

Probabilistic Full Abstraction

joint work with **T. Ehrhard** and **M. Pagani**

Christine Tasson

Christine.Tasson@irif.fr

Laboratoire IRIF - Université Paris Diderot

*A denotational semantics for **discrete** probabilistic
higher-order functional computation,
which is **fully abstract***

(based on **quantitative** semantics)

- ① General framework: Domains vs Quantitative semantics
- ② PCoh: Probabilistic Coherent Spaces
- ③ Probabilistic Call by Name
- ④ Probabilistic Call by Push Value

*A denotational semantics for **discrete** probabilistic
higher-order functional computation,
which is **fully abstract***

(based on **quantitative** semantics)

- ① **General framework: Domains vs Quantitative semantics**
- ② PCoh: Probabilistic Coherent Spaces
- ③ Probabilistic Call by Name
- ④ Probabilistic Call by Push Value

General Framework	Domains Semantics	Quantitative Semantics
Types	Continuous dcpos $(X, \leq)$	Proba. spaces $(X , P(X) \subseteq (\mathbb{R}^+)^{ X })$
Programs	Scott Continuous	Analytic Functions
Probability	Proba. monad	Values as proba. distr.

Bibliography

1976 Plotkin
 1981 Kozen
 1989 Plotkin and Jones
 1998 Jung and Tix
 2013 Goubault Larrecq and Varraca
 2013 Mislove

Bibliography

1988 Girard
 1994 Blute, Panangaden and Seely
 2002 Hasegawa
 2004 Girard
 2011 Danos and Ehrhard
 2014 Ehrhard, Pagani, T.
 2016 Ehrhard, T.

General Framework	Domains Semantics	Quantitative Semantics
Types	Continuous dcpos $(X, \leq)$	Proba. spaces $(X , P(X) \subseteq (\mathbb{R}^+)^{ X })$
Programs	Scott Continuous	Analytic Functions
Probability	Proba. monad	Values as proba. distr.

How to interpret a program $M : \text{nat} \Rightarrow \text{nat}$

Type:

$\mathbb{N}_\perp$ flat domain,
 $\mathcal{V}(\mathbb{N}_\perp)$ proba. distr. over $\mathbb{N}_\perp$,

Prog: $\llbracket M \rrbracket : \mathbb{N}_\perp \rightarrow \mathcal{V}(\mathbb{N}_\perp)$,
 $\llbracket \text{let } n=x \text{ in } M \rrbracket : \mathcal{V}(\mathbb{N}_\perp) \rightarrow \mathcal{V}(\mathbb{N}_\perp)$

$$x \mapsto \left(\sum_n \llbracket M \rrbracket_{n,q} x_n \right)_q$$

Type:

$|\text{Nat}| = \mathbb{N}$
 $P(\text{Nat})$ subproba. dist. over $\mathbb{N}$

Prog: $\llbracket M \rrbracket : P(\text{Nat}) \rightarrow P(\text{Nat})$

$$x \mapsto \left(\sum_{\mu=[n_1, \dots, n_k]} \llbracket M \rrbracket_{\mu,q} \prod_{i=1}^k x_{n_i} \right)_q$$

General Framework	Domains Semantics	Quantitative Semantics
Types	Continuous dpos $(X, \leq)$	Proba. spaces $(X , P(X) \subseteq (\mathbb{R}^+)^{ X })$
Programs	Scott Continuous	Analytic Functions
Probability	Proba. monad	Values as proba. distr.

Problematic in **domain**

Finding a full subcategory of continuous dpos that is:
Cartesian Closed and **closed** under the proba. monad $\mathcal{V}$.

Full Abs.: **PCOH/pPCF**

Prob $(C[M], \underline{n})$

$\forall n, \forall C[]$
 $\underline{\quad}$

Prob $(C[N], \underline{n})$

iff

$\llbracket M \rrbracket = \llbracket N \rrbracket$.

