The Powerdomain of Continuous Random Variables

Jean Goubault-Larrecq, Daniele Varacca

LSV - ENS Cachan, PPS - Paris Diderot

LICS, June 21, 2011
Open Problem:

Does there exist a Cartesian closed category (=interpret $\sigma \rightarrow \tau$) of continuous domains, closed under the probabilistic powerdomain (=interpret $\forall\tau$)?

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

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
Continuous Random Variables

Continuous Valuations

**Classical view** [JonesPlotkin89]: interpret \( \mathcal{V}_\mathcal{T} \) as space of continuous valuations (=measures on a topology).

**Definition (Continuous Valuation)**

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

\[
\begin{align*}
\nu(\emptyset) &= 0 \quad \text{(strictness)} \\
U \subseteq V &\implies \nu(U) \leq \nu(V) \\
\nu(U \cup V) + \nu(U \cap V) &= \nu(U) + \nu(V) \\
\nu(\bigcup_{i \in I} U_i) &= \sup_{i \in I} \nu(U_i)
\end{align*}
\]

We shall also require \( \nu(X) = 1 \) (probability).
A Prominent Example.

For any $x \in X$, the Dirac valuation $\delta_x$ 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

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

\[ \{0, 1\}^{\leq \omega} : \text{the Cantor tree.} \]

\[ \begin{array}{cccccccc}
00 & 01 & 10 & 01 & 10 & 10 & 01 & 11 \\
00 & 01 & 10 & 10 & 11 & 01 & 11 & 11 \\
00 & 01 & 11 & 11 \\
0 & 1 \\
e & 1 \\
\end{array} \]
Examples

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

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

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

\{0, 1\}^{\leq \omega}:

the Cantor tree.

- Basic open sets: \(\uparrow x\) for finite sequence \(x\)

- Evaluating
  \[
  \frac{1}{4} \delta_{00} + \frac{1}{6} \delta_{01} + \frac{1}{3} \delta_{01} + \frac{1}{4} \delta_{11}
  \]
  on \(\uparrow 01\)
Examples

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

${0, 1}^{\leq \omega}$: 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 $\uparrow 010$
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

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

Goubault-Larrecq, Varacca
The Powerdomain of Continuous Random Variables
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

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

Goubault-Larrecq, Varacca

The Powerdomain of Continuous Random Variables
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.

E.g., \( p = 0.2, q = 0.8 \).
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 \(\Lambda\) (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 $\Lambda$ (on the top elts)
Examples

$\{0, 1\}^\omega$: 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 $\Lambda$ (on the top elts)
Examples

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

The support of \(\Lambda\) 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 \(\Lambda\) (on the top elts)
- The support \(\text{supp} \nu\), is the complement of the largest \(U\) such that \(\nu(U) = 0\)
Examples

\(\{0, 1\}^{\leq \omega}: \text{the Cantor tree}\).

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 \(\Lambda\) (on the top elts).

The support \(\text{supp} \nu\), is the complement of the largest \(U\) such that \(\nu(U) = 0\).

\[\frac{1}{4} \delta_{00} + \frac{1}{6} \delta_0 + \frac{1}{3} \delta_{01} + \frac{1}{4} \delta_{11}\]
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

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

- induces a measure on $X$ (the image measure)
- $\Omega$ is the sample space
- $X$ is the space of observations or outcomes
A continuous random variable is a continuous valuation $\nu$ on some space $\Omega$, together with a continuous function $f : \text{supp} \, \nu \to X$.

