The Powerdomain of Continuous Random Variables

Jean Goubault-Larrecq, Daniele Varacca

LSV - ENS Cachan, PPS - Paris Diderot

LICS, June 21, 2011

Semantics of Higher-Order Probabilistic Languages

$$
\begin{array}{rcll}
\sigma, \tau & ::= & \gamma & \\
& \mid & \sigma \to \tau & \text{functions} \\
& \mid & \mathrm{V}\tau & \text{probability} \\
& \mid & \ldots & \text{distributions}
\end{array}
$$

$$
\begin{array}{rcll}
M, N, P & ::= & x_\tau & \\
& \mid & \lambda x_\sigma \cdot M & \\
& \mid & MN & \\
& \mid & \ldots & \\
& \mid & \divideontimes & \text{fair coin} \\
& \mid & \mathtt{val}\; M & \\
& \mid & \mathtt{let}\; x = M \;\mathtt{in}\; N & \text{sequence}
\end{array}
$$

Open Problem:

Does there exist a Cartesian closed category (=interpret $\sigma \to \tau$) of continuous domains, closed under the probabilistic powerdomain (=interpret $\mathrm{V}\tau$)?

We still do not know, but present an interesting alternative.

Road Map

1. Continuous Random Variables
   - The Classical Probabilistic Powerdomain
   - The Definition of Continuous Random Variables
   - In the CCC of BC-Domains
   - Equational Theories
2. Semantics
   - A Probabilistic Higher Order Language
   - Semi-Decidability of Testing

Road Map

1. Continuous Random Variables
   - The Classical Probabilistic Powerdomain
   - The Definition of Continuous Random Variables
   - In the CCC of BC-Domains
   - Equational Theories
2. Semantics
   - A Probabilistic Higher Order Language
   - Semi-Decidability of Testing

Outline

Continuous Valuations

Classical view [JonesPlotkin89]: interpret $\mathbb{V}\tau$ as space of continuous valuations (=measures on a topology).

Definition (Continuous Valuation)

A function $\nu : \mathrm{Opens}(X) \to [0, 1]$ with:

$$
\begin{array}{rcl}
\nu(\emptyset) & = & 0 \quad \text{(strictness)} \\
U \subseteq V & \Rightarrow & \nu(U) \leq \nu(V) \\
\nu(U \cup V) + \nu(U \cap V) & = & \nu(U) + \nu(V) \\
\nu(\bigcup^{\uparrow}_{i \in I} U_i) & = & \sup^{\uparrow}_{i \in I} \nu(U_i)
\end{array}
$$

We shall also require $\nu(X) = 1$ (probability).

Dirac Valuations

A Prominent Example.

For any $x \in X$, the Dirac valuation δ_x is defined as

$$\delta_x(U) = \begin{cases} 1 & \text{if } x \in U \\ 0 & \text{otherwise} \end{cases}$$

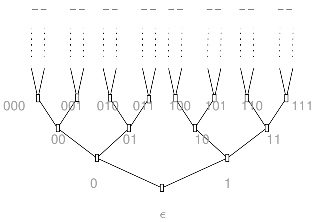
Simple valuations are finite linear combinations of Dirac valuations

$$\sum_{i=1}^{n} a_i \delta_{x_i}$$

with $a_1, \ldots, a_n \geq 0$, $\sum_{i=1}^{n} a_i = 1$.

Examples

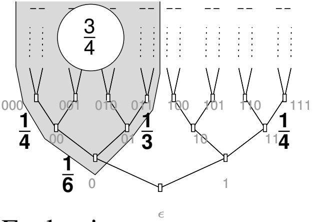
$\{0,1\}^{\leq\omega}$:
the Cantor tree.



- Basic open sets: $\uparrow x$ for finite sequence x

Examples

$\{0,1\}^{\leq\omega}$:
the Cantor tree.

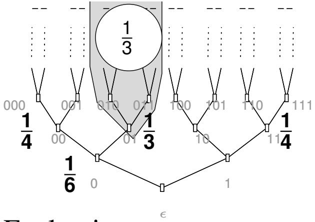


Evaluating
$\frac{1}{4}\delta_{00} + \frac{1}{6}\delta_0 + \frac{1}{3}\delta_{01} + \frac{1}{4}\delta_{11}$
on $\uparrow 0$

- Basic open sets: $\uparrow x$ for finite sequence x

Examples

$\{0,1\}^{\leq\omega}$:
the Cantor tree.

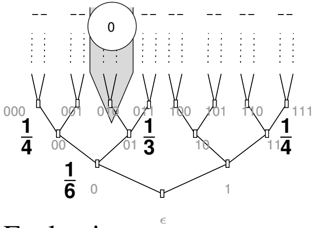


Evaluating
$\frac{1}{4}\delta_{00} + \frac{1}{6}\delta_0 + \frac{1}{3}\delta_{01} + \frac{1}{4}\delta_{11}$
on $\uparrow 01$

- Basic open sets: $\uparrow x$ for finite sequence x

Examples

$\{0,1\}^{\leq\omega}$:
the Cantor tree.

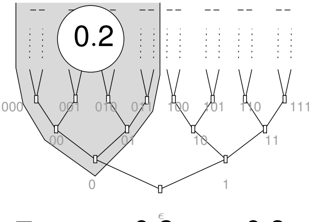


Evaluating
$\frac{1}{4}\delta_{00} + \frac{1}{6}\delta_0 + \frac{1}{3}\delta_{01} + \frac{1}{4}\delta_{11}$
on $\uparrow 010$

- Basic open sets: $\uparrow x$ for finite sequence x

Examples

$\{0,1\}^{\leq\omega}$:
the Cantor tree.

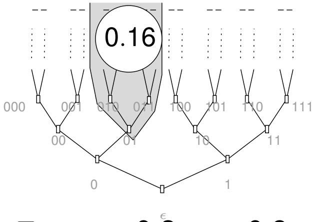


E.g., $p = 0.2$, $q = 0.8$.