*A denotational semantics to **discrete** probabilistic
higher-order functional computation,
which is **fully abstract***

(based on **quantitative** semantics)

- ① General framework: Domains vs Quantitative semantics
- ② **PCoh: Probabilistic Coherent Spaces**
- ③ Probabilistic Call by Name
- ④ Probabilistic Call by Push Value

Types as **Probabilistic Coherent Spaces**: $(|X|, P(X))$

Proba. Space

$|X|$: the **web**, a (potentially infinite) set of final states

$P(X)$: a set of vectors $\subseteq (\mathbb{R}^+)^{|X|}$ such that

closure: $P(X)^{\perp\perp} = P(X)$ with

$$\forall u, v \in (\mathbb{R}^+)^{|X|}, \langle u, v \rangle = \sum_{a \in |X|} u_a v_a$$

$$\forall P \subseteq (\mathbb{R}^+)^{|X|}, P^\perp = \{v \in (\mathbb{R}^+)^{|X|} ; \forall u \in P, \langle u, v \rangle \leq 1\}$$

bounded covering: $\forall a \in |X|,$

$$\exists v \in P(X) ; v_a \neq 0 \quad \text{and} \quad \exists p > 0, ; \forall v \in P(X), v_a \leq p.$$

Proposition: Proba. spaces as Domains

$(|X|, P(X))$ is a **Proba. space** iff $P(X)$ is bounded covering,
Scott Closed (downwards-closed and dcpo) and **Convex**.

Types as **Probabilistic Coherent Spaces**: $(|X|, P(X))$

Example:

$$P(X) \subseteq (\mathbb{R}^+)^{|X|}$$

$$|1| = \{*\}$$

$$P(1) = [0, 1]$$

$$|\mathbf{Bool}| = \{t, f\}$$

$$P(\mathbf{Bool}) = \{(x_t, x_f) ; x_t + x_f \leq 1\}$$

$$|\mathbf{Nat}| = \{0, 1, 2, \dots\}$$

$$P(\mathbf{Nat}) = \{x \in [0, 1]^{\mathbb{N}} ; \sum_n x_n \leq 1\}$$

$$|\mathbf{Bool} \Rightarrow 1| = \{[t^n, f^m] ; n, m \in \mathbb{N}\},$$

$$P(\mathbf{Bool} \Rightarrow 1) = \{Q \in (\mathbb{R}^+)^{|\mathbf{Bool} \Rightarrow 1|} ;$$

$$\forall x_t + x_f \leq 1, \sum_{n,m=0}^{\infty} Q_{[t^n, f^m]} x_t^n x_f^m \leq 1\}$$

Proposition: Proba. spaces as Domains

$(|X|, P(X))$ is a **Proba. space** iff $P(X)$ is bounded covering,
Scott Closed (downwards-closed and dcpo) and **Convex**.

Pcoh : Linear Category

Objects: Proba. Spaces

Morphisms: Linear Functions

Call by Name

$$A \Rightarrow B = !A \multimap B$$

Pcoh_!: Kleisli Category

Objects: Proba. Spaces

Morphisms: Analytic Functions

- **Smcc** ($1, \otimes, \multimap$)
- biproduct
- **Comonad** ($!, \text{der}, \text{dig}$)
- **Sym. Comonoid** ($!A, 1, \otimes$)
- **CCC**
- (PCF+coin)

Pcoh(X, Y)

Matrices $Q \in (\mathbb{R}^+)^{|X| \times |Y|}$ such that:

$$\forall x \in P(X), Q \cdot x = \left(\sum_{a \in |X|} Q_{a,b} x_a \right)_b \in P(Y)$$

Example

Pcoh(Nat, Nat): Stochastic Matrices $Q \in (\mathbb{R}^+)^{\mathbb{N} \times \mathbb{N}}$.

$$\forall x \in (\mathbb{R}^+)^{\mathbb{N}}; \sum_{n \in \mathbb{N}} x_n \leq 1, \sum_{m, n \in \mathbb{N}} Q_{m,n} x_n \leq 1$$

Free Symmetric Comonoid and Comonad

Exponential

$!X = \mathcal{M}_{\text{fin}}(|X|)$ the set of finite multisets

$$P(!X) = \{x^! ; x \in P(X)\}^{\perp\perp} \text{ where } x^!_{[a_1, \dots, a_n]} = \prod_{i=1}^n x_{a_i}$$

Example

Let $\text{coin}(p) = (p, 1 - p) \in P(\mathbf{Bool}) = \{(p, q) ; p + q \leq 1\}$.

$$\text{coin}(p)^!_{[]} = 1, \quad \text{coin}(p)^!_{[t,t]} = p^2, \quad \text{coin}(p)^!_{[t,f]} = p(1-p), \dots$$

Theorem (2017: Crubillé - Ehrhard - Pagani - T.)

