid \forall A_m^n \subset U, x \notin A_m^n\}$ converges to zero, as $n \to \infty$ (for $P(U) - P_n(U) = P(B_U^n)$). It is easy to check that for any $q_i \in Q$, $P_n(V_{q_i}) \geq \frac{1}{2}P(V_{q_i})$, whenever $n \geq i$. We now prove that for any $\varepsilon > 0$ and n there exists $m > n$ such that $P(B_U^m) \leq \frac{1}{2}P(B_U^n) + \varepsilon$.

If $P(B_U^n) = 0$, then we have done. Otherwise, since B_U^n is a finite union of disjoint crescents, it follows from Lemma 3 that there exist $r_1, \ldots, r_j \in B_U^n$ such that

$$P\left(\left(\bigcup_{1 \leq i \leq j} V_{r_i}\right) \cap B_U^n\right) \geq P(B_U^n) - \varepsilon.$$

Thus, whenever $m > n$ is sufficiently large such that S_m contains $r_1, \ldots, r_j$, then $V_{r_1}, \ldots, V_{r_j}$ are included in U, and consequently

$$P(B_U^m) \leq \tfrac{1}{2}P(B_U^n) + \varepsilon.$$

On the other hand, since B_U^n is decreasing $\lim_{n\to\infty} P(B_U^n) = P(\bigcap_n B_U^n)$ exists. Therefore, it follows from the above inequality that $\lim_{n\to\infty} P(B_U^n) = 0$.

This yields $\sup_n P_n(U) = P(U)$.

Remark. In the case of consistently complete cpo's, there exists a short proof for this theorem (see [16]).

Corollary 1. *Suppose $P, P' \in \mathscr{P}_D$ and $P \sqsubseteq_{\mathscr{P}} P'$. For every increasing sequence (P_n) in $\mathscr{F}_D$ such that $P = \bigsqcup_n P_n$, there exists an increasing sequence P'_n in $\mathscr{F}_D$ such that $P' = \bigsqcup_n P'_n$ and $P_n \sqsubseteq_{\mathscr{P}} P'_n$ for all n.*

Proof. By the above theorem, there exists a sequence (P''_n) such that $P' = \bigsqcup_n P''_n$. We now define a subsequence $(P'_n) = (P''_{N_n})$ of (P''_n) which also satisfies $P_n \sqsubseteq_{\mathscr{P}} P'_n$, for any n. Since $|P_n|$ is finite, there exists N_n such that the set of the N_nth first elements of Q, considered in the proof of the above theorem for defining (P''_n), includes $|P_n|$. Consequently, by the facts $P \sqsubseteq_{\mathscr{P}} P'$ and $P_n(U) = P(\bigcup\{V_q | q \in |P_n|\})$, $P_n \sqsubseteq_{\mathscr{P}} P''_{N_n}$.

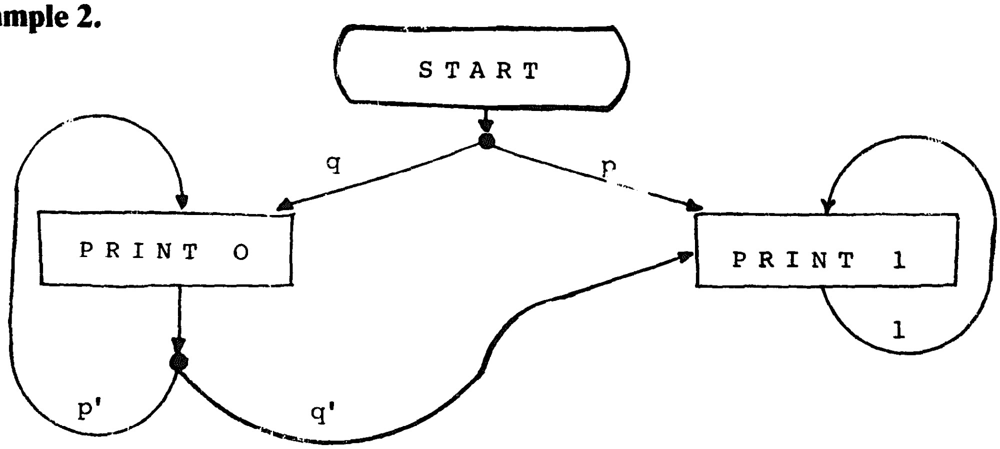
Theorem 4. *$(\mathscr{P}_D, \sqsubseteq_{\mathscr{P}})$ is a cpo.*

