GDR IM 2015 - LABRI - Bordeaux
2-3 February

Probabilistic Coherent Spaces vs Probabilistic PCF an accurate Semantics.

joint work with **Thomas Ehrhard** and **Michele Pagani**

Christine Tasson
Christine.Tasson@pps.univ-paris-diderot.fr

Laboratoire PPS - Université Paris Diderot

An example of Randomized Algorithm

- Formalize its syntax.
- Reason on its semantics.

A Full Abstraction Result in a Probabilistic Setting

- Semantics : PCoh, Probabilistic Coherent Spaces [Girard04,Danos-Ehrhard11]
- Syntax : PPCF, a Probabilistic extension of PCF [Plotkin77]

Full Abstraction :

A Bridge between Syntax and Semantics.

« *Decide what you want to say before you worry how you are going to say it.* » **The Scott-Strachey Approach to Programming Language Theory, preface, Scott (77)**

Denotational semantics :

a program as a function between mathematical spaces

Operational semantics :

a program as a sequence of computation steps

« *Full Abstraction studies connections between denotational and operational semantics.* » **LCF Considered as a Programming Language, Plotkin (77)**

Operational semantics :

Proba$(P \to^* v)$ is the probability that P computes v.

Denotational semantics :

Programs seen as **distribution transformers** which are **very regular**, so that

Probabilistic Full Abstraction :

$$[\![P]\!] = [\![Q]\!] \quad \underset{\text{Full Completeness}}{\overset{\text{Adequacy}}{\Longleftrightarrow}} \quad P \simeq_o Q$$

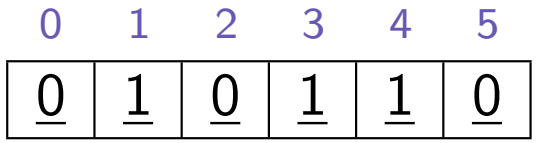
$$\forall C[\,],\ \text{Proba}(C[P] \to^* v) = \text{Proba}(C[Q] \to^* v)$$

Randomized algorithm :

A Las Vegas example.

An example of Randomized algorithm

Input : A $\underline{0}/\underline{1}$ array of length $n \geq 2$ in which half cells are $\underline{0}$.



$f : 0, 2, 5 \mapsto \underline{0}, \quad 1, 3, 4 \mapsto \underline{1}$

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

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

This algorithm succeeds with probability one.

- Success in 1 step is : $\frac{1}{2}$.
- Success in 2 steps is : $\frac{1}{2^2}$.
- Success in n steps is : $\frac{1}{2^n}$.

Success in any steps is :

$$\sum_{k=1}^{\infty} \frac{1}{2^k} = 1.$$

Modeling Probabilistic Data and Programs :

Type : set of positive vectors

set of probability distributions

Program : weighted relation, a positive matrix

distribution transformer

Interaction : composition seen as multiplication

Example : `nat`

`Coin: nat` returns the toss of a fair coin.

`Unif n: nat` returns uniformly any $\{0, \ldots, n\}$.

Non Determinism, a first approximation : $|\texttt{nat}| = \mathbb{N}$.

$$|\texttt{Coin}| = \{0, 1\} \qquad \text{and} \qquad |\texttt{Unif n}| = \{0, \ldots, n\}$$

Enriching with positive coefficients : $[\![\texttt{nat}]\!] \subseteq (\mathbb{R}^+)^{\mathbb{N}}$.

$$[\![\texttt{Coin}]\!] = \underset{\substack{\downarrow \\ 0}}{\tfrac{1}{2}}, \underset{\substack{\downarrow \\ 1}}{\tfrac{1}{2}}, \underset{\substack{\downarrow \\ 2}}{0}, \ldots) \quad \text{and} \quad [\![\texttt{Unif n}]\!] = \left(\underset{\substack{\downarrow \\ 0}}{\tfrac{1}{n+1}}, \ldots, \underset{\substack{\downarrow \\ n}}{\tfrac{1}{n+1}}, 0, \ldots\right)$$

Subprobability Distributions over $\mathbb{N}$:

$$[\![\texttt{nat}]\!] = \left\{ (\lambda_n)_{n \in \mathbb{N}} \mid \forall n, \lambda_n \in \mathbb{R}^+ \text{ and } \sum_n \lambda_n \leq 1 \right\}$$

Example : $\mathtt{Unif} : \mathtt{nat} \to \mathtt{nat}$

Input : an integer n

Output : any integer $\{0, \ldots, n\}$ uniformly chosen.