This exponential computes the free symmetric comonoid.

Free Symmetric Comonoid and Comonad

Exponential

$!X = \mathcal{M}_{\text{fin}}(|X|)$ the set of finite multisets

$$P(!X) = \{x^! ; x \in P(X)\}^{\perp\perp} \text{ where } x^!_{[a_1, \dots, a_n]} = \prod_{i=1}^n x_{a_i}$$

Symmetric Comonoid

$$\begin{aligned} \text{Cocontr.} : !X &\xrightarrow{c^{!X}} !X \otimes !X \\ \text{Cowek.} : !X &\xrightarrow{w^{!X}} \mathbf{1} \end{aligned}$$

Comonad

$$\begin{aligned} \text{Comult.} : \text{dig}_{!X} : !!X &\rightarrow !X \\ \text{Counit} : \text{der}_{!X} : !X &\rightarrow X \end{aligned}$$

Theorem (2017: Crubillé - Ehrhard - Pagani - T.)

This exponential computes the free symmetric comonoid.

$$\mathbf{Pcoh}_!(X, Y) = \mathbf{Pcoh}(!X, Y)$$

Matrices $Q \in (\mathbb{R}^+)^{\mathcal{M}_{\text{fin}}(|X|) \times |Y|}$ such that

$$\forall U \in P(!X), Q \cdot U = \left(\sum_{m \in \mathcal{M}_{\text{fin}}(|X|)} Q_{m,b} U_m \right)_b \in P(Y)$$

Non-Linear Morphisms are **analytic** and **Scott Continuous**.

$$\mathbf{Pcoh}_!(\mathbf{Bool}, 1) = \{Q \in (\mathbb{R}^+)^{|\mathbf{Bool} \Rightarrow 1|} \text{ s.t. } Q_{[t^n, f^m]} \leq \frac{(n+m)^{n+m}}{n^n m^m}\}$$

```
let rec f x =
  if x then if x then f x
            else ()
        else if x then ()
            else f x
```

denotes

$$\sum_{n,m=0}^{\infty} \frac{(n+m)!}{n! m!} x_t^{2n+1} x_f^{2m+1}$$

$$\mathbf{Pcoh}_!(X, Y) = \mathbf{Pcoh}(!X, Y)$$

Density

Matrices $Q \in (\mathbb{R}^+)^{\mathcal{M}_{\text{fin}}(|X|) \times |Y|}$ such that if $x_m^! = \prod_{a \in m} x_a^{m(a)}$

$$\forall x \in P(X), Q(x) = \left(\sum_{m \in \mathcal{M}_{\text{fin}}(|X|)} Q_{m,b} x_m^! \right)_b \in P(Y)$$

Non-Linear Morphisms are **analytic** and **Scott Continuous**.

$$\mathbf{Pcoh}_!(\mathbf{Bool}, 1) = \{Q \in (\mathbb{R}^+)^{|\mathbf{Bool} \Rightarrow 1|} \text{ s.t. } Q_{[t^n, f^m]} \leq \frac{(n+m)^{n+m}}{n^n m^m}\}$$

```
let rec f x =
  if x then if x then f x
            else ()
        else if x then ()
            else f x
```

denotes

$$\sum_{n,m=0}^{\infty} \frac{(n+m)!}{n! m!} x_t^{2n+1} x_f^{2m+1}$$

$$\mathbf{Pcoh}_!(X, Y) = \mathbf{Pcoh}(!X, Y)$$

Density

Matrices $Q \in (\mathbb{R}^+)^{\mathcal{M}_{\text{fin}}(|X|) \times |Y|}$ such that if $x_m^! = \prod_{a \in m} x_a^{m(a)}$

$$\forall x \in P(X), Q(x) = \left(\sum_{m \in \mathcal{M}_{\text{fin}}(|X|)} Q_{m,b} x_m^! \right)_b \in P(Y)$$

Non-Linear Morphisms are **analytic** and **Scott Continuous**.

