ASL 2013 - University of Waterloo
8-11 May

Probabilistic Coherent Spaces vs Probabilistic PCF
A Full Abstraction Result.

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]
- Syntax : PPCF, a Probabilistic extension of PCF [Plotkin77]

Derivation, the key stone of Probabilistic Full Abstraction

- Taylor expansion
- Well-pointedness and derivation

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)**

FA relates Semantical and Observational equivalences :

$[\![P]\!] = [\![Q]\!]$	Adequacy $\Longrightarrow$ $\Longleftarrow$ Full Completeness	$P \simeq_o Q$ $(\forall C[\,],\ C[P] \to^* v \iff C[Q] \to^* v)$

How to prove Full Completeness :

1. By **contradiction**, start with $[\![P]\!] \neq [\![Q]\!]$
2. Find **testing function** : f such that $f[\![P]\!] \neq f[\![Q]\!]$
3. Prove **definability** :
   $\exists C[\cdot],\ \forall P,\ f[\![P]\!] = [\![C[P]]\!]$ and $C[P] \to p$.
4. Conclude :
   $\exists C[\cdot],\ [\![C[P]]\!] \neq [\![C[Q]]\!] \Rightarrow p \neq q \Rightarrow P \not\simeq_o Q$.

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 $\underline{0}$.

$\underline{0}$	$\underline{1}$	$\underline{0}$	$\underline{1}$	$\underline{1}$	$\underline{0}$

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

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

Program : function seen as a positive matrix

Interaction : composition seen as multiplication

Example : `nat`

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

`Random n: nat` returns uniformly any $\{0, \dots, n-1\}$.

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

$$|\texttt{Coin}| = \{0, 1\} \quad \text{and} \quad |\texttt{Random n}| = \{0, \dots, n-1\}$$

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

$$[\![\texttt{Coin}]\!] = (\underset{0}{\tfrac{1}{2}}, \underset{1}{\tfrac{1}{2}}, \underset{2}{0}, \dots) \quad \text{and} \quad [\![\texttt{Random n}]\!] = (\underset{0}{\tfrac{1}{n}}, \dots, \underset{n-1}{\tfrac{1}{n}}, 0, \dots)$$

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 : $\texttt{Random} : \texttt{nat} \rightarrow \texttt{nat}$

Input : an integer n

Output : any integer $\{0, \ldots, n-1\}$ uniformly chosen.

Non Determinism : $|\texttt{Random}| \subseteq |\texttt{nat}| \times |\texttt{nat}|$ is a relation.

$$|\texttt{Random}| = \{(n,k) \;\mid\; n \in \mathbb{N},\; k \in \{0, \ldots, n-1\}\}$$

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

$$\begin{array}{c} \begin{array}{ccccc} \overset{1}{\downarrow} & \overset{2}{\downarrow} & \cdots & \overset{n}{\downarrow} & \cdots \end{array} \\ \left(\begin{array}{ccccc} 1 & \frac{1}{2} & \cdots & \frac{1}{n} & \cdots \\ 0 & \frac{1}{2} & \cdots & \frac{1}{n} & \cdots \\ \vdots & 0 & \ddots & \vdots & \\ & \vdots & 0 & \frac{1}{n} & \\ & & \vdots & \ddots & \ddots \end{array}\right) \end{array} \begin{array}{l} \\ \rightarrow 0 \\ \rightarrow 1 \\ \vdots \\ \rightarrow n-1 \\ \vdots \end{array}$$

Modeling Probabilistic **Programs**

Once : nat → nat

Input : an integer `n`

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

$$\begin{array}{c} \begin{array}{cccc} 0 & 1 & \cdots & \cdots \\ \downarrow & \downarrow & & \end{array} \\ \left(\begin{array}{cccc} 0 & \frac{1}{2} & \frac{1}{2} & \cdots \\ 0 & \frac{1}{2} & \frac{1}{2} & \cdots \\ 0 & 0 & 0 & \cdots \\ \cdots & 0 & \cdots & \ddots \\ 1 & 0 & \cdots & \\ \cdots & 0 & \cdots & \ddots \end{array}\right) \begin{array}{l} \to 0 \\ \to 1 \\ \vdots \\ \vdots \\ \to 42 \\ \vdots \end{array} \end{array}$$