Non Determinism : $|\mathtt{Unif}| \subseteq |\mathtt{nat}| \times |\mathtt{nat}|$ is a relation.

$$|\mathtt{Unif}| = \{(n, k) \mid n \in \mathbb{N},\ k \in \{0, \ldots, n\}\}$$

Enriching with positive coefficients : $[\![\mathtt{Unif}]\!] \in (\mathbb{R}^+)^{(\mathbb{N}\times\mathbb{N})}$.

$$\begin{array}{c} \begin{array}{ccccc} \scriptstyle 0 \downarrow & \scriptstyle 1 \downarrow & \cdots & \scriptstyle n \downarrow & \cdots \end{array} \\ \begin{pmatrix} 1 & \frac{1}{2} & \cdots & \frac{1}{n+1} & \cdots \\ 0 & \frac{1}{2} & \cdots & \frac{1}{n+1} & \cdots \\ \vdots & 0 & \ddots & \vdots & \\ & \vdots & 0 & \frac{1}{n+1} & \\ & & \vdots & \ddots & \ddots \end{pmatrix} \end{array} \begin{array}{l} \\ \to 0 \\ \to 1 \\ \vdots \\ \to n \\ \vdots \end{array}$$

`Once : nat → nat`

Input : an integer `n`

Output : `if n=0 then 42 else Coin`

$$\begin{array}{c} \begin{array}{cccc} \downarrow 0 & \downarrow 1 & \cdots & \cdots \end{array} \\ \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} & \cdots \\ 0 & \frac{1}{2} & \frac{1}{2} & \cdots \\ 0 & 0 & 0 & \cdots \\ \cdots & 0 & \cdots & \ddots \\ 1 & 0 & \cdots & \\ \cdots & 0 & \cdots & \ddots \end{pmatrix} \end{array} \begin{array}{l} \\ \rightarrow 0 \\ \rightarrow 1 \\ \vdots \\ \vdots \\ \rightarrow 42 \\ \vdots \end{array}$$

`Twice : nat → nat`

Input : an integer `n`

Output : `if n=0 then 42 else Unif n`

$$\begin{array}{rcl} ([0], 42) & \mapsto & 1 \\ ([n_1, n_2], k) & \mapsto & \frac{1}{n_1+1} + \frac{1}{n_2+1} \\ & \text{if} & 0 \leq k \leq n_1 \leq n_2 \\ ([n_1, n_2], k) & \mapsto & \frac{1}{n_2+1} \\ & \text{if} & n_1 < k \leq n_2 \\ \text{Otherwise} & & 0 \end{array}$$

`Twice : nat → nat`

Input : an integer `n`

Output :
```
if n=0 then 42
else Unif n
```

$$
\begin{array}{rcl}
([0], 42) & \mapsto & 1 \\
([n_1, n_2], k) & \mapsto & \frac{1}{n_1+1} + \frac{1}{n_2+1} \\
 & \text{if} & 0 \leq k \leq n_1 \leq n_2 \\
([n_1, n_2], k) & \mapsto & \frac{1}{n_2+1} \\
 & \text{if} & n_1 < k \leq n_2 \\
\text{Otherwise} & & 0
\end{array}
$$

`Memo : nat → nat`

Input : an integer `n`

Output :
```
Let z be n in
if z=0 then 42
else Unif z
```

$$
\begin{array}{rcl}
([0], 42) & \mapsto & 1 \\
([n], k) & \mapsto & \frac{1}{n+1} \\
 & \text{if} & 0 \leq n \\
\text{Otherwise} & & 0
\end{array}
$$

Probabilistic Data :

If $\mathtt{x}:\mathtt{nat}$, then $[\![\mathtt{x}]\!] = (\mathtt{x_n})_{\mathtt{n}\in\mathbb{N}}$

where x_n is the probability that $\mathtt{x}$ is n.