$$\mathbf{Pcoh}_!(\mathbf{Bool}, 1) = \{Q \in (\mathbb{R}^+)^{|\mathbf{Bool} \Rightarrow 1|} \text{ s.t. } Q_{[t^n, f^m]} \leq \frac{(n+m)^{n+m}}{n^n m^m}\}$$

```
let rec f x =
  if x then if x then f x
            else ()
  else if x then ()
         else f x
```

pb of DEFINABILITY

$$\sum_{n,m=0}^{\infty} \frac{(n+m)!}{n! m!} x_t^{2n+1} x_f^{2m+1}$$

*A denotational semantics to **discrete** probabilistic
higher-order functional computation,
which is **fully abstract***

(based on **quantitative** semantics)

- ① General framework: Domains vs Quantitative semantics
- ② PCoh: Probabilistic Coherent Spaces
- ③ **Probabilistic Call by Name**
- ④ Probabilistic Call by Push Value

Theorem (2014: Ehrhard - Pagani - T.)

Pcoh

$$\llbracket M \rrbracket = \llbracket N \rrbracket$$

Adequacy



Full Abstraction

pPCF

$$M \simeq_o N$$

$$\text{Prob}(C[M] \xrightarrow{*} n) \stackrel{\forall C[\cdot] \forall n}{=} \text{Prob}(C[N] \xrightarrow{*} n)$$

Adequacy Lemma (2011: Danos - Ehrhard):

If $\vdash M : \text{nat}$, then $\forall n \in \mathbb{N}, \llbracket M \rrbracket_n = \mathbf{Prob}(M \rightarrow^* n)$.

Key Ingredients of Full Abstraction

- Find **testing terms** that depend only on points of the web.
- Use regularity of **analytic functions**.

How to encode a LasVegas Algorithm?

Input: A 0/1 array of length $n \geq 2$ s.t. $\frac{1}{2}$ cells are 0.

0	1	2	3	4	5
<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>1</u>	<u>0</u>

$f : 0, 2, 5 \mapsto \underline{0}$

$1, 3, 4 \mapsto \underline{1}$

Output: Find the index of a cell containing 0.

Caml:

```
let rec LasVegas (f: nat -> nat) (n:nat) =  
  let k = random n in  
  if (f k = 0) then k  
  else LasVegas f n
```

**pPCF:
CBN**

```
fix (λLasVegas(nat⇒nat)⇒nat⇒nat λfnat⇒nat λnnat  
    (λknat if (f k = 0) then k  
    else LasVegas f n) (rand n)
```

How to encode a LasVegas Algorithm?

Input: A $\underline{0}/\underline{1}$ array of length $n \geq 2$ s.t. $\frac{1}{2}$ cells are $\underline{0}$.

0	1	2	3	4	5
<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>1</u>	<u>0</u>

$f : 0, 2, 5 \mapsto \underline{0}$

$1, 3, 4 \mapsto \underline{1}$

Output: Find the index of a cell containing $\underline{0}$.

Caml:
let in
CBV

```
let rec LasVegas (f: nat -> nat) (n:nat) =  
  let k = random n in  
  if (f k = 0) then k  
  else LasVegas f n
```

pPCF:
CBN

```
fix (λLasVegas(nat⇒nat)⇒nat⇒nat λfnat⇒nat λnnat  
  (λknat if (f k = 0) then k  
    else LasVegas f n) (rand n)
```

Storage Operator

```
let k = rand n in if k = 0 then k else 42
```

Integer in Pcoh: $\llbracket \text{nat} \rrbracket = \mathbf{Nat} = (\mathbb{N}, P(\mathbf{Nat}) = \{(\lambda_n) \mid \sum_n \lambda_n \leq 1\})$

Equipped with a coalgebraic structure in the *linear* Pcoh:

- Cocontraction: $c^{\text{nat}} : \text{nat} \rightarrow \text{nat} \otimes \text{nat}$
- Coweakening: $w^{\text{nat}} : \text{nat} \rightarrow \mathbf{1}$

Bibliography

- 1990 Krivine, Opérateurs de mise en mémoire et Traduction.
- 1999 Levy, Call by Push Value, a subsuming paradigm.
- 2000 Nour, On Storage operator.
- 2016 Curien, Fiore, Munch-Maccagnoni, A Theory of Effects and Resources .

What sem. object to encode Storage Operator.

The Eilenberg Moore Category: **Pcoh**[!]

