Lecture Notes
Part III of MPRI 2 – 02
2021 - 2022

Michele Pagani
pagani@irif.fr

February 18, 2022

Contents

List of exercises

These notes are a continuation of the lecture notes by Thomas Ehrhard, `https://www.irif.fr/~ehrhard/pub/mpri-2020-2021.pdf`.

1 The Probabilistic Extension pPCF of PCF

1.1 The Syntax of pPCF

Figure 1 sketches the probabilistic extension of PCF, written pPCF. Let Γ be a typing context and A be a type, we denote by Λ_Γ^A the set of all terms M such that $\Gamma \vdash M : A$. In the case where Γ is empty, and so the elements of Λ_Γ^A are closed, we use Λ_0^A to denote that set. A *program* will be a closed term of pPCF of ground type ι, i.e. an element of Λ_0^ι

By a simple inspection of the typing rules, the reader can check the following.

Remark: Let M be a term and Γ be a typing context. There is at most one type A such that $\Gamma \vdash M : A$.

Exercise 1. Give an example of expression M generated by the grammar of Figure 1b, such that M cannot be typed by the rules of Figure 1c. Can you find an M using only abstractions, applications and variables? and another M using only only variables, numerals, coin, branchings and $\mathsf{succ}(M)$?

Answer of Exercise 1. *The expressions* $\mathsf{succ}(\lambda x.x)$ *or* $\lambda x.\,(x)\,x$ *cannot be simply typed. By structural induction, one can prove that an expression generated with only variables, numerals,* coin*, branchings and* $\mathsf{succ}(M)$ *is always typable with the ground type* ι*.*

The *reduction relation* for evaluating pPCF terms is given in Figure 1d. In the β-rule (topmost leftmost rule of Figure 1d), the term $M\,[N/x]$ stands for M where the variable x is substituted with the term N, avoiding the capture of the free variables in N. If $M \xrightarrow{p} M'$ is the conclusion of one axiom rule (i.e. one of the rules in the first three lines of Figure 1d), then we call M the *redex* of the reduction, M' its *contractum* and p the *probability* to happen. This

$$A, B, \ldots := \iota \mid A \Rightarrow B$$

(a) The grammar of types, ι is the *ground type* of natural numbers.

$$M, N, \ldots := \underline{n} \mid x \mid \mathsf{succ}(M) \mid \mathsf{if}(M, P, z \cdot R) \mid \lambda x^A\, M \mid (M)\, N \mid \mathsf{fix}(M) \mid \mathsf{coin}$$

(b) The grammar of terms, with $n \in \mathbb{N}$, $p \in [0,1]$, and x, $y \ldots$ variables.

$$\frac{}{\Gamma \vdash \underline{n} : \iota} \qquad \frac{}{\Gamma, x : A \vdash x : A} \qquad \frac{}{\Gamma \vdash \mathsf{coin} : \iota} \qquad \frac{\Gamma \vdash M : \iota}{\Gamma \vdash \mathsf{succ}(M) : \iota}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x^A\, M : A \Rightarrow B} \qquad \frac{\Gamma \vdash M : A \Rightarrow B \qquad \Gamma \vdash N : A}{\Gamma \vdash (M)\, N : B}$$

$$\frac{\Gamma \vdash M : A \Rightarrow A}{\Gamma \vdash \mathsf{fix}(M) : A} \qquad \frac{\Gamma \vdash M : \iota \qquad \Gamma \vdash P : A \qquad \Gamma, z : \iota \vdash R : A}{\Gamma \vdash \mathsf{if}(M, P, z \cdot R) : A}$$

(c) The typing rules, with $\Gamma = y_1 : A_1, \ldots, y_k : A_k$ a typing context, $k \in \mathbb{N}$ and $y_i \neq y_j$ whenever $i \neq j$.

$$\frac{}{\left(\lambda x^A\, M\right) N \xrightarrow{1} M\,[N/x]} \qquad \frac{}{\mathsf{fix}(M) \xrightarrow{1} (M)\, \mathsf{fix}(M)}$$

$$\frac{}{\mathsf{succ}(\underline{n}) \xrightarrow{1} \underline{n+1}} \qquad \frac{}{\mathsf{if}(\underline{0}, P, z \cdot R) \xrightarrow{1} P} \qquad \frac{}{\mathsf{if}(\underline{n+1}, P, z \cdot R) \xrightarrow{1} R\,[\underline{n}/z]}$$

$$\frac{}{\mathsf{coin} \xrightarrow{1/2} \underline{0}} \qquad \frac{}{\mathsf{coin} \xrightarrow{1/2} \underline{1}}$$

$$\frac{M \xrightarrow{p} M'}{(M)\, N \xrightarrow{p} (M')\, N} \qquad \frac{M \xrightarrow{p} M'}{\mathsf{succ}(M) \xrightarrow{p} \mathsf{succ}(M')}$$

$$\frac{M \xrightarrow{p} M'}{\mathsf{if}(M, P, z \cdot R) \xrightarrow{p} \mathsf{if}(M', P, z \cdot R)}$$

(d) The reduction relation $M \xrightarrow{p} M'$, with $p \in [0,1]$, M, M' pPCF terms.

Figure 1: Résumé of pPCF.

reduction is called *weak-head reduction* (or simply weak reduction) since it always reduces the leftmost outermost redex and never reduces redexes under abstractions. We say that M is *weak-normal*, or a *value*, if there is no reduction $M \xrightarrow{p} M'$.

Lemma 1 (Substitution) *Assume* $\Gamma, x : A \vdash M : B$ *and* $\Gamma \vdash N : A$*, then* $\Gamma \vdash M\,[N/x] : B$.

Exercise 2. Prove Lemma 1.

Answer of Exercise 2. *By induction on the derivation of* $\Gamma, x : A \vdash M : B$.

Proposition 2 (Subject reduction) *Assume* $M \xrightarrow{p} M'$*. If* $\Gamma \vdash M : A$*, then* $\Gamma \vdash M' : A$.

Exercise 3. Give a proof of Proposition 2.

Answer of Exercise 3. *By structural induction on a derivation of* $M \xrightarrow{p} M'$*. All cases are easy, but for the* β *and if-reduction, where the substitution lemma should be used.*

Exercise 4. Give a counterexample to the inverse of subjection reduction, called subject expansion: give an example of reduction $M \xrightarrow{p} M'$ and of type A, environment Γ, such that $\Gamma \vdash M' : A$ but it is false that $\Gamma \vdash M : A$.

Answer of Exercise 4. $M = (\lambda x^{\iota}\,\underline{0})\,y \xrightarrow{d} \underline{0} = M'$*. We have* $\vdash M' : \iota$*, while* M *cannot be typed under the empty context.*

Exercise 5. Characterise the set of closed values of pPCF.

Answer of Exercise 5. *The closed values are either numerals or abstractions. In fact, these are normal forms for* $\xrightarrow{p}$*. Viceversa, if* M *is a closed normal form for* $\xrightarrow{p}$*, we prove that it is a numeral or an abstraction, by structural induction on* M*.*

Notice that M *cannot be a variable since it is closed, neither a fixpoint nor* coin*, otherwise it would reduce. If* $M = \mathsf{succ}(N)$ *for some closed term* N*, then* N *also must be a normal form (see rules Figure 1d) so that by induction hypothesis* N *is a numeral and hence* $M = \mathsf{succ}(N)$ *is not normal. The case* $M = \mathsf{if}(N, P, z \cdot R)$ *is similar. In case* $M = (P)\,Q$*, we have that* P *also is a closed normal form. By typing,* P *cannot be a numeral, so it is an abstraction and hence* M *is a* β*-redex.*

A *reduction sequence* from a term M to a term M' is a finite sequence $\varphi = (M_i)_{i=0}^{k}$ such that $M_0 = M$, $M_k = M'$ and for every $i < k$, $M_i \xrightarrow{p_i} M_{i+1}$ for some probability $p_i \in [0, 1]$. By inspection of the rules in Figure 1d, the reader can check that the probability p_i in $M_i \xrightarrow{p_i} M_{i+1}$ is unique, given M_i and M_{i+1}. The *length of* φ is k and the *probability* $\mathsf{p}(\varphi)$ *of* φ is the product $\prod_{i=0}^{k-1} p_i$.

We say that a term M *deterministically reduces* to a value V, written $M \to_{\mathsf{d}}{}^{*} V$, if there is a reduction sequence φ from M to V of probability 1. Notice that such a reduction is unique, i.e. any other reduction sequence starting from M is a prefix of φ. The following exercise exploits the deterministic fragment of pPCF.

Exercise 6. Define terms representing the following functions:

1. the predecessor function, i.e. a term pred such that:

$$(\mathsf{pred})\,\underline{n} \to_{\mathsf{d}}{}^{*} \begin{cases} \underline{0} & \text{if } n = 0 \\ \underline{n-1} & \text{if } n > 0 \end{cases}$$

2. the addition function, i.e. a term add such that:

$$(\mathsf{add})\,\underline{n}\,\underline{m} \to_{\mathsf{d}}{}^{*}\ \underline{n+m}$$

3. the exponential function, i.e. a term exp_2 such that:

$$(\mathsf{exp}_2)\,\underline{n} \to_{\mathsf{d}}{}^{*}\ \underline{2^n}$$

4. the comparison function, i.e. a term cmp such that:

$$(\mathsf{cmp})\,\underline{n}\,\underline{m} \to_{\mathsf{d}}{}^{*} \begin{cases} \underline{0} & \text{if } n \leq m \\ \underline{1} & \text{if } n > m \end{cases}$$

Answer of Exercise 6.

$$\mathsf{pred} = \lambda x^{\iota}\,\mathsf{if}(x, \underline{0}, z \cdot z) \qquad \mathsf{add} = \lambda x^{\iota}\,\mathsf{fix}(\lambda a^{\iota \Rightarrow \iota}\,\lambda y^{\iota}\,\mathsf{if}(y, x, z \cdot \mathsf{succ}((a)\,z)))$$

$$\mathsf{exp}_2 = \mathsf{fix}(\lambda e^{\iota \Rightarrow \iota}\,\lambda x^{\iota}\,\mathsf{if}(x, 1, z \cdot (\mathsf{add})\,(e)\,z\ (e)\,z))$$

$$\mathsf{cmp} = \mathsf{fix}(\lambda c^{\iota \Rightarrow \iota \Rightarrow \iota}\,\lambda x^{\iota}\,\lambda y^{\iota}\,\mathsf{if}(x, \underline{0}, z \cdot \mathsf{if}(y, \underline{1}, z' \cdot (c)\,z\,z')))$$

The constructor coin is the stochastic primitive of pPCF, leading to different outcomes. Given a term M and a value V, we define the set of different reduction sequences from M to V as:

$$\mathsf{Path}^{\leq n}(M, V) = \{\varphi \mid \varphi \text{ reduction sequence of length } \textit{at most } n \text{ from } M \text{ to } V\} \tag{1}$$

$$\mathsf{Path}(M, V) = \bigcup_{n \in \mathbb{N}} \mathsf{Path}^{\leq n}(M, V) \tag{2}$$

The quantity $\sum_{\varphi \in \mathsf{Path}(M,V)} \mathsf{p}(\varphi)$ defines the probability that M reduces to V. We will formalise this idea in Section 1.3 by representing the reduction relation as a discrete time Markov chain whose states are terms, weak-normal terms being stationary. Before that, let us recall some notions we need in the sequel.

1.2 Compendium of Markov Chains

Let S be a countable set and let $R \in [0,1]^{S \times S}$ be a matrix with S-indexed rows and columns. One says that R is *sub-stochastic* if $\forall i \in S, \sum_{j \in S} R_{i,j} \leq 1$, we call R *stochastic* whenever the previous sum is equal to 1 for all i. Given two such matrices R and T, their *product* RT is given by

$$\forall (i,j) \in S^2, (RT)_{i,j} = \sum_{k \in I} R_{i,k} T_{k,j}$$

which is also a (sub-)stochastic matrix. Given $n \in \mathbb{N}$, we denote by R^n the n-fold product of R, which is the diagonal matrix if $n = 0$.

A stochastic matrix represents a one-step evolution of a discrete-time Markov process. A typical example is a random-walk, as the following one.

Example. Let $S = \mathbb{N}$ and consider the following matrix over $[0,1]^{S\times S}$:

$$W_{i,j} = \begin{cases} 1 & \text{if } i = j = 0, \\ \frac{1}{2} & \text{if } i > 0 \text{ and } (j = i-1 \text{ or } j = i+1), \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Notice that W is stochastic. In fact, W defines a Markov process describing a particle travelling over $\mathbb{N}$: once the particle reaches 0, it will stay there, otherwise it will move $+1$ or -1 with equal probability $\frac{1}{2}$. The matrix W^n will then describe the state of the particle after n iterations.

Given a stochastic matrix R over S, the set of *stationary states* of R is defined by:

$$S_1^R = \{i \in S \mid R_{i,i} = 1\} \tag{4}$$

so that if $i \in S_1^R$ and $R_{i,j} \neq 0$ then $i = j$.

Let $(i,j) \in S \times S_1^R$. Then the n-indexed sequence $(R^n)_{i,j} \in [0,1]$ is monotone. Indeed, for all n we have

$$(R^{n+1})_{i,j} = \sum_{k\in S} (R^n)_{i,k} R_{k,j} \geq (R^n)_{i,j} R_{j,j} = (R^n)_{i,j}$$

So we can define a matrix $R^\infty \in [0,1]^{S\times S}$ as follows

$$(R^\infty)_{i,j} = \begin{cases} \sup_{n\in\mathbb{N}} (R^n)_{i,j} & \text{if } (i,j) \in S \times S_1^R \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

The matrix S^∞ is a sub-stochastic matrix because, given $i \in I$

$$\begin{aligned} \sum_{j\in S} (R^\infty)_{i,j} &= \sum_{j\in S_1^R} \sup_{n\in\mathbb{N}} (R^n)_{i,j} \\ &= \sup_{n\in\mathbb{N}} \sum_{j\in S_1^R} (R^n)_{i,j} \quad \text{by the monotone convergence theorem} \\ &\leq \sup_{n\in\mathbb{N}} \sum_{j\in S} (R^n)_{i,j} = 1 \end{aligned}$$

1.3 The Markov Chain of pPCF

Given a context Γ and a type A, we consider Λ_Γ^A as a set of states, and we define the reduction relation as a stochastic matrix Red given by

$$\mathsf{Red}(\Gamma, A)_{M,M'} = \begin{cases} p & \text{if } M \xrightarrow{p} M' \\ 1 & \text{if } M \text{ is a value and } M' = M \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

We also use the notation $\mathsf{Red}(A)$ for the matrix $\mathsf{Red}(\Gamma, A)$ when the typing context is empty. Also, we will simply write Red if the typing annotation is irrelevant or clear from the context. The number $\mathsf{Red}(\Gamma, A)_{M,M'}$ is the probability of M to reduce to M' in one step. Notice that all weak-normal terms are stationary states of $\mathsf{Red}(\Gamma, A)$, but not all stationary states are weak-normal terms. Therefore, if V is a weak-normal form, then the n-fold product $\mathsf{Red}(\Gamma, A)^n_{M,V}$ gives the probability that M reduces to V in at most n steps. This is precised by the following proposition (recall notation (1)).

Proposition 3 *Let M be term and V be a value in Λ_Γ^A. One has*

$$\mathsf{Red}(\Gamma, A)^n_{M,V} = \sum_{\varphi \in \mathsf{Path}^{\leq n}(M,V)} \mathsf{p}(\varphi)\,.$$

Hence, $\mathsf{Red}(\Gamma, A)^\infty_{M,V} = \sum_{\varphi \in \mathsf{Path}(M,V)} \mathsf{p}(\varphi)$.

Exercise 7. Prove Proposition 3.

Answer of Exercise 7. *By induction on n. For $n = 0$, if $M = V$, we have $\mathsf{Red}(\Gamma, A)^0_{M,V} = 1$ by definition of diagonal matrix, and $\sum_{\varphi \in \mathsf{Path}^{\leq 0}(M,V)} \mathsf{p}(\varphi) = 1$ as $\varphi \in \mathsf{Path}^{\leq 0}(M, V)$ contains the empty path. If $M \neq V$, then $\mathsf{Red}(\Gamma, A)^0_{M,V} = 0$ as well as $\mathsf{Path}^{\leq 0}(M, V)$ is empty.*

For $n > 0$, we have:

$$\begin{aligned}
\mathsf{Red}(\Gamma, A)^n_{M,V} &= \sum_{M' \in \Lambda_\Gamma^A} \mathsf{Red}(\Gamma, A)_{M,M'} \mathsf{Red}(\Gamma, A)^{n-1}_{M',V} && \text{by def.} \\
&= \sum_{M' \in \Lambda_\Gamma^A} \mathsf{Red}(\Gamma, A)_{M,M'} \Big(\sum_{\varphi \in \mathsf{Path}^{\leq n-1}(M',V)} \mathsf{p}(\varphi) \Big) && \text{by IH} \\
&= \sum_{M' \in \Lambda_\Gamma^A} \sum_{\varphi \in \mathsf{Path}^{\leq n-1}(M',V)} \mathsf{Red}(\Gamma, A)_{M,M'} \mathsf{p}(\varphi) \\
&= \sum_{\varphi \in \mathsf{Path}^{\leq n}(M,V)} \mathsf{p}(\varphi) && \text{by def.}
\end{aligned}$$

The last statement is immediate: $\mathsf{Red}(\Gamma, A)^\infty_{M,V} = \sup_n \mathsf{Red}(\Gamma, A)^n_{M,V} = \sup_n \sum_{\varphi \in \mathsf{Path}^{\leq n}(M,V)} \mathsf{p}(\varphi) = \sum_{\varphi \in \mathsf{Path}(M,V)} \mathsf{p}(\varphi)$.

Exercise 8. Does Red have stationary states that are not weak-head normal terms? and what about Red^2?