Probabilistic Program : $\mathtt{P} : \mathtt{nat} \to \mathtt{nat}$

where $[\![\mathtt{P\ x}]\!]_\mathtt{n}$ is the probability that $\mathtt{P\ x}$ computes n.

$$[\![\mathtt{Once}]\!] \in (\mathbb{R}^+)^{\mathbb{N}\times\mathbb{N}} \qquad [\![\mathtt{Twice}]\!] \in (\mathbb{R}^+)^{\mathcal{M}_{\mathsf{fin}}(\mathbb{N})\times\mathbb{N}}$$

$$[\![\mathtt{Once\ x}]\!]_\mathtt{n} = [\![\mathtt{Once}]\!] \cdot [\![\mathtt{x}]\!] = \sum_k [\![\mathtt{Once}]\!]_{(\mathtt{k},\mathtt{n})}\, [\![\mathtt{x}]\!]_\mathtt{k}$$

$$[\![\mathtt{Twice\ x}]\!]_\mathtt{n} = [\![\mathtt{Twice}]\!] \cdot [\![\mathtt{x}]\!]^! = \sum_\mu [\![\mathtt{Twice}]\!]_{(\mu,\mathtt{n})} \prod_{\mathtt{k}\in\mu} [\![\mathtt{x}]\!]_\mathtt{k}$$

Syntax :

probabilistic PCF

A Typed Probabilistic Functional Programing Language

Types : $\sigma, \tau = \mathtt{nat} \mid \sigma \Rightarrow \tau$

Programs :

$$\mathtt{N}, \mathtt{P}, \mathtt{Q} := \underline{\mathtt{n}} \mid \mathbf{succ}(\mathtt{N}) \mid \mathtt{x} \mid \lambda \mathtt{x}^{\sigma}\, \mathtt{P} \mid (\mathtt{P})\mathtt{Q} \mid \mathbf{fix}(\mathtt{N})$$
$$\mid \mathbf{if}\,(N, P, [z]\,Q), \text{ with } z \text{ a variable}$$
$$\mid \mathbf{coin}(p), \text{ with } p \in \mathbb{Q} \cap [0,1]$$

Typing : $\Gamma \vdash P : \sigma$

$$\frac{\Gamma \vdash N : \mathtt{nat} \qquad \Gamma \vdash P : \sigma \qquad \Gamma, z : \mathtt{nat} \vdash \mathtt{Q} : \sigma}{\Gamma \vdash \mathbf{if}\,(N, P, [z]\,Q) : \sigma}$$

$$\frac{p \in \mathbb{Q} \cap [0,1]}{\mathbf{coin}(p) : \mathtt{nat}}$$

A Typed Probabilistic Functional Programing Language

Types : $\sigma, \tau = \mathtt{nat} \mid \sigma \Rightarrow \tau$

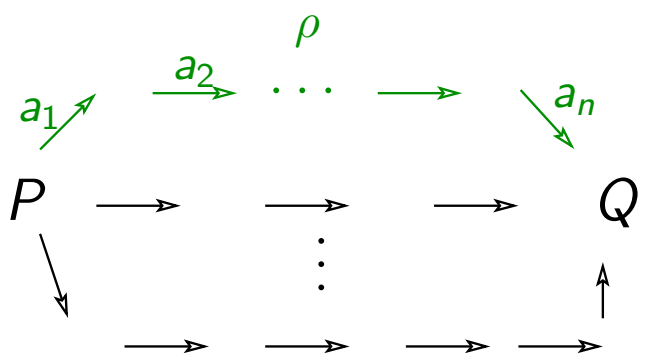
Programs :

$$\mathtt{N}, \mathtt{P}, \mathtt{Q} := \underline{\mathtt{n}} \mid \mathbf{succ}(\mathtt{N}) \mid \mathtt{x} \mid \lambda \mathtt{x}^{\sigma}\, \mathtt{P} \mid (\mathtt{P})\mathtt{Q} \mid \mathbf{fix}(\mathtt{N})$$
$$\mid \mathbf{if}\,(N, P, [z]\,Q), \text{ with } z \text{ a variable}$$
$$\mid \mathbf{coin}(p), \text{ with } p \in \mathbb{Q} \cap [0,1]$$