Coalgebras $P = (\underline{P}, h_P)$ with $\underline{P} \in \mathbf{Pcoh}$ and $h_P \in \mathbf{Pcoh}(\underline{P}, !\underline{P})$:

$$\begin{array}{ccc} \underline{P} & \xrightarrow{h_P} & !\underline{P} \\ & \searrow \text{Id} & \downarrow \text{der}_{\underline{P}} \\ & & \underline{P} \end{array}$$

$$\begin{array}{ccc} \underline{P} & \xrightarrow{h_P} & !\underline{P} \\ h_P \downarrow & & \downarrow \text{dig}_{\underline{P}} \\ !\underline{P} & \xrightarrow{!h_P} & !!\underline{P} \end{array}$$

Coalgebras have a comonoid structure: values can be **stored**.

Types interpreted as coalgebras:

$!X$ by def. of the exp. | $\otimes, \oplus$ and fix preserve coalgebras.

Example

Stream: $S_\phi = \phi \otimes !S_\phi$ | **List:** $\lambda_0 = \mathbf{1} \oplus (\phi \otimes \lambda_0)$

*A denotational semantics to **discrete** probabilistic
higher-order functional computation,
which is **fully abstract***

(based on **quantitative** semantics)

- ① General framework: Domains vs Quantitative semantics
- ② PCoh: Probabilistic Coherent Spaces
- ③ Probabilistic Call by Name
- ④ **Probabilistic Call by Push Value**

Probabilistic Call By Push Value

Types:

(positive) $\phi, \psi, \dots := \mathbf{1} \mid !\sigma \mid \phi \otimes \psi \mid \phi \oplus \psi \mid \alpha \mid \text{Fix } \alpha \cdot \phi$

(general) $\sigma, \tau \dots := \phi \mid \phi \multimap \sigma$

Values: (positive type)

$V, W \dots := x \mid () \mid M^! \mid (V, W) \mid \text{in}_1 V \mid \text{in}_2 V \mid \text{fold}(V).$

Programs: (general type)

$M, N \dots := x \mid () \mid M^! \mid \text{der}(M) \mid \lambda x^\phi M \mid \langle M \rangle N \mid \text{fix } x^{! \sigma} M$
 $\mid \text{in}_1 M \mid \text{in}_2 M \mid \text{case}(M, x_1 \cdot N_1, x_2 \cdot N_2)$
 $\mid (M, N) \mid \text{pr}_1 M \mid \text{pr}_2 M \mid \text{fold}(M) \mid \text{unfold}(M)$
 $\mid \text{coin}(p), p \in [0, 1] \cap \mathbb{Q}$

Typing context: $\mathcal{P} = (x_1 : \phi_1, \dots, x_k : \phi_k)$

Probabilistic Call By Push Value

Types:

$$\sigma \Rightarrow \tau = !\sigma \multimap \tau$$

(positive) $\phi, \psi, \dots := \mathbf{1} \mid !\sigma \mid \phi \otimes \psi \mid \phi \oplus \psi \mid \alpha \mid \text{Fix } \alpha \cdot \phi$

(general) $\sigma, \tau \dots := \phi \mid \phi \multimap \sigma$

Values:

$V, W \dots := x \mid () \mid M^! \mid (V, W) \mid \text{in}_1 V \mid \text{in}_2 V \mid \text{fold}(V).$

Programs: $\lambda x^\sigma M = \lambda x^{!\sigma} M$ and $(M)N = \langle M \rangle N^!$

$M, N \dots := x \mid () \mid M^! \mid \text{der}(M) \mid \lambda x^\phi M \mid \langle M \rangle N \mid \text{fix } x^{!\sigma} M$
 $\mid \text{in}_1 M \mid \text{in}_2 M \mid \text{case}(M, x_1 \cdot N_1, x_2 \cdot N_2)$
 $\mid (M, N) \mid \text{pr}_1 M \mid \text{pr}_2 M \mid \text{fold}(M) \mid \text{unfold}(M)$
 $\mid \text{coin}(p), p \in [0, 1] \cap \mathbb{Q}$

Typing context: $\mathcal{P} = (x_1 : \phi_1, \dots, x_k : \phi_k)$

Probabilistic Call By Push Value

Types: $\text{nat} = \text{Fix } \alpha \cdot \mathbf{1} \oplus \alpha$ and $\sigma \Rightarrow \tau = !\sigma \multimap \tau$