- Basic open sets: $\uparrow x$ for finite sequence x
- Any biased coin (p, q) with $p + q = 1$ induces a continuous valuation $\nu(x) = p^a(1-p)^b$ where a is the number of 0's in x, while b is the number of 1's

Examples

$\{0, 1\}^{\leq \omega}$:
the Cantor tree.

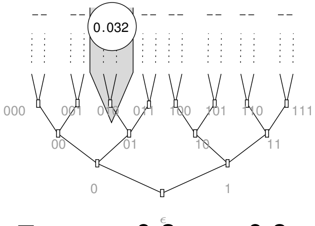


E.g., $p = 0.2$, $q = 0.8$.

- Basic open sets: $\uparrow x$ for finite sequence x
- Any biased coin (p, q) with $p + q = 1$ induces a continuous valuation $\nu(x) = p^a(1 - p)^b$ where a is the number of 0's in x, while b is the number of 1's

Examples

$\{0,1\}^{\leq\omega}$:
the Cantor tree.

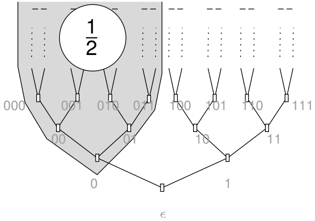


E.g., $p = 0.2$, $q = 0.8$.

- Basic open sets: $\uparrow x$ for finite sequence x
- Any biased coin (p, q) with $p + q = 1$ induces a continuous valuation $\nu(x) = p^a(1-p)^b$ where a is the number of 0's in x, while b is the number of 1's

Examples

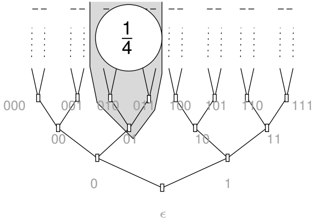
$\{0,1\}^{\leq\omega}$:
the Cantor tree.



- Basic open sets: $\uparrow x$ for finite sequence x
- Any biased coin (p, q) with $p + q = 1$ induces a continuous valuation $\nu(x) = p^a(1-p)^b$ where a is the number of 0's in x, while b is the number of 1's
- If $p = q = 1/2$ the induced valuation is the uniform valuation Λ (on the top elts)

Examples

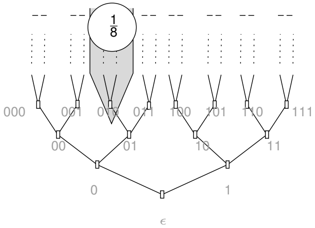
$\{0,1\}^{\leq\omega}$:
the Cantor tree.



- Basic open sets: $\uparrow x$ for finite sequence x
- Any biased coin (p, q) with $p + q = 1$ induces a continuous valuation $\nu(x) = p^a(1-p)^b$ where a is the number of 0's in x, while b is the number of 1's
- If $p = q = 1/2$ the induced valuation is the uniform valuation Λ (on the top elts)

Examples

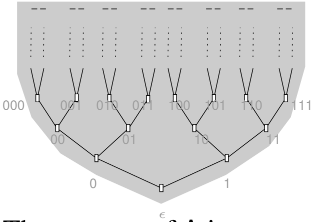
$\{0,1\}^{\leq\omega}$:
the Cantor tree.



- Basic open sets: $\uparrow x$ for finite sequence x
- Any biased coin (p, q) with $p + q = 1$ induces a continuous valuation $\nu(x) = p^a(1-p)^b$ where a is the number of 0's in x, while b is the number of 1's
- If $p = q = 1/2$ the induced valuation is the uniform valuation Λ (on the top elts)

Examples

$\{0,1\}^{\leq\omega}$:
the Cantor tree.

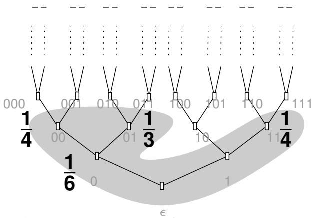


The support of Λ is
the whole Cantor tree

- Basic open sets: $\uparrow x$ for finite sequence x
- Any biased coin (p, q) with $p + q = 1$ induces a continuous valuation $\nu(x) = p^a(1-p)^b$ where a is the number of 0's in x, while b is the number of 1's
- If $p = q = 1/2$ the induced valuation is the uniform valuation Λ (on the top elts)
- The support $\operatorname{supp}\nu$, is the complement of the largest U such that $\nu(U) = 0$

Examples

$\{0,1\}^{\leq\omega}$:
the Cantor tree.



The support of $\frac{1}{4}\delta_{00} + \frac{1}{6}\delta_0 + \frac{1}{3}\delta_{01} + \frac{1}{4}\delta_{11}$

- Basic open sets: $\uparrow x$ for finite sequence x
- Any biased coin (p, q) with $p + q = 1$ induces a continuous valuation $\nu(x) = p^a(1-p)^b$ where a is the number of 0's in x, while b is the number of 1's
- If $p = q = 1/2$ the induced valuation is the uniform valuation Λ (on the top elts)
- The support $\operatorname{supp}\nu$, is the complement of the largest U such that $\nu(U) = 0$

The Troublesome Probabilistic Powerdomain

The functor **V** preserves the category of continuous domains.

The category of continuous domains is not Cartesian closed.

No Cartesian closed subcategory of continuous domains is known to be preserved by **V**.

No known (interesting) denotational semantics of probabilistic higher order languages.