Proof. It is sufficient to prove that every increasing sequence $(P_n)_{n=0,1,2,\ldots}$ in $\mathscr{P}_D$ has a lub. By the above theorem and its corollary, there exist sequences $(P_n^m)_{m=0,1,\ldots}$, for $n = 0, 1, \ldots$ in $\mathscr{F}_D$ such that $P_n = \bigsqcup_m P_n^m$ for any n, and $P_n^m \sqsubseteq_{\mathscr{P}} P_{n+1}^m$ for any m and n. Then we have $(\bigsqcup_n P_n)(U) = \sup_n P_n^n(U)$ for any open U.

Example 1. We are now able to treat the second introductory example formally. Let Q be the denumerable set of finite strings on $\{0, 1\}$. Then any open subset U of D equals $\bigcup\{qD \mid q \in Q \cap U\}$, where $qD = \{qx \mid x \in D\}$. Let $P_n = \{(x, \frac{1}{2}^n) \mid x \in Q$ and $\lg(x) = n\}$, where $\lg(x)$ is the length of the finite string x. It is easy to check that (P_n) is increasing and, therefore by virtue of Lemma 2, $P = \bigsqcup_n P_n$ exists. P is not uniquely determined by its values on singletons, but it is by its values on $\mathscr{O}$. In order to compute $P(U)$, where $U \in \mathscr{O}$, let $A(U)$ be the set of the minimal elements of $U \cap Q$. Then $(qD)_{q \in A(U)}$ is a class (possibly empty) of pairwise disjoint open sets such that $U = \bigcup\{qD \mid q \in A(U)\}$. Consequently

$$P(U) = \sum_{q \in A(U)} P(qD) = \sum_{q \in A(U)} 1/2^{\lg(q)}.$$

Example 2.



$p, q \geq 0, \quad p + q = 1, \quad p', q' \geq 0, \quad p' + q' = 1.$

Fig. 2.

The probabilistic flow chart program' shown in Fig. 2 differs from a usual one in that it admits at two points different random choices, characterized by the pairs (p, q) and (p', q') respectively. One can easily check that if x_n is the printed string at the nth step (i.e. after the apparition of the nth character), then it takes values $0^i\,1^{n-i}$ with probability $qp'^{i-1}q'$ (where $1 \le i \le n-1$), 1^n with probability p and 0^n with probability qp'^{n-1}. Thus the probability distribution related to the nth step of the computation is given by

$$P_n = \{(0^n, qp'^{n-1})\} \cup \{(0^i 1^{n-i}, qp'^{i-1}q') \mid 1 \le i \le n-1\} \cup \{(1^n, p)\}.$$

This is an increasing sequence of probability distributions on $(D, \sqsubseteq)$ (where $(D, \sqsubseteq)$ is the same as in the previous example) and its lub is given by

$$\bigsqcup_n P_n = \begin{cases} \{(1^\omega, p)\} \cup \{(0^{i+1}1^\omega, qp'^i q') \mid i \ge 0\}, & \text{if } q' > 0, \\ \{(1^\omega, p), (0^\omega, q)\}, & \text{if } q' = 0, \end{cases}$$

where a^ω is the infinite string $aaa\ldots$.

Remark. The previous results show that $(\mathcal{P}_D, \sqsubseteq_{\mathcal{P}})$ is a cpo and $\mathcal{P}_D$ is generated by $\mathcal{F}_D$. Actually it is possible to prove that $\mathcal{F}_D$ has countable subsets generating $\mathcal{F}_D$. Consider, for example,

$$\mathcal{R}_D = \{P \in \mathcal{F}_D \mid \forall x \in |P|, P(x) \text{ is rational}\}.$$

It is easy to see that every element of $\mathcal{F}_D$ is the lub of some increasing sequence in $\mathcal{R}_D$.

Nonetheless $\mathcal{P}_D$ is not algebraic in general; indeed $\{(\bot, 1)\}$ is its only isolated element. Consider the cpo in Fig. 3. In this example $\mathcal{F}_D = \mathcal{P}_D$. Let $P = \{(\bot, p), (\top, 1-p)\}$, where $0 \le p < 1$ and $P_n = \{(\bot, p+1/n), (\top, 1-p-1/n)\}$, for $n \ge 1/(1-p)$. Then $\bigsqcup_n P_n = P$; but for no n, $P \sqsubseteq_{\mathcal{P}} P_n$. This should not be surprising, since the lattice $[0, 1]$ equipped with the usual ordering is not algebraic.