Answer of Exercise 8. *The only possible stationary states of* Red *are the weak-head normal terms: the proof is by inspection of the rules in Figure 1d, checking that whenever $M \xrightarrow{1} M'$, we have $M' \neq M$. Indeed, the case of β-reduction is not trivial (notice that in untyped λ-calculus we have that $(\lambda x\,(x)\,x)\,(\lambda x\,(x)\,x) \xrightarrow{1} (\lambda x\,(x)\,x)\,(\lambda x\,(x)\,x)$). In case of* pPCF*, if $M \xrightarrow{1} M$ by β-reduction we should have $M = (\lambda x^A\, M_1)\, M_2 = M_1[M_2/x]$. This means $M_1 = (P)\,Q$ with $P[M_2/x] = \lambda x^A\, M_1$ and $Q[M_2/x] = M_2$. Moreover, suppose that $\Gamma \vdash M : B$, so that $\Gamma, x : A \vdash M_1 : B$ and $\Gamma \vdash M_2 : A$, with $x : A$ not in Γ. We consider two cases:*

- *if $P = x$, then from $P[M_2/x] = \lambda x^A\, M_1$, we have $M_2 = \lambda x^A\, M_1$, so $A \Rightarrow B = A$, which is impossible;*
- *if $P \neq x$, then from $P[M_2/x] = \lambda x^A\, M_1$, $P = \lambda y^A\, P'$ with $P'[M_2/x] = M_1$. Since x is a free variable in M_1, this means that M_2 should have x free also. But this contradicts the fact that $\Gamma \vdash M_2 : A$, with x not in Γ.*

On the contrast, the term $\mathsf{fix}(\lambda x.x)$ *is an example of not weak-head normal term but stationary for* Red^2*, in fact* $\mathsf{fix}(\lambda x.x) \xrightarrow{1} (\lambda x.x)\,\mathsf{fix}(\lambda x.x) \xrightarrow{1} \mathsf{fix}(\lambda x.x)$.

Exercise 9. A stochastic program can have different notions of termination. Given a program M, we say that :

- *M strongly terminates* (ST), whenever the set $\bigcup_n \mathsf{Path}(M, \underline{n})$ is finite;

- *M positively almost surely terminates* (PAST), whenever the expected runtime

$$\sum_{n\in\mathbb{N}}\sum_{\varphi\in\mathsf{Path}(M,\underline{n})}\mathsf{p}(\varphi)\mathrm{length}(\varphi)$$

  is finite;

- *M almost surely terminates* (AST), whenever $\sum_n \mathsf{Red}^{\infty}_{M,\underline{n}} = 1$.

Prove that ST $\to$ PAST $\to$ AST and that no implication can be inverted. (*This exercise is not trivial. You can have a look at [1] to have some inspiration...*).

Answer of Exercise 9. ST $\to$ PAST *is immediate (notice that* $\bigcup_n \mathsf{Path}(M,\underline{n})$ *is a disjoint sum). As for* PAST $\to$ AST*. By Proposition 3 we have that:*

$$\sum_{n\in\mathbb{N}}\sum_{\varphi\in\mathsf{Path}(M,\underline{n})}\mathsf{p}(\varphi)\mathrm{length}(\varphi) = \sum_{k=1}^{\infty}(1-\sum_{n\in\mathbb{N}}\mathsf{Red}^{k}_{M,\underline{n}})$$

Then, $\sum_{k=1}^{\infty}(1-\sum_{n\in\mathbb{N}}\mathsf{Red}^{k}_{M,\underline{n}}) < \infty$ *implies* $\lim_{k\to\infty}(1-\sum_{n\in\mathbb{N}}\mathsf{Red}^{k}_{M,\underline{n}}) = 0$*, so* $\lim_{k\to\infty}\sum_{n\in\mathbb{N}}\mathsf{Red}^{k}_{M,\underline{n}} = 1$ *and we conclude as* $\lim_{k\to\infty}\sum_{n\in\mathbb{N}}\mathsf{Red}^{k}_{M,\underline{n}} = \sum_{n\in\mathbb{N}}\mathsf{Red}^{\infty}_{M,\underline{n}}$.

For the counterexamples of the inversions, consider the terms:

$$M_1 = \mathsf{fix}(\lambda x^{\iota}\,\mathsf{if}(\mathsf{coin}, x, z\cdot\underline{0}))$$
$$M_2 = \mathsf{fix}(\lambda f^{\iota\Rightarrow\iota}\,\lambda x^{\iota}\,\mathsf{if}(x, \mathsf{if}(\mathsf{coin}, \underline{0}, z\cdot(f)\,(\mathsf{exp}_2)\,x), z\cdot(f)\,z))\underline{1}$$

Clearly M_1 *is not ST. However, one can check that* M_1 *reduces to itself in* 4 *steps with probability* $\frac{1}{2}$ *and to* $\underline{0}$ *always in* 4 *steps with probability* $\frac{1}{2}$*. So that:*

$$\sum_{n\in\mathbb{N}}\sum_{\varphi\in\mathsf{Path}(M_1,\underline{n})}\mathsf{p}(\varphi)\mathrm{length}(\varphi) = \sum_{i=1}^{\infty}\frac{4i}{2^i} = 2\sum_{i=1}^{\infty}\frac{i}{2^{i-1}} = 8$$

so that M_1 *is PAST. Concerning* M_2*, one have that the expected runtime diverges as the reduction sequences are of length exponentials in the number of probabilistic choices.* M_2 *however is easily proven to be AST.*

1.4 Basic Examples

We illustrate the expressive power of pPCF by encoding in this language simple probabilistic algorithms. We explain intuitively the behaviour of these programs, but a formal proof of their soundness would require more sophisticated tools, like a denotational semantics. In fact, the next section will provide one of such semantics, based on probabilistic coherence spaces.

"Let" construction. This version of pPCF, which is globally call-by-name, offers however the possibility of handling integers in a call-by-value way. For instance, we can define the typical call-by-value "let" construction as follows

$$\mathsf{let}\ x\ \mathsf{be}\ M\ \mathsf{in}\ N = \mathsf{if}(M, N\,[\underline{0}/x]\,, z\cdot N\,[\mathsf{succ}(z)/x]) \tag{7}$$

and this construction is restricted to the type of natural numbers; it can be typed as:

$$\frac{\Gamma\vdash M:\iota \qquad \Gamma, x:\iota\vdash N:A}{\Gamma\vdash \mathsf{let}\ x\ \mathsf{be}\ M\ \mathsf{in}\ N:A}$$

The effect of this construction is that, before replacing x with M in N, M must be evaluated to a value $\underline{n}$. This is particularly important in the case where M is a probabilistic integer since this construction allows to "roll the dice" only once and then provide N with as many copies of the result as needed.

In accordance with this intuition, one can also check that the following reduction inference is derivable from the rules of Figure 1d

$$\frac{M \xrightarrow{p} M'}{\mathsf{let}\ x\ \mathsf{be}\ M\ \mathsf{in}\ N \xrightarrow{p} \mathsf{let}\ x\ \mathsf{be}\ M'\ \mathsf{in}\ N} \tag{8}$$

whereas *it is not true* that

$$\frac{M \xrightarrow{p} M'}{N\,[M/x] \xrightarrow{p} N\,[M'/x]} \tag{9}$$

Exercise 10. Prove (8) and give a counterexample to (9).

Answer of Exercise 10. *One can notice that* (8) *is an instance of the contextual if-rule in Figure 1d. A counterexample of* (9) *is for* $N = (\mathsf{add})\,xx$ *and* $M = \mathsf{coin}$. *We have* $M \xrightarrow{\frac{1}{2}} \underline{0}$, *but* $N[M/x]$ *does not reduce to* $N[\underline{0}/x] = (\mathsf{add})\,\underline{0}\,\underline{0}$. *The only one-step contractums of* $N[M/x]$ *are* $(\mathsf{add})\,\underline{0}\,\mathsf{coin}$ *and* $(\mathsf{add})\,\underline{1}\,\mathsf{coin}$, *with probability* $\frac{1}{2}$. *From there we get, in several steps, the values* $\underline{0}$ *and* $\underline{2}$, *each with probability* $\frac{1}{4}$, *and* $\underline{1}$ *with probability* $\frac{1}{2}$. *On the contrast,* $N[\underline{0}/x]$ *deterministically evaluates to* $\underline{0}$, *and* $N[\underline{1}/x]$ *deterministically evaluates to* $\underline{2}$.

We have of course

$$\frac{}{\mathsf{let}\ x\ \mathsf{be}\ \underline{n}\ \mathsf{in}\ N \xrightarrow{1} N\,[\theta(n)/x]}$$

where $\theta(0) = \underline{0}$ and $\theta(n+1) = \mathsf{succ}(\underline{n})$ (which reduces to $\underline{n+1}$ in one deterministic step) by definition of this construction.

Random Generators. Using the functions defined in Exercice 6, we can define a closed term unif_2 of type $\iota \Rightarrow \iota$ which, given an integer n, yields a uniform probability distribution on the integers $0, \ldots, 2^n - 1$:

$$\mathsf{unif}_2 = \mathsf{fix}(\lambda f^{\iota\Rightarrow\iota}\, \lambda x^{\iota}\, \mathsf{if}(x, \underline{0}, z \cdot \mathsf{if}(\mathsf{coin}, (f)\,z, z' \cdot (\mathsf{add})\,(\mathsf{exp}_2)\,z\,(f)\,z))) \tag{10}$$

Observe that, when evaluating $(\mathsf{unif}_2)\,M$ (where $\vdash M : \iota$), the term M is evaluated only once thanks to the CBV feature of the conditional construct. Indeed, we do not want the upper bound of the interval on which we produce a probability distribution to change during the computation (the result would be unpredictable!).

Exercise 11. Using the unif_2 and let constructions, define a term unif which, given an integer n, yields a *uniform probability distribution* on the integers $0, \ldots, n$.

Answer of Exercise 11. *Given* $n \in \mathbb{N}$, *the idea is to apply iteratively* unif_2 *until the result is* $\leq n$:

$$\mathsf{unif} = \lambda x^{\iota}\, \mathsf{let}\ y\ \mathsf{be}\ x\ \mathsf{in}\ \ \mathsf{fix}(\lambda f^{\iota}\, \mathsf{let}\ z\ \mathsf{be}\ \ (\mathsf{unif}_2)\,y\ \mathsf{in}\ \mathsf{if}((\mathsf{cmp})\,z\,y, z, w \cdot f))$$

One checks easily that $\vdash \mathsf{unif} : \iota \Rightarrow \iota$. *It is not hard to check that the resulting distribution is uniform (with probability* $\frac{1}{n+1}$ *for each possible result). Notice that this algorithm is almost sure terminating, but not strongly terminating, as the recursive call does not decrease any parameter (see Exercice 9). What about its expected runtime?*

Exercise 12. Define a closed term binom of type $\iota \Rightarrow \iota$ which, given an integer n, yields a (fair) *binomial distribution* out of n trials, i.e. $(\mathsf{binom})\,\underline{n}$ evaluates to $\underline{k}$ with the probability of getting k-times $\underline{1}$ in a sequence of n independent evaluations of coin.

Answer of Exercise 12.

$$\mathsf{binom} = \mathsf{fix}(\lambda f^{\iota\Rightarrow\iota}\,\lambda x^{\iota}\,\mathsf{if}(x, \underline{0}, z \cdot \mathsf{if}(\mathsf{coin}, (f)\,z, w \cdot \mathsf{succ}((f)\,z))))$$

Notice in fact that $(\mathsf{binom})\,\underline{n}$ *will perform exactly* n *recursive calls, each recursive call being preceded by exactly one evaluation of a* coin *redex. So that we can represent the evaluation tree of* $(\mathsf{binom})\,\underline{n}$ *as a complete binary tree of height* n *where each branching is labelled by either* $\underline{0}$ *(if the corresponding evaluation of* coin *returns* $\underline{0}$*) or* $\underline{1}$*. Notice that* $(\mathsf{binom})\,\underline{n}$ *evaluates to* $\underline{k}$ *exactly on the branches where we have had* k *evaluations of* coin *to* $\underline{1}$*, independently from the order of the evaluations. Now, the number of different branches of this tree having exactly* k *evaluations of* coin *to* $\underline{1}$ *(independently from their order) is given by the binomial coeffiecient* $\binom{n}{k} = \frac{n!}{k!(n-k)!}$*. Also, any branch happens with equal probability given by* $\frac{1}{2^n}$*, so that* $(\mathsf{binom})\,\underline{n}$ *evaluates to* $\underline{k}$ *with probability* $\frac{1}{2^n}\binom{n}{k}$*, this describing the binomial law.*

Las Vegas algorithms. A Las Vegas algorithm is a randomized algorithm that always gives the correct result but its running time depends on the draws from the random variables in the algorithm.

Exercise 13. One of the simplest example of a Las Vegas algorithm can be used to find zeros in a finite array: given a function $f : \mathbb{N} \to \mathbb{N}$ and $n \in \mathbb{N}$, find a $k \in \{0, \ldots, n\}$ such that $f(k) = 0$. This can be done by iterating random choices of k until we get a value such that $f(k) = 0$. Define a closed term M of type $(\iota \Rightarrow \iota) \Rightarrow \iota \Rightarrow \iota$ that implements this algorithm.

Answer of Exercise 13.

$$M = \lambda f^{\iota\Rightarrow\iota}\,\lambda x^{\iota}\,\mathsf{fix}(\lambda r^{\iota}\,\mathsf{let}\ y\ \mathsf{be}\ (\mathsf{unif})\,x\ \mathsf{in}\ \mathsf{if}((f)\,y, y, z \cdot r))$$

with $\vdash M : (\iota \Rightarrow \iota) \Rightarrow \iota \Rightarrow \iota$.

One can notice that our CBV version of the conditional is fundamental in solving Exercise 13. In fact, we strongly believe that this algorithm cannot be written with the usual version of the conditional (as in standard PCF) but we didn't really try to prove this. Do you have some hints in proving (or disproving) this conjecture?

Random-walks. We can define a random-walk over $\mathbb{N}$ as a closed term W of type $\iota \Rightarrow \iota$, meaning that a particle at position $i \in \mathbb{N}$ will evolve in one step to position $j \in \mathbb{N}$ with the probability of $(W)\,\underline{i}$ to evaluate to $\underline{j}$.

Exercise 14. Define a closed term W of type $\iota \Rightarrow \iota$ representing the random-walk of Equation (3).

Answer of Exercise 14. $W = \lambda x^{\iota}\,\mathsf{if}(x, \underline{0}, z \cdot \mathsf{if}(\mathsf{coin}, \mathsf{succ}(\mathsf{succ}(z)), z' \cdot z))$

The following exercise give you an exemple of how natural is the use of higher-order combinators for probabilistic programming. One can in fact defines an iterator of random processes independently from the specific process to iterate.

Exercise 15. Define a closed term iter of type $(\iota \Rightarrow \iota) \Rightarrow \iota \Rightarrow \iota \Rightarrow \iota$ that takes a term W representing a random-walk, a numeral $\underline{n}$ and returns a term of type $\iota \Rightarrow \iota$ simulating n-iterations of W.

Answer of Exercise 15.

$$\mathsf{iter} = \lambda w^{\iota \Rightarrow \iota}\, \mathsf{fix}(\lambda f^{\iota \Rightarrow \iota \Rightarrow \iota}\, \lambda n^{\iota}\, \lambda x^{\iota}\, \mathsf{if}(n, x, z \cdot (w)\,(f)\,zx))$$

In the above exercices, we just argue intuitively that the solutions actually satisfy the required specification. In fact, proving the soundness formally can be quite burdensome: for example, try to prove that the term $(\mathsf{iter})\, W\, \underline{n}$, with W and iter defined in resp. Exercice 14 and 15, expresses in pPCF the matrix W^n, for W given in (3). The major difficulty is that the operational semantics of pPCF, i.e. the definition of the matrix Red^{∞} is not defined compositionally but with respect to a Makov chain (section 1.3). The next section will present the probabilistic coherence spaces as a denotational model of pPCF. One major feature of a denotational semantics is to be defined compositionally on the structure of a term. The adequacy theorem will then prove the equivalence between the denotational model and the definition of Red^{∞} on ground types, so allowing for compositional proofs of soundness.

2 The standard model of pPCF in $\mathbf{Pcoh}_!$

In order to interpret pPCF in a denotational model, we need:

1. a cartesian closed category, for modelling the simply typed λ-calculus (namely: variables, abstraction and application) and its β-reduction,
2. completely partially ordered hom-sets, for modelling the fix-point operator,
3. convex hom-sets, for sampling from random data,
4. and an object of numerals, in order to express numerals, successor and our zero-test conditional.

We consider the category $\mathbf{Pcoh}_!$, which is the Kleisli category associated with the !-comonad of **Pcoh**. We recall briefly the categorical structure of $\mathbf{Pcoh}_!$ from the linear logic structure of **Pcoh**. The benefit of starting from a linear logic category is to be able to express at a denotational level the linearity of some programming primitives of pPCF, which is a remarkable feature for a denotational semantics of a probabilistic programming language.

2.1 The structure of $\mathbf{Pcoh}_!$ out of that of Pcoh

The category $\mathbf{Pcoh}_!$. An *object* of $\mathbf{Pcoh}_!$ is a PCS $X = (|X|, \mathsf{P}X)$, and the set $\mathbf{Pcoh}_!(X,Y)$ of *morphisms from X to Y* is the set of matrices $f \in \mathbb{R}^{+\mathcal{M}_{\mathrm{fin}}(|X|)\times|Y|}$ such that

$$\forall x \in \mathsf{P}X, \quad \widehat{f}(x) = f \cdot x^{(!)} = \left(\sum_{m \in \mathcal{M}_{\mathrm{fin}}(|X|)} f_{m,b} x^m \right)_{b \in |Y|} \in \mathsf{P}Y \tag{11}$$

where $x^{(!)}$ is the vector in $\mathsf{P}!X$ defined by $x^{(!)}_m = x^m = \prod_{a \in \mathsf{supp}(m)} x_a^{m(a)}$, for $m \in \mathcal{M}_{\mathrm{fin}}(|X|)$.