Outline

Random Variables

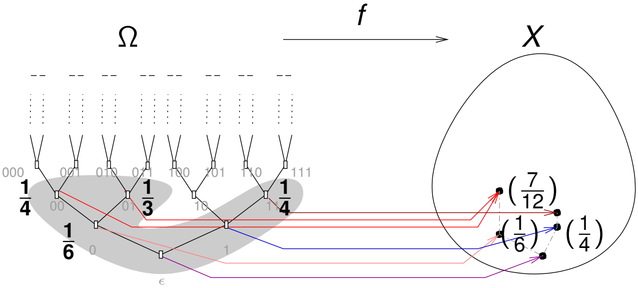
Random variable=
measure on a space Ω + a measurable map $f : \Omega \to X$:

- induces a measure on X (the image measure)
- Ω is the sample space
- X is the space of *observations* or outcomes

Continuous Random Variables

A continuous random variable is a continuous valuation ν on some space Ω, together with a continuous function $f : \operatorname{supp} \nu \to X$.

We will fix Ω to be the Cantor tree.



The Ordering on CRVs

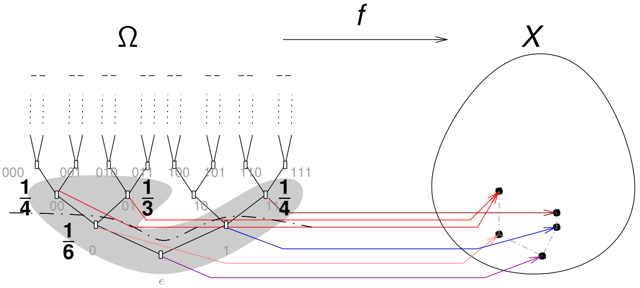
If $F = \operatorname{supp} \nu$, let $p_F(w)$ be largest prefix of w in F (projection).

Definition ($\leq$)

$(\nu, f) \leq (\nu', f')$ iff:

"increase supp, preserve probabilities" ν is img of ν' by $p_{\operatorname{supp} \nu}$

"increase values" $f \circ p_{\operatorname{supp} \nu} \leq f'$



The Ordering on CRVs

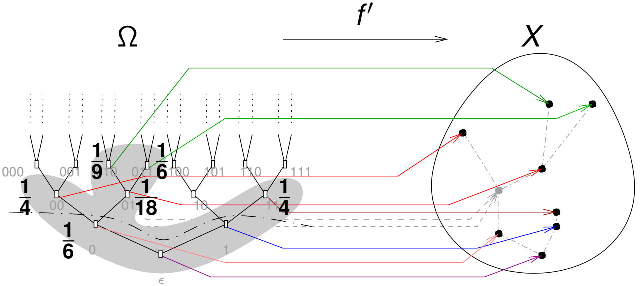
If $F = \operatorname{supp} \nu$, let $p_F(w)$ be largest prefix of w in F (projection).

Definition ($\leq$)

$(\nu, f) \leq (\nu', f')$ iff:

"increase supp, preserve probabilities" ν is img of ν' by $p_{\operatorname{supp} \nu}$

"increase values" $f \circ p_{\operatorname{supp} \nu} \leq f'$



The Ordering on CRVs

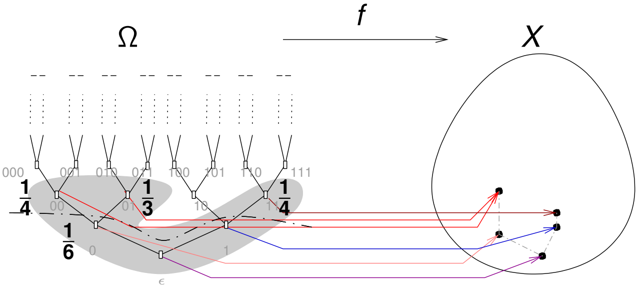
If $F = \operatorname{supp} \nu$, let $p_F(w)$ be largest prefix of w in F (projection).

Definition ($\leq$)

$(\nu, f) \leq (\nu', f')$ iff:

"increase supp, preserve probabilities" ν is img of ν' by $p_{\operatorname{supp} \nu}$

"increase values" $f \circ p_{\operatorname{supp} \nu} \leq f'$



The Ordering on CRVs

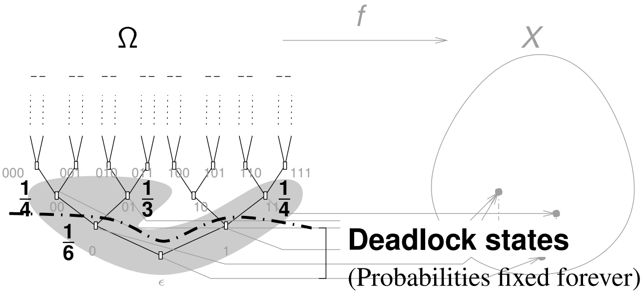
If $F = \text{supp}\,\nu$, let $p_F(w)$ be largest prefix of w in F (projection).

Definition ($\leq$)

$(\nu, f) \leq (\nu', f')$ iff:

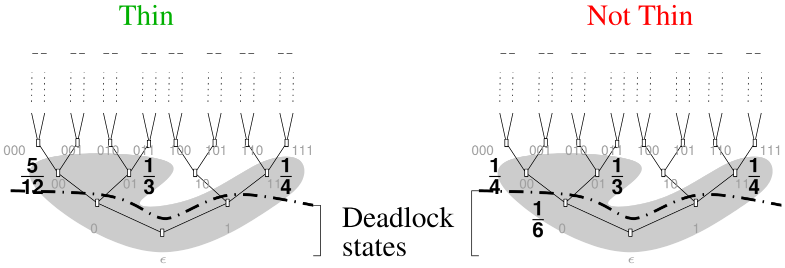
"increase supp, preserve probabilities" ν is img of ν' by $p_{\text{supp}\,\nu}$

"increase values" $f \circ p_{\text{supp}\,\nu} \leq f'$



Thin Random Variables

A continuous valuation that does not deadlock is called thin, as all the information can be gathered on the maximal elements of the support (a “thin” set).



