Probabilistic Call-By-Push-Value Adequacy and Full Abstraction

QSLC Marseille

Thomas Ehrhard and Christine Tasson
IRIF — CNRS and University Paris Diderot

September 2nd, 2016

A technical appendix to Christine Tasson's talk.

Probabilistic coherence spaces: basic duality

Given a set I and $\mathcal{X} \in (\mathbb{R}^+)^I$, define

$$\mathcal{X}^\perp = \{u' \in (\mathbb{R}^+)^I \mid \forall u \in \mathcal{X} \ \sum_{i \in I} u_i u'_i \leq 1\}\,.$$

Then $\mathcal{X} \subseteq \mathcal{Y} \Rightarrow \mathcal{Y}^\perp \subseteq \mathcal{X}^\perp$ and $\mathcal{X} \subseteq \mathcal{X}^{\perp\perp}$.
Hence $\mathcal{X}^\perp = \mathcal{X}^{\perp\perp\perp}$.

A probabilistic coherence space is a structure $X = (|X|, \mathrm{P}(X))$ where

- $|X|$ is a set (finite or countable)
- $\mathrm{P}(X) \subseteq (\mathbb{R}^+)^{|X|}$ with $\mathrm{P}(X)^{\perp\perp} \subseteq \mathrm{P}(X)$, that is $\mathrm{P}(X)^{\perp\perp} = \mathrm{P}(X)$.

To avoid ∞ coefficients, we assume moreover that $\forall a \in |X|$:

- $\exists u \in \mathrm{P}(X)\ u_a > 0$
- $\exists A > 0\, \forall u \in \mathrm{P}(X)\ u_a < A$

Then $X^\perp = (|X|, \mathrm{P}(X)^\perp)$ is also a probabilistic coherence space.

$\mathsf{P}(X)$ can be ordered: $u \leq v$ if $\forall a \in |X| \quad u_a \leq v_a$.
Then $\mathsf{P}(X)$ is an ω-continuous domain.

If $u, v \in \mathsf{P}(X)$ and $\alpha, \beta \in \mathbb{R}^+$ such that $\alpha + \beta \leq 1$ then $\alpha u + \beta v \in \mathsf{P}(X)$.

Example: $\mathsf{N} = (\mathbb{N}, \{u \in (\mathbb{R}^+)^{\mathbb{N}} \mid \sum_{k \in \mathbb{N}} u_k \leq 1\})$ (like ℓ^1).
We have $\mathsf{N}^\perp = (\mathbb{N}, \{u' \in (\mathbb{R}^+)^{\mathbb{N}} \mid \forall k \in \mathbb{N}\ u'_k \leq 1\})$ (like ℓ^∞).

Remark: $\mathrm{P}(X) \subseteq (\mathbb{R}^+)^{|X|}$ defines a probabilistic coherence space iff it is

- downwards-closed
- directed-complete
- convex

and satisfies

- $\exists u \in \mathrm{P}(X)\ u_a > 0$
- $\exists A > 0\, \forall u \in \mathrm{P}(X)\ u_a < A$

Linear morphisms

A category **Pcoh**:

- objects: probabilistic coherence spaces
- morphisms: $t \in \mathbf{Pcoh}(X, Y)$ if $t \in (\mathbb{R}^+)^{|X| \times |Y|}$ is a matrix such that

$$\forall u \in \mathrm{P}(X)\, \forall v' \in \mathrm{P}(Y)^\perp \quad \sum_{(a,b) \in |X| \times |Y|} t_{a,b} u_a v'_b \leq 1\,.$$

Same thing as a Scott continuous function $f : \mathrm{P}(X) \to \mathrm{P}(Y)$ such that $f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$:

$$f(u)_b = \sum_{a \in |X|} t_{a,b} u_a$$

Pcoh is an ω-cartesian $*$-autonomous category

- $X \otimes Y = (|X| \times |Y|, \{u \otimes v \mid u \in \mathrm{P}(X) \text{ and } v \in \mathrm{P}(Y)\}^{\perp\perp})$ where $(u \otimes v)_{(a,b)} = u_a v_b$.
- $X \multimap Y = (X \otimes Y^{\perp})^{\perp}$.
- Dualizing object $\perp = (\{*\}, [0,1])$ so that $X \multimap \perp$ is trivially isomorphic to $X^{\perp}$.
- $\&_{i \in I} X_i = (\bigcup_{i \in I} \{i\} \times |X_i|, \{u \in (\mathbb{R}^+)^{\bigcup_{i \in I} \{i\} \times |X_i|} \mid \forall i \ u(i) \in \mathrm{P}(X_i)\} \simeq \prod_{i \in I} \mathrm{P}(X_i))$ where $u(i)$ is the restriction to $|X_i|$.
- Therefore also $\bigoplus_{i \in I} X_i$.

