Continuous Random Variables

Jean Goubault-Larrecq*
LSV, ENS Cachan, CNRS, INRIA

Daniele Varacca
*Preuves, Programmes et Systèmes,
UMR 7126, CNRS and University Paris Diderot*

Abstract—We introduce the domain of continuous random variables (CRV) over a domain, as an alternative to Jones and Plotkin's probabilistic powerdomain. While no known Cartesian-closed category is stable under the latter, we show that the so-called thin (uniform) CRVs define a strong monad on the Cartesian-closed category of bc-domains. We also characterize their inequational theory, as (fair-)coin algebras. We apply this to solve a recent problem posed by M. Escardó: testing is semi-decidable for EPCF terms. CRVs arose from the study of the second author's (layered) Hoare indexed valuations, and we also make the connection apparent.

Keywords-domain theory, probabilistic powerdomain, bc-domain, indexed valuation, monad, random variable.

I. Introduction

It is natural to model probabilistic choice in typed higher-order languages by using the probabilistic powerdomain monad $\mathbf{V}$, based on continuous valuations [1]. An outstanding problem in this area is the existence of a Cartesian-closed category of continuous dcpos and Scott-continuous maps on which $\mathbf{V}$ restricts as an endofunctor [2].

We will show that, for purpose of semantics, this issue can be sidestepped completely. We propose another monad of so-called *continuous random variables* (CRV), modeled after the notion of random variable commonly used in probability theory: instead of modeling random choice on a space X by a measure (or a continuous valuation) ν, we model it by a pair (ν, f) where ν is a measure on some measurable set Ω, and f is a measurable map from Ω to X. This is used to draw $\omega \in \Omega$ at random according to ν, and then outputting $f(\omega)$. Every random variable gives rise to a measure on X, the image measure $f[\nu]$, but there is more information in the random variable than in $f[\nu]$: if ν picks 1 or 0 with probability a, resp., $1 - a$, and f is a constant map $\lambda\_ \cdot x$, then $f[\nu]$ will always pick x, independently of a.

Related Work: Random variables are a classic in probability theory. The second author suggested that his own, fairly abstract notion of indexed valuations could perhaps be characterized concretely by some form of random variable construction [3, Section 4.6]. The present work originated from this idea, but what we have come up with is a different notion. The first to recognize the importance of random variables in domain theory is M. Mislove [4]. His discrete random variables match the Plotkin kind of indexed

valuations exactly, and he established the remarkable result that the Cartesian-closed category of FS-domains is stable under the Plotkin indexed valuation functor. This is to be compared with our results that the smaller category of bc-domains (which are also a simpler concept) is stable under various functors of CRVs; and we believe that CRVs are also a more concrete concept, easier to fathom, than indexed valuations. Our thin CRVs are related to the so-called layered Hoare kind of indexed valuations [3, Section 4.7].

M. Escardó also used a similar idea [5]: he compiles a rich language with non-deterministic and probabilistic choice into maps taking sequences of bits drawn at random (or non-deterministically) to values. We make the connection clear in Section VIII, and use this to solve a problem he left open.

Outline: After some preliminaries (Section II), we introduce our kind of random variables, the *continuous* random variables (CRV), in Section III. The thin, resp. uniform CRVs are the interesting ones (Section IV), but it is simpler to study the general kind first. Our main result here is that there *is* a Cartesian-closed category of continuous dcpos that is stable under the $\theta\mathbf{R}_1$ (resp., $\nu\mathbf{R}_1$) functor of thin (resp., uniform) CRVs, viz. the very well-behaved category $\mathbf{BCD}$ of bc-domains. As we show in Section V, $\theta\mathbf{R}_1$ and $\nu\mathbf{R}_1$ give rise to strong monads, and we characterize their inequational theories as those of *coin (resp., fair-coin) algebras*; these notions are new, too. Section VI serves to relate thin CRVs and continuous valuations. We apply all this in Section VII and show that thin CRVs are as good as continuous valuations in giving semantics to a rich higher-order language with choice. This is used to solve an open problem due to M. Escardó [5] in Section VIII. This work originated in our desire to give a concrete description to the second author's *indexed valuations* [3]. Although they are not identical objects, we relate CRVs and layered Hoare indexed valuations in Section IX. We conclude in Section X.

II. Preliminaries

We refer the reader to [6], [7] on domain theory. We write $f\langle A \rangle$ for $\{f(x) \mid x \in A\}$, $f_{|A}$ is the restriction of f to A. Functions taking their values in a poset will always be ordered pointwise, i.e., $f \leq g$ iff $f(x) \leq g(x)$ for every x. Let X be a poset, with ordering $\leq$; when $x \leq y$, we say that x is *below* y, or that y is *above* x. We write $\uparrow x$ for $\{y \in X \mid x \leq y\}$, $\downarrow x = \{y \in X \mid y \leq x\}$; also, for a subset A, $\uparrow A$ will denote $\bigcup_{x \in A} \uparrow x$. A *directed family* $(x_i)_{i \in I}$ in X is

non-empty and such that for all $i, j \in I$, there is a $k \in K$ such that $x_i, x_j \leq x_k$. A *dcpo* is a poset where every such directed family has a *supremum* (or *sup*) $\sup_{i \in I} x_i$. A *Scott-continuous* map between dcpos is a monotonic map that preserves sups of directed families. Equivalently, a Scott-continuous map f is a continuous map in the ordinary sense ($f^{-1}(V)$ is open for every open V), once we equip all dcpos with their *Scott topology*, whose (Scott-)opens are the upward-closed subsets U (i.e., if $x \in U$ and $x \leq y$ then $y \in U$) such that the directed families whose sup is in U have a member in U already. A *closed* set is the complement of an open set. The *closure* $cl(A)$ of a set A is the smallest closed set containing A. For every open U, $U \cap cl(A) \neq \emptyset$ iff $U \cap A \neq \emptyset$.

Any closed subset F of a dcpo is again a dcpo. Note that, by Zorn's Lemma, every element x of F is below some element in $\operatorname{Max} F$, the set of all maximal elements of F.

We say that x is *way-below* y, and write $x \ll y$, iff every directed family whose sup is above y contains an element above x. Clearly, $x \leq y \ll z \leq t$ implies $x \ll t$. A dcpo X is *continuous* iff $\downarrow x = \{y \in X \mid y \ll x\}$ is directed and has x as sup. It is equivalent to require that X has a *basis* B, i.e., a subset such that $\downarrow x \cap B$ is directed and has x as sup, for every $x \in X$. In a continuous dcpo X (resp., with basis B), the opens are the unions of *basic opens* $\uparrow x = \{y \in X \mid x \ll y\}$ (resp., with $x \in B$). An element x is *finite* iff $x \ll x$. A dcpo is *algebraic* iff every element is the sup of the directed family of finite elements below it: the *basic opens* are then $\uparrow x = \{y \in X \mid x \leq y\}$, x finite.

A (bounded) *valuation* ν on a dcpo is a map from opens to elements of $\mathbb{R}^+$ such that $\nu(\emptyset) = 0$, $\nu(U \cup V) + \nu(U \cap V) = \nu(U) + \nu(V)$, $\nu(U) \leq \nu(V)$ whenever $U \subseteq V$. It is *continuous* iff for every directed family $(U_i)_{i \in I}$ of opens, $\nu(\bigcup_{i \in I} U_i) = \sup_{i \in I} \nu(U_i)$. The *Dirac valuation* δ_x, where $\delta_x(U) = 1$ if $x \in U$, $\delta_x(U) = 0$ otherwise, is an example. The *simple valuations* are finite linear combinations $\sum_{i=1}^n a_i \delta_{x_i}$ with $a_i \in \mathbb{R}^+$. $\mathbf{V}(X)$ is the poset of all continuous valuations, ordered by $\nu \leq \nu'$ iff $\nu(U) \leq \nu'(U)$ for every open U [1]. For each $a \in \mathbb{R}^+$, $\mathbf{V}_a(X)$ is the dcpo of those $\nu \in \mathbf{V}(X)$ with total mass $\nu(X) = a$. Directed sups of continuous valuations are pointwise, i.e., $(\sup_{i \in I} \nu_i)(U) = \sup_{i \in I} (\nu_i(U))$. $\mathbf{V}_1(X)$ is the dcpo of continuous *probability* valuations.

Given any continuous map $p : X \to Y$, and $\nu \in \mathbf{V}(X)$, the *image valuation* $p[\nu]$ is defined by $p[\nu](V) = \nu(p^{-1}(V))$. We note that $\operatorname{id}[\nu] = \nu$, and $p[q[\nu]] = (p \circ q)[\nu]$. If $\nu = \sum_{i=1}^n a_i \delta_{x_i}$, then $p[\nu] = \sum_{i=1}^n a_i \delta_{p(x_i)}$.

We let Ω be the *Cantor tree* $\Sigma^* \cup \Sigma^\infty$, the set of all finite and infinite words over the binary alphabet $\Sigma = \{1, 0\}$, ordered by prefix. The subspace $\operatorname{Max} \Omega$ is homeomorphic to the Cantor set $2^\mathbb{N}$, one of the standard Polish spaces used in probability theory [7, Example V-6.4]. Let t_n be the *nth truncation map*: $t_n(\omega)$ is the largest prefix of ω of length at most n. This is a continuous map with finite image. Ω is also a *tree* (it has a least element ϵ, and whenever $\omega_1, \omega_2 \leq \omega$, then $\omega_1 \leq \omega_2$ or $\omega_2 \leq \omega_1$), and an algebraic dcpo, whose finite elements are
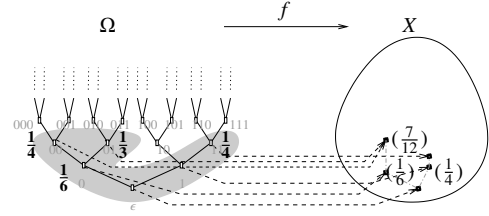

Figure 1.   A CRV

the finite words: its open subsets are the *pairwise disjoint* (hence countable) unions $\biguplus_{i \in I} \uparrow \omega_i$ of sets $\uparrow \omega_i$, ω_i finite. The *uniform valuation* Λ on Ω is then defined uniquely by $\Lambda(\biguplus_{i \in I} \uparrow \omega_i) = \sum_{i \in I} \frac{1}{2^{|\omega_i|}}$, where $|\omega_i|$ is the length of ω_i.

III. CRVs

The *support* $\operatorname{supp} \nu$ of a continuous valuation ν on Ω is the complement of the largest open subset U such that $\nu(U) = 0$.

Definition III.1 *A continuous random variable (CRV) on a dcpo X is a pair (ν, f), where ν is a continuous valuation on Ω, and f is a continuous map from $\operatorname{supp} \nu$ to X.*

The ν part describes the law obeyed by the random coin flips done so far. E.g., $\nu = \frac{1}{4} \delta_{11} + \frac{1}{6} \delta_0 + \frac{1}{3} \delta_{01} + \frac{1}{4} \delta_{00}$ draws the word 11 with probability $\frac{1}{4}$, 0 with probability $\frac{1}{6}$, and so on (see Figure 1); $\operatorname{supp} \nu$ is pictured in gray: in general, $\operatorname{supp} \sum_{i=1}^n a_i \delta_{\omega_i}$ is $\downarrow\{\omega_1, \ldots, \omega_n\}$.

The f part states how each sequence ω of coin flips maps to an actual element $f(\omega)$ of X. Note that distinct sequences ω, ω' of coin flips can map to the same element of X. We only require f to be defined only for elements of $\operatorname{supp} \nu$: $\operatorname{supp} \nu$ is the domain of sequence of coin flips that one has made in the past, and f is only required to be defined on these, not on any future coin flip.