Theorem 5. *The mapping $\theta : D \to \mathcal{P}_D$, defined by $\theta(x) = \{(x, 1)\}$ is continuous.*

Proof. For any increasing sequence (x_n) in D and any open set U, we have

$$\begin{aligned} \Big\{\Big(\bigsqcup_n x_n, 1\Big)\Big\}(U) &= \textbf{if} \bigsqcup_n x_n \in U \textbf{ then } 1 \textbf{ else } 0 \\ &= \sup_n\, (\textbf{if } x_n \in U \textbf{ then } 1 \textbf{ else } 0) \\ &= \bigsqcup_n \{(x_n, 1)\}(U). \end{aligned}$$

Fig. 3.

Remark. The above result allows us to embed D in $\mathscr{P}_D$. From now on we identify $\sqsubseteq_{\mathscr{P}}$ with $\sqsubseteq$ and $\{(x, 1)\} \in \mathscr{P}_D$ with $x \in D$, whenever no ambiguity is possible.

4. Operations on $\mathscr{P}_D$

The first operation introduces a random element.

4.1. Random selection

In considering programs which choose different computations at random, we may treat the simple but interesting case of those which may select at random between two possibilities in steps of their computations. The more general case of programs which use finite probabilistic branchings may be transformed into this case (for any probabilistic finite branching there exists an equivalent finite sequence of probabilistic bi-branchings).

The following definition formalizes this idea:

Definition 3. For $a \in [0, 1]$ and $P, P' \in \mathscr{P}_D$, we let

$$R(a)(P)(P') = a \,.\, P + (1-a) \,.\, P'.$$

A simple computation shows that $R(a)(P)(P') \in \mathscr{P}_D$. We often denote $R(a)(P)(P')$ by a more usual notation $a \,.\, P + (1-a) \,.\, P'$ and call it the *random selection between P and P' under probability a*. The following results are immediate consequences of this definition:

(i) $R(0)(P)(P') = P'$;
(ii) $R(1)(P)(P') = P$;
(iii) if $0 < a < 1$, then $|a \,.\, P + (1-a) \,.\, P| = |P| \cup |P'|$.

Theorem 6. *R is continuous with respect to each of its arguments.*

Proof. (i) Obviously if $a_n \to a$, then $R(a_n) \to R(a)$;

(ii) $R(a)(P)(P')$ is continuous with respect to P. Suppose that (P_n) is an increasing sequence in $\mathscr{P}_D$. For any open set U, we have

$$\begin{aligned}\Big[a \cdot \bigsqcup_n P_n + (1-a) \cdot P'\Big](U) &= a \cdot \bigsqcup_n P_n(U) + (1-a) \cdot P'(U)\\ &= a \cdot \sup_n P_n(U) + (1-a) \cdot P'(U)\\ &= \sup_n [a \cdot P_n(U) + (1-a) \cdot P'(U)]\\ &= \bigsqcup_n [a \cdot P_n + (1-a) \cdot P'](U);\end{aligned}$$

(iii) The proof for the continuity of R with respect to P' is similar.

Remark. It is possible to generalize the notion of random selection for a sequence (P_n) of probability distributions with respect to a sequence (a_n) of non-negative real numbers such that $\sum a_n = 1$ (both sequences may be finite or infinite, but they must have the same cardinality). Then it is not difficult to prove similar results for this generalized notion of random selection.

4.2. *Probabilistic extension of a continuous function*

In the Scott theory of fixed point semantics [10], computable functions are supposed to be continuous transformations on the cpo of states. Here, dealing with a nondeterministic computation, where each state has a probability to appear, we should be able to apply such functions to probability distributions on the set of states. Operationally this means that, if D is the cpo of states and f is a continuous function on it and if π is a nondeterministic computation which yields a probability distribution P on D, then if we want to compose π and f we must be able to define the meaning of $f(P)$. From a mathematical point of view we are led to extend the continuous $f: D \to D$ to $\mathcal{P}_D \to \mathcal{P}_D$.

In the sequel, for any domains D and D', $[D \to D']$ denotes the class of continuous functions from D into D'.