(positive) $\phi, \psi, \dots := \mathbf{1} \mid !\sigma \mid \phi \otimes \psi \mid \phi \oplus \psi \mid \alpha \mid \text{Fix } \alpha \cdot \phi$

(general) $\sigma, \tau \dots := \phi \mid \phi \multimap \sigma$

Values: $\underline{0} = \text{in}_1()$ and $\underline{n+1} = \text{in}_2 n$

$V, W \dots := x \mid () \mid M^! \mid (V, W) \mid \text{in}_1 V \mid \text{in}_2 V \mid \text{fold}(V).$

Programs: $\text{succ}(M) = \text{in}_2 M$

$M, N \dots := x \mid () \mid M^! \mid \text{der}(M) \mid \lambda x^\phi M \mid \langle M \rangle N \mid \text{fix } x^{! \sigma} M$
 $\mid \text{in}_1 M \mid \text{in}_2 M \mid \text{case}(M, x_1 \cdot N_1, x_2 \cdot N_2)$
 $\mid (M, N) \mid \text{pr}_1 M \mid \text{pr}_2 M \mid \text{fold}(M) \mid \text{unfold}(M)$
 $\mid \text{coin}(p), p \in [0, 1] \cap \mathbb{Q}$

Typing context: $\mathcal{P} = (x_1 : \phi_1, \dots, x_k : \phi_k)$

Probabilistic Call By Push Value

Types: $\text{nat} = \text{Fix } \alpha \cdot \mathbf{1} \oplus \alpha$ and $\sigma \Rightarrow \tau = !\sigma \multimap \tau$

(positive) $\phi, \psi, \dots := \mathbf{1} \mid !\sigma \mid \phi \otimes \psi \mid \phi \oplus \psi \mid \alpha \mid \text{Fix } \alpha \cdot \phi$

(general) $\sigma, \tau \dots := \phi \mid \phi \multimap \sigma$

Values: $\underline{0} = \text{in}_1()$ and $\underline{n+1} = \text{in}_2 n$

$V, W \dots := x \mid () \mid M^! \mid (V, W) \mid \text{in}_1 V \mid \text{in}_2 V \mid \text{fold}(V).$

Programs: $\text{let } x = M \text{ in } N = \text{case}(M, y \cdot N[\underline{0}/x], z \cdot N[\text{succ}(z)/x])$

$M, N \dots := x \mid () \mid M^! \mid \text{der}(M) \mid \lambda x^\phi M \mid \langle M \rangle N \mid \text{fix } x^{! \sigma} M$
 $\mid \text{in}_1 M \mid \text{in}_2 M \mid \text{case}(M, x_1 \cdot N_1, x_2 \cdot N_2)$
 $\mid (M, N) \mid \text{pr}_1 M \mid \text{pr}_2 M \mid \text{fold}(M) \mid \text{unfold}(M)$
 $\mid \text{coin}(p), p \in [0, 1] \cap \mathbb{Q}$

Typing context: $\mathcal{P} = (x_1 : \phi_1, \dots, x_k : \phi_k)$

Some glimpse of **pCBPV** operational semantics.

Weak Reduction for Values.

$$\frac{}{\text{der}(M^!) \xrightarrow{w} M} \quad \frac{}{\langle \lambda x^\phi M \rangle V \xrightarrow{w} M[V/x]}$$

$$\frac{}{\text{case}(\text{in}_i V, x_1 \cdot M_1, x_2 \cdot M_2) \xrightarrow{w} M_i[V/x_i]}$$

Probabilistic Reduction.

$$\frac{M \xrightarrow{w} M'}{M \xrightarrow{1} M'} \quad \frac{}{\text{coin}(p) \xrightarrow{p} \underline{0} = \text{in}_1()} \quad \frac{}{\text{coin}(p) \xrightarrow{1-p} \underline{1} = \text{in}_2(\text{in}_1())}$$

$$\frac{M \xrightarrow{p} M'}{\text{der}(M) \xrightarrow{p} \text{der}(M')} \quad \frac{M \xrightarrow{p} M'}{\langle M \rangle V \xrightarrow{p} \langle M' \rangle V} \quad \frac{N \xrightarrow{p} N'}{\langle M \rangle N \xrightarrow{p} \langle M \rangle N'}$$

$$\frac{M \xrightarrow{p} M'}{\text{case}(M, x_1 \cdot M_1, x_2 \cdot M_2) \xrightarrow{p} \text{case}(M', x_1 \cdot M_1, x_2 \cdot M_2)}$$

Some glimpse of **pCBPV** operational semantics.