We say that ν is a *simple* CRV iff ν is a simple valuation $\sum_{i=1}^n a_i \delta_{\omega_i}$. Then $f[\nu] = \sum_{i=1}^n a_i \delta_{f(\omega_i)}$: the resulting coefficients are shown as parenthesized fractions on the right part of Figure 1. The CRV (ν, f) keeps the information that the element of X chosen with probability $\frac{7}{12}$ was obtained either as $f(00)$ (with probability $\frac{1}{4}$) or as $f(01)$ (with probability $\frac{1}{3}$); $f[\nu]$ only keeps the total number $\frac{7}{12} = \frac{1}{4} + \frac{1}{3}$.

For each closed subset F of Ω, there is a unique projection p_F onto F, i.e., a unique continuous map $p_F : \Omega \to F$ such that $p_F(\omega) \leq \omega$ for every $\omega \in \Omega$, with equality if $\omega \in F$; and $p_F(\omega)$ is $\sup(F \cap \downarrow \omega)$. Uniqueness follows from the fact that Ω is a tree, and continuity from this and the fact that F is closed.

Definition III.2 *Let X be a dcpo. The* layered ordering $\leqq$ *on the set $\mathbf{R}(X)$ of all CRVs on X is defined by $(\nu, f) \leqq (\nu', f')$ iff $\nu = p_F[\nu']$ and $f \circ p_{F|F'} \leq f'$, where $F = \operatorname{supp} \nu$ and $F' = \operatorname{supp} \nu'$.*

If $\nu' = \sum_{j=1}^n b_j \delta_{\omega'_j}$, $(\nu, f) \leqq (\nu', f')$ iff ν is the projected valuation $\sum_{j=1}^n b_j \delta_{p_F(\omega'_j)}$. That is, starting from a simple CRV
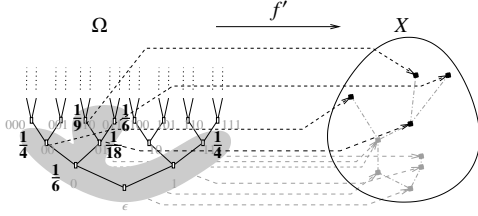
Figure 2. A larger CRV

(v, f) of Figure 1, we obtain a larger one in the layered ordering $\leqq$ by redistributing the mass from some maximal words in supp v (here 01, with mass $\frac{1}{3}$) to larger words (here 010 with mass $\frac{1}{9}$, 011 with mass $\frac{1}{6}$, keeping some mass, $\frac{1}{18}$, on 01). The total mass $v(\Omega)$ is unchanged.

While we redistribute masses from v to v', we are also allowed to increase the values $f(\omega)$ to larger points $f'(\omega)$, $\omega \in$ supp v, mapping the new words $\omega \in$ supp $v' \setminus$ supp v to even larger points: see Figure 2, right.

The poset $\mathbf{R}(X), \leqq$ is the disjoint union of the so-called *layers* $\mathbf{R}_a(X)$, one for each $a \in \mathbb{R}^+$, where $\mathbf{R}_a(X)$ is the set of CRVs (v, f) with $v(\Omega) = a$. We shall be particularly interested in $\mathbf{R}_1(X)$, the poset of *probability CRVs*.

One alternate, non-layered ordering would declare (v, f) below (v', f') iff $f \circ p_{F|F'} \leq f'$, as before, but with $v \leq p_F[v']$ instead of $v = p_F[v']$. Our layering is deliberate, and was suggested as more natural by A. Jung in the setting of indexed valuations. Intuitively, $\leqq$ enforces that each $\omega \in$ Max F is some sequence of coin flips that can be extended in the future, while $\omega \in F \setminus$ Max F represents a sequence of coin flips followed by deadlock. In Figure 1, we have not deadlocked at $\omega = \epsilon$ (we made a first flip, with probability 1), but we have deadlocked at $\omega = 0$ with probability $\frac{1}{6}$; once we arrived at $\omega = 01$ (with probability $\frac{1}{3}$), we can proceed as in Figure 2, deadlocking with conditional probability $\frac{1}{6}$ (hence with total probability $\frac{1}{3} \times \frac{1}{6} = \frac{1}{18}$).

To show that $\mathbf{R}(X)$ is a dcpo, we first study the support map supp $: \mathbf{V}(\Omega) \to \mathcal{H}_\emptyset(\Omega)$, and show that it is monotonic and Scott-continuous. $\mathcal{H}_\emptyset(\Omega)$ is the *lifted Hoare powerdomain*, i.e., the set of closed subsets (including $\emptyset$ here), ordered by inclusion. This is a dcpo, with $\sup_{i \in I} F_i = cl(\bigcup_{i \in I} F_i)$. We also observe that $\mathcal{H}_\emptyset(\Omega)$ is *meet-continuous*, i.e., $cl(\bigcup_{i \in I} F_i) \cap F' = cl(\bigcup_{i \in I}(F_i \cap F'))$ for every $F' \in \mathcal{H}_\emptyset(\Omega)$. This is because $\mathcal{H}_\emptyset(\Omega)$ is a completely distributive lattice [7].

Projections have a number of useful properties: (A) For all closed subsets F, F' of Ω, $p_F \circ p_{F'} = p_{F \cap F'}$; (B) For any closed subset F, for every open subset U of Ω, $p_F^{-1}(U) \subseteq U$; (C) If $(F_i)_{i \in I}$ is a directed family in $\mathcal{H}_\emptyset(\Omega)$, and F is its sup $cl(\bigcup_{i \in I} F_i)$, then for every open U, $p_F^{-1}(U) = \bigcup_{i \in I} p_{F_i}^{-1}(U)$; (D) For all closed subsets F, F' of Ω, for every $\omega \in \Omega$, $p_{F \cup F'}(\omega) = \max(p_F(\omega), p_{F'}(\omega))$ and $p_{F \cap F'}(\omega) = \min(p_F(\omega), p_{F'}(\omega))$; (note that $p_F(\omega)$ and $p_{F'}(\omega)$ are comparable, since they are both below ω and Ω is a tree;) (E) Given any $v \in \mathbf{V}(\Omega)$, and any closed subset

$F \supseteq$ supp v, $v = p_F[v]$; (F) Given any $v \in \mathbf{V}(\Omega)$, and any closed subset F, supp $p_F[v] = F \cap$ supp v. The following, for example, rests on (B), (C), and (A), and the continuity of supp.

Proposition III.3 *Let X be a dcpo. Then $\mathbf{R}(X)$, $\mathbf{R}_a(X)$ are dcpos. The sup of a directed family $(v_i, f_i)_{i \in I}$ is (v, f), where v is the pointwise directed sup $\sup_{i \in I} v_i$, and $f(\omega) = \sup_{i \in I} f_i(p_{F_i}(\omega))$ (defining $F_i = supp\, v_i$) for every $\omega \in supp\, v$. Moreover, $supp\, v$ is the sup of $(F_i)_{i \in I}$ in $\mathcal{H}_\emptyset(\Omega)$.*

Jones and Plotkin proved that $\mathbf{V}(X)$ was a continuous dcpo as soon as X was [1]. We have a similar result for CRVs.

Theorem III.4 *If X is a continuous dcpo, then so are $\mathbf{R}(X)$ and $\mathbf{R}_a(X)$. Given the way-below relation $\ll$ on X, the way-below relation $\lll$ on $\mathbf{R}(X)$, resp. $\mathbf{R}_a(X)$, is given by $(v, f) \lll (v', f')$ iff v has finite support F, $v = p_F[v']$, and for every $\omega \in F$, $f(\omega) \ll f'(\omega)$. The finite CRVs form a basis.*

Proof: (Sketch.) (1) Assume $(v, f) \lll (v', f')$, and let $F = $ supp v, $F' = $ supp v'. Let $F_n = t_n\langle F'\rangle$, the image of F' by t_n. Then $(p_{F_n}[v'], f'_{|F_n \cap F'})_{n \in \mathbb{N}}$ is directed, and its sup is (v', f'). (This uses (C) and (E).) So $(v, f) \leqq (p_{F_n}[v'], f'_{|F_n \cap F'})$ for some $n \in \mathbb{N}$. Using (F), $F \subseteq F_n$, so v has finite support. Also, $F \subseteq F_n$, so $v = p_{F \cap F_n}[v']$ (by (A)) $= p_F[v']$.

Say that a vector $\vec{x} = (x_\omega)_{\omega \in F}$ in X is *monotone* iff $\omega \leq \omega'$ implies $x_\omega \leq x_{\omega'}$, and consider the collection D_F of all monotone vectors $\vec{x}$ with $x_\omega \ll f'(\omega)$ for every $\omega \in F$. Order D_F componentwise. Using the fact that F is finite, D_F is directed, and the pointwise sup of D_F is $(f'(\omega))_{\omega \in F}$. For each $\vec{x} \in D_F$, define $f'_{\vec{x}} : F' \to X$ as mapping each $\omega \in F$ to x_ω, and each $\omega \in F' \setminus F$ to $f'(\omega)$. This is monotone. Scott-continuity is easy since F is finite. Then $(v', f'_{\vec{x}})_{\vec{x} \in D_F}$ is directed, and its sup is (v', f'). Since $(v, f) \lll (v', f')$, there is an $\vec{x} \in D_F$ such that $(v, f) \leqq (v', f'_{\vec{x}})$. In particular, $f(\omega) \leq x_\omega \ll f'(\omega)$ for every $\omega \in F$.

(2) Conversely, assume that $F = $ supp v is finite, that $v = p_F[v']$, and that $f(\omega) \ll f'(\omega)$ for every $\omega \in F$. The fact that F is finite makes it easy to check that $(v, f) \lll (v', f')$.

(3) By (1), every element (v, f) of $\mathbf{R}(X)$, with $F = $ supp v, is the sup of the directed family $(p_{F_n}[v], (f_{|F_n \cap F})_{\vec{x}})$, $n \in \mathbb{N}$, $\vec{x} \in D_{F_n}$. Directedness comes from the standard fact that if $(a_j)_{j \in J}$ is a directed family, and each a_j is the sup of a directed family $(a_{jk})_{k \in K_j}$ such that a_{jk} is way-below a_j for every k, then $(a_{jk})_{j \in J, k \in K_j}$ is also directed. ∎

$\mathbf{R}(X)$ cannot be a lattice, since for example (δ_0, f) and $(\frac{1}{2}\delta_\epsilon + \frac{1}{2}\delta_0, g)$ have no common upper bound, whatever f and g. But we can make it a *bc-domain*, i.e., a continuous, bounded-complete dcpo, where bounded-complete means that any finite set of elements that has an upper bound has a least one. (In particular, a bc-domain has a least element.)

Theorem III.5 *If X is a bc-domain, then so is $\mathbf{R}_a(X)$ for each $a \in \mathbb{R}^+$.*

Proof: It suffices to show that it has a least element—$(a\delta_\epsilon, \{\epsilon \mapsto \bot\})$, where $\bot$ is the least element of X—and has sups of all upper bounded pairs. Write $\vee$ the (partial) binary sup operation in X. Let (ν, f), (ν', f') be two elements of $\mathbf{R}(X)$ with an upper bound (ν'', f''). Let $F = \operatorname{supp} \nu$, $F' = \operatorname{supp} \nu'$, $F'' = \operatorname{supp} \nu''$. Since supp is monotonic, $F, F' \subseteq F''$. We claim that $(p_{F \cup F'}[\nu''], g)$ is the least upper bound of (ν, f) and (ν', f'), where $g(\omega) = f(p_F(\omega)) \vee f'(p_{F'}(\omega))$ for every $\omega \in F \cup F'$. Note that $F \cup F'$ is the support of $p_{F \cup F'}[\nu'']$, by (F). So $(p_{F \cup F'}[\nu''], g)$ is a CRV.