Operational Semantics : $P \xrightarrow{\mathtt{a}} Q$

P reduces to Q in one step with probability a

$\mathbf{Proba}(P \xrightarrow{*} Q) = \sum_{\rho} w(\rho)$



$w(\rho) = a_1 \cdots a_n$

$$\mathbf{if}\,(\underline{0}, P, [z]\,Q) \xrightarrow{1} P$$
$$\mathbf{if}\,(\underline{n+1}, P, [z]\,Q) \xrightarrow{1} Q[n/z]$$

$$\mathbf{coin}(p) \xrightarrow{\mathtt{p}} \underline{0}$$
$$\mathbf{coin}(p) \xrightarrow{(1-\mathtt{p})} \underline{1}$$

Predecessor : $\mathtt{nat} \Rightarrow \mathtt{nat}$ takes integer n and returns 0 if $n = 0$ and $n - 1$ otherwise.

$$\mathbf{pred} = \lambda x^{\mathtt{nat}}\, \mathbf{if}\, (x, \underline{0}, [z]\, z)$$

Addition : $\mathtt{nat} \Rightarrow \mathtt{nat} \Rightarrow \mathtt{nat}$ takes integer n and m and returns $n + m$.

$$\mathbf{add} = \lambda x^{\mathtt{nat}}\, \mathbf{fix}(\lambda a^{\mathtt{nat}\Rightarrow\mathtt{nat}}\, \lambda y^{\mathtt{nat}}\, \mathbf{if}\, (y, x, [z]\, \mathbf{succ}((a)z)))$$

Exponential : $\mathtt{nat} \Rightarrow \mathtt{nat}$ takes integer n returns 2^n.

$$\mathbf{exp} = \mathbf{fix}(\lambda e^{\mathtt{nat}\Rightarrow\mathtt{nat}}\, \lambda x^{\mathtt{nat}}\, \mathbf{if}\, (x, \underline{1}, [z]\, (\mathbf{add})(e)z(e)z))$$

Comparison : $\mathtt{nat} \Rightarrow \mathtt{nat} \Rightarrow \mathtt{nat}$ takes integer n and m and returns 0 if $n \leq m$ and 1 otherwise.

$$\mathbf{cmp} = \mathbf{fix}(\lambda c^{\mathtt{nat}\Rightarrow\mathtt{nat}\Rightarrow\mathtt{nat}}\, \lambda x^{\mathtt{nat}}\, \lambda y^{\mathtt{nat}}\, \mathbf{if}\, (x, \underline{0}, [z]\, \mathbf{if}\, (y, \underline{1}, [z']\, (c)zz')))$$

Memorization of the value of an expression of type $\mathtt{nat}$.

$$\mathbf{let}\, x\, \mathbf{be}\, M\, \mathbf{in}\, N = \mathbf{if}\, (M, N[0/x], [z]\, N[\mathbf{succ}(z)/x])$$

Uniform$_2$: $\mathtt{nat} \Rightarrow \mathtt{nat}$ takes integer n and returns a uniform probability distribution over $\{0, \ldots, 2^n - 1\}$

$$\mathbf{Unif_2} =$$
$$\mathbf{fix}(\lambda u^{\mathtt{nat}\Rightarrow\mathtt{nat}}\, \lambda x^{\mathtt{nat}}\, \mathbf{if}\, (x, \underline{0}, [z]\, \mathbf{if}\, (\mathbf{coin}(\tfrac{1}{2}), (u)z, [z']\, (\mathbf{add})(\mathbf{exp})z(u)z)))$$

Uniform : $\mathtt{nat} \Rightarrow \mathtt{nat}$ takes integer n and returns a uniform probability distribution over $\{0, \ldots, n\}$

$$\mathbf{Unif} =$$
$$\lambda x^{\mathtt{nat}}\, \mathbf{let}\, y\, \mathbf{be}\, x\, \mathbf{in}\, \mathbf{fix}(\lambda u^{\mathtt{nat}}\, \mathbf{let}\, z\, \mathbf{be}(\mathbf{Unif_2})y\, \mathbf{in}\, \mathbf{if}\, ((\mathbf{cmp})zy, z, [w]\, (u)y))$$

Caml encoding :