We will fix $\Omega$ to be the Cantor tree.
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” \( \nu \) is img of \( \nu' \) by \( p_{\text{supp} \nu} \)
- “increase values” \( f \circ p_{\text{supp} \nu} \leq f' \)
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” \( \nu \) is img of \( \nu' \) by \( p_{\text{supp} \nu} \)
- “increase values” \( f \circ p_{\text{supp} \nu} \leq f' \)
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” $\nu$ is img of $\nu'$ by $p_{\text{supp} \nu}$
- “increase values” $f \circ p_{\text{supp} \nu} \leq f'$
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” \( \nu \) is img of \( \nu' \) by \( p_{\text{supp} \, \nu} \)
- “increase values” \( f \circ p_{\text{supp} \, \nu} \leq f' \)

Deadlock states

(Probabilities fixed forever)
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 $\Lambda$ is thin.
Definition (Thin CRV (\(\nu, f\)))

- \(\nu\) is a thin continuous valuation on \(\Omega\)
- \(f\) is a continuous map from \(\text{Max sup} \nu\) to \(X\)

... so \(f\) is defined only on the non-deadlock elements of \(\text{supp } \nu\).

Note to the purist: if \(X\) is a bc-domain (needed later anyway), \(f\) extends canonically to \(\text{supp } \nu\). 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.
Explicitly,

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

"Flip no coin, return $x$ right away"
The Monad of Thin CRVs

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

"concatenate sequences of coin flips"

(sequential composition)

E.g., take $h$

Then:

$h^\dagger$:
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 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 $\theta \mathbb{R}(D)$.*

**Proof** (sketch.)

- Thin CRVs arise as retract from semi-thin CRVs (i.e., $(\nu, f)$ where $\nu$ thin, but $f$ defined on whole of 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 $(\nu, f) \ll (\nu', f')$ iff $\nu$ has finite support, $(\nu, f) \preceq (\nu', f')$ and $f(w) \ll f'(w)$ for every $w$.
  - Least upper bound of $(\nu, f)$ and $(\nu', f')$ if they have an upper bound $(\nu'', f'')$ at all: project $(\nu'', f'')$ onto supp $\nu \cup$ supp $\nu'$.

We can use thin CRVs for semantics!
Continuous Random Variables

Semantics

Valuations Random Variables CCC Theories

Uniform CRVs

Definition (Uniform CRVs)

\( (\nu, f) \) uniform iff thin + \( \nu = \rho_{\text{supp} \nu}(\Lambda) \) (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 \( \nu R(D) \).**

Proof: Sups of uniform CRVs taken in \( \theta R(D) \) 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
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 \( \mathcal{I} \mathcal{V} \) [This paper, variant]

1. \( x \oplus_p y = y \oplus_{1-p} x \)
2. \( x \oplus_p (y \oplus_q z) = (x \oplus_{p \frac{p}{p+q-pq}} y) \oplus_{p+q-pq} z \)
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)
Equational Theory for $\theta R$ [This paper]

1. $x \oplus_p y = y \oplus_{1-p} x$
2. $x \oplus_p (y \oplus_q z) = (x \oplus_{\frac{p}{p+q-pq}} y) \oplus_{\frac{p+q-pq}{p+q-pq}} z$
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 $x$, $y$, $p \in [0,1]$
Equational Theory for $\nu \mathbb{R}$ [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

## 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

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
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

\[ \gamma ::= \text{Bool} \mid \text{Nat} \mid \ldots \quad \text{base types} \]

\[ \sigma, \tau ::= \gamma \]

\[ \quad \sigma \times \tau \quad \text{pairs} \]

\[ \quad \sigma \rightarrow \tau \quad \text{functions} \]

\[ \quad \forall \tau \quad \text{probability distributions} \]

\[ \ldots \]

\[ M, N, P ::= x_\tau \quad \text{all sorts} \]

\[ \quad \lambda x_\sigma \cdot M \quad \text{of constructs} \]

\[ \quad MN \quad \text{from the} \]

\[ \quad \text{if } M \text{ then } N \text{ else } P \quad \text{PCF language,} \]

\[ \quad Y^\tau M \quad \text{or extensions} \]

\[ \ldots \]

\[ \ast \quad \text{fair coin} \]

\[ \quad \text{val } M \quad \text{monadic return} \]

\[ \quad \text{let } x = M \text{ in } N \quad \text{sequential composition} \]
The Valuation Semantics

\[ \llbracket x = M \text{ in } N \rrbracket_1 = \mathcal{U} \mapsto \int x \llbracket N \rrbracket_1(x)(U)d\llbracket M \rrbracket_1 \]

\[ \llbracket \forall \tau \rrbracket_1 = \mathbf{V}(\llbracket \tau \rrbracket_1) \]

\[ \llbracket \_ \_ \_ \rrbracket_1 = \text{the standard valuation-based semantics} \]