We claim that $(\nu, f) \leqq (p_{F \cup F'}[\nu''], g)$. Indeed, $p_F[p_{F \cup F'}[\nu'']] = p_{F \cap (F \cup F'')}[\nu'']$ (by (A)) $= p_F[\nu''] = \nu$. Also, $f(p_{F|F \cup F'}(\omega)) = f(p_F(\omega)) \leq g(\omega)$ for every $\omega \in F \cup F'$. So $(\nu, f) \leqq (p_{F \cup F'}[\nu''], g)$, and similarly for (ν', f').

It remains to show that $(p_{F \cup F'}[\nu''], g) \leqq (\nu''', f''')$ for any upper bound (ν''', f''') of (ν, f) and (ν', f').

We must first show that $p_{F \cup F'}[\nu'] = p_{F \cup F'}[\nu'']$. From (D), $p_{F \cup F'}^{-1}(U) = p_F^{-1}(U) \cup p_{F'}^{-1}(U)$ and $p_{F \cap F'}^{-1}(U) = p_F^{-1}(U) \cap p_{F'}^{-1}(U)$. So $p_{F \cup F'}[\nu''](U) = \nu''(p_{F \cup F'}^{-1}(U)) = \nu''(p_F^{-1}(U)) + \nu''(p_{F'}^{-1}(U)) - \nu''(p_{F \cap F'}^{-1}(U))$ by modularity. Since $(\nu, f) \leqq (\nu'', f'')$, $\nu''(p_F^{-1}(U)) = \nu(U)$, and similarly $\nu''(p_{F'}^{-1}(U)) = \nu'(U)$. Also, $p_{F \cap F'} = p_F \circ p_{F'}$ by (A), so $\nu''(p_{F \cap F'}^{-1}(U)) = \nu'(p_F^{-1}(U))$ (also, $= \nu(p_{F'}^{-1}(U))$). So $p_{F \cup F'}[\nu''] = \nu + \nu' - p_F[\nu']$ (also, $= \nu + \nu' - p_{F'}[\nu]$). This is independent of the chosen upper bound (ν'', f''). So $\nu + \nu' - p_F[\nu']$ also equals $p_{F \cup F'}[\nu''']$.

Finally, $g \circ p_{F \cup F'|\operatorname{supp} \nu'''} \leq f'''$ is clear: for every $\omega \in \operatorname{supp} \nu'''$, $g(p_{F \cup F'}(\omega)) = f(p_F(p_{F \cup F'}(\omega))) \vee f'(p_{F'}(p_{F \cup F'}(\omega))) = f(p_F(\omega)) \vee f'(p_{F'}(\omega))$ by (A). ∎

The importance of this result is that the category of bc-domains is Cartesian-closed [7, Exercise II-2.31].

IV. Thin and Uniform CRVs

$\mathbf{R}$ does not form a monad: the formula for $h^\dagger$ in Section V, or any natural variant, would not be monotonic on $\mathbf{R}(X)$. Alternatively we observe that CRVs form a coin algebra (See Theorem V.2), but not the free coin algebra.

To obtain a free algebra, and thus a monad, we restrict to *thin* CRVs. We also investigate the further refinement of *uniform* CRVs.

Call a simple valuation $\sum_{i=1}^m a_i \delta_{\omega_i}$ on Ω, where $a_i \neq 0$, *thin* iff $\{a_1, \ldots, a_m\}$ is an antichain, i.e., no two distinct ω_is are comparable. I.e., given a simple valuation ν, and letting $F = \operatorname{supp} \nu$, ν is thin iff ν can be written $\sum_{\omega \in \operatorname{Max} F} a_\omega \delta_\omega$—and $a_\omega \neq 0$ for each $\omega \in \operatorname{Max} F$. Using an expression we used in Section III, we can say that the coin flipping process does not deadlock.

For every thin simple valuation ν on Ω, $t_n[\nu]$ is also thin. Let us generalize, and for every continuous valuation ν on Ω, define ν to be *thin* iff $t_n[\nu]$ (which is simple) is thin for every $n \in \mathbb{N}$. E.g., the uniform valuation Λ is thin, since $t_n[\Lambda] = \sum_{\omega \text{ of length } n} \frac{1}{2^n} \delta_\omega$.

Lemma IV.1 *The sup of any directed family $(\nu_i)_{i \in I}$ of thin continuous valuations on Ω, with the same total mass $a = \nu_i(\Omega) \in \mathbb{R}^+$, is also thin.*

All the information on a thin continuous valuations can be obtained from the maximal elements of the support. We exploit this in the following definition.

Definition IV.2 *Let X be a dcpo. A thin CRV on X is a pair (ν, f) where ν is a thin continuous valuation on Ω and f is a continuous map from $\operatorname{Max} F$ to X, where $F = \operatorname{supp} \nu$. The set $\theta \mathbf{R}(X)$ of all thin CRVs on X (resp., $\theta \mathbf{R}_a(X)$ of those with $\nu(\Omega) = a$) is ordered by: $(\nu, f) \leqq (\nu', f')$ iff $\nu = p_F[\nu']$ and $f \circ p_{F|\operatorname{Max} F'} \leq f'$, where $F = \operatorname{supp} \nu$ and $F' = \operatorname{supp} \nu'$.*

The continuity of $f : \operatorname{Max} F \to X$ must be understood in usual topological way, where X is equipped with its Scott topology, and $\operatorname{Max} F$ with the subspace topology from Ω. Note that thin CRVs are not exactly special cases of CRVs as f is not everywhere defined on F.

The definition of the ordering is similar to Definition III.2. However there is a additional subtlety: the condition $f \circ p_{F|\operatorname{Max} F'} \leq f'$ is only well-defined if p_F indeed maps elements of $\operatorname{Max} F'$ to elements in the domain of f, namely $\operatorname{Max} F$. This is ensured by the following lemma.

Lemma IV.3 *Let ν, ν' be thin valuations on Ω, $F = \operatorname{supp} \nu$, $F' = \operatorname{supp} \nu'$, and assume $\nu = p_F[\nu']$. Then $p_F(\omega') \in \operatorname{Max} F$ for every $\omega' \in \operatorname{Max} F'$.*

This would fail if we didn't assume ν thin: take e.g., $\nu' = \frac{1}{2}\delta_0 + \frac{1}{2}\delta_1$, $\nu = p_{\downarrow 1}[\nu'] = \frac{1}{2}\delta_\epsilon + \frac{1}{2}\delta_1$, and consider $p_{\downarrow 1}(0)$.

Recall that a set K is *compact* iff for every open cover $(U_i)_{i \in I}$ (i.e., each U_i is open and $K \subseteq \bigcup_{i \in I} U_i$) that is directed, $K \subseteq U_i$ for some $i \in I$.

Corollary IV.4 *For every thin continuous valuation ν on Ω, letting $F = \operatorname{supp} \nu$, $\operatorname{Max} F$ is compact in Ω.*

Proof: (Sketch)Let F_n be the closed set of all words of length at most n, and recall that $t_n = p_{F_n}$. Using Lemma IV.3 on $t_n[\nu]$ and ν, $\operatorname{Max} F \subseteq \uparrow \operatorname{Max}(F_n \cap F)$ for each $n \in \mathbb{N}$. Conversely, if $\omega \in \bigcap_{n \in \mathbb{N}} \uparrow \operatorname{Max}(F_n \cap F)$, we show that $p_F(\omega) \in \operatorname{Max} F$. It follows that $\uparrow \operatorname{Max} F$ is the intersection of the chain of finitely generated upper sets $\uparrow \operatorname{Max}(F_n \cap F)$, $n \in \mathbb{N}$. In a dcpo (such as Ω), such intersections are compact [7, Lemma III-5.6], as an application of Rudin's Lemma. Since $\uparrow \operatorname{Max} F$ is compact, so is $\operatorname{Max} F$. ∎

An interesting special case of thin CRV is when words $\omega \in \operatorname{Max} F$ are picked by drawing their letters at random, independently, with probability $\frac{1}{2}$ for 1 and $\frac{1}{2}$ for 0.

Definition IV.5 *A continuous valuation ν on Ω is said to be* partially uniform *iff $\nu = p_F[\Lambda]$ where $F = \operatorname{supp} \nu$. A thin CRV (ν, f) is said to be* uniform *iff ν is partially uniform. The set of uniform CRV is denoted as $\upsilon \mathbf{R}(X)$ (resp., $\upsilon \mathbf{R}_a(X)$).*

Proposition IV.6 *Let X be a dcpo. Then $\theta \mathbf{R}(X)$, $\theta \mathbf{R}_a(X)$, $\upsilon \mathbf{R}(X)$, $\upsilon \mathbf{R}_a(X)$ are dcpos. The sup of a directed family $(\nu_i, f_i)_{i \in I}$ is (ν, f), where $\nu = \sup_{i \in I} \nu_i$, and $f(\omega) = \sup_{i \in I} f_i(p_{F_i}(\omega))$ (defining $F_i = \operatorname{supp} \nu_i$) for every $\omega \in \operatorname{Max} F$ (with $F = \operatorname{supp} \nu$).*

For the ν part this is proved as Proposition III.3. For the f part, $f = \sup_{i \in I} f_i \circ p_{F_i \text{Max} F}$ is continuous, because the inverse image of any (Scott-)open V is $\bigcup_{i \in I}(\text{Max}\, F \cap p_{F_i}^{-1}(f_i^{-1}(V)))$, a union of opens in Max F. Thinness is by Lemma IV.1, and partial uniformity of ν is easy.

The main result of the section is the following:

Theorem IV.7 *If X is a bc-domain, then so are $\theta \mathbf{R}_a(X)$ and $\upsilon \mathbf{R}_a(X)$ for every $a \in \mathbb{R}^+$. A basis is given by the simple thin (resp., uniform) CRVs.*

Proof: (Sketch) Call a CRV (ν, f) on X *semi-thin* iff ν is a thin continuous valuation (but with f defined everywhere on the support). The set $\sigma \mathbf{R}(X)$ of semi-thin CRVs on X is also a bc-domain. First of all it is continuous with the same way-below relation as for general CRVs. Then we proceed as in Theorem III.5, but we must also show that, if ν, ν', ν'' are thin, $\nu = p_F[\nu'']$ and $\nu' = p_{F'}[\nu'']$ with $F = \text{supp}\,\nu$, $F' = \text{supp}\,\nu'$, then $p_{F \cup F'}[\nu'']$ is also thin.

We first examine the case where ν'' has finite support, i.e., is simple. Let $F'' = \text{supp}\,\nu''$. Since ν'' is thin, $\nu'' = \sum_{\omega \in \text{Max}\, F''} a_\omega \delta_\omega$, where each a_ω is non-zero. So $\nu = p_F[\nu''] = \sum_{\omega \in \text{Max}\, F''} a_\omega \delta_{p_F(\omega)}$. Since ν is also thin, for every $\omega \in \text{Max}\, F''$ (using $a_\omega \neq 0$), $p_F(\omega)$ must be in Max F.