Notice that the sum in (11) might diverge for arbitrary matrices $f \in \mathbb{R}^{+|X|\times|Y|}$ and vectors $x \in \mathbb{R}^{+|X|}$.

Exercise 16. Recall the PCSs $\mathsf{1} = (\{*\}, [0,1])$ and $\mathsf{Bool} = \mathsf{1} \oplus \mathsf{1} = (\{\mathtt{t}, \mathtt{f}\}, \{(\lambda_\mathtt{t}, \lambda_\mathtt{f}) \in [0,1]^2 \ ; \ \lambda_\mathtt{t} + \lambda_\mathtt{f} \leq 1\})$. Give the following examples of matrices in $\mathbb{R}^{+\mathcal{M}_{\mathrm{fin}}(|\mathsf{Bool}|)\times|\mathsf{1}|}$:

1. a matrix f such that $\widehat{f}$ is a total function from $\mathbb{R}^{+|\mathsf{Bool}|}$ to $\mathbb{R}^{+|\mathsf{1}|}$, but it does not map PBool into $\mathsf{P1}$, so $f \notin \mathbf{Pcoh}_!(\mathsf{Bool}, \mathsf{1})$;
2. a matrix g such that $\widehat{g}$ is a total function from PBool to $\mathsf{P1}$, so $g \in \mathbf{Pcoh}_!(\mathsf{Bool}, \mathsf{1})$, but $\widehat{g}$ diverges on some vectors of $\mathbb{R}^{+|\mathsf{Bool}|}$ outside PBool. (*Hint: recall the example of analytic function on the booleans given in Ehrhard's notes*).

Answer of Exercise 16.

1. *Take for example the function* $f_{m,*} = \begin{cases} 2 & \text{if } m = [], \\ 0 & \text{otherwise.} \end{cases}$. *We have* $\widehat{f}(x) = 2$, *so* $\widehat{f}$ *is well-defined on the whole* $\mathbb{R}^{+2}$, *however the codomain of* $\widehat{f}$ *is ouside* $\mathsf{P1} = [0,1]$.
2. *Take for example the function*

$$g_{[\mathtt{t}^n, \mathtt{f}^k], *} = \begin{cases} 2^n & \text{if } n = k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

We have that $\widehat{g}(x) = \sum_{n=1}^{\infty} 2^n x_\mathtt{t}^n x_\mathtt{f}^n$. *If* $x \in \mathsf{PBool}$, *so* $x_\mathtt{t} + y_\mathtt{f} \leq 1$, *the maximal value of this function is reached when* $x_\mathtt{f} = 1 - x_\mathtt{t}$, *so that we can consider the function* $\lambda \mapsto \sum_{n=1}^{\infty} 2^n \lambda^n (1 -$

$\lambda)^n$, *with* $\lambda \in [0,1]$. *The quantity* $\lambda^n(1-\lambda)^n$ *is maximal for* $\lambda = \frac{1}{2}$, *so that* $\sum_{n=1}^{\infty} 2^n \lambda^n (1-\lambda)^n \leq \sum_{n=1}^{\infty} \frac{1}{2^n} \leq 1$ *and we have* $g \in \mathbf{Pcoh}_!(\mathsf{Bool}, 1)$. *On the contrast, if we take* $x = (1,1)$, *then of course* $\widehat{g}(x)$ *diverges.*

Exercise 17. Prove that $\mathbf{Pcoh}_!(X,Y) = \mathbf{Pcoh}(!X, Y)$. What is the difference between (11) and the condition necessary for inferring $f \in \mathbf{Pcoh}(!X, Y)$?

Answer of Exercise 17. $f \in \mathbf{Pcoh}(!X, Y)$ *means:*

$$\forall z \in \mathsf{P}(!X), f \cdot z \in \mathsf{P}Y$$

The above equation trivially implies (11), *as* $x^{(!)} \in \mathsf{P}(!X)$. *Let us prove the converse.*

Take $u \in \mathsf{P}(!X)$, $y \in \mathsf{P}Y$, *we have to prove that:* $\langle f \cdot u, y \rangle \leq 1$. *Notice that we have:*

$$\langle f \cdot u, y \rangle = \langle f, u \otimes y \rangle = \langle f^{\perp} \cdot y, u \rangle$$

By hypothesis we have moreover that $f^{\perp} \cdot y \in \{x^{(!)}; x \in \mathsf{P}X\}^{\perp} = (\mathsf{P}!X)^{\perp}$, *we conclude that* $\langle f^{\perp} \cdot y, u \rangle \leq 1$, *as* $u \in \mathsf{P}(!X)$.

The *identity on* X is given by the dereliction matrix $\mathsf{der}_X \in \mathbf{Pcoh}(!X, X)$:

$$\mathsf{Id}^{\mathsf{KI}}{}_{X\,m,a} = \mathsf{der}_{X\,m,a} = \begin{cases} 1 & \text{if } m = [a], \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

In fact, we have $\widehat{\mathsf{Id}^{\mathsf{KI}}{}_X}(x) = \mathsf{der}_X \cdot x^{(!)} = x$, for every $x \in \mathsf{P}X$.

The *composition* of a morphism $f \in \mathbf{Pcoh}_!(X,Y)$ and a morphism $g \in \mathbf{Pcoh}_!(Y,Z)$ is obtained via the matrix composition, the digging and the functorial promotion of **Pcoh**:

$$g \circ f = g(!f)\,\mathsf{dig}_X \tag{13}$$

where we recall that $\mathsf{dig}_X \in \mathbf{Pcoh}(!X, !!X)$ and $!f \in \mathbf{Pcoh}(!!X, !Y)$ are:

$$\mathsf{dig}_{X\,m,M} = \begin{cases} 1 & \text{if } m = \sum M, \\ 0 & \text{otherwise.} \end{cases} \qquad !f_{M,p} = \sum_{r \in L(M,p)} \frac{p!}{r!} f^r \tag{14}$$

with $f^r = \prod_{(m,b) \in \mathsf{supp}(r)} f_{m,b}^{r(m,b)}$, $p! = \prod_{a \in |X|} p(a)!$ is the multiset factorial and $L(M,p)$ is the set of all $h \in \mathcal{M}_{\mathrm{fin}}(\mathsf{supp}(M), \mathsf{supp}(p))$ such that:

$$\forall m \in \mathsf{supp}(M), M(m) = \sum_{b \in \mathsf{supp}(p)} h(m,b) \text{ and } \forall b \in \mathsf{supp}(p), p(b) = \sum_{m \in \mathsf{supp}(M)} h(m,b)$$

Exercise 18. Given $f \in \mathbf{Pcoh}_!(X,Y)$, $g \in \mathbf{Pcoh}_!(Y,Z)$ and $x \in \mathsf{P}X$, prove that $\widehat{g \circ f}(x) = \widehat{g}(\widehat{f}(x))$. (*Hint: use the categorical properties of* dig *and* $!$). Conclude that $g \circ f \in \mathbf{Pcoh}_!(X,Z)$.

Answer of Exercise 18.

$$\begin{aligned}
\widehat{g \circ f}(x) &= (g(!f)\,\mathsf{dig}_X) \cdot x^{(!)} && \textit{by definition} \\
&= (g(!f)) \cdot (\mathsf{dig}_X \cdot x^{(!)}) = (g(!f)) \cdot x^{(!)(!)} && \textit{by def. of } \mathsf{dig} \\
&= g \cdot ((!f) \cdot x^{(!)(!)}) = g \cdot (f \cdot x^{(!)})^{(!)} && \textit{by funct. of } ! \\
&= \widehat{g}(\widehat{f}(x)) && \textit{by def. of } \widehat{\ }
\end{aligned}$$

We can conclude that $g \circ f \in \mathbf{Pcoh}_!(X,Z)$*, since by hypothesis* $\widehat{f}(x) \in \mathsf{P}Y$ *and hence* $\widehat{g}(\widehat{f}(x)) \in \mathsf{P}Z$*, so condition* (11) *holds.*

We can give an explicit definition of the coefficients of a composition of $\mathbf{Pcoh}_!$ morphisms by, given $f \in \mathbf{Pcoh}_!(X,Y)$ and $g \in \mathbf{Pcoh}_!(Y,Z)$:

$$(g \circ f)_{m,c} = \sum_{[b_1,\dots,b_h] \in \mathcal{M}_{\mathrm{fin}}(|Y|)} \left(\sum_{\substack{(m_1,\dots,m_h) \text{ s.t.} \\ \sum_i m_i = m}} \prod_{i=1}^{h} f_{m_i,b_i} \right) g_{[b_1,\dots,b_h],c} \tag{15}$$

Notice that although the writing of Equation (15) depends on an explicit enumeration of the occurrences in the multiset $[b_1,\dots,b_h]$, the resulting scalar is independent from that enumeration, as the inner sum varies over all possible sequences associating the parts of a partition of m to the different b_i's.

Recall from Ehrhard's notes that a crucial feature of $\mathbf{Pcoh}_!$ is to be well-pointed, meaning that a matrix $f \in \mathbf{Pcoh}_!(X,Y)$ is univocally characterised by its behaviour as the map $\widehat{f}$:

Proposition 4 (Functional characterization) *Given two matrices* $f, f' \in \mathbf{Pcoh}_!(X,Y)$*, one has* $f = f'$ *(as matrices) iff* $\widehat{f} = \widehat{f'}$ *(as maps* $\mathsf{P}X \to \mathsf{P}Y$*).*

This property is extremely convenient, as one can define a morphism of $\mathbf{Pcoh}_!$ extensionally, without the need of giving the coefficients of the matrix associated with the morphisms. In fact, we will use this property in Figure 2c, when giving a functional definition of the denotation of the pPCF terms.

Cartesian closeness. The product of $\mathbf{Pcoh}_!$ is the same as that of $\mathbf{Pcoh}$, with the projections composed with der, that is, given a countable collection of PCSs $(X_i)_{i\in I}$, we have:

$$|\&_{i\in I} X_i| = \bigcup_{i\in I} \{i\} \times |X_i|$$

$$\mathsf{P}\&_{i\in I} X_i = \{x \in \mathbb{R}_{\geq 0}^{|\&_{i\in I} X_i|} \; ; \; \forall i \in I, (x_{(i,a)})_{a\in|X_i|} \in \mathsf{P}X_i\}$$

$$\pi_j^{\mathsf{KI}} = \pi_j \, \mathsf{der}_{\&_{i\in I} X_i} \in \mathbf{Pcoh}_!\big(\&_{i\in I} X_i, X_j\big) \quad \text{i.e. } (\pi_j^{\mathsf{KI}})_{m,a} = \begin{cases} 1 & \text{if } m = [(i,a)] \text{ and } j = i \\ 0 & \text{otherwise} \end{cases}$$

Recall that, given a collection $f_i \in \mathbf{Pcoh}_!(Y,X_i) = \mathbf{Pcoh}(!Y,X_i)$ for $i \in I$, the morphism $\langle f_i \rangle_{i\in I} \in \mathbf{Pcoh}_!(Y, \&_{i\in I} X_i)$ can be explicitly defined by:

$$(\langle f_i \rangle_{i\in I})_{m,(i,b)} = (f_i)_{m,b}$$

Exercise 19. Prove the universal property of the product in $\mathbf{Pcoh}_!$, i.e. given a collection $f_i \in \mathbf{Pcoh}_!(Y,X_i)$ for $i \in I$, the morphism $\langle f_i \rangle_{i\in I} \in \mathbf{Pcoh}_!(Y, \&_{i\in I} X_i)$ is the only one satisfying $(\pi_j^{\mathsf{KI}} \circ \langle f_i \rangle_{i\in I}) = f_j$ for every $j \in I$.

Answer of Exercise 19.

$$\begin{aligned} (\pi_j^{\mathsf{KI}} \circ \langle f_i \rangle_{i\in I}) &= \pi_j \, \mathsf{der}(!\langle f_i \rangle) \, \mathsf{dig} \\ &= \pi_j \langle f_i \rangle_{i\in I} \\ &= f_j \end{aligned}$$

The unicity follows from the unicity of $\langle f_i \rangle$ *for* π_j *and the universal property of* der *and* dig*.*

In the following we will use the infix notation $X \,\&\, Y$ and $\langle f, g \rangle$ for binary cartesian products. Also, we will denote by T the zero-ary product, which is the PCS of empty web.

Exercise 20. One might be tempted to give a different definition of projection as, for example in the binary case $X_1 \,\&\, X_2$, by giving the couple of morphisms $p_i \in \mathbf{Pcoh}_!(X_1 \,\&\, X_2, X_i)$, for $i \in \{1,2\}$, given by: $(p_i)_{m,a} = 1$, if $m(i,a) > 0$, otherwise $(p_i)_{m,a} = 0$. Prove that the triple $(X_1 \,\&\, X_2, p_1, p_2)$ does not give a product over X_1, X_2 for any PCS X_1 and X_2.

Answer of Exercise 20. *One way of arguing that $(X_1 \,\&\, X_2, p_1, p_2)$ does not define a product is by showing that it fails the universal property of products for some X_1 and X_2 and morphisms $f_i \in \mathbf{Pcoh}_!(Z, X_i)$. Take for example $X_1 = X_2 = Z = \mathbf{1} = (\{*\}, [0,1])$, and try to define a morphism $h \in \mathbf{Pcoh}_!(1, 1\&1)$ which is the pairing of (two occurrences of) the identity $\mathsf{Id}^{\mathsf{KI}}{}_1 \in \mathbf{Pcoh}_!(1,1)$, i.e. h should be the unique morphism such that $p_i \circ h = \mathsf{Id}^{\mathsf{KI}}{}_1$. Notice that:*

$$(p_i \circ h)_{[\star],\star} = h_{[\star],(i,\star)} h_{[],(3-i,\star)}$$

From the above equation and the hypothesis $p_i \circ h = \mathsf{Id}^{\mathsf{KI}}{}_1$, we get:

$$h_{[\star],(1,\star)} = h_{[],(2,\star)} = 1, \qquad\qquad h_{[\star],(2,\star)} = h_{[],(1,\star)} = 1$$

However, by considering $(p_i \circ h)_{[],\star}$, we should have $h_{[],(1,\star)} h_{[],(2,\star)} = 0$, which is in contradiction with the above equalities.

A crucial ingredient necessary to lift the closeness structure of **Pcoh** to $\mathbf{Pcoh}_!$ is the strong monoidal isomorphisms $\mathsf{mat}(\mathsf{m}^0) \in \mathbf{Pcoh}(1, !\mathsf{T})$ and $\mathsf{mat}(\mathsf{m}^2_{|\mathsf{X}_1|,|\mathsf{X}_2|}) \in \mathbf{Pcoh}(!X_1 \otimes !X_2, !(X_1 \,\&\, X_2))$, transforming the tensor product of promoted spaces into the promotion of a product:

$$\mathsf{mat}(\mathsf{m}^0)_{*,[]} = 1 \qquad\qquad \mathsf{mat}(\mathsf{m}^2)_{(m_1,m_2),q} = \begin{cases} 1 & \text{if } q(i,a) = m_i(a) \\ & \text{for } i \in \{1,2\},\ a \in |X_i|, \\ 0 & \text{otherwise.} \end{cases} \tag{16}$$

The *object of morphisms* is defined by Girard's decomposition:

$$X \Rightarrow Y = !X \multimap Y = \mathbf{Pcoh}(!X, Y) = \mathbf{Pcoh}_!(X, Y) \tag{17}$$

The *evaluation* morphism $\mathsf{ev}^{\mathsf{KI}} \in \mathbf{Pcoh}_!((X \Rightarrow Y) \,\&\, X, Y)$ and the *curryfication* $\mathsf{Cur}^{\mathsf{KI}}(f) \in \mathbf{Pcoh}_!(Z, X \Rightarrow Y)$, for every $f \in \mathbf{Pcoh}_!(Z \,\&\, X, Y)$ are then obtained by their corresponding constructions in **Pcoh** as follows:

$$\mathsf{ev}^{\mathsf{KI}} = \mathsf{ev}(\mathsf{der}_{X \Rightarrow Y} \otimes \mathsf{Id}_{!X}) \mathsf{mat}(\mathsf{m}^2_{|\mathsf{X} \Rightarrow \mathsf{Y}|,|\mathsf{X}|})^{-1} \quad \text{i.e. } \mathsf{ev}^{\mathsf{KI}}{}_{(m,p),b} = \begin{cases} 1 & \text{if } m = [(p,b)], \\ 0 & \text{otherwise.} \end{cases} \tag{18}$$

$$\mathsf{Cur}^{\mathsf{KI}}(f) = \mathsf{Cur}(f \mathsf{mat}(\mathsf{m}^2_{|\mathsf{Z}|,|\mathsf{X}|})^{-1}) \qquad\qquad \text{i.e. } \mathsf{Cur}^{\mathsf{KI}}(f)_{m,(p,b)} = f_{(m,p),b} \tag{19}$$

Notice that in the above two equations we deliberately use the relational strong monoidal isomorphisms in order to represent with a pair (m,p) of two multisets a multiset over the disjoint union of the supports of m and p.