Definition 4. Let $f: D \to D$ be a continuous and consequently measurable function (i.e. $f^{-1}(\mathcal{B}) \subset \mathcal{B}$, see [5, p. 162]). Then $\bar{f}: \mathcal{P}_D \to \mathcal{P}_D$, called the *probabilistic extension* of f, is defined as follows.

$$\bar{f}(P)(A) = P[f^{-1}(A)] \quad \text{for any } P \in \mathcal{P}_D \text{ and any } A \in \mathcal{B}; \qquad (\bar{f}(P) = P \circ f^{-1}).$$

It is well-known and also easy to check that $\bar{f}(P)$ is a probability measure on $\mathcal{B}$ (see [5, pp. 162–163]).

Theorem 7. *If* $f \in [D \to D]$ *and* $P \in \mathcal{F}_D$, *then* $|\bar{f}(P)| = f(|P|)$.

Proof. Suppose $x \in D$. Then $x \in |\bar{f}(P)|$ if and only if $\bar{f}(P)(x) > 0$. But this means $P[f^{-1}(\{x\})] > 0$. Therefore, since $|P|$ is finite, $x \in |\bar{f}(P)|$ if and only if there exists $y \in |P|$ such that $f(y) = x$. This clearly implies $|\bar{f}(P)| = f(|P|)$.

Theorem 8. *For any* $f \in [D \to D]$ *and* $x \in D$, $\bar{f}(x) = f(x)$, *i.e.* $\bar{f}(\{(x, 1)\}) = \{(f(x), 1)\}$.

Proof. First, let $x \in Q$ and apply Theorem 7 to the probability distribution $\{(x, 1)\}$ to prove $\bar{f}(\{(x, 1)\}) = \{(f(x), 1)\}$. The theorem then follows as a consequence of the continuity of $\lambda x \cdot \{(x, 1)\}: D \to \mathcal{P}_D$.

Theorem 9. *If* $f \in [D \to D]$, *then* $\bar{f} \in [\mathcal{P}_D \to \mathcal{P}_D]$.

Proof. Let (P_n) be any increasing sequence in $\mathscr{P}_D$ and U be any open set. We have

$$\left[\bar{f}\left(\bigsqcup_n P_n\right)\right](U)=\left(\bigsqcup_n P_n\right)f^{-1}(U) \quad \text{(by definition)}$$

$$=\sup_n P_n(f^{-1}(U)) \quad \text{(since } f^{-1}(U) \text{ is open)}$$

$$=\sup_n \bar{f}(P_n)(U)=\left[\bigsqcup_n \bar{f}(P_n)\right](U).$$

Theorem 10. *The mapping $\lambda f\cdot \bar{f}:[D\to D]\to[\mathscr{P}_D\to\mathscr{P}_D]$ is continuous.*

Proof. Consider an increasing sequence (f_n) of continuous functions on D, any $P\in\mathscr{P}_D$ and $U\in\mathcal{O}$. Then we have

$$\left(\overline{\bigsqcup_n f_n}\right)(P)(U)=P\left[\left(\bigsqcup_n f_n\right)^{-1}(U)\right].$$

On the other hand, $x\in(\bigsqcup_n f_n)^{-1}(U)$, if and only if $\bigsqcup_n f_n(x)\in U$. But this latter is true if and only if $f_n(x)\in U$ for some n, which is equivalent to $x\in\bigcup_n f_n^{-1}(U)$. Consequently

$$\left(\overline{\bigsqcup_n f_n}\right)(P)(U)=P\left(\bigcup_n f_n^{-1}(U)\right).$$

It is easy to see that, since $f_n\sqsubseteq f_{n+1}, f_n^{-1}(U)\subset f_{n+1}^{-1}(U)$ and consequently

$$\left(\overline{\bigsqcup_n f_n}\right)(P)(U)=\sup_n P(f_n^{-1}(U))=\bigsqcup_n \bar{f}_n(P)(U).$$

Theorem 11. *If $f_1, f_2\in[D\to D]$, then $\overline{f_1\circ f_2}=\bar{f}_1\circ\bar{f}_2$.*

Proof. Result of a simple computation.

Remark. The above results allow us to embed $[D\to D]$ in $[\mathscr{P}_D\to\mathscr{P}_D]$. From now on we identify $\bar{f}$ with f, for any $f\in[D\to D]$.

Theorem 12. *If $f\in[D\to D]$, $a\in[0,1]$ and $P, P'\in\mathscr{P}_D$, then*

$$f(a\cdot P+(1-a)\cdot P')=a\cdot f(P)+(1-a)\cdot f(P').$$

Proof. Result of a simple computation.