Twice : nat → nat

Input : an integer `n`

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

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

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

$$[\![\mathtt{Once}]\!] \in (\mathbb{R}^+)^{\mathbb{N}\times\mathbb{N}}$$

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

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

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

Syntax :

probabilistic PCF

A Typed Probabilistic Functional Programing Language

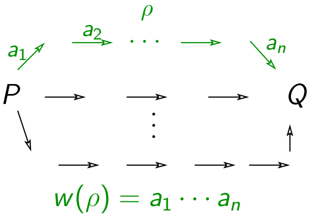
Types : $\sigma, \tau = \mathtt{nat} \mid \sigma \Rightarrow \tau$

Probabilistic PCF :

$$\mathtt{N}, \mathtt{P}, \mathtt{Q} := \underline{\mathtt{n}} \mid \mathsf{pred}(\mathtt{N}) \mid \mathsf{succ}(\mathtt{N}) \mid \mathtt{x} \mid \lambda \mathtt{x}^{\sigma}\, \mathtt{P} \mid (\mathtt{P})\mathtt{Q} \mid \mathsf{fix}(\mathtt{M})$$
$$\mid \text{if } (N = \underline{0}) \text{ then } P \text{ else } Q \mid a \cdot P + b \cdot Q, \text{ when } a + b \leq 1$$

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

P reduces to Q in one step with probability a



$$\text{if } (\underline{0} = \underline{0}) \text{ then } P \text{ else } Q \xrightarrow{1} P$$

$$\text{if } (\underline{n+1} = \underline{0}) \text{ then } P \text{ else } Q \xrightarrow{1} Q$$