Exercise 21. By using the properties of the morphisms of **Pcoh**, prove that:

1. $\widehat{\mathsf{ev}^{\mathsf{KI}}}(\langle f, x \rangle) = \widehat{f}(x)$
2. $(\widehat{\widehat{\mathsf{Cur}^{\mathsf{KI}}(f)}}(x))(z) = \widehat{f}(\langle x, z \rangle)$

Answer of Exercise 21.

$$\begin{aligned}
\widehat{\mathsf{ev}^{\mathsf{Kl}}}(\langle f, x\rangle) &= (\mathsf{ev}(\mathsf{der} \otimes !X)\mathsf{mat}(\mathsf{m}^2)^{-1}) \cdot (\langle f, x\rangle)^{(!)} \\
&= (\mathsf{ev}(\mathsf{der} \otimes !X)) \cdot (\mathsf{mat}(\mathsf{m}^2)^{-1} \cdot (\langle f, x\rangle)^{(!)}) \\
&= (\mathsf{ev}(\mathsf{der} \otimes !X)) \cdot (f^{(!)} \otimes x^{(!)}) \\
&= \mathsf{ev} \cdot ((\mathsf{der} \otimes !X) \cdot (f^{(!)} \otimes x^{(!)})) \\
&= \mathsf{ev} \cdot (f \otimes x^{(!)}) \\
&= f \cdot x^{(!)} \\
&= \widehat{f}(x)
\end{aligned}$$

$$\begin{aligned}
(\widehat{\widehat{\mathsf{Cur}^{\mathsf{Kl}}}(f)}(x))(z) &= ((\mathsf{Cur}(f\mathsf{mat}(\mathsf{m}^2_{|\mathsf{Z}|,|\mathsf{X}|})^{-1})) \cdot x^{(!)}) \cdot z^{(!)} \\
&= (f\mathsf{mat}(\mathsf{m}^2_{|\mathsf{Z}|,|\mathsf{X}|})^{-1}) \cdot (x^{(!)} \otimes z^{(!)}) \\
&= f \cdot \langle x, z\rangle^{(!)} \\
&= \widehat{f}(\langle x, z\rangle)
\end{aligned}$$

Cpo-enriched hom-sets. A categorical model of a typed programming language associates the types with objects of the category and the programs with morphisms from the input type interpretation to the output type interpretation. Some programming primitives may need some structure on the hom-sets, for example the fix-point operator (giving recursion) needs the hom-set to be cpo-enriched.

There is actually an equivalence between the sets $\mathsf{P}X$ associated with PCSs X and the sets of the morphisms of **Pcoh** and $\mathbf{Pcoh}_!$. Namely, given a PCS X, $\mathsf{P}X$ is equivalent to the set $\mathbf{Pcoh}(1, X)$ as well as $\mathbf{Pcoh}_!(\mathsf{T}, X)$. Viceversa, the sets $\mathbf{Pcoh}(X, Y)$ and $\mathbf{Pcoh}_!(X, Y)$ are equivalent respectively to the sets $\mathsf{P}(X \multimap Y)$ and $\mathsf{P}(X \Rightarrow Y)$. Henceforth, studying the structure of $\mathsf{P}X$ for generic X corresponds to study the structure of the hom-sets of the categories **Pcoh** and $\mathbf{Pcoh}_!$, which is what we will do in this subsection.

Given a PCS X, recall that $\mathsf{P}X$ is endowed with the partial order defined component-wise:

$$x \leq x' \text{ iff } \forall a \in |X|, x_a \leq x'_a \tag{20}$$

Recall that the vectors in $\mathsf{P}X$ are bounded in a fixed direction, i.e. $\forall a \in |X|, \exists \lambda \in \mathbb{R}_{\geq 0}, \forall x \in \mathsf{P}X, x_a \leq \lambda$. Therefore, giving an increasing ω-*chain*, i.e. a countable increasing family of vectors in $\mathsf{P}X$, its limit can be defined as the component-wise supremum:

$$\text{given } (x_i)_{i\in\mathbb{N}} \in \mathsf{P}X \text{ s.t. } x_i \leq x_{i+1}, \text{ we define } \sup_i(x_i) = \big(\sup_i(x_{ia})\big)_{a\in|X|} \tag{21}$$

The following proposition states that $\mathbf{Pcoh}_!$ behaves well with such a notion of limit.

Proposition 5 (Scott continuity) *Let X, Y be PCSs, $(x_i)_{i\in\mathbb{N}} \in \mathsf{P}X$ be an increasing ω-chain,*

1. $\sup_i(x_i) \in \mathsf{P}X$,
2. *for every $f \in \mathbf{Pcoh}_!(X, Y)$, $(\widehat{f}(x_i))_{i\in\mathbb{N}}$ is increasing and $\widehat{f}(\sup_i(x_i)) = \sup_i\big(\widehat{f}(x_i)\big)$.*

Exercise 22. Prove Proposition 5.

Answer of Exercise 22. *For 1, given $y \in \mathsf{P}X^{\perp}$, we have:* $\langle \sup_i(x_i), y\rangle = \sup_i \langle x_i, y\rangle \leq 1$.

For 2, notice that $x_i \leq x_{i+1}$ implies $x_i^{(!)} \leq x_{i+1}^{(!)}$ and hence $f \cdot x_i^{(!)} \leq f \cdot x_{i+1}^{(!)}$ as addition and multiplication (with positive reals) are monotone increasing. We conclude that $\widehat{f}$ also is monotone increasing and so $(\widehat{f}(x_i))_{i\in\mathbb{N}}$ is an increasing ω-chain. Similarly, $\widehat{f}(\sup_i(x_i)) = \sup_i\big(\widehat{f}(x_i)\big)$ is an immediate consequence of Equation 11 and the fact that addition and multiplication (with positive reals) commutes with suprema.

An immediate consequence of the component-wise definition in (21) is that, given two ω-chains $(x_i)_{i\in\mathbb{N}} \in \mathsf{P}X$ and $(y_j)_{j\in\mathbb{N}} \in \mathsf{P}Y$, we have:

$$\langle \sup_{i\in\mathbb{N}} x_i, \sup_{j\in\mathbb{N}} y_j\rangle = \sup_{i\in\mathbb{N}}\sup_{j\in\mathbb{N}}\langle x_i, y_j\rangle = \sup_{j\in\mathbb{N}}\sup_{i\in\mathbb{N}}\langle x_i, y_j\rangle = \sup_{i\in\mathbb{N}}\langle x_i, y_i\rangle \in \mathsf{P}(X \,\&\, Y) \tag{22}$$

Exercise 23. Given increasing $(f_i)_{i\in\mathbb{N}} \in \mathsf{P}(X \Rightarrow Y)$ and $(x_i)_{i\in\mathbb{N}} \in \mathsf{P}X$, prove that:

$$\widehat{(\sup_i f_i)}(\sup_i(x_i)) = \sup_i(\widehat{f_i}(x_i)).$$

Answer of Exercise 23. *By Exercice 21, Equation* (22) *and Proposition 5:*

$$\widehat{(\sup_i f_i)}(\sup_i(x_i)) = \widehat{\mathsf{ev}^{\mathsf{Kl}}}(\sup_i\langle f_i, x_i\rangle) = \sup_i \widehat{\mathsf{ev}^{\mathsf{Kl}}}(\langle f_i, x_i\rangle) = \sup_i(\widehat{f_i}(x_i))$$

The two properties of Proposition 5 justifies the standard definition of the least fix-point operator for $\mathbf{Pcoh}_!$. Given a PCS X, we set $\mathsf{Y}_n \in \mathbf{Pcoh}_!(X \Rightarrow X, X)$ for any $n \in \mathbb{N}$ and its limit $\mathsf{Y} \in \mathbf{Pcoh}(X \Rightarrow X, X)$ as:

$$\mathsf{Y}_0 = 0, \qquad \mathsf{Y}_{n+1} = \mathsf{ev}^{\mathsf{Kl}} \circ \langle \mathsf{Id}, \mathsf{Y}_n\rangle, \qquad \mathsf{Y} = \sup_n \mathsf{Y}_n.$$

Exercise 24.

1. Prove that $(\mathsf{Y}_n)_n$ is a increasing chain in $\mathsf{P}((X \Rightarrow X) \Rightarrow X)$, so that $\mathsf{Y} = \sup_n \mathsf{Y}_n$ is well-defined.
2. Prove that, for any $n \in \mathbb{N}$, any $f \in \mathsf{P}(X \Rightarrow X)$, $\widehat{\mathsf{Y}}_{n+1}(f) = \widehat{f}(\widehat{\mathsf{Y}}_n(f))$. Conclude the fix-point equation: $\widehat{\mathsf{Y}}(f) = \widehat{f}(\widehat{\mathsf{Y}}(f))$.

Answer of Exercise 24.

1. *Remark that $\circ$ and pairing are monotone increasing. Therefore, by induction on n, we have $\mathsf{Y}_n \leq \mathsf{Y}_{n+1}$. The base of induction is trivial, since 0 is the minimum.*
2. *By definition*

$$\begin{aligned}
\widehat{\mathsf{Y}}_{n+1}(f) &= \widehat{(\mathsf{ev}^{\mathsf{Kl}} \circ \langle \mathsf{Id}, \mathsf{Y}_n\rangle)}(f) && \text{by definition}\\
&= \big(\widehat{\mathsf{ev}^{\mathsf{Kl}}}(\widehat{\langle \mathsf{Id}, \mathsf{Y}_n\rangle}(f))\big) && \text{by Ex. 18}\\
&= \big(\widehat{\mathsf{ev}^{\mathsf{Kl}}}(\langle f, \widehat{\mathsf{Y}_n}(f)\rangle)\big) && \text{by def. pairing}\\
&= \widehat{f}(\widehat{\mathsf{Y}}_n(f)) && \text{by Ex 21}
\end{aligned}$$

The fix-point equation is a trivial consequence of the above equality and Proposition 5.

This means that the standard least fix-point operator Y can be described as a power series, which is not completely obvious at first sight.

Convex hom-sets. Random data will be denoted by barycentric sums: for example, if $x, x' \in \mathsf{P}X$ will be the denotation of two values of some type X, and $\lambda \in [0,1]$, then $\lambda x + (1-\lambda)x'$ will represent a random program evaluating with probability λ to x, and with probability $(1-\lambda)$ to x'. The following proposition states then the PCSs are closed under barycentric sums:

Proposition 6 (Convexity) *Let X be a PCS, $\forall (x_i)_{i\in I} \in \mathsf{P}X$, $\forall (\lambda_i)_{i\in I} \in [0,1]$ s.t. $\sum_{i\in I} \lambda_i = 1$, we have: $\sum_{i\in I} \lambda_i x_i \in \mathsf{P}X$.*

Exercise 25. Prove Proposition 6.

Answer of Exercise 25. *Given $y \in \mathsf{P}X^{\perp}$, we have: $\langle \sum_i \lambda_i x_i, y\rangle = \sum_i \lambda_i \langle x_i, y\rangle \leq 1$.*

The object of numerals. The object of numerals is an object N associated with the ground type ι of natural numbers and having enough structure to express the basic operations of pPCF over ι: constants, successor and conditionals based on a zero testing.

In $\mathbf{Pcoh}_!$, one can define this object from standard constructions in the linear logic category $\mathbf{Pcoh}$. Namely, we let N to be the countable coproduct of the tensor unit:

$$\mathsf{N} = \bigoplus_{i\in\mathbb{N}} 1, \qquad \text{i.e. } \mathsf{N} = \left(\mathbb{N}, \left\{v \in [0,1]^{\mathbb{N}} ; \sum_{i\in\mathbb{N}} v_i \leq 1\right\}\right) \tag{23}$$

First of all, notice that a numeral can be associated with a constant function $\overline{n}_X \in \mathbf{Pcoh}_!(X, \mathsf{N})$ by the weakening $\mathsf{w}_X \in \mathbf{Pcoh}(!X, 1)$ and the injections $\overline{\pi_n} \in \mathbf{Pcoh}(1, \mathsf{N})$:

$$\overline{n}_X = \overline{\pi_n}\,\mathsf{w}_X \qquad \text{i.e. } \overline{n_X}_{m,k} = \begin{cases} 1 & \text{if } m = [] \text{ and } k = n, \\ 0 & \text{otherwise,} \end{cases} \tag{24}$$

Another major benefit of this definition is to lift the structure of !-coalgebra of the tensor unit 1 to N, by the morphism $h_{\mathsf{N}} : \mathbf{Pcoh}(\mathsf{N}, !\mathsf{N})$:

$$(h_{\mathsf{N}})_{n,m} = \begin{cases} 1 & \text{if } m = k[n] \text{ for some } k \in \mathbb{N} \\ 0 & \text{otherwise.} \end{cases} \tag{25}$$

The following exercise shows that h_{N} allows to duplicate and erase "true" natural numbers e_n but not general elements of PN which can be considered as "computations" and not as "values".

Exercise 26. Prove that for any $n \in \mathbb{N}$, $h_{\mathsf{N}} \cdot e_n = e_n^{(!)}$. Moreover, observe that it is not true however that $\forall u \in \mathsf{PN}\ h_{\mathsf{N}} \cdot u = u^{(!)}$, in fact what we have is: $h_{\mathsf{N}} \cdot u = \sum_{n\in\mathbb{N}} u_n {e_n}^{(!)}$

Answer of Exercise 26. *In fact, if $m = k[n]$ for some k, then $(h_{\mathsf{N}} \cdot e_n)_m = 1 = (e_n)^m = (e_n^{(!)})_m$. Otherwise, if $m = [n'] + m'$ for some $n' \neq n$, then $(h_{\mathsf{N}} \cdot e_n)_m = 0 = (e_n)_{n'}(e_n)^{m'} = {e_n^{(!)}}_{[n']+m'}$.*

As for the second statement, consider $u = \frac{1}{2}e_0 + \frac{1}{2}e_1$. We have that $(h_{\mathsf{N}} \cdot u)_{[0,1]} = 0$ while $u^{(!)}_{[0,1]} = \frac{1}{4}$. In general, we have that $(h_{\mathsf{N}} \cdot u) = h_{\mathsf{N}} \cdot (\sum_{n\in\mathbb{N}} u_n e_n) = \sum_{n\in\mathbb{N}} u_n (h_{\mathsf{N}} \cdot e_n) = \sum_{n\in\mathbb{N}} u_n {e_n}^{(!)}$.

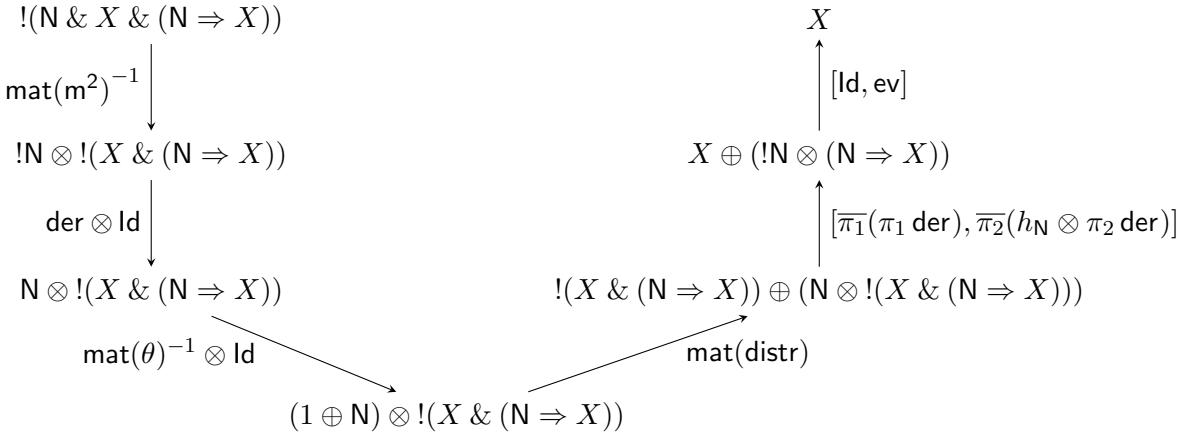
Finally, N enjoys the strong isos $\mathsf{mat}(\theta) \in \mathbf{Pcoh}(1 \oplus \mathsf{N}, \mathsf{N})$ given by the relation θ:

$$\begin{array}{rccc} \theta : & |1 \oplus \mathsf{N}| & \to & |\mathsf{N}| \\ & (1, *) & \mapsto & 0 \\ & (2, n) & \mapsto & n+1 \end{array}$$

The successor morphism $\overline{\mathsf{suc}} \in \mathbf{Pcoh}_!(\mathsf{N},\mathsf{N})$ is then the composition of dereliction, the right injection and the above isomorphism:

$$\overline{\mathsf{suc}} = \mathsf{mat}(\theta)\overline{\pi_2}\,\mathsf{der} \quad \text{i.e. } \overline{\mathsf{suc}}_{m,n} = \begin{cases} 1 & \text{if } n>0 \text{ and } m=[n-1], \text{ or } n=0 \text{ and } m=[0], \\ 0 & \text{otherwise.} \end{cases}$$

Our conditional, which gathers a zero-test and a predecessor operation, is based on the inverse of $\mathsf{mat}(\theta)$ and the !-coalgebra morphism h_{N}. We define $\overline{\mathsf{If}} \in \mathbf{Pcoh}_!(\mathsf{N} \,\&\, X \,\&\, (\mathsf{N} \Rightarrow X), X)$ by:



where we omit to explicit the associativity and neutrality isos of $\otimes$, $\mathsf{mat}(\mathsf{distr})_{X_1,X_2,Z} \in \mathbf{Pcoh}((X_1 \oplus X_2) \otimes Z, (X_1 \otimes Z) \oplus (X_2 \otimes Z))$ is the strong isos of the distributive lax of $\otimes$ over $\oplus$ given by the following relation:

$$\begin{array}{rccl} \mathsf{distr}: & |(X_1 \oplus X_2) \otimes Z| & \to & |(X_1 \otimes Z) \oplus (X_2 \otimes Z)| \\ & ((i,a),b) & \mapsto & (i,(a,b)) \end{array}$$

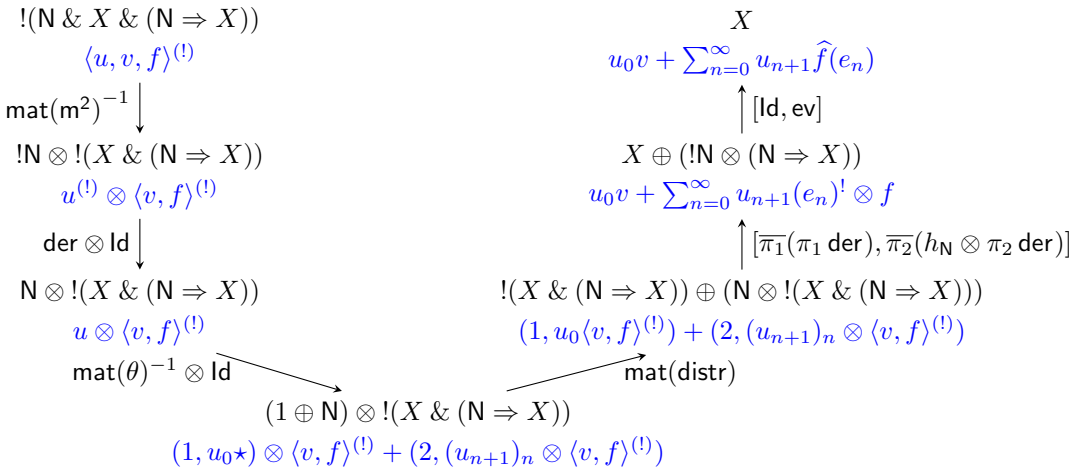
with also $\overline{\pi_i} \in \mathbf{Pcoh}(X_i, X_1 \oplus X_2)$ being the injection of the coproduct $X_1 \oplus X_2$, for $i \in \{1,2\}$, and $[f_1, f_2] \in \mathbf{Pcoh}(X_1 \oplus X_2, Z)$ being the copairing of $f_i \in \mathbf{Pcoh}(X_i, Z)$.