Remark. The notion of probabilistic extension may be generalized for functions from $[D\to D']$, where D' is a domain. In particular, if $f\in[D^n\to D]$ and $P=$

$(P_1, \ldots, P_n) \in (\mathcal{P}_D)^n$, we let

$$\bar{f}(P_1, \ldots, P_n)(A) = \Big(\prod_{1 \leq i \leq n} P_i\Big)(f^{-1}(A)), \quad \forall A \in \mathcal{B},$$

where $\prod_{1 \leq i \leq n} P_i$ is the product measure on the product space (see [5, pp. 143–145] or [8, pp. 135–136]).

The verification of Theorems 7, 8, 9, 10, 12 when $f \in [D \to D']$ and of Theorem 11 when $f_2 \in [D \to D']$ and $f_1 \in [D' \to D'']$, does not present any problems.

5. A relation between $\mathcal{P}_D$ and $\mathcal{P}[D]$.

In their study of nondeterminism, Plotkin [13] and Smyth [19] assume that any infinite subset of $\mathcal{P}[D]$ must contain $\perp$. In $\mathcal{P}_D$, we do not have any similar assumption, since it is not difficult to define a discrete probability distribution P (i.e. $P(|P|) = 1$) such that $|P|$ is countably infinite and yet $\perp \notin |P|$.

Although a more fundamental study on relations between $\mathcal{P}_D$ and Plotkin's $\mathcal{P}[D]$ seems possible, here we develop it for a very particular case.

Theorem 13. *Let D be ω-discrete (i.e. flat and countable) and $\mathcal{P}[D]$ its powerdomain equipped with the Egli–Milner order* [13]. *Let $\Psi : \mathcal{P}_D \to \mathcal{P}[D]$ be defined by $\Psi(P) = |P| \cup \{\perp\}$. Then*

(i) *Ψ is continuous*;

(ii) *if $0 < p < 1$, then $\Psi(p \cdot P + (1-p) \cdot P') = \Psi(P) \cup \Psi(P')$*;

(iii) *if $f \in [D \to D]$ and $f(\perp) = \perp$, then $\Psi(f(P)) = f(\Psi(P))$, $\forall P \in \mathcal{P}_D$.*

Proof. Result of an easy computation.

6. A treewise approach to theory of nondeterministic computations

In [17], the author introduces a random walk on the set of terms in order to study the operational semantics for a nondeterministic typed λ-calculus. We use here a variant of Smyth's method [19] to explain how the process of computation works. This process for a particular nondeterministic (or more precisely probabilistic) computation is modelled by an arborescence T with infinite paths as follows.

In T each vertex of depth n corresponds to a possible intermediate result of the computation at its nth step and has an evaluation E, which is an isolated element of the cpo D of states. Therefore if x is a vertex of T, then $E(x)$, its evaluation, is an element of Q. The idea is that these vertices result from finite computations and consequently should be evaluated by isolated elements of D. Other elements of D are used to evaluate the limits along paths which are increasingly evaluated. This evaluation depends on the nature of problems in the deterministic case and not on the new probabilistic notions involved here. The existence of an arc (x, y), where $\text{depth}(x) = n$ and $\text{depth}(y) = n+1$, corresponds to the fact that x is a possible intermediate result at the nth step which may produce y at the next step. In the deterministic case it commonly admitted that the successive steps of computation produce an increasing chain in D. Therefore it will be a natural extension of this assumption to suppose that if y is a successor of x in T, then $E(x) \sqsubseteq E(y)$. In order to make a homogenous study, we replace a pendant vertex x (which corresponds to a final result in the computation) by the infinite path $(x, x, x, \ldots)$. As Plotkin [13] and Smyth [19], we consider only computations with the possibility of selecting between a finite number of processes at random at their successive steps. This restriction is largely justified by Theorem 3 (which proves every probability distribution is the lub of a sequence of finite probability distributions). Under the above assumptions, each vertex x has either only one successor y or else more successors $y_1, \ldots, y_n$. In the first case we let $p(x, y) = 1$ and in the second one $p(x, y_1) = p_1, \ldots, p(x, y_n) = p_n$, where $p_1, \ldots, p_n$ are non-negative real numbers such that $\sum_{1 \leq i \leq n} p_i = 1$ and depend on the involved problem.

