Full abstraction for probabilistic PCF

Thomas Ehrhard, Michele Pagani and Christine Tasson
CNRS, IRIF, Univ Paris Diderot, Sorbonne Paris Cité
F-75205 Paris, France

November 3, 2015

Abstract

We present a probabilistic version of PCF, a well-known simply typed universal functional language. The type hierarchy is based on a single ground type of natural numbers. Even if the language is globally call-by-name, we allow a call-by-value evaluation for ground type arguments in order to provide the language with a suitable algorithmic expressiveness. We describe a denotational semantics based on probabilistic coherence spaces, a model of classical Linear Logic developed in previous works. We prove an adequacy and an equational full abstraction theorem showing that equality in the model coincides with a natural notion of observational equivalence.

Introduction

PCF is a paradigmatic functional programming language introduced by Dana Scott in 1969 and further studied by many authors, see in particular [Plo77].

The denotational semantics of PCF and of its extensions by various kinds of effects is one of the major research topics in the semantics of programming languages because of the relative simplicity of the language combined with its computational expressiveness and because of its extremely clean and canonical mathematical semantics. The development of major functional programming languages such as Ocaml, Haskell or F# benefited from these theoretical studies.

As far as purely functional features of these languages are considered, the standard setting of cartesian closed categories with a distinguished object for interpreting natural numbers and fix-point operators are sufficient. Most considered such categories have complete partially ordered sets as objects and all Scott continuous functions as morphisms. Extending such models with a probabilistic effect in order to build a model of a probabilistic functional language is a notoriously difficult problem, especially if we insist on objects to contain a reasonably "small" dense subset[1], see in particular [JT98]. More precisely, it seems very difficult to find cartesian closed categories of continuous domains equipped with a probabilistic powerdomain monad.

There is however another approach to the denotational semantics of probabilistic functional languages. Initiated in [Gir04] (based on earlier quantitative

[1]By this we mean that all objects of the sought category should contain a dense subset whose cardinality is less than a fixed cardinal. This is necessary in particular if we want the category to host models of the pure lambda-calculus.

ideas coming from [Gir88, Gir99, Ehr02]), this theory of *probabilistic coherence spaces* was further developed in [DE11] where it has been shown to provide a model of classical Linear Logic allowing also to interpret arbitrary fix-points of types, and hence to host many models of the pure lambda-calculus. We further studied this semantics in [EPT11] where we proved an adequacy theorem in a pure lambda-calculus model, and in [ETP14] we also proved a full abstraction theorem for a probabilistic version of PCF, interpreted in the probabilistic coherence space model.

The goal of the present paper is to provide a more detailed presentation of this full abstraction result, recording also the proof of adequacy. With respect to [ETP14], our new presentation provides a major improvement concerning the syntax of the programming language under consideration.

Indeed, in this previous work we considered a *fully call-by-name* (CBN) version of probabilistic PCF. In this language, a closed term of type ι (the type of natural numbers) determines a sub-probability distribution on the natural numbers (with n we associate the probability that M reduces to the constant $\underline{n}$ of the language). A closed term P of type $\iota \Rightarrow \iota$ which receives M as argument will reduce M each time it needs its value (because the language is fully CBN) and will get different results each time unless the sub-probability distribution defined by M is concentrated on a single natural number. There are clearly cases where this is not a desirable behavior: sometimes we need to flip a coin and to use the result several times!

As an example, consider the problem of writing a program which takes an array f of integers of length n and returns an index i such that $f(i) = 0$; we want to apply a "Las Vegas" random algorithm consisting in choosing i randomly (with a uniform probability on $\{0, \dots, n-1\}$) repeatedly until we find an i such that $f(i) = 0$. This is implemented by means of a while loop (or, more precisely, of a recursively defined function since we are in a functional setting) where at each step we choose i randomly, test the value of $f(i)$ (first use of i) and return i (second use) if $f(i) = 0$. It is intuitively clear that this basic algorithm cannot be implemented with the usual conditional of PCF (it might be interesting and challenging to prove it).