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

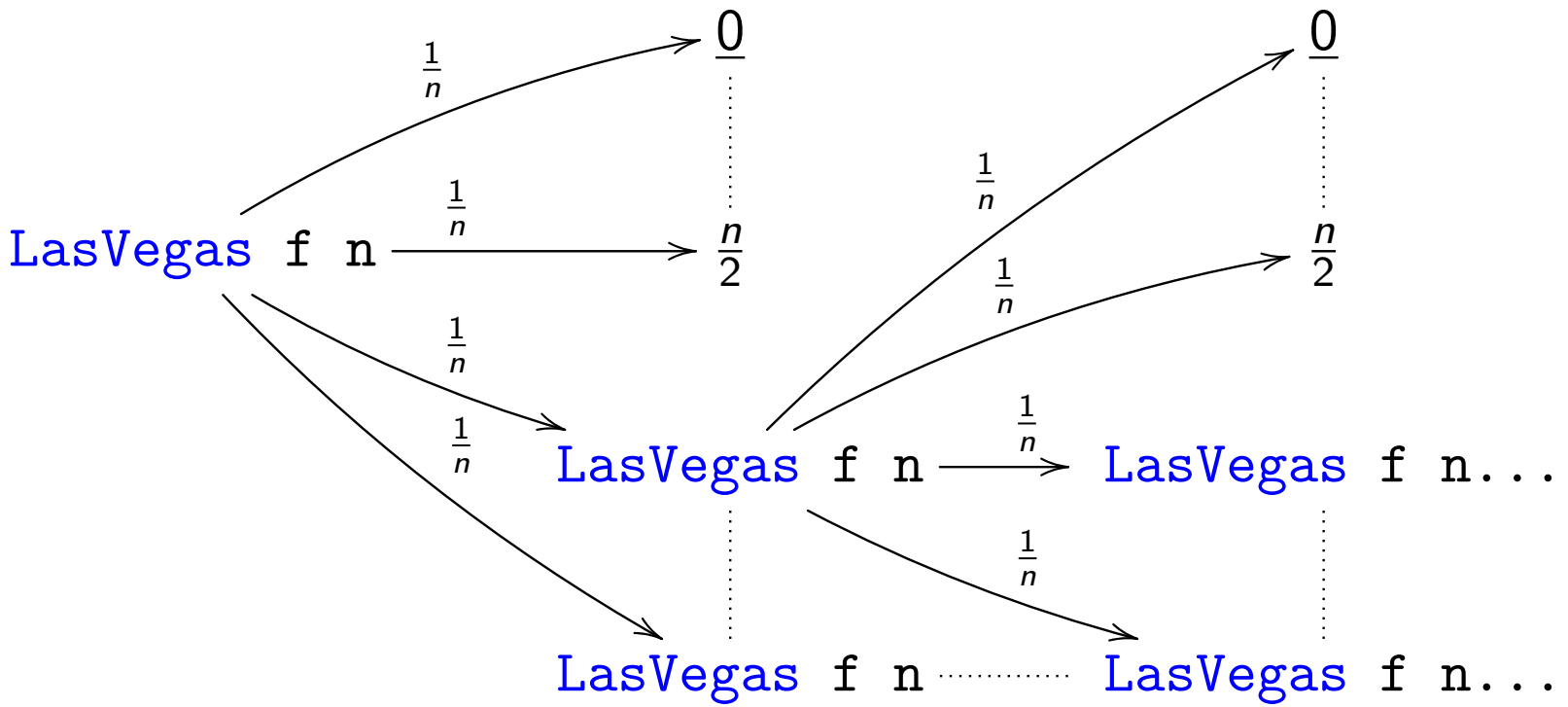
PCF encoding :

$$\texttt{LasVegas} = \textbf{fix}\,\big(\lambda\,\texttt{LV}^{(\texttt{nat}\Rightarrow\texttt{nat})\Rightarrow\texttt{nat}\Rightarrow\texttt{nat}}\ \ \lambda\texttt{f}^{\texttt{nat}\Rightarrow\texttt{nat}}\ \ \lambda\texttt{n}^{\texttt{nat}}$$
$$\textbf{let}\ \texttt{k}\ \textbf{be}\ \texttt{Unif n}\ \textbf{in}$$
$$\textbf{if}\ (\texttt{f k, k, (LV) f n})$$