Following this idea, we call such an arborescence together with the function p on its arcs as above a *computational arborescence*. An *evaluation* of a computational arborescence is a function E from the set of vertices into Q such that if y is a successor of x, then $E(x) \sqsubseteq E(y)$. For each n $(n = 0, 1, \ldots)$ a probability distribution P_n is defined on the set A_n of vertices having depth n:

$$P_0 = \{(r, 1)\}, \quad \text{where } r \text{ is the root of } T;$$

$$P_{n+1}(y) = P_n(x)p(x, y), \quad \text{where } n \text{ is the father of } y;\ y \in A_{n+1}.$$

It is easy to check that P_n is a probability distribution on A_n, furthermore it defines in an obvious way a probability distribution $\bar{P}_n \in \mathscr{F}_D$:

$$\forall a \in Q, \bar{P}_n(a) = \sum_{x \in E^{-1}(\{a\})} P_n(x).$$

Roughly speaking $\bar{P}_0, \bar{P}_1, \bar{P}_2, \ldots$ correspond to the successive evaluations of the probabilistic computation at times $0, 1, 2, \ldots$ respectively.

Consider now two successive cross-sections A_n and A_{n+1} of T at depth n and $n+1$, $\bar{P}_n$ and $\bar{P}_{n+1}$. An informal survey suggests that since, for any $x \in A_n$, each successor $y \in A_{n+1}$ of x has more information than x, then $\bar{P}_{n+1}$ is the result of transmitting $\bar{P}_n$ to 'better' elements and should be regarded as an 'improvement' of $\bar{P}_n$. At this point it is not obvious that this ordering, which is naturally induced by the usual assumption, is the same as $\sqsubseteq_{\mathscr{P}}$ introduced previously. The following theorem fills this gap and proves the equivalence of $\sqsubseteq_{\mathscr{P}}$ and this concept.

Theorem 14. *Suppose $P, P' \in \mathscr{F}_D$. Then $P \sqsubseteq P'$ if and only if there exists a computational arborescence T with an evaluation E and a positive integer n such that $P = \bar{P}_n$ and $P' = \bar{P}_{n+1}$, where $\bar{P}_n$ and $\bar{P}_{n+1}$ are defined with respect to T and E as above.*

Outline of proof. By virtue of Theorem 2, it is sufficient to prove that the existence of T mentioned above is equivalent to (i). The 'if' part of the theorem is easily checked. The 'only if' part of the theorem is proved by using Ford and Fulkerson's theorem on the maximal flow in a graph (see [4, p. 82]).

7. An Application

De Bakker [1, 2] and Plotkin [13] consider an extra operation, union (or OR) operation, which corresponds to a nondeterministic choice. Here, we introduced the notion of 'random selection' which is informally the counterpart of nondeterministic choice. In a paper [17], the author develops a probabilistic typed λ-calculus, where programs are probabilistic terms of ground types. Here, by a 'probabilistic program' we simply mean a program (in any language), where the possibility of this extra operation is admitted. A rough method to transform a pure nondeterministic program into a probabilistic program is to substitute for union operations a random selection under probability $\frac{1}{2}$.

Example 3. Consider again the first introductory example for a formal treatment:

$$Y(\lambda x\,.\,p \to 0, q \to x+1),$$

where p and q are non-negative real numbers such that $p+q=1$. The domain of interpretation and its ordering is given by Fig. 1. In this example $+$ is interpreted as the natural extension of addition on $D=\mathbf{N}\cup\{+\infty\}$, $\mathrm{p}\to\cdots,\mathrm{q}\to\cdots$ as the random selection under probability p and Y as the least fixed point operator. The functions $\lambda x\cdot 0$ and $\lambda x\cdot x+1$ on D are continuous. Consequently, by virtue of Theorem 9, they have probabilistic extensions in $[\mathscr{P}_D \to \mathscr{P}_D]$. Therefore, by Theorem 6, the function $\phi:\mathscr{P}_D\to\mathscr{P}_D$, defined by $\phi=\lambda P\cdot(p\cdot 0+q\cdot(1+P))$, is continuous. Thus, $Y(\lambda x\cdot p\to 0, q\to x+1)$ should be interpreted as the least fixed point of ϕ, which is given by $\bigsqcup_n \phi^n(\perp)$, see [10].