Weak Reduction for Values.

$$\frac{}{\text{der}(M^!) \xrightarrow{w} M} \quad \frac{}{\langle \lambda x^\phi M \rangle V \xrightarrow{w} M[V/x]}$$

$$\frac{}{\text{case}(\text{in}_i V, x_1 \cdot M_1, x_2 \cdot M_2) \xrightarrow{w} M_i[V/x_i]}$$

Probabilistic Reduction.

$$\frac{M \xrightarrow{w} M'}{M \xrightarrow{1} M'} \quad \frac{}{\text{coin}(p) \xrightarrow{p} \underline{0} = \text{in}_1()} \quad \frac{}{\text{coin}(p) \xrightarrow{1-p} \underline{1} = \text{in}_2(\text{in}_1())}$$

$$\frac{M \xrightarrow{p} M'}{\text{der}(M) \xrightarrow{p} \text{der}(M')} \quad \frac{M \xrightarrow{p} M'}{\langle M \rangle V \xrightarrow{p} \langle M' \rangle V} \quad \frac{N \xrightarrow{p} N'}{\langle M \rangle N \xrightarrow{p} \langle M \rangle N'}$$

$$\frac{M \xrightarrow{p} M'}{\text{case}(M, x_1 \cdot M_1, x_2 \cdot M_2) \xrightarrow{p} \text{case}(M', x_1 \cdot M_1, x_2 \cdot M_2)}$$

Some glimpse of **pCBPV** operational semantics.

Weak Reduction for Values.

$$\frac{}{\text{der}(M^!) \xrightarrow{w} M} \quad \frac{}{\langle \lambda x^\phi M \rangle V \xrightarrow{w} M[V/x]}$$
$$\frac{}{\text{case}(\text{in}_i V, x_1 \cdot M_1, x_2 \cdot M_2) \xrightarrow{w} M_i[V/x_i]}$$

Probabilistic Reduction.

$$\frac{M \xrightarrow{w} M'}{M \xrightarrow{1} M'} \quad \frac{}{\text{coin}(p) \xrightarrow{p} \underline{0} = \text{in}_1()} \quad \frac{}{\text{coin}(p) \xrightarrow{1-p} \underline{1} = \text{in}_2(\text{in}_1())}$$
$$\frac{M \xrightarrow{p} M'}{\text{der}(M) \xrightarrow{p} \text{der}(M')} \quad \frac{M \xrightarrow{p} M'}{\langle M \rangle V \xrightarrow{p} \langle M' \rangle V} \quad \frac{N \xrightarrow{p} N'}{\langle M \rangle N \xrightarrow{p} \langle M \rangle N'}$$
$$\frac{M \xrightarrow{p} M'}{\text{case}(M, x_1 \cdot M_1, x_2 \cdot M_2) \xrightarrow{p} \text{case}(M', x_1 \cdot M_1, x_2 \cdot M_2)}$$

Theorem (2016: Ehrhard - T.)

PCoh

$$\llbracket M \rrbracket = \llbracket N \rrbracket$$

Adequacy



Full Abstraction

pCBPV

$$P \simeq_o Q$$

$$\text{Prob}(C[M], ()) \stackrel{\forall C[]}{=} \text{Prob}(C[N], ())$$

Key Ingredients of Adequacy:

- Handle **values** separately
- Logical relations: **fixpoint** of types (hidden step indexing, biorthogonality closure, fixpoints of pairs of logical relations)
- **Density**: Morphisms on positive types are characterized by their action on coalgebraic points.

Key Ingredients of Full Abstraction:

- Find **testing terms** that depend only on points of the web.
- Use regularity of **analytic functions** and **density**

pCBPV a funct. lang. suitable for writing proba. programs

- Combines CBN and CBV
- Values are of positive Types, they can be duplicated or erased accordingly to the comonoidal structure of their interpretation
- Programs can handle base types such as streams
- Full abstraction (with no quotient needed)

Further directions:

- Combine Non-determinism and Probability by constructing a non-deterministic monad on **Pcoh**_I.
- Move up from discrete to continuous probability.