PCF encoding :

$$\texttt{LasVegas} = \textbf{fix}\,\big(\lambda\,\mathtt{LV}^{(\mathtt{nat}\Rightarrow\mathtt{nat})\Rightarrow\mathtt{nat}\Rightarrow\mathtt{nat}}\ \ \lambda\mathtt{f}^{\mathtt{nat}\Rightarrow\mathtt{nat}}\ \ \lambda\mathtt{n}^{\mathtt{nat}}$$
$$\textbf{let}\ \mathtt{k}\ \textbf{be}\ \mathtt{Unif}\ \mathtt{n}\ \textbf{in}$$
$$\textbf{if}\ (\mathbf{f}\ \mathtt{k},\ \mathtt{k},\ (\mathtt{LV})\ \mathtt{f}\ \mathtt{n})$$

Operational Semantics :



Quantitative Semantics :

Probabilistic Coherent Spaces (Pcoh)

Types (Object) : representing randomized data : `nat`, ...

Programs (Maps) : `Input Type` $\longrightarrow$ `Output Type`

`Interaction (Composition):`

`Input Type` $\xrightarrow{\texttt{P}}$ `Intermediate Type` $\xrightarrow{\texttt{Q}}$ `Output Type`

Orthogonality : $x, y \in (\mathbb{R}^+)^{|\sigma|}$.

$$x \perp y \iff \sum_{a \in |\sigma|} x_a y_a \in [0,1].$$

Given a set $\mathrm{P} \subseteq (\mathbb{R}^+)^{|\sigma|}$ we define $\mathrm{P}^\perp$, the *orthogonal* of P, as

$$\mathrm{P}^\perp := \{y \in (\mathbb{R}^+)^{|\sigma|} \mid \forall x \in \mathrm{P} \ \ \langle x, y \rangle \leq 1\}.$$

Probabilistic Coherent Space : $\mathcal{X} = (|\mathcal{X}|, \mathrm{P}(\mathcal{X}))$

where $|\mathcal{X}|$ is a countable set and $\mathrm{P}(\mathcal{X}) \subseteq (\mathbb{R}^+)^{|\mathcal{X}|}$

such that the following holds :

closedness : $\mathrm{P}(\mathcal{X})^{\perp\perp} = \mathrm{P}(\mathcal{X})$,

boundedness : $\forall a \in |\mathcal{X}|, \exists \mu > 0, \forall x \in \mathrm{P}(\mathcal{X}), x_a \leq \mu$,

completeness : $\forall a \in |\mathcal{X}|, \exists \lambda > 0, \lambda e_a \in \mathrm{P}(\mathcal{X})$.

Objects of PCoh : $\mathcal{X} = (|\mathcal{X}|, \mathrm{P}(\mathcal{X}))$

where $|\mathcal{X}|$ is a countable set
and $\mathrm{P}(\mathcal{X}) \subseteq (\mathbb{R}^+)^{|\mathcal{X}|}$

Type Example : $\boxed{[\![\mathtt{nat}]\!] = (\mathbb{N}, \mathrm{P}(\mathtt{nat}) = \{(\lambda_\mathtt{n}) \mid \sum_\mathtt{n} \lambda_\mathtt{n} \leq 1\})}$

Data Example : if $\mathtt{M} : \mathtt{nat}$, then $[\![\mathtt{M}]\!] \in \mathrm{P}(\mathtt{nat}) \subseteq (\mathbb{R}^+)^{\mathbb{N}}$
is a subprobability distributions.

Coin($\frac{1}{2}$) : $[\![\mathtt{Coin}(\frac{1}{2})]\!] = (\frac{1}{2}, \frac{1}{2}, 0, \dots)$

Maps of PCoh : $f : (|\mathcal{X}|, \mathrm{P}(\mathcal{X})) \to (|\mathcal{Y}|, \mathrm{P}(\mathcal{Y}))$

defined as a **matrix** $M(f) \in (\mathbb{R}^+)^{\mathcal{M}_{\mathrm{fin}}(|\mathcal{X}|)\times|\mathcal{Y}|}$

thanks to **Taylor formula :**

$$f(x) = \sum_{\mu \in \mathcal{M}_{\mathrm{fin}}(|\sigma|)} M(f)_\mu \cdot x^\mu$$

with $x^\mu = \prod_{a \in \mathrm{Supp}(x)} x_a^{\mu(a)}$

f can be seen as an **entire function** $f : (\mathbb{R}^+)^{|\mathcal{X}|} \to (\mathbb{R}^+)^{|\mathcal{Y}|}$

preserving probabilistic coherence, $f(\mathrm{P}(\mathcal{X})) \subseteq \mathrm{P}(\mathcal{Y})$

Example : if $\mathtt{P} : \mathtt{nat} \to \mathtt{nat}$, then $[\![\mathtt{P}]\!] : (\mathbb{R}^+)^{\mathbb{N}} \to (\mathbb{R}^+)^{\mathbb{N}}$ is an entire function preserving subprobability distributions.