Exponential

Let $u \in \mathrm{P}(X)$ and $m \in \mathcal{M}_{\mathrm{fin}}(|X|)$ (finite multisets), we set

$$u^m = \prod_{a \in |X|} u_a^{m(a)} .$$

Then $u^! \in (\mathbb{R}^+)^{\mathcal{M}_{\mathrm{fin}}(|X|)}$ is defined by $u^!_m = u^m$.

$!X$ is defined by $|!X| = \mathcal{M}_{\mathrm{fin}}(|X|)$ and

$$\mathrm{P}(!X) = \{u^! \mid u \in \mathrm{P}(X)\}^{\perp\perp} .$$

It is a functor **Pcoh** $\to$ **Pcoh** which has a structure of symmetric monoidal comonad...
Pcoh is a model of classical Linear Logic.

Kleisli category $\mathbf{Pcoh}_!$ as a category of functions

Given $s \in \mathbf{Pcoh}_!(X, Y) = \mathbf{Pcoh}(!X, Y)$ and $u \in \mathrm{P}(X)$, we set

$$s(u) = s\, u^! = \left(\sum_{m \in |!X|} s_{m,b} u^m \right)_{b \in |Y|} \in \mathrm{P}(Y)\,.$$

This is a Scott continuous function $\hat{s} : \mathrm{P}(X) \to \mathrm{P}(Y)$.
But not all continuous functions $\mathrm{P}(X) \to \mathrm{P}(Y)$ are of the shape $\hat{s}$!
Composition in $\mathbf{Pcoh}_!$ coincides with composition of such functions $\hat{s}$.

By cartesian closedness and Scott continuity we have well-behaved fixpoint operators $\mathcal{Y}_X \in \mathbf{Pcoh}_!(!X \multimap X, X)$.

Fixpoints of types

The class of probabilistic coherence spaces can be endowed with an order relation, say that $X \subseteq Y$ if

- $|X| \subseteq |Y|$.
- If $u \in \mathrm{P}(X)$ then $z(u) \in \mathrm{P}(Y)$ where $z(u)$ is the extension of $u \in (\mathbb{R}^+)^{|X|}$ to $(\mathbb{R}^+)^{|Y|}$ with 0's.
- If $u \in \mathrm{P}(Y)$ then $r(u) \in \mathrm{P}(X)$ where $r(u)$ is the restriction of u to $|X|$.

$(\mathbf{Pcoh}, \subseteq)$ is a complete partially ordered class and all connectives (including linear negation) are Scott continuous operators on this class.

Dense coalgebras

$P = (\underline{P}, \mathrm{h}_P)$ a coalgebra: so $\underline{P} \in \mathbf{Pcoh}$ and $\mathrm{h}_P \in \mathbf{Pcoh}(\underline{P}, !\underline{P})$.

$u \in \mathrm{P}(\underline{P})$, seen as an element of $\mathbf{Pcoh}(1, \underline{P})$, is a coalgebra morphism iff: $\mathrm{h}_P\, u = u^!$. Let $\mathrm{P}^!(P)$ be the set of these particular elements of $\mathrm{P}(\underline{P})$ (they form a complete **pre**domain, $0 \notin \mathrm{P}^!(P)$).

Definition

P is *dense* if, for any $X \in \mathbf{Pcoh}$ and $t, t' \in \mathbf{Pcoh}(\underline{P}, X)$, one has $(\forall u \in \mathrm{P}^!(P)\ t\, u = t'\, u) \Rightarrow t = t'$.

Fact

$(!X, dig_X)$ is dense, and dense coalgebras are closed under all constructions of LL, including fixpoints of types. So for any positive type φ, the coalgebra $[\varphi]^!$ is dense.