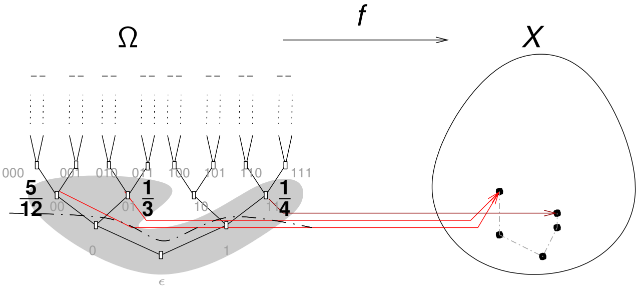
Note: the uniform valuation Λ is thin.

Thin Random Variables

Definition (Thin CRV (ν, f))

- ν is a thin continuous valuation on Ω
- f is a continuous map from Max supp ν to X

  ...so f is defined only on the non-deadlock elements of supp ν.



Note to the purist: if X is a bc-domain (needed later anyway), f extends canonically to supp ν. So thin CRVs are CRVs in this sense.

The Monad of Thin CRVs

Theorem

Thin CRVs form a monad.

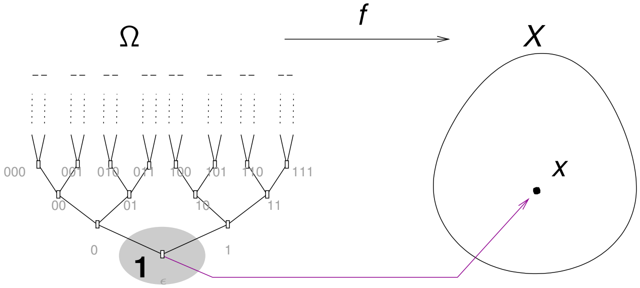
Proof: Arise as a free dcpo-algebra for some equational theory (see later.) □

- This says things such as $(A; B); C = A; (B; C)$, and other expected equations.
- **Not** the case for (non-thin) CRVs.

The Monad of Thin CRVs

Explicitly,

- $\theta\mathbf{R}(X)$ is space of thin CRVs over X;
- unit $\eta_X : X \to \theta\mathbf{R}(X)$ maps x to



"Flip no coin, return x right away"

The Monad of Thin CRVs

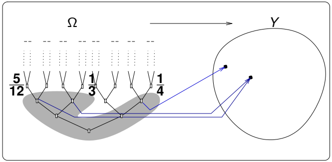
Extension $h^\dagger : \theta\mathbf{R}(X) \to \theta\mathbf{R}(Y)$ of $h : X \to \theta\mathbf{R}(Y)$:

"concatenate sequences of coin flips"

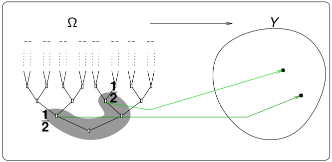
(sequential composition)

E.g., take h

$x_1 \longmapsto$

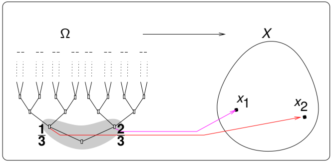


$x_2 \longmapsto$

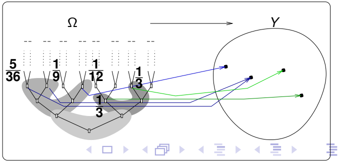


Then:

$h^\dagger$:



$\longmapsto$



Outline

1. Continuous Random Variables
   - The Classical Probabilistic Powerdomain
   - The Definition of Continuous Random Variables
   - In the CCC of BC-Domains
   - Equational Theories
2. Semantics
   - A Probabilistic Higher Order Language
   - Semi-Decidability of Testing

The Category of Bc-Domains

Definition

A dcpo D is a bc-domain iff

- it is continuous (there is a notion of approximation)
- it is bounded-complete (any finite set of elements that has an upper bound has a least one)

- The bc-domains are exactly the densely injective T_0 spaces [Scott, Escardó], a fact we require in the paper.

The Cartesian Closed Category of Bc-Domains

Theorem (Jung)

The category of bc-domains and continuous functions is Cartesian closed.

Thin CRVs and Bc-Domains

Theorem

Thin CRVs over a bc-domain D form a bc-domain $\theta\mathbf{R}(D)$.

Proof (sketch.)

- Thin CRVs arise as retract from semi-thin CRVs (i.e., (ν, f) where ν thin, but f defined on whole of $\operatorname{supp}\nu$), construction through dense injectivity
- Retracts of bc-domains are bc-domains, so prove semi-thin CRVs form a bc-domain:
- Approximation on semi-thin CRVs $(\nu, f) \lessdot (\nu', f')$ iff ν has finite support, $(\nu, f) \leqq (\nu', f')$ and $f(w) \ll f'(w)$ for every w
- Least upper bound of (ν, f) and (ν', f') if they have an upper bound (ν'', f'') at all: project (ν'', f'') onto $\operatorname{supp}\nu \cup \operatorname{supp}\nu'$. □

We can use thin CRVs for semantics!

Uniform CRVs

Definition (Uniform CRVs)

(ν, f) uniform iff thin + $\nu = p_{\text{supp}\,\nu}(\Lambda)$ (proj. of uniform valuation).

"Flip all bits with probability $\frac{1}{2}$, independently"

Theorem

Uniform CRVs also form a monad.

Theorem

Uniform CRVs over a bc-domain D form a bc-domain $\upsilon\mathbf{R}(D)$.

Proof: Sups of uniform CRVs taken in $\theta\mathbf{R}(D)$ are uniform. □

We can use uniform CRVs for semantics!

Outline

1. Continuous Random Variables
   - The Classical Probabilistic Powerdomain
   - The Definition of Continuous Random Variables
   - In the CCC of BC-Domains
   - Equational Theories
2. Semantics
   - A Probabilistic Higher Order Language
   - Semi-Decidability of Testing

Equational Theories

Sorry, I don't think we'll have time for a complete tour.