Typing judgement : $\Gamma \vdash Q : \tau$ with $\Gamma = (x_1 : \sigma_1, \dots, x_n : \sigma_n)$

$$[\![Q]\!]^\Gamma : \mathrm{P}([\![\sigma_1]\!]) \times \cdots \times \mathrm{P}([\![\sigma_n]\!]) \to \mathrm{P}([\![\tau]\!])$$

Examples : $\mathrm{P}([\![\mathtt{nat}]\!]) = (\mathbb{N}, \mathrm{P}(\mathtt{nat}) = \{(\lambda_n) \mid \sum_n \lambda_n \leq 1\})$

$$[\![\underline{n}]\!] = (0, \dots, 0, \underset{\uparrow n}{1}, 0, \dots) \qquad [\![\mathbf{coin}(p)]\!] = (p, 1-p, 0, \dots)$$

$$[\![x_i]\!]^\Gamma(\vec{u}) = [\![x_1 : A_1, \dots, x_n : A_n \vdash x_i]\!](\vec{u}) = u_i$$

$$[\![\mathbf{if}\,(N, P, [z]\,Q)]\!]^\Gamma(\vec{u}) = [\![N]\!]^\Gamma(\vec{u})_0 [\![P]\!]^\Gamma(\vec{u}) + \sum_{n=0}^{\infty} [\![N]\!]^\Gamma(\vec{u})_{n+1} [\![Q[n/z]]\!]^\Gamma(\vec{u})$$

Once : nat → nat $\quad \lambda$`n if n=0 then 42 else Coin`

$$\begin{aligned}
[\![\texttt{Once}]\!](x)_0 &= \tfrac{1}{2}\textstyle\sum_{n\geq 1} x_n \\
[\![\texttt{Once}]\!](x)_1 &= \tfrac{1}{2}\textstyle\sum_{n\geq 1} x_n \\
[\![\texttt{Once}]\!](x)_{42} &= x_0
\end{aligned}$$

Twice : nat → nat $\quad \lambda$`n if n=0 then 42 else Random n`

$$[\![\texttt{Twice}]\!](x)_k = \sum_{p=1}^{k}\sum_{q\geq k+1}\tfrac{1}{q}x_p x_q + \sum_{p=1}^{k+1}\sum_{q\geq k+1}(\tfrac{1}{p}+\tfrac{1}{q})x_p x_q, \text{ if } k \neq 42$$

$$[\![\texttt{Twice}]\!](x)_{42} = x_0 + \sum_{p=1}^{42}\sum_{q\geq 43}\tfrac{1}{q}x_p x_q + \sum_{p=1}^{43}\sum_{q\geq 43}(\tfrac{1}{p}+\tfrac{1}{q})x_p x_q$$

A model of PPCF :

in particular, **PCoh** is a model of linear logic.

Compositionality :

For $C : \sigma \Rightarrow \tau, P : \sigma$,

$$[\![(C)P]\!]_- = \sum_{\mu \in \mathcal{M}_{\mathsf{fin}}(|\sigma|)} [\![C]\!]_{\mu,-} [\![P]\!]^{\mu}$$

Adequacy Lemma :

Let $M : \mathtt{nat}$ be a closed program. Then for all n,

$$\mathrm{Proba}(M \xrightarrow{*} \underline{n}) = [\![M]\!]_n.$$

LasVegas f n : nat

$$\textbf{Proba}(\mathtt{LasVegas\ f\ n} \to^* \bullet) = \sum_k [\![\mathtt{LasVegas\ f\ n}]\!]_k = 1$$

Probabilistic Full Abstraction :

The completeness theorem

FA relates Semantical and Observational equivalences :