Soundness

If $x_1 : \varphi_1, \ldots, x_n : \varphi_n \vdash M : \sigma$ then $[M]_{\vec{x}} \in \mathbf{Pcoh}([\varphi_1] \otimes \cdots \otimes [\varphi_n], [\sigma])$ can be considered as a (Scott continuous) function

$$\mathrm{P}^!([\varphi_1]^!) \times \cdots \times \mathrm{P}^!([\varphi_n]^!) \to [\sigma]$$

and this function fully determines $[M]_{\vec{x}}$ by density of the $[\varphi_i]^!$'s.

Soundness: for $\vdash M : \sigma$,

$$[M] = \sum_{M'} \Pr(M \to M')[M']$$

This implies that, if $\vdash M : 1$ then

$$\Pr(M \to^* ()) \leq [M]$$

Adequacy is: $\Pr(M \to^* ()) \geq [M]$

Main tool: a relation $\mathcal{R}(\sigma)$ between

- terms M such that $\vdash M : \sigma$
- and elements $u \in \mathsf{P}([\sigma])$

with $\mathcal{R}(1)$ given by

$$(M, u) \in \mathcal{R}(1) \Leftrightarrow \mathsf{Pr}(M \to^* ()) \geq u$$

and then prove

Lemma (Logical Relation Lemma for closed terms)

$$\vdash M : \sigma \Rightarrow (M, [M]) \in \mathcal{R}(\sigma)$$

Problem:

- Fixpoints of types prevent from defining $\mathcal{R}(\sigma)$ by a simple induction on σ
- The absence of positivity restrictions on variable occurrences in recursive types prevents from defining $\mathcal{R}(\mathsf{Fix}\,\zeta \cdot \varphi)$ as a least fixpoint.

Main idea (Pitts): for σ *closed*, use instead pairs of relations $\mathcal{R}(\sigma) = (\mathcal{R}^-(\sigma), \mathcal{R}^+(\sigma))$ where $\mathcal{R}^\varepsilon(\sigma)$ is as before. Order these pairs by

$$\mathcal{R} \sqsubseteq \mathcal{S} \text{ if } \mathcal{R}^+ \subseteq \mathcal{S}^+ \text{ and } \mathcal{S}^- \subseteq \mathcal{R}^-$$

We use $\mathsf{Rel}(\sigma)$ for this poset (remember: σ is closed).

Second idea: deal with values in a special way.

For φ positive and *closed*, we define $\mathrm{Rel}^{\mathsf{v}}(\varphi)$ as the poset of all $\mathcal{V} = (\mathcal{V}^+, \mathcal{V}^-)$ where $\mathcal{V}^\varepsilon$ is a set of pairs of *value-relations* (V, v) with

- $\vdash V : \varphi$ is a closed *value*
- $v \in \mathrm{P}^!([\varphi])$

Now we can interpret *open* types as monotone operations on pairs of value-relations:

$$\mathcal{R}(\sigma)_{\vec{\zeta}} : \prod_{i=1}^{n} \mathsf{Rel}^{\mathsf{v}}(\varphi_i) \to \mathsf{Rel}(\sigma \left[\vec{\varphi}/\vec{\zeta}\right])$$

$$\mathcal{V}(\varphi)_{\vec{\zeta}} : \prod_{i=1}^{n} \mathsf{Rel}^{\mathsf{v}}(\varphi_i) \to \mathsf{Rel}^{\mathsf{v}}(\varphi \left[\vec{\varphi}/\vec{\zeta}\right])$$

where $\vec{\zeta} = (\zeta_1, \ldots, \zeta_n)$ is a list of type variables without repetitions and which contains all free variables of σ and φ, and $\varphi_1, \ldots, \varphi_n$ are closed positive types.

Some of the operations on relations we use in this definition

If $\mathcal{V} \in \mathsf{Rel}^{\mathsf{v}}(\varphi)$ and $\mathcal{R} \in \mathsf{Rel}(\sigma)$, we define $\mathcal{V} \multimap \mathcal{R} \in \mathsf{Rel}(\varphi \multimap \sigma)$ by:

$$(\mathcal{V} \multimap \mathcal{R})^{\varepsilon} = \{(M, s) \mid \vdash M : \varphi \multimap \sigma,\ s \in \mathsf{P}(\varphi \multimap \sigma) \\ \text{and } \forall (V, v) \in \mathcal{V}^{-\varepsilon}\ (\langle M \rangle V, s(v)) \in \mathcal{R}^{\varepsilon}\}$$

This makes sense by density of $\mathsf{P}^{!}(\varphi)$.