In fact, the explicit definition of $\overline{\mathsf{If}} \in \mathbf{Pcoh}_!(\mathsf{N} \,\&\, X \,\&\, (\mathsf{N} \Rightarrow X), X)$ as a matrix is:

$$\overline{\mathsf{If}}_{(m_1,m_2,m_3),a} = \begin{cases} 1 & \text{if } m_1=[0],\ m_2=[a],\ m_3=[], \\ 1 & \text{if } m_1=[n+1],\ m_2=[],\ m_3=[([n^k],a)] \text{ for } k \geq 0, \\ 0 & \text{otherwise} \end{cases} \tag{26}$$

Exercise 27. Given $u \in \mathsf{PN}$, $v \in \mathsf{P}X$ and $f \in \mathsf{P}(\mathsf{N} \Rightarrow X)$, prove that $\widehat{\overline{\mathsf{If}}}(u,v,f) = u_0 v + \sum_{n=0}^{\infty} u_{n+1} \widehat{f}(e_n)$.

Answer of Exercise 27. *We sketch the proof by travelling through the diagram defining $\overline{\mathsf{If}}$, every single step being an easy consequence of the definitions.*



2.2 The interpretation pPCF

Section 2.1 has detailed all basic bricks of $\mathbf{Pcoh}_!$ that we can assemble now in Figure 2, defining the standard model of pPCF.

Subfigure 2a gives the denotation of types of pPCF and, given a context $\Gamma = x_1 : A_1, \dots, x_n : A_n$, a type A and a term M such that $\Gamma \vdash M : A$, then Subfigure 2b defines by structural induction on M the denotation of M as:

$$[\![M]\!]_\Gamma \in \mathbf{Pcoh}_!([\![\Gamma]\!], [\![A]\!]) = \mathbf{Pcoh}(![\![\Gamma]\!], [\![A]\!]) \tag{27}$$

where $[\![\Gamma]\!] = [\![A_1]\!] \,\&\, \cdots \,\&\, [\![A_k]\!]$. Moving from $\mathbf{Pcoh}_!$ to $\mathbf{Pcoh}$ means swapping between the denotation of M seen as a morphism in a cartesian closed category with domain the interpretation of the input types and this same denotation of M seen as a morphism in a linear logic category with domain the *promotion* of the denotation of the input types.

Recall that Proposition 4 states that the analytical maps between PCSs are univocally characterised by their functional behaviour. This allows for a further equivalent definition of the semantics of M as the set-theoretical map:

$$\widehat{[\![M]\!]_\Gamma} : \mathsf{P}[\![A_1]\!] \times \cdots \times \mathsf{P}[\![A_n]\!] \to \mathsf{P}[\![A]\!] \tag{28}$$

which is detailed by Figure 2c.

Exercise 28. Check the equations of Figure 2c with the definitions in Figure 2b.

Answer of Exercise 28. *The* If *equation is a consequence of Exercise 27, the abstraction and application cases follow from Exercise 21. The fix-point equation is from Exercise 24, and all other cases can be easily checked from the definitions in Figure 2b.*

Exercise 29. Compute the functional behaviour of the denotation of the terms pred, add, exp_2, cmp defined in Exercise 6.

Answer of Exercise 29.

Computation of $[\![\mathsf{pred}]\!]$. *We have:*

$$\begin{aligned}
\widehat{[\![\mathsf{pred}]\!]}(u) &= [\![\lambda x^\iota\, \mathsf{if}\widehat{(x, \underline{0}, z \cdot z)}]\!](u) \\
&= [\![\mathsf{if}\widehat{(x, \underline{0}, z \cdot z)}]\!]_{x:\iota}(u) \\
&= u_0 e_0 + \sum_{n=0}^{\infty} u_{n+1} e_n
\end{aligned}$$

$$[\![\iota]\!] = \mathsf{N} \qquad\qquad [\![A \Rightarrow B]\!] = [\![A]\!] \Rightarrow [\![B]\!]$$

(a) The interpretation of types.

$$[\![x]\!]_{\Gamma,x:A} = \Gamma \,\&\, A \xrightarrow{\pi^{\mathsf{Kl}}_{n+1}} A \qquad [\![\lambda x^A\, M]\!]_\Gamma = \Gamma \xrightarrow{\mathsf{Cur}^{\mathsf{Kl}}([\![M]\!]_{\Gamma,x:A})} A \Rightarrow B$$

$$[\![(M)\,N]\!]_\Gamma = \Gamma \xrightarrow{\langle [\![M]\!]_\Gamma, [\![N]\!]_\Gamma\rangle} (A \Rightarrow B) \,\&\, A \xrightarrow{\mathsf{ev}^{\mathsf{Kl}}} B \qquad [\![\mathsf{fix}(M)]\!]_\Gamma = \Gamma \xrightarrow{[\![M]\!]_\Gamma} (A \Rightarrow A) \xrightarrow{\mathsf{Y}} A$$

$$[\![\underline{n}]\!]_\Gamma = \Gamma \xrightarrow{\overline{n}} \mathsf{N} \qquad [\![\mathsf{succ}(M)]\!]_\Gamma = \Gamma \xrightarrow{[\![M]\!]_\Gamma} \mathsf{N} \xrightarrow{\overline{\mathsf{succ}}} \mathsf{N} \qquad [\![\mathsf{coin}]\!]_\Gamma = \Gamma \xrightarrow{\frac{1}{2}[\![\underline{0}]\!]_\Gamma + \frac{1}{2}[\![\underline{1}]\!]_\Gamma} \mathsf{N}$$

$$[\![\mathsf{if}(P, Q, v \cdot R)]\!]_\Gamma = \Gamma \xrightarrow{\langle [\![P]\!]_\Gamma, [\![Q]\!]_\Gamma, \mathsf{Cur}^{\mathsf{Kl}}([\![R]\!]_{\Gamma,v:\mathsf{N}})\rangle} \mathsf{N} \,\&\, A \,\&\, (\mathsf{N} \Rightarrow A) \xrightarrow{\overline{\mathsf{If}}} A$$

(b) The denotation of a term $\Gamma \vdash M : A$ seen as a morphism $[\![M]\!]_\Gamma \in \mathbf{Pcoh}_!([\![\Gamma]\!], [\![A]\!])$. In the above diagrams, we avoid the double-bracket notation $[\![A]\!]$ for the denotation of a type A, and for environments as well. Also, the morphisms and the composition live in the category $\mathbf{Pcoh}_!$, whose structure has been detailed in Section 2.1.

$$\widehat{[\![x_i]\!]_\Gamma}(\vec{u}) = u_i$$

$$\widehat{[\![\underline{n}]\!]_\Gamma}(\vec{u}) = e_n$$

$$\widehat{[\![\mathsf{succ}(M)]\!]_\Gamma}(\vec{u}) = \sum_{n=0}^{\infty} \big(\widehat{[\![M]\!]_\Gamma}(\vec{u})\big)_n e_{n+1}$$

$$\widehat{[\![\mathsf{coin}]\!]_\Gamma}(\vec{u}) = \frac{1}{2}e_0 + \frac{1}{2}e_1$$

$$\widehat{[\![\mathsf{if}(P, Q, z \cdot R)]\!]_\Gamma}(\vec{u}) = (\widehat{[\![P]\!]_\Gamma}(\vec{u}))_0 \widehat{[\![Q]\!]_\Gamma}(\vec{u}) + \sum_{n=0}^{\infty} (\widehat{[\![P]\!]_\Gamma}(\vec{u}))_{n+1} \widehat{[\![R]\!]_{\Gamma,z:\iota}}(\vec{u}, e_n)$$

$$\big(\widehat{[\![\lambda x^A\, P]\!]_\Gamma}(\vec{u})\big)(u) = \widehat{[\![P]\!]_{\Gamma,x:A}}(\vec{u}, u)$$

$$\widehat{[\![(P)\,Q]\!]_\Gamma}(\vec{u}) = \widehat{[\![P]\!]_\Gamma}(\vec{u})(\widehat{[\![Q]\!]_\Gamma}(\vec{u}))$$

$$\widehat{[\![\mathsf{fix}(P)]\!]_\Gamma}(\vec{u}) = \widehat{\mathsf{Y}}(\widehat{[\![P]\!]_\Gamma}(\vec{u}))$$

(c) The denotation of a term $\Gamma \vdash M : A$ seen as a function $\widehat{[\![M]\!]_\Gamma} : \prod_{i=1}^n \mathsf{P}[\![A_i]\!] \to \mathsf{P}[\![A]\!]$. The writing $\vec{u}$ stands for $(u_1, \ldots, u_n) \in \mathsf{P}[\![A_1]\!] \times \cdots \times \mathsf{P}[\![A_n]\!]$.

Figure 2: The standard model of pPCF in $\mathbf{Pcoh}_!$.

Computation of $[\![\mathsf{add}]\!]$. *Henceforth, let us ease the notation by adopting the following conventions: given a matrix $f \in \mathbf{Pcoh}_!(X,Y)$, we will denote by the same writing f the function $\widehat{f}$ from $Cl(X)$ to $Cl(Y)$ associated with f. We also adopt the standard conventions of λ-calculus, so that $(f)uv$ denotes $\widehat{\left(\widehat{f}(u)\right)}(v)$.*

With these notations, we have:

$$\begin{aligned}([\![\mathsf{add}]\!])uv &= ([\![\lambda x^\iota\, \mathsf{fix}(\lambda a^{\iota\Rightarrow\iota}\, \lambda y^\iota\, \mathsf{if}(y,x,z\cdot\mathsf{succ}((a)\,z)))]\!])uv\\ &= \big([\![\mathsf{fix}(\lambda a^{\iota\Rightarrow\iota}\, \lambda y^\iota\, \mathsf{if}(y,x,z\cdot\mathsf{succ}((a)\,z)))]\!]_{x:\iota}u\big)v\end{aligned}$$

Now we have a fix-point operator, let us then compute the semantics of the body of the the fix-point operator, which depends on u:

$$\begin{aligned}(\varphi_u)fv &= ([\![\lambda a^{\iota\Rightarrow\iota}\, \lambda y^\iota\, \mathsf{if}(y,x,z\cdot\mathsf{succ}((a)\,z))]\!]_{x:\iota})ufv\\ &= ([\![\mathsf{if}(y,x,z\cdot\mathsf{succ}((a)\,z))]\!]_{x:\iota,a:\iota\Rightarrow\iota,y:\iota})ufv\\ &= v_0u + \sum_{n=0}^{\infty} v_{n+1}\sum_{k=0}^{\infty}\left((f)e_n\right)_k e_{k+1}\end{aligned}$$

By Exercise 24 we have that $(\mathsf{Y})\varphi_u = (\varphi_u)(\mathsf{Y})\varphi_u$, this together with the two above equations, where f is replaced by $(\mathsf{Y})\varphi_u$, we have:

$$\begin{aligned}([\![\mathsf{add}]\!])uv &= ((\mathsf{Y})\varphi_u)v\\ &= (\varphi_u)(\mathsf{Y})\varphi_u v\\ &= v_0u + \sum_{n=0}^{\infty} v_{n+1}\sum_{k=0}^{\infty}\left((\mathsf{Y})\varphi_u e_n\right)_k e_{k+1}\end{aligned}$$

We have then to compute $(\mathsf{Y})\varphi_u e_n$. By the above equations we get:

$$\begin{aligned}(\mathsf{Y})\varphi_u e_n &= (\varphi_u)(\mathsf{Y})\varphi_u e_n\\ &= (e_n)_0u + \sum_{h=0}^{\infty}(e_n)_{h+1}\sum_{k=0}^{\infty}\left((\mathsf{Y})\varphi_u e_h\right)_k e_{k+1}\\ &= \begin{cases} u & \text{if } n=0,\\ \sum_{k=0}^{\infty}\left((\mathsf{Y})\varphi_u e_{n-1}\right)_k e_{k+1} & \text{if } n>0.\end{cases}\\ &= \sum_{k=0}^{\infty} u_k e_{k+n}\end{aligned}$$

So, eventually, we get:

$$\begin{aligned}([\![\mathsf{add}]\!])uv &= v_0u + \sum_{n=0}^{\infty} v_{n+1}\sum_{k'=0}^{\infty}\left(\sum_{k=0}^{\infty} u_k e_{k+n}\right)_{k'} e_{k'+1}\\ &= v_0u + \sum_{n=0}^{\infty} v_{n+1}\sum_{k=0}^{\infty} u_k e_{k+n+1}\\ &= v_0(\sum_{k=0}^{\infty} u_k e_{k+0}) + \sum_{n=1}^{\infty} v_n\sum_{k=0}^{\infty} u_k e_{k+n}\\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} v_n u_k e_{k+n}\end{aligned}$$

Computation of $[\![\mathsf{exp}_2]\!]$. *TODO.*

Computation of $[\![\mathsf{cmp}]\!]$. *TODO.*

Exercise 30. Compute the functional behaviour of the denotation of the random generators unif_2, unif and binom defined in Exercise 11 and 12.

Answer of Exercise 30.

Computation of $[\![\mathsf{binom}]\!]$. *We adopt the notational conventions used in the solution of Exercise 29. We have:*

$$([\![\mathsf{binom}]\!])u = ([\![\mathsf{fix}(\lambda f^{\iota\Rightarrow\iota}\,\lambda x^{\iota}\,\mathsf{if}(x, \underline{0}, z\cdot\mathsf{if}(\mathsf{coin}, (f)\,z, w\cdot\mathsf{succ}((f)\,z))))]\!])u \tag{29}$$

We have a fix-point operator, let us then compute the semantics of the body of the the fix-point operator:

$$\begin{aligned}
(\varphi)fu &= ([\![\lambda f^{\iota\Rightarrow\iota}\,\lambda x^{\iota}\,\mathsf{if}(x, \underline{0}, z\cdot\mathsf{if}(\mathsf{coin}, (f)\,z, w\cdot\mathsf{succ}((f)\,z)))]\!])fu\\
&= ([\![\mathsf{if}(x, \underline{0}, z\cdot\mathsf{if}(\mathsf{coin}, (f)\,z, w\cdot\mathsf{succ}((f)\,z)))]\!]_{f:\iota\Rightarrow\iota, x:\iota})fu\\
&= u_0e_0 + \sum_{n=0}^{\infty} u_{n+1}([\![\mathsf{if}(\mathsf{coin}, (f)\,z, w\cdot\mathsf{succ}((f)\,z))]\!]_{f:\iota\Rightarrow\iota, x:\iota, z:\iota})fue_n\\
&= u_0e_0 + \sum_{n=0}^{\infty} u_{n+1}\frac{1}{2}\left((f)e_n + \sum_{k=0}^{\infty}((f)e_n)_ke_{k+1}\right)\\
&= u_0e_0 + \sum_{n=0}^{\infty} u_{n+1}\frac{1}{2}\sum_{k=0}^{\infty}((f)e_n)_k(e_k + e_{k+1})
\end{aligned}$$

By Exercise 24 we have that $(\mathsf{Y})\varphi = (\varphi)(\mathsf{Y})\varphi$, this together with the two above equations, where f is replaced by $(\mathsf{Y})\varphi$, we have:

$$\begin{aligned}
([\![\mathsf{binom}]\!])u &= ((\mathsf{Y})\varphi)u\\
&= (\varphi)(\mathsf{Y})\varphi u\\
&= u_0e_0 + \sum_{n=0}^{\infty} u_{n+1}\frac{1}{2}\sum_{k=0}^{\infty}((\mathsf{Y})\varphi e_n)_k(e_k + e_{k+1})\\
&= u_0e_0 + \sum_{n=0}^{\infty} u_{n+1}\frac{1}{2}\sum_{k=0}^{\infty}((\varphi)(\mathsf{Y})\varphi e_n)_k(e_k + e_{k+1})
\end{aligned}$$

So we have to compute $(\varphi)(\mathsf{Y})\varphi e_n$. The above equations then give:

$$\begin{aligned}
(\varphi)(\mathsf{Y})\varphi e_n &= (e_n)_0e_0 + \sum_{h=0}^{\infty}(e_n)_{h+1}\frac{1}{2}\sum_{k=0}^{\infty}((\mathsf{Y})\varphi e_h)_k(e_k + e_{k+1})\\
&= \begin{cases} e_0 & \text{if } n = 0,\\ \frac{1}{2}\sum_{k=0}^{\infty}((\mathsf{Y})\varphi e_{n-1})_k(e_k + e_{k+1}) & \text{if } n > 0.\end{cases}
\end{aligned}$$