In short:

- Nice characterizations through equational theories
- We exhibit relationship with DV's indexed valuations
- Nice interplay with angelic non-determinism (distributive law)

Valuations

Equational Theory for **V**

1. $x \oplus_p y = y \oplus_{1-p} x$
2. $x \oplus_p (y \oplus_q z) = (x \oplus_{\frac{p}{p+q-pq}} y) \oplus_{p+q-pq} z$
3. $x \oplus_1 y = x$, $x \oplus_0 y = y$
4. $x = x \oplus_p x$

with $x \oplus_p y$ continuous in $x, y, p \in [0, 1]$

Layered Hoare Indexed Valuations

Equational Theory for $\mathscr{I}\mathscr{V}$ [This paper, variant]

1. $x \oplus_p y = y \oplus_{1-p} x$
2. $x \oplus_p (y \oplus_q z) = (x \oplus_{\frac{p}{p+q-pq}} y) \oplus_{p+q-pq} z$
3. $x \oplus_1 y = x$, $x \oplus_0 y = y$
4. $x \leq x \oplus_p x$ (Hoare indexed)

with $x \oplus_p y$ continuous in x, y, ~~$p \in [0, 1]$~~ (layered)

Thin Random Variables

Equational Theory for $\theta\mathbf{R}$ [This paper]

1. ~~$x \oplus_p y = y \oplus_{1-p} x$~~
2. ~~$x \oplus_p (y \oplus_q z) = (x \oplus_{\frac{p}{p+q-pq}} y) \oplus_{p+q-pq} z$~~
3. ~~$x \oplus_1 y = x, x \oplus_0 y = y$~~
   $x \oplus_1 y$ independent of y, $x \oplus_0 y$ independent of x
4. $x \leq x \oplus_p x$

with $x \oplus_p y$ continuous in x, y, ~~$p \in [0, 1]$~~

Uniform Random Variables

Equational Theory for $\upsilon\mathbf{R}$ [This paper]

1. ~~$x \oplus_p y = y \oplus_{1-p} x$~~
2. ~~$x \oplus_p (y \oplus_q z) = (x \oplus_{\frac{p}{p+q-pq}} y) \oplus_{p+q-pq} z$~~
3. ~~$x \oplus_1 y = x, x \oplus_0 y = y$~~
   $x \oplus_1 y$ independent of y, $x \oplus_0 y$ independent of x
4. $x \leq x \oplus_p x$

with $x \oplus_p y$ continuous in x, y, ~~$p \in [0, 1]$~~ and $p \in \{0, \frac{1}{2}, 1\}$

Road Map

Outline

How Good are CRVs at Giving Semantics?

We claim that:

Theorem (somewhat imprecise for now)

Thin CRVs, uniform CRVs are as good as valuations in giving semantics of higher-order programming languages.

- Intuition: no primitive in the language has explicit access to the random bits.

A Higher-Order Probabilistic Language

γ	$::=$	$\texttt{Bool} \mid \texttt{Nat} \mid \ldots$	base types
σ, τ	$::=$	γ	
	$\mid$	$\sigma \times \tau$	pairs
	$\mid$	$\sigma \to \tau$	functions
	$\mid$	$\texttt{V}\tau$	probability distributions
	$\mid$	$\ldots$	

M, N, P	$::=$	x_τ	all sorts
	$\mid$	$\lambda x_\sigma \cdot M$	of constructs
	$\mid$	MN	from the
	$\mid$	$\texttt{if } M \texttt{ then } N \texttt{ else } P$	PCF language,
	$\mid$	$Y^\tau M$	or extensions
	$\mid$	$\ldots$	
	$\mid$	$\divideontimes$	fair coin
	$\mid$	$\texttt{val } M$	monadic return
	$\mid$	$\texttt{let } x = M \texttt{ in } N$	sequential composition

The Valuation Semantics

$[\![\_]\!]_1$ is the standard valuation-based semantics

Definition ($[\![\_]\!]_1$)

$$[\![\mathrm{V}\tau]\!]_1 = \mathbf{V}([\![\tau]\!]_1)$$

$$\begin{aligned} [\![\divideontimes]\!]_1 &= \tfrac{1}{2}\delta_1 + \tfrac{1}{2}\delta_0 && \text{fair coin} \\ [\![\mathtt{val}\, M]\!]_1 &= \delta_{[\![M]\!]_1} \\ [\![\mathtt{let}\, x = M \,\mathtt{in}\, N]\!] &= U \mapsto \int_x [\![N]\!]_1 (x)(U) d\, [\![M]\!]_1 \end{aligned}$$

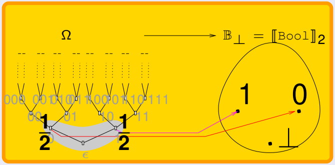
The Random Variable Semantics

$[\![\_]\!]_2$ is the uniform CRV-based semantics

Definition ($[\![\_]\!]_2$)

$$[\![\mathrm{V}\tau]\!]_2 = \upsilon\mathbf{R}([\![\tau]\!]_2)$$

$$[\![\ast]\!]_2 = $$



fair coin

$$[\![\mathtt{val}\ M]\!]_2 = \eta([\![M]\!]_2)$$

$$[\![\mathtt{let}\ x = M\ \mathtt{in}\ N]\!]_2 = (x \mapsto [\![N]\!]_2(x))^\dagger([\![M]\!]_2)$$

Note: The `val` and `let` cases are as in every monad.

$[\![\tau]\!]_2$ (not $[\![\tau]\!]_1$) is a bc-domain for every τ.