If $\mathcal{R} \in \mathsf{Rel}(\sigma)$ then $!\mathcal{R} \in \mathsf{Rel}^{\mathsf{v}}(!\sigma)$ is defined by

$$!\sigma^{\varepsilon} = \{(M^{!}, s^{!}) \mid (M, s) \in \mathcal{R}^{\varepsilon}\}$$

If φ is closed and positive and $\mathcal{V} \in \mathrm{Rel}^{\mathsf{v}}(\varphi)$, then $\overline{\mathcal{V}} \in \mathrm{Rel}(\varphi)$ is given by:

$\overline{\mathcal{V}}^{\varepsilon}$ is the set of all (M, u) such that $\vdash M : \varphi$, $u \in \mathrm{P}([\varphi])$ and, for all $(T, t) \in (\mathcal{V} \multimap \mathcal{R}(1))^{-\varepsilon}$, one has $(\langle T \rangle M, t(u)) \in \mathcal{R}(1)$.

Remember that $\mathcal{R}(1)$ given by

$$(M, u) \in \mathcal{R}(1) \Leftrightarrow \Pr(M \to^{*} ()) \geq u$$

etc. All these operations are monotone

Type fixpoints

For φ closed, $\mathsf{Rel}^{\mathsf{v}}(\varphi)$ is a complete semi-lattice by

$$\bigsqcap_{i \in I} \mathcal{R}_i = (\bigcup_{i \in I} \mathcal{R}_i^-, \bigcap_{i \in I} \mathcal{R}_i^+)$$

so that we can apply the Knaster-Tarski Fixpoint Theorem:

$$\mathcal{V}(\varphi)_{\vec{\zeta}}(\vec{\mathcal{V}}) = \bigsqcap \{\mathcal{V} \in \mathsf{Rel}^{\mathsf{v}}(\varphi \left[\vec{\varphi}/\vec{\zeta}\right]) \mid \mathsf{fold}(\mathcal{V}(\psi)_{\vec{\zeta},\zeta}(\vec{\mathcal{V}}, \mathcal{V})) \sqsubseteq \mathcal{V}\}$$

for $\varphi = \mathsf{Fix}\, \zeta \cdot \psi$, the φ_i's are closed and $\mathcal{V}_i \in \mathsf{Rel}^{\mathsf{v}}(\varphi_i)$ for $i = 1, \ldots, n$. Then

$$\mathcal{V}(\varphi)_{\vec{\zeta}}(\vec{\mathcal{V}}) = \mathsf{fold}(\mathcal{V}(\psi)_{\vec{\zeta},\zeta}(\vec{\mathcal{V}}, \mathcal{V}(\varphi)_{\vec{\zeta}}(\vec{\mathcal{V}})))$$

In that way we have defined $\mathcal{R}(\sigma) \in \mathsf{Rel}(\sigma)$ and $\mathcal{V}(\varphi) \in \mathsf{Rel}^{\mathsf{V}}(\varphi)$.

The second step of the proof consists in proving that $\mathcal{R}(\sigma)^+ = \mathcal{R}(\sigma)^-$ (it is not clear whether the same holds for $\mathcal{V}(\varphi)$ but it is not required).

$\mathcal{R}(\sigma)^+ \subseteq \mathcal{R}(\sigma)^-$ is by induction on types + abstract non-sense. The converse needs more work.

Proving the converse inclusion

One defines *restriction operators* which are terms of CBPV

$\mathsf{p}(n,\sigma)$ and $\mathsf{p}^{\mathsf{v}}(n,\varphi)$ (when φ is positive) typed as follows: $\vdash \mathsf{p}(n,\sigma) : !\sigma \multimap \sigma$ and $\vdash \mathsf{p}^{\mathsf{v}}(n,\varphi) : \varphi \multimap \varphi$.