To be able to write such an algorithm, we need to modify PCF a bit, allowing to use ground terms in a call-by-value (CBV) fashion (to simplify the presentation we use ι as single ground type).

Our choice has been to modify the conditional construct. The usual conditional construct $\mathsf{if}(M, P, Q)$ of PCF is operationally interpreted as follows: one first reduces M until one gets an integer n (or, more precisely, the corresponding term $\underline{n}$). If $n = 0$, one evaluates P and otherwise, one evaluates Q, in the current context of course. Again, the trouble is that, in the second case, the value obtained for M, namely $\underline{n}$, is lost, whereas Q might need it. This problem can be easily solved by using M within Q each time this value is needed. Although clearly inefficient, this solution is perfectly correct in the usual deterministic version of PCF. It is absolutely inadequate in our probabilistic setting since M should be considered as a *probabilistic process* whose reduction, or execution, will produce integer values with a sub-probability distribution depending on it. There is no reason for M to produce, within Q, the same result $\underline{n}$ that it reduced to during its first evaluation.

For these reasons, when M reduces to $\underline{n+1}$, our conditional construction $\mathsf{if}(M, P, z{\cdot}Q)$ allows to feed Q with $\underline{n}$ through the variable z (this has the positive side effect of making the predecessor function definable); in other words we have the reduction rules

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

$$\frac{M \to M'}{\mathsf{if}(M, P, z \cdot Q) \to \mathsf{if}(M', P, z \cdot Q)}$$

This means that our conditional construct allows to use a CBV reduction strategy, limited to the ground type of natural numbers.

From the point of view of Linear Logic and of its denotational models, this feature is completely justified by the fact that the object interpreting the type of natural numbers has a canonical structure of coalgebra for the ! exponential functor. Intuitively, this means that *evaluated natural numbers* can be freely discarded and duplicated. Pushing this idea further leads to consider a calculus [Ehr15a] close to Levy's Call-By-Push-Value [Lev06] whose probabilistic version will be considered in a forthcoming paper.

Contents. We present the syntax of Probabilistic PCF (pPCF) and its weak-reduction relation, that we formalize as an infinite dimensional stochastic matrix (indexed by pPCF terms). Based on this operational semantics, we define a notion of observational equivalence. Two terms of type σ in a typing context Γ are equivalent if, for any context $C^{\Gamma\vdash\sigma}$ of type ι in context Γ (with holes of type σ), the probability that $C[M]$ reduces to $\underline{0}$ (say) is equal to the probability that $C[M']$ reduces to $\underline{0}$.

Then we give various examples of programs written in this language, some of them will be essential in the proof of the Full Abstraction Theorem. In particular we implement the above mentioned simple Las Vegas algorithm.

Next, we introduce the model of Probabilistic Coherence Spaces (PCS), presented as a model of classical Linear Logic. We describe the interpretation of pPCF terms, presenting the semantics of terms as functions (this is possible because the Kleisli category of the !-comonad of this model is well-pointed). We prove an Adequacy Theorem which states that, for any closed term M of ground type ι and any $n \in \mathbb{N}$, the probability that M reduces to $\underline{n}$ is equal to the probability of n in the sub-probability distribution on $\mathbb{N}$ which is the semantics of M in the PCS model. This implies that any two closed terms of type σ which have the same interpretation in PCS are observationally equivalent.

Last we prove the converse implication showing that PCS is a Fully Abstract model of pPCF. The proof uses strongly the fact that, in our model, morphisms are analytic functions (with real non-negative coefficients) and that the coefficients of the entire series of two such functions are the same if the functions coincide on an open subset of their domain. Section 4 is devoted to this theorem and to its detailed proof; it starts with a more accurate description of our proof method.

1 Probabilistic PCF

There is only one ground type ι, types are defined by

$$\sigma, \tau, \ldots := \iota \mid \sigma \Rightarrow \tau$$

The terms of pPCF are defined as follows:

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

where $n \in \mathbb{N}$, $p \in [0,1] \cap \mathbb{Q}$ is a probability and x, $y \ldots$ are variables.