It follows that $\{p_{F \cup F'}(\omega) \mid \omega \in \text{Max}\, F''\}$ is an antichain. Otherwise, one could find $\omega_1, \omega_2 \in \text{Max}\, F''$ such that $p_{F \cup F'}(\omega_1) < p_{F \cup F'}(\omega_2)$ (writing $a < b$ for $a \leq b$ and $a \neq b$). By (D), $\max(p_F(\omega_1), p_{F'}(\omega_1)) < \max(p_F(\omega_2), p_{F'}(\omega_2))$, which implies $p_F(\omega_1) < p_F(\omega_2)$ or $p_{F'}(\omega_1) < p_{F'}(\omega_2)$; both are impossible since the first two are in Max F, the last two are in Max F', as the previous paragraph shows, and Max F and Max F' are antichains. So $p_{F \cup F'}[\nu'']$ is thin.

In the general case, let F_n be the set of words of length at most n, and observe that $t_n = p_{F_n}$. Then $t_n[p_{F \cup F'}[\nu'']] = p_{F_n \cap (F \cup F')}[\nu'']$ (by (A)) $= p_{((F_n \cap F) \cup (F_n \cap F')) \cap F_n}[\nu''] = p_{(F_n \cap F) \cup (F_n \cap F')}[t_n[\nu'']]$. Now $t_n[\nu'']$ is thin, is an upper bound of $t_n[\nu]$ and of $t_n[\nu']$, $F_n \cap F = \text{supp}\, t_n[\nu]$ and $F_n \cap F' = \text{supp}\, t_n[\nu']$ by (F). Since $t_n[\nu'']$ is simple, we apply the above result: $t_n[p_{F \cup F'}[\nu'']]$ is thin. Since n is arbitrary, $p_{F \cup F'}[\nu'']$ is thin.

Then we define the maps $r : \sigma \mathbf{R}(X) \to \theta \mathbf{R}(X)$ and $s : \theta \mathbf{R}(X) \to \sigma \mathbf{R}(X)$, as $r(\nu, f) = (\nu, f_{|\text{Max}\, F})$ and $s(\nu, f) = (\nu, f^*)$, where $F = \text{supp}\,\nu$; f^* is the largest continuous extension of f to the whole of F: this exists because X is a bc-domain [7, Proposition II-3.9], and Max F is dense in F. We use the explicit formula $f^*(\omega) = \sup_{\omega' \text{ finite prefix of } \omega} \inf f\langle \uparrow \omega' \cap \text{Max}\, F\rangle$. It can be shown that r and s form a *retraction*, i.e., they are continuous and $r \circ s = \text{id}_{\theta \mathbf{R}(X)}$. We shall then conclude since every retract of a bc-domain is a bc-domain [6, Proposition 4.1.3], and the image of a basis by r is a basis [6, Lemma 3.1.3]. (The proof for the uniform case is essentially the same.)

The main difficulty is showing the continuity of s. Let $(\nu_i, f_i)_{i \in I}$ be a directed family of thin CRVs on X, $F_i = \text{supp}\,\nu_i$, and (ν, f) their sup, with $F = \text{supp}\,\nu = cl(\bigcup_{i \in I} F_i)$.

We must show that $f^* \leq \sup_{i \in I} f_i^* \circ p_{F_i|F}$; the converse inequality is by monotonicity. It suffices to show that, for every $\omega \in F$, for every $x \in X$ such that $x \ll f^*(\omega)$, there is an $i \in I$ such that $x \leq f_i^*(p_{F_i}(\omega))$. Using the definition of f and $x \ll f^*(\omega)$, one obtains that $((f_i \circ p_{F_i})^{-1}(\Uparrow x))_{i \in I}$ is a (directed) open cover of $\uparrow \omega' \cap \text{Max}\, F$. It is an easy consequence of Corollary IV.4 that $\uparrow \omega' \cap \text{Max}\, F$ is compact in Ω. So there is an $i \in I$ such that $\uparrow \omega' \cap \text{Max}\, F \subseteq (f_i \circ p_{F_i})^{-1}(\Uparrow x)$, from which we deduce $x \leq \inf f_i \circ p_{F_i}\langle \uparrow \omega' \cap \text{Max}\, F\rangle$.

There is also a $j \in I$ such that $\omega' \in F_j$: indeed, the open $\uparrow \omega'$ meets $F = cl(\bigcup_{j \in I} F_j)$ (at ω), hence some F_j. By directedness, we can assume $i = j$. Then $\uparrow \omega' \cap \text{Max}\, F_i \subseteq p_{F_i}\langle \uparrow \omega' \cap \text{Max}\, F\rangle$. So $x \leq \inf f_i\langle \uparrow \omega' \cap \text{Max}\, F_i\rangle$. Since ω' is a finite prefix of ω and $\omega' \in F_i$, ω' is also a finite prefix of $p_{F_i}(\omega)$. So $x \leq f_i^*(p_{F_i}(\omega))$. ∎

V. The Monads of Thin CRVs, of Uniform CRVs

We now show that $\theta \mathbf{R}_1$ and $\upsilon \mathbf{R}_1$ define monads in the category **BCD** of bc-domains. It is easy to extend this to $\theta \mathbf{R}$, $\upsilon \mathbf{R}$, $\theta \mathbf{R}_a$ and $\upsilon \mathbf{R}_a$, for every $a \geq 1$.

Let $\omega.\omega'$ be the ordinary concatenation of ω and ω' if ω is a finite word, and as ω otherwise. Note that the function $(\omega.)$ mapping ω' to $\omega.\omega'$ is Scott-continuous; beware that $\omega.\omega'$ is not continuous, even not monotonic, in ω.

There are several equivalent definitions of a monad $(\theta \mathbf{R}_1, \boldsymbol{\eta}, \boldsymbol{\mu})$. One of the simplest [8] is given by a transformation $\boldsymbol{\eta}$, i.e., a collection of morphisms $\boldsymbol{\eta}_X : X \to \theta \mathbf{R}_1(X)$ for each object X, plus an *extension* morphism $h^\dagger : \theta \mathbf{R}_1(X) \to \theta \mathbf{R}_1(Y)$, for each morphism $h : X \to \theta \mathbf{R}_1(Y)$, such that: (a) $\boldsymbol{\eta}_X^\dagger = \text{id}_{\theta \mathbf{R}_1(X)}$; (b) $h^\dagger \circ \boldsymbol{\eta}_X = h$ for every morphism $h : X \to \theta \mathbf{R}_1(Y)$; (c) $k^\dagger \circ h^\dagger = (k^\dagger \circ h)^\dagger$ for all morphisms $k : Y \to \theta \mathbf{R}_1(Z)$, $h : X \to \theta \mathbf{R}_1(Y)$. If so, then $\theta \mathbf{R}_1$ defines a functor, whose action on morphisms $h : X \to Y$ is $\theta \mathbf{R}_1(h) = (\boldsymbol{\eta}_Y \circ h)^\dagger$, $\boldsymbol{\eta}$ is a natural transformation, and the *multiplication* $\boldsymbol{\mu}_X : \theta \mathbf{R}_1^2(X) \to \theta \mathbf{R}(X)$ is a natural transformation defined as $\text{id}_{\theta \mathbf{R}_1(X)}^\dagger$.

Define $\boldsymbol{\eta}_X(x)$ as $(\delta_\epsilon, \{\epsilon \mapsto x\})$. This is Scott-continuous in x, using Proposition IV.6. Also, $\boldsymbol{\eta}_X(x)$ is thin, even uniform.

We define $h^\dagger$ on continuous dcpos, through suitable approximates. Given a thin simple probability CRV $(\nu, f) \in \theta \mathbf{R}_1(X)$, i.e., one such that $F = \text{supp}\,\nu$ is finite—write ν as $\sum_{\omega \in \text{Max}\, F} a_\omega \delta_\omega$—and given a *simple* map $h : X \to \theta \mathbf{R}(Y)$, i.e., one such that for every $x \in X$, $h(x)$ is a thin simple probability CRV—say $h(x) = (\nu'_x, f'_x)$ where $F'_x = \text{supp}\,\nu'_x$ is finite and $\nu'_x = \sum_{\omega' \in \text{Max}\, F'_x} a'_{x\omega'} \delta_{\omega'}$—we define $h^\dagger(\nu, f)$ as (ν'', f'') where $\nu'' = \sum_{\omega \in \text{Max}\, F, \omega' \in \text{Max}\, F'_{f(\omega)}} a_\omega a'_{f(\omega)\omega'} \delta_{\omega.\omega'}$ and $f''(\omega.\omega') = f'_{f(\omega)}(\omega')$ for all $\omega \in \text{Max}\, F$, $\omega' \in \text{Max}\, F'_{f(\omega)}$. (This is well-defined because ω is a finite word, and continuous because the topology of $\text{Max}\,\text{supp}\,\nu'' = \{\omega.\omega' \mid \omega \in \text{Max}\, F, \omega' \in \text{Max}\, F'_{f(\omega)}\}$ is discrete.) To avoid an accumulation of indices in proofs, we note that ν'' can be written more synthetically as $\sum_{\omega \in \text{Max}\, F} a_\omega.(\omega.)[\nu'_{f(\omega)}]$. It is an easy exercise to show that, if ν is partially uniform and each $\nu'_{f(\omega)}$ is partially uniform, then so is ν''.

For two bc-domains X, Z, the space $[X \rightarrow Z]$ of all continuous maps from X to Z is again a bc-domain [7, Proposition II-4.20], and has a basis of finite sups of step functions. A step function is a map $z\chi_U$ where $z \in Z$ and U is open in X, defined as $z\chi_U(x) = z$ if $x \in U$, $z\chi_U(x)$ is the least element $\perp$ of Z otherwise. It is an easy refinement to show that we can restrict to step functions $z\chi_U$ where z is taken from a fixed basis of Z. This applies to $Z = \theta\mathbf{R}_1(Y)$ whenever Y is a bc-domain, by Theorem IV.7 (and subsequent discussion). So $[X \rightarrow \theta\mathbf{R}_1(Y)]$ has a basis of *simple* functions.

Proposition V.1 *Let X, Y be bc-domains. The formula* $\sup_{\substack{h' \ simple:X\rightarrow\theta\mathbf{R}_1(Y),h'\ll h \\ (v',f') \ simple \lll (v,f)}} h'^\dagger(v',f')$ *defines the unique Scott-continuous extension of the map $\lambda h \ simple : X \rightarrow \theta\mathbf{R}_1(Y), (v,f) \ simple \in \theta\mathbf{R}_1(X) \cdot h^\dagger(v,f)$ to $[X \rightarrow \theta\mathbf{R}_1(Y)] \times \theta\mathbf{R}_1(X)$.*

Proof: (Sketch.) This follows from the standard lemma, sometimes called Scott's extension formula, that the above formula defines the largest continuous map below $Dggr = \lambda h \ simple : X \rightarrow \theta\mathbf{R}_1(Y), (v,f) \ simple \in \theta\mathbf{R}_1(X) \cdot h^\dagger(v,f)$, given that the domain of definition of $Dggr$ is a basis, provided $Dggr$ is monotonic; and that this is its unique continuous extension if $Dggr$ is itself Scott-continuous on its domain of definition. This is checked by laborious computations. ∎

We write $h^\dagger$ for the continuous extension obtained in Proposition V.1. Since $h^\dagger(v,f)$ is uniform whenever (v,f) is a simple uniform CRV and $h(x)$ is also simple and uniform, the same formula also restricts to a continuous map $h, (v,f) \mapsto h^\dagger(v,f)$ from $[X \rightarrow \upsilon\mathbf{R}_1(Y)] \times \upsilon\mathbf{R}_1(X)$ to $\upsilon\mathbf{R}_1(Y)$.