By lexicographic induction on (n,σ) and (n,φ).

Restriction operators: examples

$$\mathsf{p}(n, \varphi \multimap \sigma) = \lambda f^{!(\varphi \multimap \sigma)}\, \lambda x^{\varphi}\, \langle \mathsf{p}(n, \sigma) \rangle (\langle \mathsf{der}(f) \rangle \langle \mathsf{p}^{\mathsf{v}}(n, \varphi) \rangle x)^{!}$$

$$\mathsf{p}^{\mathsf{v}}(0, \mathsf{Fix}\, \zeta \cdot \varphi) = \lambda x^{\mathsf{Fix}\, \zeta \cdot \varphi}\, \Omega^{\mathsf{Fix}\, \zeta \cdot \varphi}$$

$$\mathsf{p}^{\mathsf{v}}(n+1, \mathsf{Fix}\, \zeta \cdot \varphi) = \lambda x^{\mathsf{Fix}\, \zeta \cdot \varphi}\, \mathsf{fold}(\langle \mathsf{p}^{\mathsf{v}}(n, \varphi\, [\mathsf{Fix}\, \zeta \cdot \varphi / \zeta]) \rangle \mathsf{unfold}(x))$$

These terms have a very simple interpretation which can be presented as follows

$$[\mathrm{p}(n,\varphi)]_{(a,b)} = \begin{cases} 1 & \text{if } a = b \in \mathrm{I}^{\mathrm{v}}(n,\varphi) \\ 0 & \text{otherwise.} \end{cases}$$

$$[\mathrm{p}(n,\sigma)]_{(c,b)} = \begin{cases} 1 & \text{if } c = [b] \text{ and } b \in \mathrm{I}(n,\sigma) \\ 0 & \text{otherwise.} \end{cases}$$

where $\mathrm{I}(n,\sigma) \subseteq |[\sigma]|$ and $\mathrm{I}^{\mathrm{v}}(n,\varphi) \subseteq |[\varphi]|$ are monotone families of sets defined by induction on (n,σ) and (n,φ), such that

$$\bigcup_{n=0}^{\infty} \mathrm{I}(n,\sigma) = |[\sigma]| \text{ and } \bigcup_{n=0}^{\infty} \mathrm{I}^{\mathrm{v}}(n,\varphi) = |[\varphi]|$$

Then one can prove

Lemma

Let σ be a closed type and let $n \in \mathbb{N}$. If $(M, u) \in \mathcal{R}(\sigma)^-$ then

$$(M, [\mathsf{p}(n, \sigma)](u^!)) \in \mathcal{R}(\sigma)^+$$

Let φ be a closed positive type and let $n \in \mathbb{N}$. If $(V, v) \in \mathcal{V}(\varphi)^-$ then

$$(V, [\mathsf{p}^{\mathsf{v}}(n, \varphi)](v)) \in (\overline{\mathcal{V}(\varphi)})^+ = \mathcal{R}(\varphi)^+$$

The sought inclusion $\mathcal{R}^- \subseteq \mathcal{R}^+$ follows by closeness properties.

So now with any closed type σ we have associated a unique relation $\mathcal{R}(\sigma)$ and with any closed positive type φ we have associated a unique relation $\mathcal{V}(\varphi)$. We get adequacy by a standard proof by induction on terms.

Theorem (Logical Relation Lemma)

Assume that $x_1 : \varphi_1, \ldots, x_k : \varphi_k \vdash M : \sigma$ *and let* $(V_i, v_i) \in \mathcal{R}(\varphi_i)$ *(where* V_i *is a value and* $v_i \in \mathsf{P}^!([\varphi_i])$*) for* $i = 1, \ldots, k$*. Then* $(M[V_1/x_1, \ldots, V_k/x_k], [M]x_1, \ldots, x_k(v_1, \ldots, v_k)) \in \mathcal{R}(\sigma)$.

Full abstraction for CBPV

Notice: we have full abstraction, but not full completeness.

We have defined $\iota = \mathsf{Fix}\,\zeta \cdot (1 \oplus \zeta)$. Then $[\iota]^! = \mathsf{N}$.