Let $P, Q : \sigma$ $\qquad \forall \alpha \in |\sigma|,\ [\![P]\!]_\alpha = [\![Q]\!]_\alpha$

Adequacy $\Downarrow$ $\Uparrow$ Full Completeness

$$\forall C : \sigma \Rightarrow \mathtt{nat},\ \forall n \in |\mathtt{nat}|,$$
$$\mathrm{Proba}((C)P \xrightarrow{*} n) = \mathrm{Proba}((C)Q \xrightarrow{*} n))$$

Adequacy proof :

1. Apply Adequacy Lemma : $\forall n,\ \mathrm{Proba}((C)P \xrightarrow{*} \underline{n}) = [\![(C)P]\!]_n$.
2. Apply Compositionality :

$$\forall n,\ [\![(C)P]\!]_n \quad = \quad \sum_{\mu \in \mathcal{M}_{\mathrm{fin}}(|\sigma|)} [\![C]\!]_{\mu,n} \prod_{\alpha \in \mu} [\![P]\!]_\alpha^{\mu(\alpha)}$$

FA relates Semantical and Observational equivalences :

Let $P, Q : \sigma$ $\qquad \forall \alpha \in |\sigma|,\ [\![P]\!]_\alpha = [\![Q]\!]_\alpha$

Adequacy $\Downarrow \Uparrow$ Full Completeness

$$\forall C : \sigma \Rightarrow \mathtt{nat},\ \forall n \in |\mathtt{nat}|,$$
$$\mathrm{Proba}((C)P \xrightarrow{*} n) = \mathrm{Proba}((C)Q \xrightarrow{*} n))$$

Adequacy proof :

1. Apply Adequacy Lemma : $\forall n,\ \mathrm{Proba}((C)P \xrightarrow{*} \underline{n}) = [\![(C)P]\!]_n$.
2. Apply Compositionality :

$$\forall n,\ [\![(C)P]\!]_n = \sum_{\mu \in \mathcal{M}_{\mathrm{fin}}(|\sigma|)} [\![C]\!]_{\mu,n} \prod_{\alpha \in \mu} [\![P]\!]_\alpha^{\mu(\alpha)}$$
$$= \sum_{\mu \in \mathcal{M}_{\mathrm{fin}}(|\sigma|)} [\![C]\!]_{\mu,n} \prod_{\alpha \in \mu} [\![Q]\!]_\alpha^{\mu(\alpha)} = [\![(C)Q]\!]_n$$

FA relates Semantical and Observational equivalences :

Let $P, Q : \sigma$ $\qquad \forall \alpha \in |\sigma|,\ [\![P]\!]_\alpha = [\![Q]\!]_\alpha$

Adequacy $\Downarrow \Uparrow$ Full Completeness

$$\forall C : \sigma \Rightarrow \mathtt{nat},\ \forall n \in |\mathtt{nat}|,$$
$$\mathrm{Proba}((C)P \xrightarrow{*} n) = \mathrm{Proba}((C)Q \xrightarrow{*} n))$$

Full Completeness proof :

1. By **contradiction** : $\exists \alpha \in |\sigma|\,,\ [\![P]\!]_\alpha \neq [\![Q]\!]_\alpha$
2. Find **testing context** : T_α such that $[\![(T_\alpha)P]\!]_0 \neq [\![(T_\alpha)Q]\!]_0$
3. Prove **definability** : $T_\alpha \in PPCF$
4. Apply **Adequacy** :
   $\mathrm{Proba}((T_\alpha)P \xrightarrow{*} 0) \neq \mathrm{Proba}((T_\alpha)Q \xrightarrow{*} 0)$.

Sum up

- A **Probabilistic** extension of **PCF** encoding `LasVegas`
- A Quantitative semantics **Pcoh** enjoying
  - Regularity : $f(x) = \sum_{\mu \in \mathcal{M}_{\text{fin}}(|\sigma|)} M(f)_\mu \cdot x^\mu$
  - Adequacy : $\forall n,\ \text{Proba}(P \xrightarrow{*} \underline{n}) = [\![P]\!]_n$.
- **Full Abstraction** exploiting mathematical properties.

Connected works

- **Probabilistic power domains** [Saheb-Djahromi, Lawson, Plotkin and Jones, Goubault-Larrecq and Varracca]
- **Probabilistic Games** [Harmer-Danos]