CRVs are as Good as Valuations

Theorem (Random Variables are as Good as Valuations)

Let M be any closed term of ground type γ. Then

$$[\![M]\!]_1 = [\![M]\!]_2$$

Proof: Define a logical relation $(R_\tau)_{\tau \text{ type}}$, where $R_\tau \subseteq [\![\tau]\!]_1 \times [\![\tau]\!]_2$:

$$\begin{array}{rcl} \mu\ R_{\mathrm{V}\tau}\ (\nu, f) & \text{iff} & \int_x h_1(x) d\mu = \int_w h_2(f(w)) d\nu \text{ whenever } h_1\ \widehat{R_\tau}\ h_2 \\ h_1\ \widehat{R_\tau}\ h_2 & \text{iff} & h_1(x_1) = h_2(x_2) \text{ whenever } x_1\ R_\tau\ x_2 \end{array}$$

"μ is *obs. indistinguishable* from image measure $\nu \circ f^{-1}$ of (ν, f)"

Prove the Basic Lemma: $[\![M]\!]_1\ R_\tau\ [\![M]\!]_2$ for all $M : \tau$.
At ground types, R_γ is equality: conclude. □

Outline

Probabilistic Testing

Definition (Testing Equivalence)

$M, N : \mathtt{V\ Bool}$ are probabilistically equivalent iff $\mathit{Prob}[M \Downarrow 1] = \mathit{Prob}[N \Downarrow 1]$

- Escardó [2009] also defines may-testing, must-testing equivalence (replace *Prob* by $\exists$, $\forall$) — I'll skip this, see paper.
- Formally requires operational semantics

$$\frac{}{\divideontimes \Downarrow 1} \qquad \frac{}{\divideontimes \Downarrow 0} \qquad \frac{M \Downarrow V}{\mathtt{val}\ M \Downarrow \mathtt{val}\ V} \qquad \frac{M \Downarrow \mathtt{val}\ V \quad N[x := V] \Downarrow V'}{\mathtt{let}\ x = M\ \mathtt{in}\ N \Downarrow V'}$$

- *Prob* defined by "$\divideontimes \Downarrow 1$ or $\divideontimes \Downarrow 0$ with prob. $\frac{1}{2}$"

Decidability?

Escardó's goal [2009] is to show that probabilistic testing is semi-decidable.

Theorem

Probabilistic testing is undecidable.

Proof: by reduction from PFA reachability ([Paz71,CondonLipton89,BlondelCanterini03], see nice proof of undecidability by [GimbertOualhadj, ICALP'09]).

Going Denotational

Definition (Testing Equivalence)

$M, N : \texttt{V Bool}$ are probabilistically equivalent iff
$\int 1 d \llbracket M \rrbracket_1 = \int 1 d \llbracket N \rrbracket_1$.

This is equivalent to previous definition by computational adequacy.
Escardó describes all this elegantly by adding a testing operator $\int$ (integration) into the language.

Escardó's MMP

Let MMP [Escardó09] be PCF+the V monad(+others)+testing operators.

$$
\begin{array}{rcll}
\gamma & ::= & \texttt{Bool} \mid \texttt{Nat} \mid \texttt{I} \mid \ldots & \text{base types } (\llbracket I \rrbracket = [0,1]_\sigma) \\
M, N, P & ::= & x_\tau & \\
& \mid & \lambda x_\sigma \cdot M \mid MN \mid Y^\tau M & \\
& \mid & \texttt{if } M \texttt{ then } N \texttt{ else } P & \\
& \mid & \ldots & \\
& \mid & \circledast & \text{fair coin} \\
& \mid & \texttt{val } M & \text{monadic return} \\
& \mid & \texttt{let } x = M \texttt{ in } N & \text{sequential composition} \\
& \mid & \max \mid \min \mid \underline{\oplus} & \text{average } ((x+y)/2) \\
& \mid & \int MN \quad \text{integration} & (\llbracket \int MN \rrbracket \sim \int_x \llbracket M \rrbracket (x) d \llbracket N \rrbracket)
\end{array}
$$

$M, N : \mathrm{V}\,\texttt{Bool}$ are eqv iff $\left\llbracket \int 1 M \right\rrbracket_1 = \left\llbracket \int 1 N \right\rrbracket_1$

Escardó's Argument

Theorem

Probabilistic (also, may-, must-) testing is semi-decidable.

Proof ideas:

- Escardó [2009] reduces this to the problem of showing

$$[\![\phi(M)]\!]_1 = [\![M]\!]_1 \text{ for } M : \mathtt{I}$$

  where $\phi(M)$ is term that implements $\int$ using $\oplus$ and fixpoints. Target language is real PCF, which is computable (e.g., every implementable boolean question is semi-decidable).

- Manages to do using $[\![\mathbb{V}\ \tau]\!]_1$ as free cone algebra.
  … only works when $[\![\tau]\!]_1$ continuous, i.e., at low orders.

Escardó's Argument

Theorem

Probabilistic (also, may-, must-) testing is semi-decidable.

Proof ideas:

- Escardó [2009] reduces this to the problem of showing

$$[\![\phi(M)]\!]_1 = [\![M]\!]_1 \text{ for } M : \mathtt{I}$$

  where $\phi(M)$ is term that implements $\int$ using $\oplus$ and fixpoints.
  Target language is real PCF, which is computable (e.g., every implementable boolean question is semi-decidable).
- Manages to do using $[\![\mathtt{V}\ \tau]\!]_1$ as free cone algebra.
  ... only works when $[\![\tau]\!]_1$ continuous, i.e., at low orders.
- We know that $[\![\_]\!]_1 = [\![\_]\!]_2$ at ground types. So prove

$$[\![\phi(M)]\!]_2 = [\![M]\!]_2 \text{ for } M : \mathtt{I}$$

- now we are in the cozy category of bc-domains, at all types. □

Related Work

- The troublesome probabilistic powerdomain [JungTix98]
- Indexed valuations [V03] very much related to CRVs.
- Indexed valuations (although not the kind presented here) preserve FS-domains [Mislove07]
- Models of non-deterministic+probabilistic choice [MOW03,TKP05,JGL07]
- Testing of higher-order programs [Escardó09]

Summary

- New monads of prob. choice, through random variables
- A definite plus, compared to the prob. powerdomain **V**: they live in the cozy CCC of bc-domains
- Clarifies notion of indexed valuation (see paper)
- Random variables as good as valuations for semantics (at ground types)
- We solved an problem left open by M. Escardó: prob. (and may-, must-) testing of extended PCF is semi-decidable.