Let φ be a positive type, with any $a \in |[\varphi]|$, we associate a closed terms (defined by mutual induction on the size of a, without the coin construct)

- $\vdash a^0 : \varphi \multimap !\iota \multimap 1$

and if σ is any type, with any $a \in |[\sigma]|$, we associate

- $\vdash a^+ : !\iota \multimap \sigma$ (if σ positive, this is a value)
- $\vdash a^- : !\sigma \multimap !\iota \multimap 1$

Given $u \in \mathrm{P}([\varphi])$, $[a^0](u) \in \mathrm{P}(!\mathrm{N} \multimap 1)$, so it is *a priori* a powerseries on ω variables (one for each element of $|\mathrm{N}| = \mathbb{N}$).

- There is a number $l^0(a)$ which depends only on a such that, for any $u \in \mathsf{P}([\varphi])$ the power series $[a^0](u)$ depends only on its first $l^0(a)$ parameters.
- There is also a number $\mathbf{m}^0(a) \in \mathbb{N}^+$ which depend only on a (a kind of multinomial coefficient) such that the following holds.

Fact

For any $v \in \mathsf{P}^!([\varphi]^!)$, the coefficient of the monomial $\zeta_1 \cdots \zeta_{l^0(a)}$ in the power series $[a^0](v)(\zeta_1, \ldots, \zeta_{l^0(a)})$ is $\mathbf{m}^0(a)v_a$.

Of course there are similar statements for a^- and a^+.

It follows that, if $v, v' \in \mathrm{P}^!([\varphi]^!)$ are such that $v_a \neq v'_a$, the power series $[a^0](v)(\zeta_1, \ldots, \zeta_{l^0(a)})$ and $[a^0](v')(\zeta_1, \ldots, \zeta_{l^0(a)})$ are different.

So there are $p_1, \ldots, p_{l^0(a)} \in [0,1] \cap \mathbb{Q}$ such that

$$[a^0](v)(p_1, \ldots, p_{l^0(a)}) \neq [a^0](v')(p_1, \ldots, p_{l^0(a)})$$

Therefore there is a closed term $\vdash C : \varphi \multimap 1$ such that

$$[C](v) \neq [C](v')$$

and this (together with adequacy) implies full abstraction.
Note: it is only here that we use the coin_p construct, for importing the p_i's into the syntax.

Definition of these terms a^0 (example)

Take $\varphi = !\sigma$ and $a \in |[\varphi]|$, so that $a = [b_1, \ldots, b_k]$ for $b_1, \ldots, b_k \in |[\sigma]|$.

By induction we have ${b_i}^- : !\sigma \multimap !\iota \multimap 1$ and the power series $[{b_i}^-](U)$ depend only on $l^-(b_i)$ parameters.

We define $a^0 : !\sigma \multimap !\iota \multimap 1$ which depends on $l^0(a) = l^-(b_1) + \cdots + l^-(b_k)$ parameters by

$$a^0 = \lambda x^{!\sigma}\, \lambda Z^{!\iota}\, \mathrm{and}_k(\langle\langle {b_1}^- \rangle x\rangle Z^1, \ldots, \langle\langle {b_k}^- \rangle x\rangle Z^k)$$

where and_k and the Z^i's are definable terms. Intuitively, Z^i is the "projection" of Z on the parameters indexed by the integers

$$(\sum_{j=1}^{i-1} l^-(b_j)) + 1, \ldots, (\sum_{j=1}^{i-1} l^-(b_j)) + l^-(b_i)$$

We also define $a^+ : !\iota \multimap \varphi$ which depends on $l^-(b_1) + \cdots l^-(b_k) + k$ parameters by

$$a^+ = \lambda Z^{!\iota}\,(\mathsf{ncase}_k(\mathsf{der}(Z), \langle {b_1}^+ \rangle Z^1, \ldots, \langle {b_k}^+ \rangle Z^k))^!$$

where

$$\frac{\mathcal{P} \vdash M : \iota \qquad (\mathcal{P} \vdash N_i : \sigma)_{i=1}^k}{\mathcal{P} \vdash \mathsf{ncase}_k(M, N_1, \ldots, N_k) : \sigma}$$

is a case construct specialized to the type ι, easily definable using the definition $\iota = \mathsf{Fix}\,\zeta \cdot 1 \oplus \zeta$ and the general case construct of CBPV.