$$a \cdot P + b \cdot Q \xrightarrow{\mathtt{a}} P$$

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

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
```

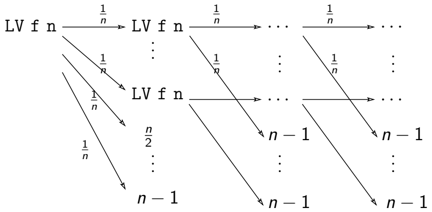
PCF encoding :

$$\textbf{fix}\ \Big(\lambda\, \texttt{LasVegas}^{(\texttt{nat}\Rightarrow\texttt{nat})\Rightarrow\texttt{nat}\Rightarrow\texttt{nat}}$$
$$\lambda \texttt{f}^{\texttt{nat}\Rightarrow\texttt{nat}}\lambda \texttt{n}^{\texttt{nat}}$$
$$\Big(\tfrac{1}{n}\lambda \texttt{g}^{\texttt{nat}\Rightarrow\texttt{nat}} g\ \ \underline{0} + \cdots + \tfrac{1}{n}\lambda \texttt{g}^{\texttt{nat}\Rightarrow\texttt{nat}} g\ \ \underline{n-1}\Big)$$
$$\lambda \texttt{k}^{\texttt{nat}}\ \texttt{if}\ (\texttt{f}\ \ \texttt{k} = \underline{0})\ \texttt{then}\ \texttt{k}$$
$$\texttt{else}\ \texttt{LasVegas}\ \texttt{f}\ \texttt{n}\Big)$$

PCF encoding :

$$\textbf{fix}\ \Big(\lambda\ \texttt{LasVegas}^{(\texttt{nat}\Rightarrow\texttt{nat})\Rightarrow\texttt{nat}\Rightarrow\texttt{nat}}\ \lambda \texttt{f}^{\texttt{nat}\Rightarrow\texttt{nat}}\lambda \texttt{n}^{\texttt{nat}}\ \Big(\tfrac{1}{n}\lambda \texttt{g}^{\texttt{nat}\Rightarrow\texttt{nat}} g\ \ \underline{1} + \cdots + \tfrac{1}{n}\lambda \texttt{g}^{\texttt{nat}\Rightarrow\texttt{nat}} g\ \ \underline{n}\Big)\ \lambda \texttt{k}^{\texttt{nat}}\ \texttt{if}\ (\texttt{f}\ \ \texttt{k} = \underline{0})\ \texttt{then}\ \texttt{k}\ \texttt{else}\ \ \texttt{LasVegas f n}\Big)$$

Operational Semantics :



Quantitative Semantics :

Probabilistic Coherent Spaces (Pcoh)

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

Programs (Maps) : `Input Type` $\rightarrow$ `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 : $\mathcal{X} = \left(|\mathcal{X}|, \mathrm{P}(\mathcal{X})\right)$
where $|\mathcal{X}|$ is a countable set
and $\mathrm{P}(\mathcal{X}) \subseteq (\mathbb{R}^+)^{|\mathcal{X}|}$

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

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 : $\frac{1}{2} \cdot \underline{0} + \frac{1}{2} \cdot \underline{1}$

$$[\![\mathtt{Coin}]\!] = \left(\tfrac{1}{2}, \tfrac{1}{2}, 0, \dots\right)$$

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

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

thanks to **Taylor formula :**

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

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

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.

Once : **nat** $\to$ **nat** λ`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** $\to$ **nat** λ`n if n=0 then 42 else Random n`

$$
\begin{aligned}
[\![\texttt{Twice}]\!](x)_k &= \sum_{p=1}^{k}\sum_{q\geq k+1}\tfrac{1}{q}x_p x_q + \sum_{p=1}^{k+1}\sum_{q\geq k+1}(\tfrac{1}{p}+\tfrac{1}{q})x_p x_q, \text{ if } k\neq 42 \\
[\![\texttt{Twice}]\!](x)_{42} &= x_0 + \sum_{p=1}^{42}\sum_{q\geq 43}\tfrac{1}{q}x_p x_q + \sum_{p=1}^{43}\sum_{q\geq 43}(\tfrac{1}{p}+\tfrac{1}{q})x_p x_q
\end{aligned}
$$

A model of PPCF :

in particular, **PCoh** is a model of ~~differential~~ 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 : nat be a closed program. Then for all n,

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

LasVegas f n : nat

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

Probabilistic Full Abstraction :

The completeness theorem

FA relates Semantical and Observational equivalences :

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

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

Adequacy $\Downarrow$ $\Uparrow$ Full Completeness

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

Adequacy proof :

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

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

FA relates Semantical and Observational equivalences :

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

Adequacy $\Downarrow$ $\Uparrow$ Full Completeness

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