Instead of checking the monad laws explicitly, we exhibit $\theta\mathbf{R}_1(X)$ (and $\upsilon\mathbf{R}_1(X)$) as free objects. This has the benefit of exhibiting the inequational theory that characterizes our construction. We still need to check monad law (a): applying the formula for $h^\dagger(v,f)$ when $h = \boldsymbol{\eta}_X$ (which is simple), $v = \sum_{\omega\in\mathrm{Max}\,F} a_\omega\delta_\omega$, and $F = \mathrm{supp}\,v$ is finite, we obtain $\boldsymbol{\eta}_X^\dagger(v,f) = (v'',f'')$, where $v'' = \sum_{\omega\in\mathrm{Max}\,F,\omega'=\epsilon}(a_\omega\times 1)\delta_{\omega.\omega'} = v$ and $f''(\omega+\epsilon) = f'_{f(\omega)}(\epsilon) = f(\omega)$. By uniqueness of extension (Proposition V.1), $\boldsymbol{\eta}_X^\dagger = \mathrm{id}_{\theta\mathbf{R}_1(X)}$.

Let $\mathbb{B}$ be the domain of Booleans, identified with $\Sigma = \{1,0\}$, with equality as ordering. The lifting $\mathbb{B}_\perp$ (where $X_\perp$ is X with a fresh least element $\perp$ added) is a bc-domain. For each $p \in (0,1)$, there is a (biased) *coin-flipping* element $\divideontimes_p = (p\delta_1 + (1-p)\delta_0, \mathrm{id}_\mathbb{B})$. We extend the notation to the cases $p = 0$ and $p = 1$: $\divideontimes_0 = (\delta_0, \{0 \mapsto 0\})$, $\divideontimes_1 = (\delta_1, \{1 \mapsto 1\})$. (Although $0.\delta_1 + 1.\delta_0 = \delta_0$, defining $\divideontimes_0$ as $(\delta_0, \mathrm{id}_\mathbb{B})$ as in the general case would be incorrect, as 1 is not in the support of δ_0.) For all elements x, y in a bc-domain Y, define the parallel conditional map pif _ then x else $y : \mathbb{B}_\perp \rightarrow Y$ so that pif 1 then x else $y = x$, pif 0 then x else $y = y$, pif $\perp$ then x else $y = \inf(x,y)$. We can then define a probabilistic choice operator $\oplus_p$ between two thin probability

CRVs by $(v,f) \oplus_p (v',f') = (\text{pif } \_ \text{ then } (v,f) \text{ else } (v',f'))^\dagger \circ \divideontimes_p$: flip a coin, and proceed with either (v,f) or (v',f').

Theorem V.2 *A coin algebra is a pair of a dcpo C with a continuous map $\oplus_p : C \times C \rightarrow C$ for each $p \in [0,1]$, satisfying: (i) $c \leq c \oplus_p c$; (ii) $\oplus_0$ is independent of its first argument: $c_1 \oplus_0 c' = c_2 \oplus_0 c'$; (iii) $\oplus_1$ is independent of its second argument: $c \oplus_1 c'_1 = c \oplus_1 c'_2$. This is a coin bc-algebra iff C is also a bc-domain.*

For every bc-domain X, $\theta\mathbf{R}_1(X)$ is a coin bc-algebra with coin-flipping operation $(v,f) \oplus_p (v',f') = (\text{pif } \_ \text{ then } (v,f) \text{ else } (v',f'))^\dagger \circ \divideontimes_p$. Actually, $\theta\mathbf{R}_1(X)$ is the free coin algebra: every continuous map $h : X \rightarrow C$ to a coin algebra C has a unique continuous extension $h^{ext} : \theta\mathbf{R}_1(X) \rightarrow C$ (i.e., $h^{ext} \circ \boldsymbol{\eta}_X = h$) that is a coin algebra morphism ($h^{ext}((v,f) \oplus_p (v',f')) = h^{ext}(v,f) \oplus_p h^{ext}(v',f')$).

Proof: Let X be a bc-domain. In every bc-domain, the binary inf map is Scott-continuous [7, Proposition I-1.8]. This applies to $\theta\mathbf{R}_1(X)$, by Theorem IV.7. So pif _ then (v,f) else (v',f') is continuous in (v,f) and (v',f'). Since $h^\dagger$ is continuous in h (Proposition V.1), it follows that $\oplus_p$ is continuous on $\theta\mathbf{R}_1(X)$. Moreover, $\boldsymbol{\eta}_X(\perp) \leqq \divideontimes_p$ in $\theta\mathbf{R}_1(\mathbb{B}_\perp)$. So, $(\text{pif } \_ \text{ then } (v,f) \text{ else } (v',f'))^\dagger(\boldsymbol{\eta}_X(\perp)) \leqq (v,f) \oplus_p (v',f')$. By monad law (a), $\inf((v,f),(v',f')) \leqq (v,f) \oplus_p (v',f')$. In particular, (i) $(v,f) \leqq (v,f) \oplus_p (v,f)$. If $p = 0$, then $(v,f) \oplus_0 (v',f') = ((0.)[v'], \lambda 0.\omega' \cdot f'(\omega'))$, which is independent of (v,f), so (ii) holds; (iii) is similar.

Consider now a continuous map $h : X \rightarrow C$ to a coin algebra C. Define h^{ext} first on simple thin probability CRVs (v,f), where $v = \sum_{\omega\in\mathrm{Max}\,F} a_\omega\delta_\omega$, $F = \mathrm{supp}\,v$ is finite, by induction on the largest length ℓ_F of a word in $\mathrm{Max}\,F$. If $\ell_F = 0$, then $v = \delta_\epsilon$, so $(v,f) = \boldsymbol{\eta}_X(f(\epsilon))$, and we must let $h^{ext}(v,f) = f(\epsilon)$. If $\ell_F \geq 1$, then $\epsilon \notin \mathrm{Max}\,F$, so every element $\omega \in \mathrm{Max}\,F$ is either of the form $1.\omega_1$ or $0.\omega_2$. Let $p = v(\uparrow 1) = \sum_{1.\omega_1\in\mathrm{Max}\,F} a_{1.\omega_1}$, and v_1 be the conditional probability $\frac{1}{p}\sum_{1.\omega_1\in\mathrm{Max}\,F} a_{1.\omega_1}\delta_{\omega_1}$ if $p \neq 0$, else δ_ϵ (this is arbitrary). Define $f_1(\omega_1) = f(1.\omega_1)$ if $p \neq 0$, and $f_1(\epsilon)$ as some arbitrary element if $p = 0$. Similarly, let $v_2 = \frac{1}{1-p}\sum_{0.\omega_2\in\mathrm{Max}\,F_2} a_{0.\omega_2}\delta_{\omega_2}$ and $f_2(\omega_2) = f(0.\omega_2)$ if $p \neq 1$, $v_2 = \delta_\epsilon$ and $f_2(\epsilon)$ arbitrary otherwise. Note that $(v,f) = (v_1,f_1) \oplus_p (v_2,f_2)$ (even if $p = 0$ or $p = 1$), so we must define $h^{ext}(v,f)$ as $h^{ext}(v_1,f_1) \oplus_p h^{ext}(v_2,f_2)$. This defines h^{ext} uniquely on simple thin probability CRVs. So, if h^{ext} is monotonic and Scott-continuous on the latter, it will extend to a unique continuous map on $\theta\mathbf{R}_1(X)$, as desired.

If (v,f) is as above, with $F = \mathrm{supp}\,v$, and (v',f') is a simple thin probability CRV above (v,f), we show that $h^{ext}(v,f) \leq h^{ext}(v',f')$ by induction on ℓ_F, splitting (v,f) recursively, with probability $p = v(\uparrow 1)$, and (v',f') in the same way, with the *same* probability $v'(\uparrow 1) = p$. When $p = 0$ or $p = 1$, we use (ii), resp. (iii) to replace the argument of $\oplus_p$ that was chosen arbitrarily by the right one. In the base case, we rest on the auxiliary claim that if $c \leq f(\omega)$ for every $\omega \in \mathrm{Max}\,F$, then $c \leq h^{ext}(v,f)$. This is by induction on ℓ_F

again.

To show that h^{ext} is Scott-continuous on simple thin probability CRVs, consider a directed family $(\nu_i, f_i)_{i \in I}$ whose sup (ν, f) is simple. Let $F = \operatorname{supp} \nu$. Since F is finite, and supp is Scott-continuous, there is an $i_0 \in I$ such that $\operatorname{supp} \nu_{i_0} = F$. Replacing the family by $(\nu_i, f_i)_{i \in I, (\nu_{i_0}, f_{i_0}) \leqq (\nu_i, f_i)}$ if necessary, we have $\operatorname{supp} \nu_i = F$ for every $i \in I$. So $\nu_i = p_F[\nu] = \nu$ by (E). That $h^{ext}(\nu, f) = \sup_{i \in I} h^{ext}(\nu, f_i)$ is then proved by induction on ℓ_F, using the fact that $\oplus_p$ is Scott-continuous. ∎

The following is proved similarly.

Theorem V.3 *A* fair-coin algebra *is a pair of a dcpo C with a continuous map* $\oplus_p : C \times C \to C$ *for each* $p \in \{0, \frac{1}{2}, 1\}$, *satisfying* (i)–(iii).

For every bc-domain X, $\nu\mathbf{R}_1(X)$ *is the free fair-coin algebra over X.*

Thin probability CRVs have a very simple (in)equational theory, given as (i)–(iii). The laws from a probabilistic choice monad [1, Section 9] fail: commutativity ($c \oplus_p c' = c' \oplus_{1-p} c$), associativity ($c \oplus_p (c' \oplus_{p'} c'') = (c \oplus_{p''} c') \oplus_{p+p'-pp'} c''$ if $p = (p + p' - pp')p''$), absorption ($c \oplus_p c = c$), and the one and zero laws ($c \oplus_1 c' = c'$, $c \oplus_0 c' = c'$) all fail.

Theorem V.2 exhibits a left adjoint to the forgetful functor from a suitable category of coin bc-algebras to **BCD**. By standard category theory, $(\theta\mathbf{R}_1, \boldsymbol{\eta}, \boldsymbol{\mu})$ is a monad, where $\boldsymbol{\mu}_X = \operatorname{id}_{\theta\mathbf{R}_1(X)}^{\dagger}$. The action of the functor $\theta\mathbf{R}_1$ on morphisms $h : X \to Y$ is then given by $\theta\mathbf{R}_1(h) = (\boldsymbol{\eta}_Y \circ h)^{\dagger}$. One sees easily that $\theta\mathbf{R}_1(h)(\nu, f) = (\nu, h \circ f)$ for every simple thin probability CRV (ν, f), hence for every $(\nu, f) \in \theta\mathbf{R}_1(X)$ by continuity.

Additionally, a *tensorial strength* for a monad $(T, \boldsymbol{\eta}, \boldsymbol{\mu})$ is a transformation $\boldsymbol{t}_{X,Y} : X \times T(Y) \to T(X \times Y)$ satisfying a certain number of equations, due to A. Kock (see [9]). Since the categories of dcpos we are interested in have finite products and enough points, Proposition 3.4 of op.cit. entails that every monad T has a unique tensorial strength, where $\boldsymbol{t}_{X,Y}(x, u) = T(\lambda y \cdot (x, y))(u)$. So:

Theorem V.4 $(\theta\mathbf{R}_1, \boldsymbol{\eta}, \boldsymbol{\mu}, \boldsymbol{t})$ *and* $(\nu\mathbf{R}_1, \boldsymbol{\eta}, \boldsymbol{\mu}, \boldsymbol{t})$ *are strong monads on* **BCD**.