It might be not yet obvious which kind of closed-form expression can be associated to the above recurrence, so let us unfold the first cases:

$$\begin{aligned}
(\varphi)(\mathsf{Y})\varphi e_0 &= e_0\\
(\varphi)(\mathsf{Y})\varphi e_1 &= \frac{1}{2}(e_0 + e_1)\\
(\varphi)(\mathsf{Y})\varphi e_2 &= \frac{1}{2^2}(e_0 + 2e_1 + e_2)\\
(\varphi)(\mathsf{Y})\varphi e_3 &= \frac{1}{2^3}(e_0 + 3e_1 + 3e_2 + e_3)
\end{aligned}$$

We can then guess (and formally prove by induction on n);

$$(\varphi)(\mathsf{Y})\varphi e_n = \frac{1}{2^n}\sum_{h=0}^{n}\binom{n}{h}e_h$$

Finally, this gives:

$$\begin{aligned}
(\llbracket\mathsf{binom}\rrbracket)u &= u_0e_0 + \sum_{n=0}^{\infty}u_{n+1}\frac{1}{2}\sum_{k=0}^{\infty}\left(\frac{1}{2^n}\sum_{h=0}^{n}\binom{n}{h}e_h\right)_k(e_k+e_{k+1})\\
&= u_0e_0 + \sum_{n=0}^{\infty}\frac{u_{n+1}}{2^{n+1}}\sum_{k=0}^{n}\binom{n}{k}(e_k+e_{k+1})\\
&= \frac{u_0}{2^0}e_0 + \sum_{n=1}^{\infty}\frac{u_n}{2^n}\sum_{k=0}^{n-1}\binom{n-1}{k}(e_k+e_{k+1})\\
&= \frac{u_0}{2^0}e_0 + \sum_{n=1}^{\infty}\frac{u_n}{2^n}\left(\binom{n-1}{0}e_0 + \left(\sum_{k=1}^{n-1}\left(\binom{n-1}{k-1}+\binom{n-1}{k}\right)e_k\right) + \binom{n-1}{n-1}e_n\right)\\
&= \frac{u_0}{2^0}e_0 + \sum_{n=1}^{\infty}\frac{u_n}{2^n}\left(\binom{n}{0}e_0 + \left(\sum_{k=1}^{n-1}\binom{n}{k}e_k\right) + \binom{n}{n}e_n\right)\\
&= \frac{u_0}{2^0}e_0 + \sum_{n=1}^{\infty}\frac{u_n}{2^n}\sum_{k=0}^{n}\binom{n}{k}e_k\\
&= \sum_{n=0}^{\infty}\frac{u_n}{2^n}\sum_{k=0}^{n}\binom{n}{k}e_k
\end{aligned}$$

Computation of $\llbracket\mathsf{unif}_2\rrbracket$. *TODO.*

Computation of $\llbracket\mathsf{unif}\rrbracket$. *TODO.*

The above exercises show how $\mathbf{Pcoh}_!$ provides a convenient framework for reasoning on programs (i) compositionally and (ii) with standard mathematical tools (arithmetics, series, etc). However, we have not yet proved that the denotation of a program actually is equivalent to its evaluation: this will be the goal of the next section, achieving the soundness and the adequacy properties.

2.3 The soundness property

The soundness of a denotational model with respect to an operational semantics states the invariance of the denotation of a program under its evaluation. This invariance turns into Theorem 9 in case of probabilistic programs. The following lemmata and definition are needed to prove the Soundness Theorem and are quite standard.

Lemma 7 (Substitution) *Assume that $\Gamma, x:A \vdash M : B$ and that $\Gamma \vdash P : A$. Then $\llbracket M\,[P/x]\rrbracket_\Gamma = \llbracket M\rrbracket_{\Gamma,x:A} \circ \langle \mathsf{Id}_{!\llbracket\Gamma\rrbracket}, \llbracket P\rrbracket_\Gamma\rangle$ in $\mathbf{Pcoh}_!$. In other words, for any $\vec{u} \in \mathsf{P}\llbracket\Gamma\rrbracket$, we have $\widehat{\llbracket M\,[P/x]\rrbracket_\Gamma}(\vec{u}) = \widehat{\llbracket M\rrbracket_{\Gamma,x:A}}(\vec{u}, \widehat{\llbracket P\rrbracket_\Gamma}(\vec{u}))$.*

Exercise 31. Prove Lemma 7.

Answer of Exercise 31. *First, notice that by Lemma 1 both* $[\![M\,[P/x]]\!]_\Gamma$ *and* $[\![M]\!]_{\Gamma,x:A} \circ \langle \mathsf{Id}_{[\![\Gamma]\!]}, [\![P]\!]_\Gamma \rangle$ *are morphisms in* $\mathbf{Pcoh}_!([\![\Gamma]\!], [\![B]\!])$*. The proof is then by induction on* M*, the simplest way to write it being to use the functional characterisation of the semantics (Figure 2c). We detail two cases, the other cases are similar.*

If $M = \underline{n}$**:** *we have* $\widehat{[\![M\,[P/x]]\!]_\Gamma}(\vec{u}) = \widehat{[\![\underline{n}]\!]_\Gamma}(\vec{u}) = e_n = \widehat{[\![\underline{n}]\!]_{\Gamma,x:A}}(\vec{u}, \widehat{[\![P]\!]_\Gamma}(\vec{u})) = \widehat{[\![M]\!]_{\Gamma,x:A}}(\vec{u}, \widehat{[\![P]\!]_\Gamma}(\vec{u}))$.

If $M = \lambda y^C\, N$**:** *we have*

$$\begin{aligned}
\big(\widehat{[\![M\,[P/x]]\!]_\Gamma}(\vec{u})\big)(u) &= \big(\widehat{[\![\lambda y^C\, N\,[P/x]]\!]_\Gamma}(\vec{u})\big)(u) && \textit{def substitution}\\
&= \widehat{[\![N\,[P/x]]\!]_{\Gamma,y:C}}(\vec{u}, u) && \textit{def semantics of } \lambda\\
&= \widehat{[\![N]\!]_{\Gamma,y:C,x:A}}(\vec{u}, u, \widehat{[\![P]\!]_{\Gamma,y:C}}(\vec{u}, u)) && \textit{induction hypothesis}\\
&= \widehat{[\![N]\!]_{\Gamma,x:A,y:C}}(\vec{u}, \widehat{[\![P]\!]_{\Gamma,y:C}}(\vec{u}, u), u) && \textit{assoc and comm \&}\\
&= \widehat{[\![N]\!]_{\Gamma,x:A,y:C}}(\vec{u}, \widehat{[\![P]\!]_\Gamma}(\vec{u}), u) && \textit{auxiliary lemma not free vars}\\
&= \big(\widehat{[\![\lambda y^C\, N]\!]_{\Gamma,x:A}}(\vec{u}, \widehat{[\![P]\!]_\Gamma}(\vec{u}))\big)(u) && \textit{def semantics of } \lambda
\end{aligned}$$

which implies $\widehat{[\![M\,[P/x]]\!]_\Gamma}(\vec{u}) = \widehat{[\![M]\!]_{\Gamma,x:A}}(\vec{u}, \widehat{[\![P]\!]_\Gamma}(\vec{u}))$*, by Proposition 4. Notice that in one equation we have used an auxiliary lemma stating that* $\widehat{[\![P]\!]_{\Gamma,y:C}}(\vec{u}, u) = \widehat{[\![P]\!]_\Gamma}(\vec{u})$*, whenever* y *is not a free variable of* P *(which can always be supposed by renaming* M*). This lemma can be proved easily by structural induction on* P*.*

The next definition and lemma formalise the fact that the operational semantics of Figure 1d, although stochastic, implements a deterministic strategy, meaning that given a term there is at most one minimal redex that can be fired by the rules of Figure 1d. This redex is underlined by what is called an evaluation context.

An *evaluation context* is a term with exactly one (typed) hole given by the following grammar, for some typing environment Γ and type A:

$$\mathsf{E}[]^{\Gamma\vdash A} := []^{\Gamma\vdash A} \mid \Big(\mathsf{E}[]^{\Gamma\vdash A}\Big)\, N \mid \mathsf{succ}(\mathsf{E}[]^{\Gamma\vdash A}) \mid \mathsf{if}(\mathsf{E}[]^{\Gamma\vdash A}, P, z \cdot r) \tag{30}$$

In the following we can omit to explicit the type of the hole if irrelevant or clear from the context.

Lemma 8 *Given a term* $\Gamma \vdash M : A$*, either* M *is a value or there exists a unique evaluation context* $\mathsf{E}[]^{\Gamma'\vdash A'}$ *and redex* R *such that* $M = \mathsf{E}[R]^{\Gamma'\vdash A'}$*, and for every* $M \xrightarrow{p} M'$*, we have* $M' = \mathsf{E}[P]^{\Gamma'\vdash A'}$ *and* $R \xrightarrow{p} P$ *by one axiom rule of Figure 1d. In particular* $\mathsf{Red}(\Gamma, A)_{M,M'} = \mathsf{Red}(\Gamma', A')_{R,P}$*.*

Proof. By inspection of the rules of Figure 1d, one can remark that if $M \xrightarrow{p} M'$ is in the conclusion of a rule, the top-level constructor of M characterises univocally the rule of which it is conclusion. □

We formulate the invariance of the interpretation of terms under weak-reduction, using the stochastic reduction matrix introduced in Equation (6).

Theorem 9 (Soundness) *Assume that* $\Gamma \vdash M : A$*. One has*

$$[\![M]\!]_\Gamma = \sum_{M' \in \Lambda_\Gamma^A} \mathsf{Red}(\Gamma, A)_{M,M'} [\![M']\!]_\Gamma \tag{31}$$

Proof. If M is a value, then $\mathsf{Red}(\Gamma, A)_{M,M'}$ is non-zero only if $M' = M$ and the equality is trivial.

Otherwise, by Lemma 8, we have that $M = \mathsf{E}[R]^{\Gamma' \vdash A'}$ for some redex R and the proof is by induction on $\mathsf{E}[]^{\Gamma' \vdash A'}$.

The base of the induction is when $M = R \xrightarrow{p} M'$ is obtained by one of the axioms of Figure 1d. We detail two cases, the other cases of the base of induction are similar:

$M = \mathsf{coin}$, then we have $\widehat{[\![M]\!]_\Gamma}(\vec{u}) = \frac{1}{2}e_0 + \frac{1}{2}e_1 = \frac{1}{2}\widehat{[\![\underline{0}]\!]_\Gamma}(\vec{u}) + \frac{1}{2}\widehat{[\![\underline{1}]\!]_\Gamma}(\vec{u}) = \sum_{M'} \mathsf{Red}(\Gamma, \iota)_{M,M'} \widehat{[\![M']\!]_\Gamma}(\vec{u})$.

$M = \left(\lambda x^A\, N\right) P$, then we have:

$$\begin{aligned}
\widehat{[\![(\lambda x^A\, N)\, P]\!]_\Gamma}(\vec{u}) &= \widehat{[\![\lambda x^A\, N]\!]_\Gamma}(\vec{u})(\widehat{[\![P]\!]_\Gamma}(\vec{u})) \\
&= \widehat{[\![N]\!]_{\Gamma, x:A}}(\vec{u}, \widehat{[\![P]\!]_\Gamma}(\vec{u})) \\
&= \widehat{[\![N\,[P/x]]\!]_{\Gamma, x:A}}(\vec{u}) \qquad \text{by Lemma 7}
\end{aligned}$$

So giving $\widehat{[\![M]\!]_\Gamma}(\vec{u}) = \sum_{M'} \mathsf{Red}(\Gamma, A)_{M,M'} \widehat{[\![M']\!]_\Gamma}(\vec{u})$, as this latter sum has only one non-null factor, corresponding to $M' = N[P/x]$.

The induction step splits in the three inductive cases of the definition of an evaluation context (Equation (30)). We detail only one case, the other cases being similar:

$M = (P)\, Q$ **with** $P = \mathsf{E}[R]^{\Gamma' \vdash A'}$ **and** $R \xrightarrow{p} R'$, then:

$$\begin{aligned}
\widehat{[\![(P)\, Q]\!]_\Gamma}(\vec{u}) &= (\widehat{[\![P]\!]_\Gamma}(\vec{u}))(\widehat{[\![Q]\!]_\Gamma}(\vec{u})) \\
&= (\sum_{P'} \widehat{\mathsf{Red}(\Gamma, B \Rightarrow A)_{P,P'}[\![P']\!]_\Gamma}(\vec{u}))(\widehat{[\![Q]\!]_\Gamma}(\vec{u})) \quad \text{by IH, denoting } P' = E[R'] \\
&= \sum_{P'} \mathsf{Red}(\Gamma, B \Rightarrow A)_{P,P'} (\widehat{[\![P']\!]_\Gamma}(\vec{u}))(\widehat{[\![Q]\!]_\Gamma}(\vec{u})) \qquad \text{by linearity} \\
&= \sum_{P'} \mathsf{Red}(\Gamma, B \Rightarrow A)_{P,P'} \widehat{[\![(P')\, Q]\!]_\Gamma}(\vec{u}) \\
&= \sum_{M'} \mathsf{Red}(\Gamma, A)_{(P)Q,M'} \widehat{[\![M']\!]_\Gamma}(\vec{u}) \qquad \text{by Lemma 8.}
\end{aligned}$$

□

As a corollary we get the following inequality.

Corollary 10 *Let M be such that $\vdash M : \iota$. Then for all $n \in \mathbb{N}$ we have*

$$\mathsf{Red}(\iota)^{\infty}_{M,\underline{n}} \leq [\![M]\!]_n\,.$$

Proof. Iterating Theorem 9 we get, for all $k \in \mathbb{N}$:

$$[\![M]\!] = \sum_{M' \in \Lambda^{\iota}_0} \mathsf{Red}(\iota)^k_{M,M'} [\![M']\!]$$

Therefore, for all $k \in \mathbb{N}$ we have $[\![M]\!]_n \geq \mathsf{Red}(\iota)^k_{M,\underline{n}}$ and the result follows, since $\underline{n}$ is weak-normal. □

$$u\ \mathcal{R}_\iota\ M \text{ iff } \forall n, u_n \leq \mathsf{Red}(\vdash \iota)^\infty_{M,\underline{n}}, \tag{33}$$

$$f\ \mathcal{R}_{A\to B}\ P \text{ iff } \forall u\ \mathcal{R}_A\ Q, \widehat{f}(u)\ \mathcal{R}_B\ (P)\,Q \tag{34}$$

Figure 3: The logical relation $\mathcal{R}_A$ between $\mathbf{Pcoh}_!$ vectors in $\mathsf{P}(\llbracket A \rrbracket)$ and closed pPCF terms of type A.

3 Adequacy of $\mathbf{Pcoh}_!$ for pPCF

The Adequacy Theorem provides the inverse inequality of Corollary 10, so getting:

Theorem 11 (Adequacy) *Let M be a program of pPCF, i.e. a term $\vdash M : \iota$. Then,*

$$\forall n \in \mathbb{N}, \mathsf{Red}(\vdash \iota)^\infty_{M,\underline{n}} = \llbracket M \rrbracket_n \tag{32}$$

We prove this theorem by using the *logical relations*, which is a powerful technique in order to verify program properties in a compositional way.

The idea is to prove Equation (32) by structural induction on M. Suppose that M is for example an application $(P)\,Q$, with $\vdash P : A \Rightarrow \iota$ and $\vdash Q : A$ with A an arbitrary type of pPCF. The problem is that Equation (32) is restricted to closed programs of *ground type*, so what is the induction hypothesis for the higher-order terms P and Q? Logical relations give an answer to this question, providing a standard way of extending a property on ground programs to statements on terms of any type (in fact any "logic based" type), so that whatever these latter compose, at the ground type you can conclude with the original property.

Logical relations are very versatile, they can be applied to different properties, not only model adequacy, different languages, not only call-by-name pPCF, and to different type constructors, not only the intuitionistic arrow. We consider here the basic version needed for Theorem 11, but you can google to have a first glance at how spread the method of logical relations are in the theory of the programming languages.

Figure 3 gives the definition of the logical relation $f\ \mathcal{R}_A\ M$ for A a type of pPCF, M a closed term of type A and f a vector in $\mathsf{P}(\llbracket A \rrbracket)$. This definition tames two different challenges of pPCF: (i) the extension of the adequacy property to arrow types, by definition (34), (ii) the partiality of pPCF (the possibility of a program to diverge) by considering general vectors in $\mathsf{P}(\llbracket A \rrbracket)$ rather then just program denotations. For this latter, the idea is that whenever $u \leq \llbracket M \rrbracket$, then this means that u is a semantical approximant of $\llbracket M \rrbracket$. The crucial point is then to prove that $\llbracket M \rrbracket\ \mathcal{R}_A\ M$ for any closed term (Lemma 17), which gives at ground type the inverse inequality of Corollary 10, so concluding with the equality (32).