\textbf{Definition (\(\llbracket \_ \_ \_ \rrbracket_1\))}

\[ \llbracket \_ \_ \_ \rrbracket_1 = \frac{1}{2} \delta_1 + \frac{1}{2} \delta_0 \]

fair coin

Goubault-Larrecq, Varacca

The Powerdomain of Continuous Random Variables
\[ \llbracket \_ \rrbracket_2 \text{ is the uniform CRV-based semantics} \]

**Definition (\([\_\_\_\_\_\_\_\_\_]_2\))**

\[ \llbracket \forall \tau \rrbracket_2 = \nu R(\llbracket \tau \rrbracket_2) \]

\[ \llbracket \_ \rrbracket_2 = \]

\[ \llbracket \text{val } M \rrbracket_2 = \eta(\llbracket M \rrbracket_2) \]

\[ \llbracket \text{let } x = M \text{ in } N \rrbracket_2 = (x \mapsto \llbracket N \rrbracket_2(x))^\dagger(\llbracket M \rrbracket_2) \]

**Note:** The \(\text{val}\) and \(\text{let}\) cases are as in every monad.

\(\llbracket \tau \rrbracket_2\) (not \(\llbracket \tau \rrbracket_1\)) is a bc-domain for every \(\tau\).
Theorem (Random Variables are as Good as Valuations)

Let $M$ be any closed term of ground type $\gamma$. Then

$$\llbracket M \rrbracket_1 = \llbracket M \rrbracket_2$$

Proof: Define a logical relation $(R_\tau)_{\tau \text{ type}}$, where $R_\tau \subseteq \llbracket \tau \rrbracket_1 \times \llbracket \tau \rrbracket_2$:

$$\mu R_{\nu \tau} (\nu, f) \iff \int_x h_1(x) d\mu = \int_w h_2(f(w)) d\nu \quad \text{whenever} \quad h_1 \overset{R_\tau}{\sim} h_2$$

$$h_1 \overset{R_\tau}{\sim} h_2 \iff h_1(x_1) = h_2(x_2) \quad \text{whenever} \quad x_1 \overset{R_\tau}{=} x_2$$

“$\mu$ is obs. indistinguishable from image measure $\nu \circ f^{-1}$ of $(\nu, f)$”

Prove the Basic Lemma: $\llbracket M \rrbracket_1 R_\tau \llbracket M \rrbracket_2$ for all $M : \tau$.

At ground types, $R_\gamma$ is equality: conclude.
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
Probabilistic Testing

**Definition (Testing Equivalence)**

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

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

\[
\begin{align*}
\therefore \Downarrow 1 & \quad \therefore \Downarrow 0 \\
\therefore \Downarrow 1 & \quad \therefore \Downarrow 0 \\
\Downarrow V & \quad \Downarrow V \\
\Downarrow \text{let } x = M \text{ in } N & \Downarrow V' \\
\Downarrow \text{let } x = M \text{ in } N & \Downarrow V'
\end{align*}
\]

- \( \text{Prob} \) defined by “\( \therefore \Downarrow 1 \text{ or } \therefore \Downarrow 0 \text{ with prob. } \frac{1}{2} \)”
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]).
Continuous Random Variables Semantics

Definition (Testing Equivalence)

\[ M, N : \forall \text{Bool} \text{ are probabilistically equivalent iff} \]
\[ \int 1 d \llbracket M \rrbracket_1 = \int 1 d \llbracket N \rrbracket_1. \]