We observe here that general CRVs also form a coin algebra, but they are not free. One of the reasons is that there is no canonical way of sending a continuous valuation over Ω to a thin valuation. Therefore, already on the one point domain (where the f part of a CRV plays no role), CRVs are not the free algebra.

To see that more concretely, consider the (non-thin) valuation $\nu = a\delta_0 + b\delta_1 + c\delta_\epsilon$ with $a + b + c = 1$ and $c > 0$. For any choice of r such that $0 \leq r \leq 1$, we can build a coin algebra homomorphism that sends ν to the thin valuation $\nu' = (a + rc)\delta_0 + (b + (1 - r)c)\delta_1$. This shows that in general there is not a unique homorphism between CRVs on the one-point domain and another coin-algebra.

Let X be a bc-domain. Since $\theta\mathbf{R}_1(X)$ is the free coin algebra (Theorem V.2), there is a unique continuous map $q_X : \theta\mathbf{R}_1(X) \to \mathbf{V}_1(X)$ such that $q_X(\delta_\epsilon, \{\epsilon \mapsto x\}) = \delta_x$ and $q_X((\nu, f) \oplus_p (\nu', f')) = pq_X(\nu, f) + (1 - p)q_X(\nu', f')$. It is reasonable to see $q_X(\nu, f)$ as the image valuation $f[\nu]$, although the latter is, formally, ill-typed. An easy induction on ℓ_F makes this precise, at least for simple thin CRVs (ν, f), where $\nu = \sum_{\omega \in \operatorname{Max} F} a_\omega \delta_\omega$, $F = \operatorname{supp} \nu$: then $q_X(\nu, f) = \sum_{\omega \in \operatorname{Max} F} a_\omega \delta_{f(\omega)}$.

There is also a strong monad $(\mathbf{V}_1, \eta, \mu, \mathbf{t})$ on the category of all dcpos [1]. Its extension operation $h^{\ddagger} : \mathbf{V}_1(X) \to \mathbf{V}_1(Y)$ (where $h : X \to \mathbf{V}_1(Y)$) is defined by $h^{\ddagger}(\mu)(V) = \int_{x \in X} h(x)(V) d\mu$, where $\int$ is the Jones integral. We shall need the following disintegration formula (Dis): $\int_{y \in Y} k(y) dh^{\ddagger}(\mu) = \int_{x \in X} \left(\int_{y \in Y} k(y) dh(x) \right) d\mu$ [1]. We write the integration variable as a subscript to $\int$; in the left-hand side, this is y (e.g., not μ), and the valuation along which we integrate is $h^{\ddagger}(\mu)$.

The definition of q_X makes it a lifting of $\operatorname{id}_X : X \to X$ to the algebras of the monads $\theta\mathbf{R}_1$, resp. $\mathbf{V}_1$ on **BCD**, hence defines a monad morphism. In particular, for every continuous map $h : X \to \theta\mathbf{R}_1(Y)$, $(q_Y \circ h)^{\ddagger} \circ q_X = q_Y \circ h^{\dagger}$, a property we shall call (Mor). A more concrete proof goes by showing that both sides are coin algebra morphisms, which coincide on elements of the form $\boldsymbol{\eta}_X(x)$, and applying Theorem V.2. (Mor) with (Dis) yields the following, second disintegration formula (Dis$_2$): $\int_{y \in Y} k(y) dq_Y(h^{\dagger}(\nu, f)) = \int_{x \in X} \left(\int_{y \in Y} k(y) dq_Y(h(x)) \right) dq_X(\nu, f)$.

VII. SEMANTICS

We now show that thin (resp., uniform) probability CRVs are as good as continuous probability valuations in giving semantics to higher-order probabilistic languages. As a case study, consider M. Escardó's probabilistic and non-deterministic extension of PCF [5]. (We write Qτ instead of his Sτ, to avoid a notational clash with the Sierpiński type S.) Call this language EPCF.

The ground types are $\gamma ::= \texttt{Bool} \mid \texttt{Nat}$, the general types are $\sigma, \tau ::= \gamma \mid \sigma \times \tau \mid \sigma \to \tau \mid \text{H}\tau \mid \text{Q}\tau \mid \text{P}\tau \mid \text{V}\tau$. Escardó's standard semantics of types τ is the dcpo $[\![\tau]\!]_1$, see below. $\mathcal{H}(X)$ is the Hoare powerdomain, $Q(X)$ is the Smyth powerdomain, and $\mathcal{P}(X)$ is the Plotkin powerdomain (see [7, Section IV-8]), but we will gloss over that part of the language: the challenge is with the probabilistic types Vτ. We also define an alternate semantics $[\![\tau]\!]_2$, which is always a bc-domain: $\mathcal{H}(X)$ and $Q(X)$ are bc-domains for every continuous dcpo X [6, Theorem 6.2.10], and $\nu\mathbf{R}_1(X)$ is a bc-domain whenever X is (Theorem IV.7). I.e., we replace $\mathbf{V}_1(X)$ (and also $\mathcal{P}(X)$), which is not a bc-domain even when

X is, by $\nu\mathbf{R}_1(X)$ (resp., $Q(X) \times \mathcal{H}(X)$).

$$
\begin{aligned}
\llbracket \text{Bool} \rrbracket_i &= \mathbb{B}_\perp & \llbracket \text{Nat} \rrbracket_i &= \mathbb{N}_\perp \\
\llbracket \sigma \times \tau \rrbracket_i &= \llbracket \sigma \rrbracket_i \times \llbracket \tau \rrbracket_i & \llbracket \sigma \to \tau \rrbracket_i &= [\llbracket \sigma \rrbracket_i \to \llbracket \tau \rrbracket_i] \\
\llbracket \text{H}\tau \rrbracket_i &= \mathcal{H}(\llbracket \tau \rrbracket_i) & \llbracket \text{Q}\tau \rrbracket_i &= Q(\llbracket \tau \rrbracket_i) \\
\llbracket \text{V}\tau \rrbracket_1 &= \mathbf{V}_1(\llbracket \tau \rrbracket_1) & \llbracket \text{V}\tau \rrbracket_2 &= \nu\mathbf{R}_1(\llbracket \tau \rrbracket_2) \\
\llbracket \text{P}\tau \rrbracket_1 &= \mathcal{P}(\llbracket \tau \rrbracket_1) & \llbracket \text{P}\tau \rrbracket_2 &= Q(\llbracket \tau \rrbracket_2) \times \mathcal{H}(\llbracket \tau \rrbracket_2)
\end{aligned}
$$

The term constructors are those of PCF [10], a higher-order lambda-calculus with constants for arithmetic and logical operations, a conditional $\texttt{if \_ then \_ else \_}$, and a fixpoint combinator $Y^\tau : (\tau \to \tau) \to \tau$; plus constants $\mathbb{V}_F^\tau : F\tau \times F\tau \to F\tau$ (non-deterministic choice; $F \in \{\text{H}, \text{Q}, \text{P}\}$), $\oplus^\tau : \text{V}\tau \times \text{V}\tau \to \text{V}\tau$ (non-biased random choice), $\eta_F^\tau : \tau \to F\tau$, $\mu_F^\tau : FF\tau \to F\tau$ and $t_F^{\sigma,\tau} : \sigma \times F\tau \to F(\sigma \times \tau)$ (unit, multiplication, tensorial strength of $F \in \{\text{H}, \text{Q}, \text{V}, \text{P}\}$); also, if M is a term of type $\sigma \to \tau$, then we have a term $FM : F\sigma \to F\tau$, $F \in \{\text{H}, \text{Q}, \text{V}, \text{P}\}$ (functor rule). The denotational semantics of these constructs is the obvious one. E.g., $\left\llbracket \eta_\text{V}^\tau \right\rrbracket_1 (x) = \delta_x$, $\left\llbracket \eta_\text{V}^\tau \right\rrbracket_2 = \boldsymbol{\eta}_{\llbracket \tau \rrbracket_2}$, $\llbracket \oplus^\tau \rrbracket_1 (\nu, \nu') = \frac{1}{2}\nu + \frac{1}{2}\nu'$, $\llbracket \oplus^\tau \rrbracket_2 ((\nu, f), (\nu', f')) = (\nu, f) \oplus_{\frac{1}{2}} (\nu', f')$.

Escardó also considers the following extension to PCF (not EPCF). PCF + S + I has two extra ground types S, with $\llbracket \text{S} \rrbracket_1 = \llbracket \text{S} \rrbracket_2 = \{\perp, \top\}$ (Sierpiński space; we have $\perp \le \top$), and I, interpreted as $[0, 1]$ with its usual ordering. The terms are also enriched with various constructs [5]. We shall only need to know that max, min, $\oplus$ (where $x \oplus y = (x + y)/2$), of type $\text{I} \times \text{I} \to \text{I}$, are definable in PCF + S + I, and that PCF + S + I is (real PCF-)computable: for any term M of ground type γ other than I, for every value ν of type γ, it is semi-decidable whether $\llbracket M \rrbracket_1 = \llbracket \nu \rrbracket_1$.

Finally, Escardó internalizes questions of may, must, may-must, and probabilistic testing of EPCF terms by considering yet another language MMP. MMP is EPCF enriched with the above extensions of PCF + S + I to PCF, and with testing primitives $\diamond : O\tau \to O\text{H}\tau$ (may testing, a.k.a., existential quantification; $O\tau$ abbreviates $\tau \to \text{S}$, the type of opens on τ), $\square : O\tau \to O\text{Q}\tau$ (must testing, a.k.a., universal quantification), and $\bigcirc : \mathcal{E}\tau \to \mathcal{E}\text{V}\tau$ (probabilistic testing, where $\mathcal{E}\tau = \tau \to \text{I}$). $\bigcirc$ is integration: $\llbracket \bigcirc \rrbracket_1 (h)(\mu) = \int_{x_1 \in \llbracket \tau \rrbracket_1} h(x_1) d\mu$. Similarly, we define $\llbracket \bigcirc \rrbracket_2 (h)(\nu, f) = \int_{x_2 \in \llbracket \tau \rrbracket_2} h(x_2) dq_{\llbracket \tau \rrbracket_2}(\nu, f)$.

The following key result states that the semantics of MMP terms depends on thin CRVs (ν, f) only through their image valuation $q_X(\nu, f)$. I.e., MMP is oblivious of the actual random bits drawn along ν in Ω. This is fairly general, and not specific to EPCF or MMP.

Theorem VII.1 *Let M be any closed MMP term of ground type. Then $\llbracket M \rrbracket_1 = \llbracket M \rrbracket_2$.*

Proof: Define a logical relation $(R_\tau)_{\tau \text{ type}}$, where $R_\tau \subseteq \llbracket \tau \rrbracket_1 \times \llbracket \tau \rrbracket_2$: R_γ is equality at each ground type γ, $h_1 R_{\sigma \to \tau} h_2$ iff $h_1(x_1) R_\tau h_2(x_2)$ for all $x_1 R_\sigma x_2$, $a_1 R_{\sigma \times \tau} a_2$ iff $\pi_1(a_1) R_\sigma \pi_1(a_2)$ and $\pi_2(a_1) R_\tau \pi_2(a_2)$ (where π_1, π_2 are projections). On non-deterministic types, let $\exists = \lambda v, h \cdot \diamond hv$, $\forall = \lambda v, h \cdot \square hv$,

$\int = \lambda v, h \cdot \bigcirc hv$, and define $C_1 R_{\text{H}\tau} C_2$ iff $\llbracket \exists \rrbracket_1 (C_1) R_{OO\tau} \llbracket \exists \rrbracket_2 (C_2)$, $Q_1 R_{\text{Q}\tau} Q_2$ iff $\llbracket \forall \rrbracket_1 (Q_1) R_{OO\tau} \llbracket \forall \rrbracket_2 (Q_2)$, $\mu R_{\text{V}\tau} (\nu, f)$ iff $\llbracket \int \rrbracket_1 (\mu) R_{\mathcal{E}\mathcal{E}\tau} \llbracket \int \rrbracket_2 (q_X(\nu, f))$. (This is defined along a well-founded ordering $>$ on types containing the subterm ordering and such that $\text{H}\tau, \text{Q}\tau, \text{P}\tau > OO\tau$, $\text{V}\tau > \mathcal{E}\mathcal{E}\tau$.) We now prove the Basic Lemma [11, Section 8.2.2], namely: whenever the free variables of $M : \tau$ are given related values, the two semantics of M are related by R_τ. This implies the Proposition when M is closed and τ is ground.