Lemma 12 (Expansion lemma) *Assume $\mathsf{Red}(\vdash \iota)_{M,M'} = 1$ with M, M' closed terms of type A, and $f \in \mathsf{P}(\llbracket A \rrbracket)$. If $f\ \mathcal{R}_A\ M'$, then $f\ \mathcal{R}_A\ M$*

Proof. Let f, M, M' as in the hypothesis. Let $A = B_1 \Rightarrow \dots B_k \Rightarrow \iota$, and consider $v_i\ \mathcal{R}_{B_i}\ N_i$ for every $1 \leq i \leq k$. We should prove that $\widehat{f(v_1)\cdots(v_k)}_n \leq \mathsf{Red}(\vdash \iota)^\infty_{((M)N_1\cdots)N_k,\underline{n}}$ for any n. Notice that we have: $\mathsf{Red}(\vdash \iota)^\infty_{((M)N_1\cdots)N_k,\underline{n}} = \sum_L \mathsf{Red}(\vdash \iota)_{((M)N_1\cdots)N_k,((L)N_1\cdots)N_k} \mathsf{Red}(\vdash \iota)^\infty_{((L)N_1\cdots)N_k,\underline{n}}$. This latter sum is equal to $\mathsf{Red}(\vdash \iota)^\infty_{((M')N_1\cdots)N_k,\underline{n}}$, because the sum has only one non-null factor, corresponding with $L = M'$. The inequality then follows from the hypothesis $f\ \mathcal{R}_A\ M'$. □

Exercise 32. Notice that the expansion lemma is stated for deterministic expansion: this is in fact what is needed for proving the interpretation lemma. Can you give and prove a more general statement that holds whenever $\mathsf{Red}(\vdash \iota)_{M,M'} = \lambda$ for a generic probability $\lambda \in [0,1]$?

Answer of Exercise 32. *The extension to stochastic reduction can be given by the following statement :*

- ⋆ *Let A be a type. Let $M, M' \in \Lambda_0^A$ and let $f \in \mathsf{P}[\![A]\!]$. Then M' $\mathcal{R}_A$ f implies M $\mathcal{R}_A$ $\mathsf{Red}(A)_{M,M'} f$.*

The proof is similar to the above lemma. By taking $A = B_1 \Rightarrow \dots B_k \Rightarrow \iota$, and $v_i \, \mathcal{R}_{B_i} \, N_i$ for the various i, we should prove:

$$\widehat{(\mathsf{Red}(A)_{M,M'} f)}(v_1)\cdots(v_k)_n = \mathsf{Red}(A)_{M,M'} \left(\widehat{f(v_1)\cdots(v_k)} \right)_n \leq \mathsf{Red}(\vdash \iota)^{\infty}_{((M)N_1\cdots)N_k,\underline{n}}$$

Now we have that $\mathsf{Red}(\vdash \iota)^{\infty}_{((M)N_1\cdots)N_k,\underline{n}} = \sum_L \mathsf{Red}(\vdash \iota)_{((M)N_1\cdots)N_k,((L)N_1\cdots)N_k} \mathsf{Red}(\vdash \iota)^{\infty}_{((L)N_1\cdots)N_k,\underline{n}} \geq \mathsf{Red}(\vdash \iota)_{((M)N_1\cdots)N_k,((M')N_1\cdots)N_k} \mathsf{Red}(\vdash \iota)^{\infty}_{((M')N_1\cdots)N_k,\underline{n}}$. *By hypothesis we know that* $\widehat{f(v_1)\cdots(v_k)} \leq \mathsf{Red}(\vdash \iota)^{\infty}_{((M')N_1\cdots)N_k,\underline{n}}$ *and so we can conclude as* $\mathsf{Red}(\vdash \iota)_{((M)N_1\cdots)N_k,((M')N_1\cdots)N_k} \leq \mathsf{Red}(A)_{M,M'}$.

Lemma 13 (Zero lemma) *Assume M is a closed term of type A, then $0 \, \mathcal{R}_A \, M$.*

Proof. Let $A = B_1 \Rightarrow \cdots \Rightarrow B_k \Rightarrow \iota$. We have to prove that for any $v_1 \, \mathcal{R}_{B_1} \, N_1, \dots, v_k \, \mathcal{R}_{B_k} \, N_k$, we have: $\widehat{(\dots \widehat{0}(\vec{u})(v_1)\dots)}(v_k) \, \mathcal{R}_\iota \, (M) \, N_1 \dots N_k$. This claim is immediate from the definitions, as $\widehat{0}(u) = 0$ for any u. □

Lemma 14 (Scott continuity) *Assume $u_0 \leq u_1 \leq u_2 \dots$ is a countable increasing family of vectors in $\mathsf{P}(\![A]\!])$ such that for any $i \in \mathbb{N}$, $u_i \, \mathcal{R}_A \, M$ for a closed term of type A. Then $\sup_{i\in\mathbb{N}} u_i \, \mathcal{R}_A \, M$.*

Proof. Let $A = B_1 \Rightarrow \cdots \Rightarrow B_k \Rightarrow \iota$. We have to prove that for any $v_1 \, \mathcal{R}_{B_1} \, N_1, \dots, v_k \, \mathcal{R}_{B_k} \, N_k$, we have: $\widehat{(\dots \widehat{\sup_{i\in\mathbb{N}} u_i}(v_1)\dots)}(v_k) \, \mathcal{R}_\iota \, (M) \, N_1 \dots N_k$. This means to prove, for any $n \in \mathbb{N}$:

$$\left(\widehat{(\dots \widehat{\sup_{i\in\mathbb{N}} u_i}(v_1)\dots)}(v_k) \right)_n \leq \mathsf{Red}(\vdash \iota)^{\infty}_{(M)N_1\dots N_k,\underline{n}}.$$

By Ex. 23, the left-hand side of the inequality is equivalent to $\sup_{i\in\mathbb{N}} \left(\widehat{(\dots \widehat{u_i(v_1)}\dots)}(v_k) \right)_n$, and so the inequality follows immediately by the hypothesis $u_i \, \mathcal{R}_A \, M$, since for any i, $\left(\widehat{(\dots \widehat{u_i(v_1)}\dots)}(v_k) \right)_n \leq \mathsf{Red}(\vdash \iota)^{\infty}_{(M)N_1\dots N_k,\underline{n}}$. □

Lemma 15 (Successor) *Assume that $\vdash N : \iota$. Then, for any $n \in \mathbb{N}$, we have*

$$\mathsf{Red}(\iota)^{\infty}_{N,\underline{n}} = \mathsf{Red}(\iota)^{\infty}_{\mathsf{succ}(N),\underline{n+1}}.$$

Proof. We prove in fact that for any k and for any N, $\mathsf{Red}(\iota)^{k}_{N,\underline{n}} = \mathsf{Red}(\iota)^{k+1}_{\mathsf{succ}(N),\underline{n+1}}$. The proof is by induction on k. If N is a numeral $\underline{h}$, then both scalars are 1 if $h = n$, otherwise both are 0, for any k.

If N is not a numeral, then we can suppose $k > 0$, otherwise both scalars are null. So:

$$\begin{aligned}
\mathsf{Red}(\iota)^k_{N,\underline{n}} &= \sum_L \mathsf{Red}(\iota)_{N,L}\mathsf{Red}(\iota)^{k-1}_{L,\underline{n}} \\
&= \sum_L \mathsf{Red}(\iota)_{N,L}\mathsf{Red}(\iota)^{k}_{\mathsf{succ}(L),\underline{n+1}} && \text{by induction hyp.} \\
&= \sum_L \mathsf{Red}(\iota)_{\mathsf{succ}(N),\mathsf{succ}(L)}\mathsf{Red}(\iota)^{k}_{\mathsf{succ}(L),\underline{n+1}} && \text{because } N \text{ not numeral} \\
&= \mathsf{Red}(\iota)^{k+1}_{\mathsf{succ}(N),\underline{n+1}}
\end{aligned}$$

□

Lemma 16 (Branching) *Assume that* $\vdash M : \iota$, $\vdash P : A$ *and* $z : \iota \vdash Q : A$ *where* $A = B_1 \Rightarrow \cdots B_k \Rightarrow \iota$. *Let* $N_1, \ldots, N_k$ *be closed terms such that* $\vdash N_i : B_i$ *for* $i = 1, \ldots, k$.

Then, for any $n \in \mathbb{N}$, *we have*

$$\begin{aligned}
&\mathsf{Red}(\iota)^\infty_{(\mathsf{if}(M,P,z\cdot Q))N_1\cdots N_k,\underline{n}} \\
&\quad = \mathsf{Red}(\iota)^\infty_{M,\underline{0}}\mathsf{Red}(\iota)^\infty_{(P)N_1\cdots N_k,\underline{n}} + \sum_{k\in\mathbb{N}} \mathsf{Red}(\iota)^\infty_{M,\underline{k+1}}\mathsf{Red}(\iota)^\infty_{(Q[\underline{k}/z])N_1\cdots N_k,\underline{n}}
\end{aligned}$$

Proof. One can easily prove by induction on $\ell \in \mathbb{N}$, the two inequalities:

$$\begin{aligned}
&\mathsf{Red}(\iota)^\infty_{(\mathsf{if}(M,P,z\cdot Q))N_1\cdots N_k,\underline{n}} \\
&\qquad \geq \mathsf{Red}(\iota)^\ell_{M,\underline{0}}\mathsf{Red}(\iota)^\ell_{(P)N_1\cdots N_k,\underline{n}} + \sum_{k\in\mathbb{N}} \mathsf{Red}(\iota)^\ell_{M,\underline{k+1}}\mathsf{Red}(\iota)^\ell_{(Q[\underline{k}/z])N_1\cdots N_k,\underline{n}}
\end{aligned}$$

$$\begin{aligned}
&\mathsf{Red}(\iota)^\ell_{(\mathsf{if}(M,P,z\cdot Q))N_1\cdots N_k,\underline{n}} \\
&\qquad \leq \mathsf{Red}(\iota)^\infty_{M,\underline{0}}\mathsf{Red}(\iota)^\infty_{(P)N_1\cdots N_k,\underline{n}} + \sum_{k\in\mathbb{N}} \mathsf{Red}(\iota)^\infty_{M,\underline{k+1}}\mathsf{Red}(\iota)^\infty_{(Q[\underline{k}/z])N_1\cdots N_k,\underline{n}}
\end{aligned}$$

which give the claim of the lemma. □

Lemma 17 (Interpretation lemma) *Assume* $\Gamma \vdash M : A$ *with* $\Gamma = x_1 : A_1, \ldots, x_k : A_k$. *Then for all closed terms* N_i *of type* A_i *vectors* $u_i \in \mathsf{P}(\llbracket A \rrbracket)$ *such that* $u_i \mathcal{R}_{A_i} N_i$ *for* $i = 1, \ldots k$, *one has:*

$$\widehat{\llbracket M \rrbracket_\Gamma}(u_1, \ldots, u_k) \mathcal{R}_A M[N_1/x_1, \ldots, N_k/x_k]. \tag{35}$$

Proof. The proof is by induction on a type derivation $\Gamma \vdash M : A$, splitting depending on the last rule of this type derivation, which corresponds also to the top-level constructor of M. In the following we will denote by $\vec{u}$ the sequence $u_1, \ldots, u_k$ and by $[\vec{N}/\vec{x}]$ the sequence of substitution $[N_1/x_1, \ldots, N_k/x_k]$.

$M = x_i$**.** In this case, $\widehat{\llbracket M \rrbracket_\Gamma}(\vec{u}) = u_i \mathcal{R}_A N_i = M[\vec{N}/\vec{x}]$.

$M = \underline{n}$**.** In this case, $\widehat{\llbracket M \rrbracket_\Gamma}(\vec{u}) = e_n \mathcal{R}_\iota \underline{n} = M[N_1/x_1, \ldots, N_k/x_k]$, as for every $m \in \mathbb{N}$, $(e_n)_m = \mathsf{Red}(\iota)^\infty_{\underline{n},\underline{m}}$.

$M = \mathsf{coin}$**.** In this case, $\llbracket M \rrbracket_\Gamma(\vec{u}) = \frac{1}{2}(e_0 + e_1) \mathcal{R}_\iota \mathsf{coin} = M[N_1/x_1, \ldots, N_k/x_k]$, as for every $m \in \mathbb{N}$, $\frac{1}{2}(e_0 + e_1)_m = \frac{1}{2}(\mathsf{Red}(\iota)_{\underline{0},\underline{m}} + \mathsf{Red}(\iota)_{\underline{1},\underline{m}}) = \mathsf{Red}(\iota)^\infty_{\mathsf{coin},\underline{m}}$.

$M = \mathsf{succ}(L)$. In this case, we have: $[\![M]\!]_\Gamma(\vec{u}) = \sum_n [\![L]\!]_\Gamma(\vec{u})_n e_{n+1}$. By induction hypothesis $\widehat{[\![L]\!]_\Gamma}(\vec{u})\ \mathcal{R}_\iota\ L[\vec{N}/\vec{x}]$, so that: $\widehat{[\![L]\!]_\Gamma}(\vec{u})_n \leq \mathsf{Red}(\iota)^\infty_{L[\vec{N}/\vec{x}],\underline{n}}$ for every n. We can conclude $\widehat{[\![M]\!]_\Gamma}(\vec{u})_n \leq \mathsf{Red}(\iota)^\infty_{M[\vec{N}/\vec{x}],\underline{n}}$, as by Lemma 15, $\mathsf{Red}(\iota)^\infty_{M[\vec{N}/\vec{x}],\underline{n+1}} = \mathsf{Red}(\iota)^\infty_{L[\vec{N}/\vec{x}],\underline{n}}$.

$M = \lambda y^B L$. In this case, $A = (B \Rightarrow C)$ and $\Gamma, y : B \vdash L : C$ for some type C. In order to prove $\widehat{[\![M]\!]_\Gamma}(\vec{u})\ \mathcal{R}_{B\Rightarrow C}\ M[\vec{N}/\vec{x}]$, we have to prove, for every $v\ \mathcal{R}_B\ P$, that $\left(\widehat{[\![M]\!]_\Gamma}(\vec{u})\right)(v)\ \mathcal{R}_{B\Rightarrow C}\ \left(M[\vec{N}/\vec{x}]\right) P$. Notice that:

- $\left(\widehat{[\![M]\!]_\Gamma}(\vec{u})\right)(v) = \widehat{[\![L]\!]_{\Gamma,y:B}}(\vec{u}, v)$ by the Figure 2c,
- $M[\vec{N}/\vec{x}]P \xrightarrow{1} L[\vec{N}/\vec{x}, P/y]$, by Figure 1d,
- and $\widehat{[\![L]\!]_{\Gamma,y:B}}(\vec{u}, v)\ \mathcal{R}_C\ L[\vec{N}/\vec{x}, P/y]$ by induction hypothesis.

We can then conclude by Lemma 12.

$M = (L)\, P$. In this case, $\Gamma \vdash L : B \Rightarrow A$ and $\Gamma \vdash P : B$ for some type B. By induction hypothesis we have that $\widehat{[\![L]\!]_\Gamma}(\vec{u})\ \mathcal{R}_{B\Rightarrow A}\ L[\vec{N}/\vec{x}]$ and $\widehat{[\![P]\!]_\Gamma}(\vec{u})\ \mathcal{R}_B\ P[\vec{N}/\vec{u}]$, so that by definition of $\mathcal{R}$ we have:

$$\widehat{[\![(L)\, P]\!]_\Gamma}(\vec{u}) = \left(\widehat{[\![L]\!]_\Gamma}(\vec{u})\right)(\widehat{[\![P]\!]_\Gamma}(\vec{u}))\ \mathcal{R}_A\ \left(L[\vec{N}/\vec{x}]\right) P[\vec{N}/\vec{x}] = \big((L)\, P\big)[\vec{N}/\vec{x}].$$

$M = \mathsf{fix}(L)$. In this case, $\Gamma \vdash L : A \Rightarrow A$ so that by induction hypothesis, $\widehat{[\![L]\!]_\Gamma}(\vec{u})\ \mathcal{R}_{A\Rightarrow A}\ L[\vec{N}/\vec{x}]$. By Lemma 13 we have that $0\ \mathcal{R}_A\ \mathsf{fix}(L[\vec{N}/\vec{x}])$, so that $\widehat{[\![L]\!]_\Gamma}(\vec{u}))(0)\ \mathcal{R}_A\ (L[\vec{N}/\vec{x}])\, \mathsf{fix}(L[\vec{N}/\vec{x}])$ and by Lemma 12, $\widehat{[\![L]\!]_\Gamma}(\vec{u})(0)\ \mathcal{R}_A\ \mathsf{fix}(L[\vec{N}/\vec{x}])$. By iterating this reasoning we can prove for every n that $\left(\widehat{[\![L]\!]_\Gamma}(\vec{u})\right)^n (0)\ \mathcal{R}_A\ \mathsf{fix}(L[\vec{N}/\vec{x}])$, so that by Lemma 14 we conclude.

$M = \mathsf{if}(L, P, z \cdot Q)$. In this case, $\Gamma \vdash L : \iota$, $\Gamma \vdash P : A$ and $\Gamma, z : \iota \vdash Q : A$. By induction hypothesis we then have: $\widehat{[\![L]\!]_\Gamma}(\vec{u})\ \mathcal{R}_\iota\ L[\vec{N}/\vec{x}]$, $\widehat{[\![P]\!]_\Gamma}(\vec{u})\ \mathcal{R}_A\ P[\vec{N}/\vec{x}]$, and $\widehat{[\![Q]\!]_{\Gamma,z}}(\vec{u}, e_n)\ \mathcal{R}_Q\ L[\vec{N}/\vec{x}, \underline{n}/\vec{z}]$, this latter because we have already proven above that $e_n\ \mathcal{R}_\iota\ \underline{n}$ for every n.