Summary

- New monads of prob. choice, through random variables
- A definite plus, compared to the prob. powerdomain **V**: they live in the cozy CCC of bc-domains
- Clarifies notion of indexed valuation (see paper)
- Random variables as good as valuations for semantics (at ground types)
- We solved an problem left open by M. Escardó: prob. (and may-, must-) testing of extended PCF is semi-decidable.

- We were initially looking for a concrete description of indexed valuations: is there any?
- Combining CRVs with non-determinism: doable? comparison with previsions/convex non-determinism?

Road Map

Outline

3 Appendix
- Equational Theories
- A More Complete Proof of Escardó's Claim

Equational Theory for Non-Determinism

Hoare Powerdomain

The Hoare powerdomain $\mathscr{H}(X)$ is the free algebra for the equational theory

- $x \uplus x = x$
- $x \uplus y = y \uplus x$
- $(x \uplus y) \uplus z = x \uplus (y \uplus z)$
- $x \leq x \uplus y$

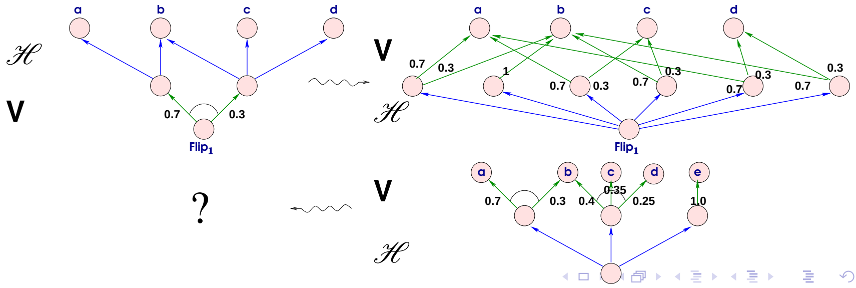
This models angelic non-determinism.
What about languages with both non-determinism and probabilities?

Distributive laws

Theorem (Varacca, PhD Thesis, 2003)

There is no distributive law between the Hoare powerdomain monad $\mathscr{H}$ and the continuous valuation monad $\mathbf{V}$.

- ... and neither $\mathscr{H}\mathbf{V}$ nor $\mathbf{V}\mathscr{H}$ a monad
- the categorical way of saying that probabilistic choice and non-deterministic choice do not commute:



Solutions

- Replace Hoare powerdomain by convex Hoare powerdomain [MOW03, TKP05]: $\mathscr{H}^{cvx}\mathbf{V}$ is a monad

  ...i.e., use randomized, not pure, schedulers to resolve non-determinism

- Use previsions [JGL07]

  ...(roughly) isomorphic to previous [JGL08a]

- Realize $\mathbf{V}$ satisfies too many equations, e.g., $x \oplus_p x = x$.

  $\leadsto$ Keep $\mathscr{H}$, but replace $\mathbf{V}$ by indexed valuations $\mathscr{I}\mathscr{V}$ [V03].

Valuations

Equational Theory for **V**

1. $x \oplus_p y = y \oplus_{1-p} x$
2. $x \oplus_p (y \oplus_q z) = (x \oplus_{\frac{p}{p+q-pq}} y) \oplus_{p+q-pq} z$
3. $x \oplus_1 y = x$, $x \oplus_0 y = y$
4. $x = x \oplus_p x$

with $x \oplus_p y$ continuous in $x, y, p \in [0, 1]$

Layered Hoare Indexed Valuations

Equational Theory for $\mathscr{I}\mathscr{V}$ [This paper, variant]

1. $x \oplus_p y = y \oplus_{1-p} x$
2. $x \oplus_p (y \oplus_q z) = (x \oplus_{\frac{p}{p+q-pq}} y) \oplus_{p+q-pq} z$
3. $x \oplus_1 y = x$, $x \oplus_0 y = y$
4. $x \leq x \oplus_p x$ (Hoare indexed)

with $x \oplus_p y$ continuous in x, y, ~~$p \in [0, 1]$~~ (layered)

Thin Random Variables

Equational Theory for θ**R** [This paper]

1. ~~$x \oplus_p y = y \oplus_{1-p} x$~~
2. ~~$x \oplus_p (y \oplus_q z) = (x \oplus_{\frac{p}{p+q-pq}} y) \oplus_{p+q-pq} z$~~
3. ~~$x \oplus_1 y = x, x \oplus_0 y = y$~~
   $x \oplus_1 y$ independent of y, $x \oplus_0 y$ independent of x
4. $x \leq x \oplus_p x$ (Hoare indexed)

with $x \oplus_p y$ continuous in x, y, ~~$p \in [0, 1]$~~ (layered)

Uniform Random Variables

Equational Theory for $\upsilon\mathbf{R}$ [This paper]

1. ~~$x \oplus_p y = y \oplus_{1-p} x$~~
2. ~~$x \oplus_p (y \oplus_q z) = (x \oplus_{\frac{p}{p+q-pq}} y) \oplus_{p+q-pq} z$~~
3. ~~$x \oplus_1 y = x, x \oplus_0 y = y$~~
   $x \oplus_1 y$ independent of y, $x \oplus_0 y$ independent of x
4. $x \leq x \oplus_p x$

with $x \oplus_p y$ continuous in x, y, ~~$p \in [0, 1]$~~ and $p \in \{0, \frac{1}{2}, 1\}$

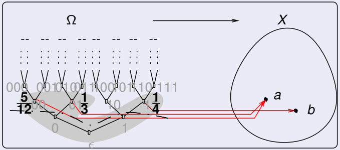
Indexed valuations

Indexed valuations are between valuations and CRVs:

Theorem

There are collapse maps

$$\theta\mathbf{R}(X) \longrightarrow \mathscr{I}\mathscr{V}(X) \longrightarrow \mathbf{V}(X)$$



$$\longmapsto \begin{array}{l}\{(a, \mathrm{prob}\,\frac{5}{12}),\\ (a, \mathrm{prob}\,\frac{1}{3}),\\ (b, \mathrm{prob}\,\frac{1}{4})\}\end{array} \longmapsto \begin{array}{l}\frac{3}{4}\delta_a\\ +\frac{1}{4}\delta_b\end{array}$$

Proof: In each arrow $A \to B$ above, B is a T-algebra and A the free T-algebra for some T.