This is proved by induction on terms. The lambda-calculus constructs are classical, and we need to show that $\llbracket c \rrbracket_1 R_\tau \llbracket c \rrbracket_2$ for each constant $c : \tau$, and that the functor rules preserve relatedness. We deal with the probabilistic constructs only here. The case of $\int : \text{V}\tau \to \mathcal{E}\mathcal{E}\tau$ is by definition. For η_V^τ, we must show that whenever $x_1 R_\tau x_2$, $\llbracket \int \rrbracket_1 (\delta_{x_1}) R_{\mathcal{E}\mathcal{E}\tau} \llbracket \int \rrbracket_2 (q_X(\boldsymbol{\eta}_{\llbracket \tau \rrbracket_2}(x_2)))$, i.e., that whenever $h_1 R_{\mathcal{E}\tau} h_2$, $\int_{y_1 \in \llbracket \tau \rrbracket_1} h_1(y_1) d\delta_{x_1} = \int_{y_2 \in \llbracket \tau \rrbracket_2} h_2(y_2) d\delta_{x_2}$; equivalently, $h_1(x_1) = h_2(x_2)$, which is clear.

For the other constructs, we show that if $h_1 R_{\sigma \to \text{V}\tau} h_2$, then $h_1^\ddagger R_{\text{V}\sigma \to \text{V}\tau} h_2^\dagger$. I.e., assume $\mu R_{\text{V}\sigma} (\nu, f)$, let $k_1 R_{\mathcal{E}\tau} k_2$, and show that $\llbracket \int \rrbracket_1 (h_1^\ddagger(\mu))(k_1) = \llbracket \int \rrbracket_2 (h_2^\dagger(\nu, f))$, i.e., that $\int_{y_1 \in \llbracket \tau \rrbracket_1} k_1(y_1) dh_1^\ddagger(\mu) = \int_{y_2 \in \llbracket \tau \rrbracket_2} k_2(y_2) dq_{\llbracket \tau \rrbracket_2}(h_2^\dagger(\nu, f))$. Let $j_1(x_1) = \int_{y_1 \in \llbracket \tau \rrbracket_1} k_1(y_1) dh_1(x_1)$, $j_2(x_2) = \int_{y_2 \in \llbracket \tau \rrbracket_2} k_2(y_2) dh_2(x_2)$. Whenever $x_1 R_\sigma x_2$, $j_1(x_1) = j_2(x_2)$, since $h_1 R_{\sigma \to \text{V}\tau} h_2$ and $k_1 R_{\mathcal{E}\tau} k_2$. So $j_1 R_{\mathcal{E}\sigma} j_2$. Since $\mu R_{\text{V}\sigma} (\nu, f)$, $\int_{x_1 \in \llbracket \sigma \rrbracket_1} j_1(x_1) d\mu = \int_{x_2 \in \llbracket \sigma \rrbracket_2} j_2(x_2) dq_{\llbracket \sigma \rrbracket_2}(\nu, f)$. By the disintegration formula (Dis), the left-hand side is $\int_{y_1 \in \llbracket \tau \rrbracket_1} k_1(y_1) dh_1^\ddagger(\mu)$, and by (Dis$_2$), the right-hand side is $\int_{y_2 \in \llbracket \tau \rrbracket_2} k_2(y_2) dq_{\llbracket \tau \rrbracket_2}(h_2^\dagger(\nu, f))$.

For $\oplus^\tau$, we realize that $\llbracket \oplus \rrbracket_1 (\mu, \mu') = (\text{pif \_ then } \mu \text{ else } \mu')^\ddagger(\frac{1}{2}\delta_1 + \frac{1}{2}\delta_0)$, while by definition $\llbracket \oplus \rrbracket_2 ((\nu, f), (\nu', f')) = (\text{pif \_ then } (\nu, f) \text{ else } (\nu', f'))^\dagger(\divideontimes_{1/2})$. To show that $\llbracket \oplus^\tau \rrbracket_1 R_{\text{V}\tau} \llbracket \oplus^\tau \rrbracket_2$, it is therefore enough to show $\frac{1}{2}\delta_1 + \frac{1}{2}\delta_0 R_{\text{VBool}} \divideontimes_{1/2}$. This is an easy consequence of $\frac{1}{2}\delta_1 + \frac{1}{2}\delta_0 = q_{\mathbb{B}_\perp}(\divideontimes_{1/2})$.

As the semantics of μ_V^τ, of the functor rule V, and of the tensorial strength $t_F^{\sigma,\tau}$ are derived from the semantics of the extension operation, we conclude. ∎

VIII. Semi-Decidability of Testing

Escardó shows that the semi-decidability of may, must, and probabilistic testing in EPCF is reducible to the question of proving $\llbracket M \rrbracket_1 = \llbracket \phi(M) \rrbracket_1$ for every closed MMP term M of ground type [5, Lemma 6.2], where ϕ is the translation given below. (We refer the reader to op.cit. for further details on the actual connection with testing.) He stumbles on the question of the existence of a Cartesian-closed category of continuous domains that would be stable under $\mathbf{V}_1$. There is one that is stable under $\nu\mathbf{R}_1$ instead, namely **BCD**, and $\nu\mathbf{R}_1$ is as good as $\mathbf{V}_1$ in giving a semantics to EPCF (Theorem VII.1). We use this to solve Escardó's question.

At the level of types, $\phi(\gamma) = \gamma$, $\phi(\sigma \times \tau) = \phi(\sigma) \times \phi(\tau)$, $\phi(\sigma \to \tau) = \phi(\sigma) \to \phi(\tau)$, and $\phi(F\tau) = \texttt{Cantor} \to \phi(\sigma)$,

where `Cantor = Nat → Bool`. On terms, we only describe ϕ for probabilistic constructs, and direct the reader to [5] for the other cases. First, $\phi(\eta_V^\tau) = \lambda x \cdot \lambda s \cdot x$. Then, $\phi(\oplus^\tau) = \lambda(k_1, k_2) \cdot \lambda s \cdot \text{if hd } s \text{ then } k_1(\text{tl } s) \text{ else } k_2(\text{tl } s)$, where hd $s = s(0)$, tl $s = \lambda n \cdot s(n+1)$. Third, $\phi(\bigcirc) = \lambda u \cdot \lambda k \cdot \text{int}(\lambda s \cdot u(k(s)))$, where int encodes integration with respect to the uniform probability measure on Cantor space: $\text{int} = Y^{(\text{Cantor} \to I) \to I}(\lambda int \cdot \lambda h \cdot \max(h(\bot), int(\lambda s \cdot h(\text{cons } 1s)) \oplus int(\lambda s \cdot h(\text{cons } 0s))))$. Here cons $= \lambda u \cdot \lambda s \cdot \lambda n \cdot \text{if } n = 0 \text{ then } u \text{ else } s(n-1)$.

The key point is that $[\![\phi(V\tau)]\!]_2$ is a fair-coin algebra: $\oplus_{\frac{1}{2}}$ is $[\![\phi(\oplus^\tau)]\!]_2$, $\oplus_0$ is $[\![\lambda(k_1, k_2) \cdot \lambda s \cdot k_2(\text{tl } s)]\!]_2$ and $\oplus_1$ is $[\![\lambda(k_1, k_2) \cdot \lambda s \cdot k_1(\text{tl } s)]\!]_2$. Since $[\![\tau]\!]_2$ is a bc-domain, $[\![V\tau]\!]_2$ is the free fair-coin algebra (Theorem V.3). So there is a unique continuous fair-coin algebra morphism $\psi : [\![V\tau]\!]_2 \to [\![\phi(V\tau)]\!]_2$ with $\psi(\eta_{[\![\tau]\!]_2}(x)) = [\![\phi(\eta_V^\tau)]\!]_2(x) = \lambda s \cdot x$.

An alternate definition of $\mathcal{I} = [\![\text{int}]\!]_2$ is $\mathcal{I} = \sup_{n \in \mathbb{N}} \mathcal{I}_n$, where $\mathcal{I}_0(h) = h(\bot)$, and $\mathcal{I}_{n+1}(h) = \mathcal{I}_n(\lambda s \cdot h(\text{cons } 1s)) \oplus \mathcal{I}_n(\lambda s \cdot h(\text{cons } 0s))$. (To show the equivalence, we need to check that $h(\bot) \leq \mathcal{I}_n(h)$, which is easy.) This makes it clear that: (Unit) $\mathcal{I}(\lambda_- \cdot a) = a$ for every $a \in X$ ($\lambda_- \cdot a$ being the constant map with value a), that: (Midp) $\mathcal{I}(\xi_1 \oplus_{\frac{1}{2}} \xi_2) = \mathcal{I}(\xi_1) \oplus \mathcal{I}(\xi_2)$ (recall that $\xi_1 \oplus_{\frac{1}{2}} \xi_2 = [\![\phi(\oplus)]\!]_2(\xi_1, \xi_2)$); (Zero) $\mathcal{I}(\xi_1 \oplus_0 \xi_2) = \mathcal{I}(\xi_2)$; (One) $\mathcal{I}(\xi_1 \oplus_1 \xi_2) = \mathcal{I}(\xi_1)$.

Using this, we show that int implements integration correctly: (Int) $\mathcal{I}(k \circ (\psi(\nu, f))) = \int_{x \in X} k(x) dq_X(\nu, f)$ whenever X is a bc-domain. Indeed, both sides define fair-coin morphisms from $(\nu, f) \in \nu \mathbf{R}_1(X)$ to $[0, 1]$ by (Midp), (Zero), and (One), and both extend k, using (Unit).

We now show that Escardó's implementation of μ_V^τ is correct, too. As usual, we go through extension instead. Let evens, odds : `Cantor` $\to$ `Cantor` be defined by evens $= \lambda s \cdot \lambda n \cdot s(2n)$, odds $= \lambda s \cdot \lambda n \cdot s(2n+1)$, and define extension $h^\circledast : (\text{Cantor} \to \sigma) \to (\text{Cantor} \to \tau)$ of $h : \sigma \to (\text{Cantor} \to \tau)$ as $\lambda j \cdot \lambda s \cdot h(j(\text{evens } s))(\text{odds } s)$. Then let $\phi(\mu_V^\tau) = (\lambda x \cdot x)^\circledast$, $\phi(Vh) = (\lambda x \cdot \eta_V^\tau(h(x)))^\circledast$ for each $h : \sigma \to \tau$, and $\phi(t_V^{\sigma,\tau}) = \lambda x \cdot \lambda u \cdot \phi(V(\lambda x \cdot (x, y)))(u)$. We also write $h^\circledast$ for the corresponding semantic form.

It is a simple exercise to show the Fubini formula (Fub): $\mathcal{I}(\lambda s \cdot k([\![\text{evens}]\!]_2 s, [\![\text{odds}]\!]_2 s)) = \mathcal{I}(\lambda s \cdot \mathcal{I}(\lambda s' \cdot k(s, s')))$, using the rectangle law $(x \oplus y) \oplus (z \oplus t) = (x \oplus z) \oplus (y \oplus t)$.