Assume that $A = B_1 \Rightarrow \cdots B_k \Rightarrow \iota$, then we have to prove that for every $u'_1\ \mathcal{R}_{B_1}\ N'_1$, $\ldots$, $u'_k\ \mathcal{R}_{B_1}\ N'_k$, we have: $\widehat{[\![M]\!]_\Gamma}(\vec{u})(\vec{u'})\ \mathcal{R}_\iota\ \left(M[\vec{N}/\vec{x}]\right)\vec{N'}$, which means, for every $\ell \in \mathbb{N}$,

$$\widehat{[\![L]\!]_\Gamma}(\vec{u})_0 \widehat{[\![P]\!]_\Gamma}(\vec{u})(\vec{u'})_\ell + \sum_n \widehat{[\![L]\!]_\Gamma}(\vec{u})_{n+1} \widehat{[\![Q]\!]_{\Gamma,z:\iota}}(\vec{u}, e_n)(\vec{u'})_\ell \leq \mathsf{Red}(\iota)^\infty_{\left(M[\vec{N}/\vec{x}]\right)\vec{N'},\underline{\ell}}$$

By induction hyptothesis we have that:

$$\widehat{[\![L]\!]_\Gamma}(\vec{u})_0 \widehat{[\![P]\!]_\Gamma}(\vec{u})(\vec{u'})_\ell \leq \mathsf{Red}(\iota)^\infty_{L[\vec{N}/\vec{x}],\underline{0}} \mathsf{Red}(\iota)^\infty_{\left(P[\vec{N}/\vec{x}]\right)\vec{N'},\underline{\ell}}$$

$$\widehat{[\![L]\!]_\Gamma}(\vec{u})_{n+1} \widehat{[\![Q]\!]_{\Gamma,z:\iota}}(\vec{u}, e_n)(\vec{u'})_\ell \leq \mathsf{Red}(\iota)^\infty_{L[\vec{N}/\vec{x}],\underline{n+1}} \mathsf{Red}(\iota)^\infty_{\left(Q[\vec{N}/\vec{x},\underline{n}]\right)\vec{N'},\underline{\ell}}, \quad \text{for every } n \in \mathbb{N}$$

We then conclude by Lemma 16. □

Proof of Theorem 11. Assume $\vdash M : \iota$. By Lemma 17, we have $[\![M]\!]\ \mathcal{R}_\iota\ M$, which means $[\![M]\!]_n \leq \mathsf{Red}(\iota)^\infty_{M,\underline{n}}$, for every n. The other other inequality is given by Corollary 10. □

4 Contextual Equivalence and Full-Abstraction

The adequacy property states the equivalence between the operational and the denotational semantics at the ground type. What about higher-order types? What does it mean for two terms of an arrow type to be equivalent in $\mathbf{Pcoh}_!$? In contrast with the ground type, the denotational equivalence of two higher-order terms does not correspond with the equality of the corresponding reduction matrices:

Exercise 33. Give an example of two closed terms M, M' of type $\iota \Rightarrow \iota$ such that $[\![M]\!] = [\![M']\!]$, but there exists a value V such that $\mathsf{Red}(\iota \Rightarrow \iota)_{M,V} \neq \mathsf{Red}(\iota \Rightarrow \iota)_{M,V}$.

Answer of Exercise 33. *Take for example the two programs implementing the identity: $M = \lambda x^\iota\ x$ and $M' = \lambda x^\iota\ \mathsf{if}(x, \underline{0}, z \cdot \mathsf{succ}(z))$. By the functional characterisation of $\mathbf{Pcoh}_!$ morphisms, we have $[\![M]\!] = [\![M']\!]$. On the contrast, $\mathsf{Red}(\iota \Rightarrow \iota)_{M,M} = 1$ while $\mathsf{Red}(\iota \Rightarrow \iota)_{M',M} = 0$.*

Exercise 33 shows that the notion of equivalence induced by the reduction matrices unfits higher-order types, as the syntactical equality of higher-order values is too strict. An operational equivalence larger than this latter is the so-called contextual equivalence, which we can define as follows.

A *context* $\mathsf{C}[]^{\Gamma\vdash A}$ is a term with exactly one hole $[]^{\Gamma\vdash A}$ for some typing environment Γ and type A. This is equivalent to extend the grammar 30 defining the evaluation contexts, with the following cases:

$$\mathsf{C}[]^{\Gamma\vdash A} := \mathsf{E}[]^{\Gamma\vdash A} \mid (M)\,\mathsf{C}[]^{\Gamma\vdash A} \mid \mathsf{if}(M, \mathsf{C}[]^{\Gamma\vdash A}, z \cdot R) \mid \mathsf{if}(M, P, z \cdot \mathsf{C}[]^{\Gamma\vdash A}) \tag{36}$$

Given an environment Γ and a type A, we define the following *contextual preorder* (also called *observational pre-order* or *Morris pre-order*) on terms $M, M' \in \Lambda^A_\Gamma$, as:

$$M \preceq_{\Gamma\vdash A} M' \text{ iff } \forall \mathsf{C}[]^{\Gamma\vdash A} \text{ of ground type}, \mathsf{Red}(\iota)^\infty_{\mathsf{C}[M]^{\Gamma\vdash A},\underline{0}} \leq \mathsf{Red}(\iota)^\infty_{\mathsf{C}[M']^{\Gamma\vdash A},\underline{0}} \tag{37}$$

We say that two terms $M, M' \in \Lambda^A_\Gamma$ are *contextually equivalent*, in symbol $M \sim_{\Gamma\vdash A} M'$, whenever $M \preceq_{\Gamma\vdash A} M'$ and $M \preceq_{\Gamma\vdash A} M'$. We may omit the typing subscript if irrelevant or clear from the context.

Exercise 34. Prove that the definition of $\preceq_{\Gamma\vdash A}$ does not depend on the chosen numeral $\underline{0}$.

Answer of Exercise 34. *Juste remark that for any $n \in \mathbb{N}$*

$$\mathsf{Red}(\iota)^\infty_{\mathsf{C}[M]^{\Gamma\vdash A},\underline{n}} = \mathsf{Red}(\iota)^\infty_{\mathsf{succ}(\mathsf{C}[M]^{\Gamma\vdash A}),\underline{n+1}} \qquad \textit{and} \qquad \mathsf{Red}(\iota)^\infty_{\mathsf{C}[M]^{\Gamma\vdash A},\underline{n+1}} = \mathsf{Red}(\iota)^\infty_{(\mathsf{pred}_\Omega)\mathsf{C}[M]^{\Gamma\vdash A},\underline{n}}$$

with $\mathsf{pred}_\Omega = \lambda x^\iota\ \mathsf{if}(x, \Omega, z \cdot z)$. So composing a context with a suitable iteration of succ or pred_Ω returns the chosen numeral.

The adequacy property implies easily the following corollary, stating that the denotational order implies the contextual pre-order.

Corollary 18 *Given two terms $M, M' \in \Lambda^A_\Gamma$, we have that:*

$$[\![M]\!]_\Gamma \leq [\![M']\!]_\Gamma \textit{ implies } M \preceq_{\Gamma\vdash A} M'$$

Hence, $[\![M]\!]_\Gamma = [\![M']\!]_\Gamma$ implies $M \sim_{\Gamma\vdash A} M'$.

Proof. Assume $[\![M]\!]_\Gamma \leq [\![M']\!]_\Gamma$ and $\mathsf{C}[]^{\Gamma\vdash A}$ be a context of ground type. By induction on $\mathsf{C}[]^{\Gamma\vdash A}$ and using Figure 2c one can easily prove that $[\![\mathsf{C}[M]^{\Gamma\vdash A}]\!]_\Gamma \leq [\![\mathsf{C}[M']^{\Gamma\vdash A}]\!]_\Gamma$, which implies $\mathsf{Red}(\iota)^\infty_{\mathsf{C}[M]^{\Gamma\vdash A},\underline{0}} \leq \mathsf{Red}(\iota)^\infty_{\mathsf{C}[M']^{\Gamma\vdash A},\underline{0}}$ by Theorem 11. □

Exercise 35.

1. Give an example of two terms M, M' such that $M \preceq_{\Gamma\vdash A} M'$, but $M' \not\preceq_{\Gamma\vdash A} M$.
2. Give an example of two different values that are contextually equivalent $V \sim_{\Gamma\vdash A} V'$.
3. Prove your assertions!

Answer of Exercise 35.

1. *Consider $M = \mathsf{pred}_\Omega = \lambda x^\iota\, \mathsf{if}(x, \Omega, z \cdot z)$ and $M' = \mathsf{pred} = \lambda x^\iota\, \mathsf{if}(x, \underline{0}, z \cdot z)$. Notice that $[\![M]\!] \leq [\![M']\!]$, so that by Corollary 18, $M \preceq_{\Gamma\vdash A} M'$. On the contrast, the context $\left([]^{\vdash \iota \Rightarrow \iota}\right)\underline{0}$ shows that $M' \not\preceq_{\Gamma\vdash A} M$, as $(M')\,\underline{0}$ converges to $\underline{0}$, while $(M)\,\underline{0}$ diverges.*
2. *The two terms $V = \lambda x^\iota\, x$ and $V' = \lambda x^\iota\, \mathsf{if}(x, \underline{0}, z \cdot \mathsf{succ}(z))$ given in the solution of Exercice 33 are a suitable examples of different values such that $V \sim_{\Gamma\vdash A} V'$, because of Corollary 18.*

A denotational model satisfying also the inverse implications of Corollary 18 is deemed *(in)equationally fully abstract* ((in)equationally FA for short). The equational full abstraction can be also simply referred as *full abstraction*. Notice that the inequational full abstraction implies the equational full abstraction, but in general it is not true the inverse implication, as we will see below with the example of $\mathbf{Pcoh}_!$.

Ehrhard's lectures show that the relational model of deterministic PCF is not equationally fully abstract (hence neither inequationally FA), giving two terms that are denoted by two different relations but that cannot be discriminated by a context of PCF. The following exercise gives a variant of that example and show how the presence of a random primitive increases considerably the discriminating power of the programming contexts.

Exercise 36. Consider the two PCF terms of type $\iota \Rightarrow \iota$, with $i \in \{1, 2\}$,

$$M_i = \lambda x^\iota\, \mathsf{if}(x, \mathsf{if}(x, \Omega, z \cdot \underline{i}), z \cdot \Omega)$$

where $\Omega = \mathsf{fix}(\lambda x^\iota\, x)$.

1. Prove that $\mathbf{Pcoh}_!$ discriminates the two terms, i.e. $[\![M_1]\!] \neq [\![M_2]\!]$.
2. How can you argue that no context of deterministic PCF can separate M_1 from M_2? (just give an hint, a formal proof is out of the scope of this exercise).
3. Give a *probabilistic* context of pPCF separating the two terms.

Answer of Exercise 36.

- *Proving $[\![M_1]\!] \neq [\![M_2]\!]$ is equivalent by Proposition 4 to find a vector $x \in \mathsf{PN}$ discriminating the the maps $\widehat{[\![M_1]\!]}$, $\widehat{[\![M_2]\!]}$. Since $[\![\Omega]\!] = 0$, notice that:*

$$\widehat{[\![M_i]\!]}(x) = x_0 \left(\sum_{n=1}^{\infty} x_n\right) e_i$$

  so that any vector in PN having non-null values on 0 and on a further natural number will be mapped to two different values by the two functions.

- *One convenient method to prove the context equivalence is by using an adequate denotational semantics of PCF equating the two terms (if any). For this example, you can use the semantics of coherence spaces, presented in the lectures by Melliès, which is an adequate model of PCF (but not of pPCF). In that semantics the web of the coherence space associated with the type*

$\iota \Rightarrow \iota$, is the set $\{(\{n\}, q)\ ;\ n, q \in \mathbb{N}\} \cup \{(\{\,\}, q)\ ;\ q \in \mathbb{N}\}$. In particular, for any point in this web, the set associated with the antecedent of $\iota \Rightarrow \iota$ is at most a singleton containing a unique number n (notice the difference with the web of the $\mathbf{Pcoh}_!$ *interpretation, which is the set of pairs of the form (m, q) for m any finite multiset of natural numbers, so possibly containing different numbers). One can easily check that no point in the coherence space web belongs to the interpretation of M_i, showing that both are denoted by the empty clique.*

By an analogous of Corollary 18 for coherence spaces and PCF*, this implies that M_1 and M_2 are contextually equivalent in* deterministic PCF.

- *By following the denotational interpretation of* $\mathbf{Pcoh}_!$*, any context giving to M_i a non trivial probabilistic distribution of $\underline{0}$ and $\underline{1}$ will separate the two terms, so for example the context:*

$$\left([]^{\vdash \iota \Rightarrow \iota}\right)\,\mathsf{coin}$$

In fact, $\mathsf{Red}(\iota)_{(M_i)\mathsf{coin},\underline{n}}$ is equal to $\frac{1}{4}$ on $n = i$ and zero otherwise.

Exercise 37. The original example given in Ehrhard's lectures was a parallel-or tester, given by the following PCF terms of type $(\iota \Rightarrow \iota \Rightarrow \iota) \Rightarrow \iota$, for $i \in \{1, 2\}$

$$M_i = \lambda f^{\iota \Rightarrow \iota \Rightarrow \iota}\, \mathsf{if}((f)\,\underline{0}\Omega, \mathsf{if}((f)\,\Omega\underline{0}, \mathsf{if}((f)\,\underline{11}, \Omega, z \cdot \underline{i}), z \cdot \Omega), z \cdot \Omega)$$

One can also check that $\mathbf{Pcoh}_!$ discriminates the two terms, as well as the contexts of pPCF. For example, prove that the following context separates the two terms:

$$\left([]^{\vdash (\iota \Rightarrow \iota \Rightarrow \iota) \Rightarrow \iota}\right)\,\mathsf{if}(\mathsf{coin}, \mathsf{or}_1, z \cdot \mathsf{or}_2)$$

with $\mathsf{or}_i = \lambda x_1^\iota\, \lambda x_2^\iota\, \mathsf{if}(x_i, \underline{0}, z \cdot \mathsf{if}(x_{3-i}, \underline{0}, z \cdot \underline{1}))$, for $i \in \{1, 2\}$. Notice that or_i is implementing an or-function (with $\underline{0}$ representing the true value) evaluating its i-th argument at first. The term $\mathsf{if}(\mathsf{coin}, \mathsf{or}_1, z \cdot \mathsf{or}_2)$ is then a kind of "probabilistic" parallel-or, evaluating at first one of its two arguments with equal probability $\frac{1}{2}$.

Answer of Exercise 37. *We use* $\mathbf{Pcoh}_!$ *to compute compositionally the result of evaluating $T_i = (M_i)\,\mathsf{if}(\mathsf{coin}, \mathsf{or}_1, z \cdot \mathsf{or}_2)$. First, notice that: $\widehat{[\![\mathsf{or}_i]\!]}(x_1)(x_2) = (x_{i0} + x_{i1}x_{(3-i)_0})e_0 + x_{11}x_{21}e_1$. So we have:*

$$[\![T_i]\!] = \widehat{[\![M_i]\!]}(\frac{1}{2}[\![\mathsf{or}_1]\!] + \frac{1}{2}[\![\mathsf{or}_2]\!]) = \frac{1}{8}e_i$$

The examples given in the above exercises are in fact instances of a much more general property: in contrast with the deterministic setting, $\mathbf{Pcoh}_!$ is equationally fully abstract for probabilistic pPCF.

Theorem 19 (Equational FA) *Given two* pPCF *terms $\Gamma \vdash M : A$ and $\Gamma \vdash M' : A$, for a typing context Γ and a type A, we have that $[\![M]\!]_\Gamma = [\![M']\!]_\Gamma$ if, and only if, $M \sim_{\Gamma \vdash A} M'$.*

This theorem is proven in [3, 2]. The basic idea is to consider $[\![M]\!]_\Gamma - [\![M']\!]_\Gamma$ as a power series with a non-null coefficient, so to find a non-zero argument where the series is non-zero and then from this argument to construct a context discriminating M from M'.

What about inequational full abstraction? Unfortunately it fails for $\mathbf{Pcoh}_!$, in fact the order on PCS, which compares the coefficients of two power series, is actually much sharper than the extensional pre-order. For example, the terms $M_1 = \lambda x^\iota\, \mathsf{if}(x, \underline{0}, z \cdot \underline{0})$ and $M_2 = \lambda x^\iota\, \underline{0}$ of type $\iota \Rightarrow \iota$ are such that $[\![M_1]\!] \not\leq [\![M_2]\!]$, but $M_1 \preceq_{\vdash \iota \Rightarrow \iota} M_2$. The fact that $[\![M_1]\!] \not\leq [\![M_2]\!]$ can be proven by computing the matrices associated with two terms:

$$[\![M_1]\!]_{m,n} = \begin{cases} 1 & \text{if } m = [k] \text{ and } n = 0, \\ 0 & \text{otherwise.} \end{cases} \qquad [\![M_2]\!]_{m,n} = \begin{cases} 1 & \text{if } m = [\,] \text{ and } n = 0, \\ 0 & \text{otherwise.} \end{cases}$$

The proof of $M_1 \preceq_{\vdash \iota \Rightarrow \iota} M_2$ is much more complex as it requires either an adequate model of pPCF denoting M_1 with a morphism smaller than M_2 (such a model exists, for example the model of Kegelspitzen [4, 5]), or it requires a context lemma, stating that to check $M_1 \preceq_{\vdash \iota \Rightarrow \iota} M_2$ is enough to consider applicative contexts, i.e. context of the form $([\,])\, L$ for L a closed term of type ι. Such a lemma can be proven by a logical relation, but we do not detail it in these lectures.

References

[1] Martin Avanzini, Ugo Dal Lago, and Akihisa Yamada. On probabilistic term rewriting. *Science of Computer Programming*, 185:102338, 2020.

[2] Thomas Ehrhard, Michele Pagani, and Christine Tasson. Full abstraction for probabilistic pcf. *J. ACM*, 65(4), April 2018.

[3] Thomas Ehrhard, Christine Tasson, and Michele Pagani. Probabilistic coherence spaces are fully abstract for probabilistic PCF. In Suresh Jagannathan and Peter Sewell, editors, *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*, pages 309–320. ACM, 2014.

[4] Klaus Keimel and Gordon D. Plotkin. Mixed powerdomains for probability and nondeterminism. *Logical Methods in Computer Science*, 13(1), 2017.

[5] Mathys Rennela. Convexity and order in probabilistic call-by-name FPC. *CoRR*, abs/1607.04332, 2016.