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

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

\[
\gamma :: \text{Bool | Nat | } I \cdot \ldots \quad \text{base types} \quad ([I] = [0, 1]_\sigma)
\]

\[
M, N, P :: x_t \\
| \quad \lambda x_\sigma \cdot M | MN | Y^\tau M \\
| \quad \text{if } M \text{ then } N \text{ else } P \\
| \quad \ldots
| \quad \ast \quad \text{fair coin}
| \quad \text{val } M \quad \text{monadic return}
| \quad \text{let } x = M \text{ in } N \quad \text{sequential composition}
| \quad \text{max | min | } \oplus \quad \text{average } ((x + y)/2)
| \quad \int MN \quad \text{integration} \quad ([\int MN] \sim \int_x [M](x) d [N])
\]

\[
M, N : \mathbb{V} \text{ Bool} \text{ are eqv iff } \left[ \int 1M \right]_1 = \left[ \int 1N \right]_1
\]
Escardó’s Argument

**Theorem**

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

**Proof ideas:**

- Escardó [2009] reduces this to the problem of showing
  \[ \llbracket \phi(M) \rrbracket_1 = \llbracket M \rrbracket_1 \text{ for } M : I \]
  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 \( \llbracket \sqcup \tau \rrbracket_1 \) as free cone algebra.
  \( \ldots \) only works when \( \llbracket \tau \rrbracket_1 \) 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

  \[
  \llbracket \phi(M) \rrbracket_1 = \llbracket M \rrbracket_1 \quad \text{for } M : I
  \]

  where \( \phi(M) \) is term that implements \( f \) 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 \( \llbracket V \tau \rrbracket_1 \) as free cone algebra.

  \( \ldots \) only works when \( \llbracket \tau \rrbracket_1 \) continuous, i.e., at low orders.

- We know that \( \llbracket _- \rrbracket_1 = \llbracket _- \rrbracket_2 \) at ground types. So prove

  \[
  \llbracket \phi(M) \rrbracket_2 = \llbracket M \rrbracket_2 \quad \text{for } M : I
  \]

- 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 [Escarlé09]
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**.
New monads of prob. choice, through random variables
A definite plus, compared to the prob. powerdomain $\mathbb{V}$: 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

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
Appendix

Equational Theories

A More Complete Proof of Escardó’s Claim
Equational Theory for Non-Determinism

**Hoare Powerdomain**

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

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

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

There is no distributive law between the Hoare powerdomain monad $H$ and the continuous valuation monad $V$.

- ... and neither $H \triangleright V$ nor $V \triangleright H$ a monad
- the categorical way of saying that probabilistic choice and non-deterministic choice do not commute:
Replace Hoare powerdomain by convex Hoare powerdomain [MOW03, TKP05]: $\mathcal{H}^{cvx}V$ is a monad
... i.e., use randomized, not pure, schedulers to resolve non-determinism

Use previsions [JGL07]
... (roughly) isomorphic to previous [JGL08a]

Realize $V$ satisfies too many equations, e.g., $x \oplus_p x = x$.

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

**Equational Theory for** $\mathbb{V}$

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 $x$, $y$, $p \in [0, 1]$
Equational Theory for $\mathcal{I}W$ [This paper, variant]

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

with $x \oplus_p y$ continuous in $x, y, p \in [0, 1]$ (layered)
Equational Theory for $\theta R$ [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)
Appendix

Uniform Random Variables

Equational Theory for $\nu R$ [This paper]

1. $x \oplus_p y = y \oplus_{1-p} x$
2. $x \oplus_p (y \oplus_q z) = (x \oplus_p y) \oplus_{p+q-pq} z$
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 are between valuations and CRVs:

**Theorem**

There are **collapse maps**

\[
\theta \mathcal{R}(X) \rightarrow \mathcal{I} \mathcal{W}(X) \rightarrow \mathcal{V}(X)
\]

**Proof:** In each arrow \( A \rightarrow B \) above, \( B \) is a \( T \)-algebra and \( A \) the free \( T \)-algebra for some \( T \).