One would expect $h^\circledast$ to implement extension, in the sense that if $\psi(\nu, f) = \xi$, then $\psi(h^\dagger(\nu, f)) = (\psi \circ h)^\circledast(\xi)$, but this is not true. Intuitively, the two extension formulae implement sequential composition, one by concatenation $\omega.\omega'$ (on finite approximates), the other one by interleaving (infinite sequences). However, defining $\xi \sim \xi'$ on $[[\![\text{Cantor}]\!]_2 \to X]$ ("ξ and ξ' define the same distribution on X") iff $\mathcal{I}(k \circ \xi) = \mathcal{I}(k \circ \xi')$ for every continuous map $k : X \to [0, 1]$, we obtain: (Ext) if $\psi(\nu, f) \sim \xi$ and $(\psi \circ h_1)(x) \sim h_2(x)$ for every $x \in X$, then $\psi(h_1^\dagger(\nu, f)) \sim h_2^\circledast(\xi)$. To check this, let $k : X \to [0, 1]$ be continuous, and define $j(x) = \mathcal{I}(k \circ (h_2(x)))$. Then $\mathcal{I}(k \circ \psi(h_1^\dagger(\nu, f))) = \int_{y \in Y} k(y) dq_Y(h_1^\dagger(\nu, f))$ (by (Int))

$= \int_{x \in X} \left(\int_{y \in Y} k(y) dq_Y(h_1(x)) \right) dq_X(\nu, f)$ (by (Dis$_2$)) $= \int_{x \in X} \mathcal{I}(k \circ (\psi(h_1(x)))) dq_X(\nu, f)$ (by (Int)) $= \int_{x \in X} \mathcal{I}(k \circ (h_2(x))) dq_X(\nu, f)$ (since $(\psi \circ h_1)(x) \sim h_2(x)) = \int_{x \in X} j(x) dq_X(\nu, f) = \mathcal{I}(j \circ (\psi(\nu, f)))$ (by (Int)) $= \mathcal{I}(j \circ \xi)$ (since $\psi(\nu, f) \sim \xi) = \mathcal{I}(\lambda s \cdot \mathcal{I}(\lambda s' \cdot k[h_2(\xi(s))(s')])) = \mathcal{I}(\lambda s \cdot k[h_2(\xi(\text{evens}(s)))(\text{odds}(s))])$ (by (Fub)) $= \mathcal{I}(k \circ (h_2^\circledast(\xi)))$.

Proposition VIII.1 *Let M be any closed MMP term of ground type. Then $[\![M]\!]_2 = [\![\phi(M)]\!]_2$.*

Proof: Define again a logical relation $(R_\tau)_{\tau \text{ type}}$, where now $R_\tau \subseteq [\![\tau]\!]_2 \times [\![\phi(\tau)]\!]_2$. We only deal with the probabilistic types and constructs—again, R_γ is equality on ground types γ, but this time we define $(\nu, f) R_{V\tau} \xi$ iff $\psi(\nu, f) \sim_\tau \xi$; the $\sim_\tau$ relation is a slight modification of $\sim$: $\xi_1 \sim_\tau \xi_2$ iff for all $k_1 R_{\tau \to I} k_2$, $\mathcal{I}(k_1 \circ \xi_1) = \mathcal{I}(k_2 \circ \xi_2)$. We then show that each constant c is related to $\phi(c)$: the case of $\bigcirc$ is by (Int), η_V^τ is by the definition of ψ, $\oplus^\tau$ is by (Midp). Finally, we show that if $h_1 R_{\sigma \to V\tau} h_2$, then $h_1^\dagger R_{V\sigma \to V\tau} h_2^\circledast$ by a slight adaptation of our proof of (Ext) above. This implies the cases of μ_V^τ, the V functor, and $t_V^{\sigma,\tau}$. ∎

So, also, $[\![M]\!]_1 = [\![\phi(M)]\!]_1$. By our earlier remarks:

Theorem VIII.2 *May, must, may-must, and probabilistic testing of EPCF terms is semi-decidable.*

One cannot hope for more, since one can easily encode probabilistic finite automata (PFA) in EPCF, and all quantitative reachability questions are undecidable for PFAs [12].

IX. LAYERED HOARE INDEXED VALUATIONS

This work originated in our desire to provide an explicit description (much like the space of all non-empty closed subsets of X is an explicit description of the Hoare powerdomain over X) of Varacca and Winskel's *indexed valuations*. These were defined as a way of obtaining a categorical distributive law between a non-deterministic and a probabilistic monad [3]. While CRVs are reasonably explicit, they do not quite match the latter: we show that (layered, Hoare) indexed valuations are intermediate between CRVs and valuations. As with CRVs, with indexed valuations, different sequences $\omega \in \Omega$ of coin flips terminating on the same value are not equated. But indexed valuations forget the identities of sequences ω, and just count their number. Additionally, computations with probability 0 are completely ignored.

The notion presented here is slightly different from the ones in [3], because of layering. The proof techniques are essentially the same.

Call a *finite random variable* (FRV) on X any finite family $\nu = (x_i, p_i)_{i \in I}$ in $X \times \mathbb{R}^+$. Write $Supp(\nu)$ for $\{i \in I \mid p_i > 0\}$, and let $\nu \equiv \xi$, where $\xi = (y_j, q_j)_{j \in J}$, iff there exists a bijection $h : Supp(\nu) \to Supp(\xi)$ such that $y_{h(i)} = x_i$ and $q_{h(i)} = q_i$ for every $i \in Supp(\nu)$. The set $IV(X)$ of *finite indexed valuations* is the set of all $\equiv$-equivalence classes of FRVs.

$(IV(X), \prec)$ is an abstract basis [6, Section 2.2.6] when X is a continuous dcpo; for ν, ξ as above (up to $\equiv$), let $\nu \prec \xi$

iff there is a surjective map $f : J \to I$ such that $x_{f(j)} \ll y_j$ and $p_i = \sum_{f(j)=i} q_j$ for every $j \in J$. (The = sign implements layering: the second author instead required $p_i \leq \sum_{f(j)=i} q_j$ in his definition of Hoare indexed valuations [3].) So one can build the round ideal completion $\mathcal{IV}(X)$ of $(IV(X), \prec)$: call this the domain of *layered Hoare indexed valuations*. We have:

Theorem IX.1 *A continuous quasi-cone is any structure* $(D, \sqsubseteq, \oplus, \underline{0}, \odot)$ *where D is a continuous dcpo,* $\oplus : D \times D \to D$ *is continuous,* $\odot : \mathbb{R}^+ \times D \to D$ *is continuous in the second argument (only! this is layering), and the following axioms are satisfied: (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)* $0 \odot A = \underline{0}$*; (5)* $1 \odot A = A$*; (6)* $p \odot (A \oplus B) = (p \odot A) \oplus (p \odot B)$*; (7)* $p \odot (q \odot A) = (pq) \odot A$*; (8)* $(p+q) \odot A \leq (p \odot A) \oplus (q \odot A)$*. For each continuous dcpo X,* $\mathcal{IV}(X)$ *is the free continuous quasi-cone over X.*

I.e., the functor $\mathcal{IV}$ is left-adjoint to the forgetful functor from the category **QCONT** of continuous quasi-cones and quasi-cone morphisms to the category **CONT** of continuous dcpos. For comparison, $\mathbf{V}(X)$ is the free *continuous cone* over X in **CONT**: their axioms are (1)-(8) above, with equality in (8), plus continuity of $\odot$. In particular, there is a unique continuous quasi-cone morphism $Flat : \mathcal{IV}(X) \to \mathbf{V}(X)$ with $Flat((\delta_i, x_i)_{i \in \{*\}}) = \delta_{x_*}$.

Every continuous quasi-cone is a coin algebra, defining $A \oplus_p B$ as $(p \odot A) \oplus ((1-p) \odot B)$. It follows easily that $\mathcal{IV}_1(X)$ is a coin algebra, hence that (for X a bc-domain) $q_X : \theta\mathbf{R}_1(X) \to \mathbf{V}_1(X)$ factors uniquely as $\theta\mathbf{R}_1(X) \xrightarrow{\rho} \mathcal{IV}_1(X) \xrightarrow{Flat} \mathbf{V}_1(X)$. As claimed above, the ρ map forgets the *identities* of sequences ω of coin flips: $\rho(\sum_{\omega \in \text{Max } F} a_\omega \delta_\omega)$ (for F finite) is the $\equiv$-*equivalence class* of the FRV $(a_\omega, \delta_\omega)_{\omega \in \text{Max } F}$.

X. Conclusion

We have defined monads $\theta\mathbf{R}_1$ and $\upsilon\mathbf{R}_1$ of thin (resp., uniform) CRVs, inspired by the second author's layered Hoare indexed valuations. They live in the well-behaved, Cartesian-closed category **BCD** of bc-domains. They also provide alternatives to the probabilistic powerdomain functor $\mathbf{V}_1$, which is not known to restrict to an endofunctor of any Cartesian-closed category of continuous dcpos: the closed terms of ground types in a rich probabilistic higher-order language have the same meaning, whether we use $\theta\mathbf{R}_1$, $\upsilon\mathbf{R}_1$, or the $\mathbf{V}_1$ monad. We have applied this to solve an open question by M. Escardó. We believe the notion should have other interesting applications as well.

References

[1] C. Jones and G. D. Plotkin, "A probabilistic powerdomain of evaluations," in *Proc. 4th IEEE Symposium on Logics in Computer Science (LICS'89)*. IEEE Computer Society Press, 1989, pp. 186–195.

[2] A. Jung and R. Tix, "The troublesome probabilistic powerdomain," *Electron. Notes Theor. Comput. Sci.*, vol. 13, pp. 70–91, 1998. Proc. Comprox III Workshop.

[3] D. Varacca, "Probability, nondeterminism and concurrency: Two denotational models for probabilistic computation," Ph.D. dissertation, Dept. of Computer Science, U. Aarhus, 2003, BRICS Dissertation Series DS-03-14.

[4] M. Mislove, "Discrete random variables over domains," *Theor. Comput. Sci.*, vol. 380, pp. 181–198, July 2007.

[5] M. Escardó, "Semi-decidability of may, must and probabilistic testing in a higher-type setting," *Electron. Notes Theor. Comput. Sci.*, vol. 249, pp. 219–242, 2009. Proc. MFPS XXV.

[6] S. Abramsky and A. Jung, "Domain theory," in *Handbook of Logic in Computer Science*, S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, Eds. Oxford University Press, 1994, vol. 3, pp. 1–168.

[7] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. Mislove, and D. S. Scott, "Continuous lattices and domains," in *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2003, vol. 93.

[8] E. G. Manes, *Algebraic Theories*, ser. Graduate Texts in Mathematics. Springer-Verlag, 1976, vol. 26.

[9] E. Moggi, "Notions of computation and monads," *Information and Computation*, vol. 93, pp. 55–92, 1991.

[10] G. D. Plotkin, "LCF considered as a programming language," *Theoretical Computer Science*, vol. 5, no. 1, pp. 223–255, 1977.

[11] J. C. Mitchell, *Foundations for Programming Languages*. MIT Press, 1996.

[12] H. Gimbert and Y. Oualhadj, "Probabilistic automata on finite words: Decidable and undecidable problems," in *Proc. 37th Intl. Coll. Automata, Languages and Programming (ICALP'10), Part II*. Springer Verlag LNCS 6199, 2010, pp. 527–538.