Note: The composite $q_X : \theta\mathbf{R}(X) \to \mathbf{V}(X)$ maps (ν, f) to the image measure of ν by f (“forgets coin flips”)

Distributive Laws

Theorem

There is a distributive law between $\mathscr{H}$ and $\theta\mathbf{R}$.

Resulting monad obtained by:

- taking unions of equational theories of $\mathscr{H}$, $\theta\mathbf{R}$
- making $\uplus$ and $\oplus_p$ distribute

Outline

3. Appendix
   - Equational Theories
   - A More Complete Proof of Escardó's Claim

Escardó's Argument

Theorem

Probabilistic (also, may-, must-) testing is semi-decidable.

Proof: [Escardó09]

1. Compile MMP to sub-language PCF $+ \mathtt{S} + \mathtt{I}$(=MMP minus $\int$):

$$\phi(\mathtt{V}\tau) \quad = \quad \mathtt{Cantor} \to \phi(\tau) \text{ where } \mathtt{Cantor} = \mathtt{Nat} \to \mathtt{Bool}$$

("infinite sequences of coin flips")

$$\phi(\int MN) \quad = \quad \mathtt{int}(\phi(N) \circ \phi(M))$$

where $\mathtt{int}$ is integration wrt. to uniform prob. on $\mathtt{Cantor}$:

$$\mathtt{int}(h) = \max(h(\bot), \mathtt{int}(\lambda s \cdot h(\text{cons } 1 s)) \underline{\oplus} \mathtt{int}(\lambda s \cdot h(\text{cons } 0 s)))$$

2. Show $[\![\phi(M)]\!]_1 = [\![M]\!]_1$ for $M : \mathtt{I}$ (*)
3. Show comp. adequacy for PCF $+ \mathtt{S} + \mathtt{I}$: $M \Downarrow V$ iff $[\![M]\!]_1 = V$.
4. Since reachability in PCF $+ \mathtt{S} + \mathtt{I}$ semi-decidable, conclude.

ϕ is Correct

So everything boils down to proving

Correctness

$[\![\phi(M)]\!]_1 = [\![M]\!]_1$ for $M : \mathtt{I}$

- Escardó proves this for M at low orders: restrict $\mathtt{V}\ \tau$ so that $[\![\mathtt{V}\ \tau]\!]_1$ is free cone algebra, e.g., $[\![\tau]\!]_1$ continuous

  "The troublesome probabilistic powerdomain"

ϕ is Correct

So everything boils down to proving

Correctness

$[\![\phi(M)]\!]_1 = [\![M]\!]_1$ for $M : \mathtt{I}$

- Escardó proves this for M at low orders: restrict $\mathtt{V}\ \tau$ so that $[\![\mathtt{V}\ \tau]\!]_1$ is free cone algebra, e.g., $[\![\tau]\!]_1$ continuous

  "The troublesome probabilistic powerdomain"
- But remember random variables as good as valuations: $[\![N]\!]_1 = [\![N]\!]_2$ for all $N : \gamma$.
- So boils down to proving $[\![\phi(M)]\!]_2 = [\![M]\!]_2$ for $M : \mathtt{I}\ldots$
- and now we are in the cozy category of bc-domains,

  at all types.

Coin Flips

Therefore:

Theorem (This paper)

Probabilistic (also, may-, must-) testing is semi-decidable.

Proof: (sketch) We must show $[\![\phi(M)]\!]_2 = [\![M]\!]_2$ whenever $M : \gamma$.

- $[\![\phi(\mathrm{V}\tau)]\!]_2$ is a fair-coin algebra, $[\![\mathrm{V}\tau]\!]_2 = \upsilon\mathbf{R}([\![\tau]\!]_2)$ is the free fair-coin algebra
  $\Rightarrow$ unique fair-coin algebra morphism $\psi : [\![\mathrm{V}\tau]\!]_2 \to [\![\phi(\mathrm{V}\tau)]\!]_2$.
- `int` implementes integration correctly:

$$[\![\mathtt{int}]\!]_2\,(k \circ \psi(\nu, f)) = \int_{x \in X} k(x) dq_X(\nu, f)$$

- Define logical relation $R_\tau \subseteq [\![\tau]\!]_2 \times [\![\phi(\tau)]\!]_2$ with $(\nu, f)\ R_{\mathrm{V}\tau}\ \xi$ iff

$$[\![\mathtt{int}]\!]_2\,(k_1 \circ \psi(\nu, f)) = [\![\mathtt{int}]\!]_2\,(k_2 \circ \xi) \text{ whenever } k_1\ R_{\tau \to \mathrm{I}}\ k_2$$

- Since R_γ is equality, conclude.

Comparing Ω and `Cantor`

CRVs and Escardó's translation both flip coins.

	uniform CRVs	ϕ translation
Monad?	Yes	No
Coin flips	$\{1,0\}^{\leq\omega}$	$\{1,0\}_{\perp}^{=\omega}$
Extension (sequential composition)	concatenation 10 110 10110	interleaving 100... 110... 110100...