**Note:** The composite \( q_X : \theta \mathcal{R}(X) \rightarrow \mathcal{V}(X) \) maps \((\nu, f)\) to the image measure of \( \nu \) by \( f \) (“forgets coin flips”)
Distributive Laws

**Theorem**

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

Resulting monad obtained by:
- taking unions of equational theories of $\mathcal{H}$, $\theta R$
- making $\bigcup$ and $\bigoplus_\rho$ distribute
Appendix

3 Appendix

- Equational Theories
- A More Complete Proof of Escardó’s Claim
Theorem

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

Proof: [Escardó09]

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

\[
\phi(V\tau) = \text{Cantor} \rightarrow \phi(\tau) \quad \text{where} \quad \text{Cantor} = \text{Nat} \rightarrow \text{Bool} \\
(\text{"infinite sequences of coin flips"})
\]

\[
\phi(\int MN) = \text{int}(\phi(N) \circ \phi(M))
\]

where \( \text{int} \) is integration wrt. to uniform prob. on \( \text{Cantor} \):

\[
\text{int}(h) = \max(h(\bot), \text{int}(\lambda s \cdot h(\text{cons 1}s)) \oplus \text{int}(\lambda s \cdot h(\text{cons 0}s)))
\]

2. Show \( [\phi(M)]_1 = [M]_1 \) for \( M : I \) \hspace{1cm} (*)

3. Show comp. adequacy for PCF + S + I: \( M \downarrow V \) iff \( [M]_1 = V \).

4. Since reachability in PCF + S + I semi-decidable, conclude.
So everything boils down to proving

### Correctness

\[ [\phi(M)]_1 = [M]_1 \text{ for } M : \mathbb{I} \]

- Escardó proves this for \( M \) at low orders: restrict \( V \tau \) so that \( [V \tau]_1 \) is free cone algebra, e.g., \( [\tau]_1 \) **continuous**
  
  “The troublesome probabilistic powerdomain”
So everything boils down to proving

**Correctness**

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

- Escardó proves this for \( M \) at low orders: restrict \( V \tau \) so that \([V \tau]_1\) 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 \( M : I \ldots \)
- 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 $M : \gamma$.

- $[[\phi(\forall \tau)]]_2$ is a fair-coin algebra, $[[\forall \tau]]_2 = \nu R([[\tau]]_2)$ is the free fair-coin algebra
  $\Rightarrow$ unique fair-coin algebra morphism $\psi : [[\forall \tau]]_2 \rightarrow [[\phi(\forall \tau)]]_2$.

- $\text{int}$ implements integration correctly:

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

- Define logical relation $R_\tau \subseteq [[\tau]]_2 \times [[\phi(\tau)]]_2$ with $(\nu, f) R_{\forall \tau} \xi$ iff
  $$[[\text{int}]]_2(k_1 \circ \psi(\nu, f)) = [[\text{int}]]_2(k_2 \circ \xi)$$ whenever $k_1 R_\tau \rightarrow_1 k_2$

- Since $R_\gamma$ is equality, conclude.
CRVs and Escardó’s translation both flip coins.

<table>
<thead>
<tr>
<th></th>
<th>uniform CRVs</th>
<th>(\phi) translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monad?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Coin flips</td>
<td>({1, 0} \leq \omega)</td>
<td>({1, 0} \equiv \omega)</td>
</tr>
<tr>
<td>Extension (sequential composition)</td>
<td>concatenation</td>
<td>interleaving</td>
</tr>
<tr>
<td></td>
<td>10 110</td>
<td>100 \ldots 110 \ldots</td>
</tr>
<tr>
<td></td>
<td>10110</td>
<td>110100 \ldots</td>
</tr>
</tbody>
</table>