Note that in the following computation, by the remarks which follow Theorems 5 and 11, $\{(x,1)\}\in\mathscr{P}_D$ is identified with $x\in D$ and $\lambda P.\ (P\mp 1)\in[\mathscr{P}_D\to\mathscr{P}_D]$ with $\lambda P\cdot(P+1)$:

$$\perp=0, \qquad \phi^0(\perp)=0,$$

$$\phi(\perp)=p\cdot 0+q\cdot(0+1)=\{(0,p),(1,q)\},$$

$$\phi^2(\perp)=p\cdot 0+q\cdot(\{(0,p),(1,q)\}+1)=\{(0,p),(1,pq),(2,q^2)\}.$$

Then it will be easy to see, by an induction on n, that

$$\phi^n(\perp)=\{(0,p),(1,pq),\ldots,(n-1,pq^{n-1}),(n,q^n)\}.$$

Consequently

$$\bigsqcup_n \phi^n(\perp) = \begin{cases} \{(i, pq^i) \mid i \in \mathbf{N}\}, & \text{if } p \neq 0, \\ \infty, & \text{if } p = 0. \end{cases}$$

Note that if we used the flat domain of $\{\perp\} \cup \mathbf{N}$ as the domain of interpretation, then the same result would be obtained with the exception that $\perp$ should be substituted for ∞.

Acknowledgment

I am grateful to Professors Robin Milner, Gordon Plotkin and John Reynolds for many stimulating discussions. The unknown referees have contributed to improve the first draft of this paper. Finally I am indebted for the hospitality of the University of Edinburgh. I would like also to thank Mrs. D. McKie and Mrs. G. Temple for typing this difficult manuscript.

References

[1] J.W. de Bakker, Recursive procedures, *Math. Centre Tracts* **24** (1971).

[2] J.W. de Bakker, Semantics and termination of nondeterministic programs, *Proc. Third International Colloquium on Automata, Languages and Programming* (Edinburgh University Press, Edinburgh, 1976) 345–477.

[3] S. K. Berberian, *Measure and Integration* (MacMillan, New York, 1965).

[4] C. Berge, *Graphs and Hypergraphs* (North-Holland, Amsterdam, 1973).

[5] P.R. Halmos, *Measure Theory* (Van Nostrand, New York, 1965).

[6] P. Hitchcock and D. Park, Induction rules and termination proofs, in: M. Nivat, Ed., *Automata, Languages and Programming* (North-Holland, Amsterdam, 1972) 225–251.

[7] D.J. Lehmann, Categories for fixpoint semantics, *Proc. IEEE. Symposium on FOCS*, Houston (1976) 122–126.

[8] M. Loève, *Probability Theory I* (Springer, Berlin, 4th ed., 1977).

[9] G. Markowsky and B. Rosen, Bases for chain-complete posets, *IBM J. Res. Develop.* **20** (2) (1976) 138–147.

[10] R. Milner, Models of LCF, foundation of computer science II, *Math. Centre Tracts* **8** (2) (1976) 49–66.

[11] R. Milner, An approach to the semantics of parallel programs, *Proc. Convegno di Informatica Teorica*, Instituto di Elaborazione delle Informatica, Pisa (1973).

[12] A. Paz, *Introduction to Probabilistic Automata* (Academic Press, New York, 1971).

[13] G. D. Plotkin, A powerdomain construction, *SIAM J. Comput.* **5** (3) (1976) 452–487.

[14] M.O. Rabin, Probabilistic algorithms, in: J.F. Traub, Ed., *Algorithms and Complexity: New Directions and Recent Results* (Academic Press, New York, 1976) 21–39.

[15] H.L. Royden, *Real Analysis* (MacMillan, New York, 1964).

[16] N. Saheb-Djahromi, Probabilistic non-determinism, Internal Report, University of Edinburgh (1977).

[17] N. Saheb-Djahromi, *Probabilistic LCF*, Mathematical Foundations of Computer Science **64** (Springer, Berlin, 1978).

[18] D. Scott. *Continuous Lattices*, Toposes, Algebraic Geometry and Logic **74** (Springer, Berlin, 1971).
[19] M. B. Smyth, *Powerdomains*, Mathematical Foundations of Computer Science **45** (Springer, Berlin, 1976).
[20] A. Tang, Borel sets in *Pω*, IRIA, Rapport de Recherche, No. 137 (1975).
[21]. R.J. Wilson, *Introduction to Graph Theory* (Longman, 1972).