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** :
   $\text{Proba}((T_\alpha)P \xrightarrow{*} 0) \neq \text{Proba}((T_\alpha)Q \xrightarrow{*} 0)$.

Assumptions

- $P, Q : \mathtt{nat}$
- $[\![P]\!]_n \neq [\![Q]\!]_n$

Goal

- $T_n : \mathtt{nat} \to \mathtt{nat}$
- $[\![(T_n)P]\!]_0 \neq [\![(T_n)Q]\!]_0$

Choose

If $T_n = \lambda x^{\mathtt{nat}}\,\text{if } (x = \underline{n}) \text{ then } \underline{0}$ Then $[\![T_n]\!]_{[n],0} = 1$

Conclude

By Compositionality, $[\![(T_n)P]\!]_0 = [\![P]\!]_n \neq [\![Q]\!]_n = [\![(T_n)Q]\!]_0$

Find a testing context : Induction Case

Assumptions

- $P, Q : \phi \Rightarrow \psi$
- $\alpha = ([\gamma_1, \ldots, \gamma_n], \beta)$
- $[\![P]\!]_\alpha \neq [\![Q]\!]_\alpha$

Goal

- $T_\alpha : (\phi \Rightarrow \psi) \to nat$
- $[\![(T_\alpha)P]\!] \neq [\![(T_\alpha)Q]\!]$
- $[\![T_\alpha]\!]_\mu \neq 0 \Leftrightarrow \mu = [\alpha]$

Compositionality

$$[\![(T_\alpha)P]\!] = \sum_{\mu \in \mathcal{M}_{\mathrm{fin}}(|\sigma|)} [\![T_\alpha]\!]_\mu \prod_{\delta \in \mu} [\![P]\!]_\delta^{\mu(\delta)}$$

Choose

$$\mathcal{T}_\alpha(\vec{X}) = \lambda f^{\phi \Rightarrow \psi}\ \mathcal{T}_\beta(\vec{Y}) \left((f) \sum_{i=1}^{k} \frac{L_i}{n} \mathcal{N}_{\gamma_i}(\vec{Z}_i') \right)$$

$$\mathcal{N}_\alpha(\vec{X}') = \lambda x^\phi \text{ if } (\wedge_{i=1}^k \mathcal{T}_{\gamma_i}(\vec{Z}_i)x = \underline{0}) \text{ then } \mathcal{N}_\beta(\vec{Y}') \text{ else } \Omega_\psi .$$

Taylor Formula

$\forall \mu,\ [\![\mathcal{T}_\alpha(\vec{X})]\!]_\mu$ is a power series in $\vec{X}$ with coeff of $\prod \vec{X} \neq 0 \iff \mu = [\alpha]$

The coeff of $\prod \vec{X}$ in $[\![(\mathcal{T}_\alpha(\vec{X}))P]\!]$ is proportional to $[\![P]\!]_\alpha$.

Summary :

- The coeff of $\prod \vec{X}$ in $[\![(\mathcal{T}_\alpha(\vec{X}))P]\!]$ is proportional to $[\![P]\!]_\alpha$.
- $[\![P]\!]_\alpha \neq [\![Q]\!]_\alpha$.
- $[\![(\mathcal{T}_\alpha(\vec{X}))P]\!]$ and $[\![(\mathcal{T}_\alpha(\vec{X}))Q]\!]$ are two real power series with different coefficients.

Definability : Find $\vec{\lambda} \in [0,1]^{(\mathbb{N})}$ then $\mathcal{T}_\alpha(\vec{\lambda})$ in ProbaPCF such that $[\![(\mathcal{T}_\alpha(\vec{\lambda}))P]\!] \neq [\![(\mathcal{T}_\alpha(\vec{\lambda}))Q]\!]$

By contradiction :

- If they were equal, their derivatives near zero would be equal.
- Coefficients of power series are computed by derivation at 0.

Differential categories in use :

Full Abstraction from **Taylor expansion**
and **Topological derivation.**

Differential Operator $f : !X \multimap Y \qquad df : X \otimes !X \multimap Y$

$$df : \underset{a}{X} \otimes \underset{\alpha}{!X} \overset{\bar{d}\otimes -}{\multimap} \underset{[a]}{!X} \otimes \underset{\alpha}{!X} \overset{\bar{c}}{\multimap} \underset{[a]+\alpha}{!X} \overset{f}{\multimap} \underset{\beta}{Y}$$

Pcoh is **not a differential category**

cocontraction does not preserve probabilistic coherence

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

$$\bar{c}(1^! \otimes 1^!) = (1+1)^!$$

with $\lambda^! = (\lambda, \lambda, \dots)$

Pcoh is embedded in **Rel**$(\mathbb{R}^{+\infty})$ which is a differential category

Well Pointedness and Derivation

Pcoh is **well pointed** — Derivation is topologic

Example : if $f :!1 \multimap 1$, then $[\![f]\!] : \mathbb{R}^+ \to \mathbb{R}^+$ such that $f(x) = \sum_k f_k x^k$

$$df(0)(x) = \lim_{t \to 0} \frac{f(tx) - f(0)}{t}$$

Rel($\mathbb{R}^{+\infty}$) is **not well pointed** — Derivation is formal

Example : if $g, h :!1 \multimap 1$, then $[\![g]\!], [\![h]\!] : \mathbb{R}^{+\infty} \to \mathbb{R}^{+\infty}$

$$g(x) = \infty x \qquad dg(0)(x) = \infty$$

$$h(x) = \infty x^2 \qquad dh(0)(x) = 2\infty x$$

Sum up

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

This is not the end of the story !

- Which models enjoy Taylor Formula ?
- Can we extend Full Abstraction to other quantitative models ?