A typing context is a sequence $\Gamma = (x_1 : \sigma_1, \ldots, x_n : \sigma_n)$ where the x_i's are pairwise distinct variables. A typing judgment is an expression $\Gamma \vdash M : \sigma$ where Γ is a typing context, M is a term and σ is a type. The typing rules are as follows:

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

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

$$\frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \lambda x^{\sigma}\, M : \sigma \Rightarrow \tau} \qquad \frac{\Gamma \vdash M : \sigma \Rightarrow \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash (M)\, N : \tau} \qquad \frac{\Gamma \vdash M : \sigma \Rightarrow \sigma}{\Gamma \vdash \mathsf{fix}(M) : \sigma}$$

$$\frac{p \in [0,1] \cap \mathbb{Q}}{\Gamma \vdash \mathsf{coin}(p) : \iota}$$

Proposition 1 *Let M be a term and Γ be a typing context. There is at most one type σ such that $\Gamma \vdash M : \sigma$.*

The proof is a simple inspection of the typing rules.

Given terms M and N and given a variable x, we use $M\,[N/x]$ for the term M where x is substituted with N.

Lemma 2 *If $\Gamma, x : \sigma \vdash M : \tau$ and $\Gamma \vdash N : \sigma$, then $\Gamma \vdash M\,[N/x] : \tau$.*

The proof us a simple induction on the structure of M.

1.1 Reduction rules

Given two terms M, M' and a real number $p \in [0,1]$, we define $M \xrightarrow{p} M'$, meaning that M reduces in one step to M' with probability p, by the following deduction system.

We define first a deterministic reduction relation $\to_{\mathsf{d}}$ as follows.

$$\frac{}{(\lambda x^{\sigma}\, M)\, N \to_{\mathsf{d}} M\,[N/x]} \qquad \frac{}{\mathsf{fix}(M) \to_{\mathsf{d}} (M)\, \mathsf{fix}(M)}$$

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

Then we define the probabilistic reduction by the following rules.

$$\frac{M \to_{\mathsf{d}} M'}{M \xrightarrow{1} M'} \qquad \frac{}{\mathsf{coin}(p) \xrightarrow{p} \underline{0}} \qquad \frac{}{\mathsf{coin}(p) \xrightarrow{1-p} \underline{1}}$$

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

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

This reduction can be 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* if there is no reduction $M \xrightarrow{p} M'$.

1.2 Observational equivalence

Using this simple probabilistic reduction relation, we want now to define a notion of observational equivalence. For this purpose, we need first to describe as simply as possible the "transitive closure" of the probabilistic reduction relation defined in Section 1.1. We represent this relation as a matrix Red indexed by terms, the number $\mathsf{Red}_{M,M'}$ being the probability of M to reduce to M' in one step. We add also that $\mathsf{Red}_{M,M} = 1$ if M is weak-normal for the weak-reduction (that is, no reduction is possible from M); in all other cases we have $\mathsf{Red}_{M,M'} = 0$. In other words, we consider the reduction as a discrete time Markov chain whose states are terms, stationary states are weak-normal terms and whose associated stochastic matrix is Red. Saying that Red is stochastic means that the coefficients of Red belong to $[0, 1]$ and that, for any given term M, one has $\sum_{M'} \mathsf{Red}_{M,M'} = 1$ (actually there are at most two terms M' such that $\mathsf{Red}_{M,M'} \neq 0$). Then if M' is normal, $\mathsf{Red}^k_{M,M'}$ (where $\mathsf{Red}^k = \overbrace{\mathsf{Red} \cdots \mathsf{Red}}^{k}$ is the kth power of Red for the matricial product) represents the probability of M to reduce to M' in *at most k steps* and we obtain the probability of M to reduce to M' by taking the lub of these numbers; to obtain this effect our assumption that M' is a stationary state is crucial. We explain this in more details now, considering first the case of a general stochastic matrix S indexed by a countable set I of states.

1.2.1 Probability of convergence to a stationary state. Let I be a countable set and let $S \in [0, 1]^{I \times I}$ to be understood as a matrix with I-indexed rows and columns. One says that S is stochastic if $\forall i \in I \; \sum_{j \in I} S_{i,j} = 1$. Given two such matrices S and T, their product ST is given by $\forall (i, j) \in I^2 \; (ST)_{i,j} = \sum_{k \in I} S_{i,k} T_{k,j}$ and is also a stochastic matrix.

Let I^S_1 be the set of stationary states, $I^S_1 = \{i \in I \mid S_{i,i} = 1\}$ (so that if $i \in I^S_1$ and $S_{i,j} \neq 0$ then $i = j$). Let $(i, j) \in I \times I^S_1$. Then the n-indexed sequence $(S^n)_{i,j} \in [0, 1]$ is monotone. Indeed, for all n we have

$$\begin{aligned}(S^{n+1})_{i,j} &= \sum_{k \in I} (S^n)_{i,k} S_{k,j} \\ &\geq (S^n)_{i,j} S_{j,j} = (S^n)_{i,j}\end{aligned}$$

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

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

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

$$\begin{aligned}
\sum_{j\in I}(S^\infty)_{i,j} &= \sum_{j\in I_1^S} \sup_{n\in\mathbb{N}}(S^n)_{i,j} \\
&= \sup_{n\in\mathbb{N}} \sum_{j\in I_1^S}(S^n)_{i,j} \quad \text{by the monotone convergence theorem} \\
&\leq \sup_{n\in\mathbb{N}} \sum_{j\in I}(S^n)_{i,j} = 1
\end{aligned}$$

Let $i, j \in I$. A *path* from i to j is a sequence $w = (i_1, \dots, i_k)$ of elements of I (with $k \geq 1$) such that $i_1 = i$, $i_k = j$ and $i_k \neq i_l$ for all $l \in \{1, \dots, k-1\}$. The *weight* of w is $\mathsf{p}(w) = \prod_{l=1}^{k-1} S_{i_l, i_{l+1}}$. The *length* of w is $k-1$. We use $\mathsf{R}(i,j)$ to denote the set of all paths from i to j.

Lemma 3 *Let $(i,j) \in I \times I_1^S$. One has*

$$S^\infty_{i,j} = \sum_{w\in\mathsf{R}(i,j)} \mathsf{p}(w)\,.$$

The proof is easy. In order to obtain this property, it is important in the definition of paths that the last element does not occur earlier.

1.2.2 The stochastic matrix of terms. Let Γ be a typing context and σ be a type. Let Λ^σ_Γ be the set of all terms M such that $\Gamma \vdash M : \sigma$. In the case where Γ is empty, and so the elements of Λ^σ_Γ are closed, we use Λ^σ_0 to denote that set.

Let $\mathsf{Red}(\Gamma, \sigma) \in [0,1]^{\Lambda^\sigma_\Gamma \times \Lambda^\sigma_\Gamma}$ be the matrix (indexed by terms typable of type σ in context Γ) given by

$$\mathsf{Red}(\Gamma,\sigma)_{M,M'} = \begin{cases} p & \text{if } M \xrightarrow{p} M' \\ 1 & \text{if } M \text{ is weak-normal and } M' = M \\ 0 & \text{otherwise.} \end{cases}$$

This is a stochastic matrix. We also use the notation $\mathsf{Red}(\sigma)$ for the matrix $\mathsf{Red}(\Gamma, \sigma)$ when the typing context is empty.

When M' is weak-normal, the number $p = \mathsf{Red}(\Gamma,\sigma)^\infty_{M,M'}$ is the probability that M reduces to M' after a finite number of steps by Lemma 3. We write $M \downarrow^p M'$ if M' is weak-normal and $p = \mathsf{Red}(\Gamma,\sigma)^\infty_{M,M'}$.

1.2.3 Observation contexts. We define a syntax for observation contexts with several typed holes, all holes having the same type. They are defined exactly as terms, adding a new "constant symbol" $[\ ]^{\Gamma\vdash\sigma}$ where Γ is a typing context and σ is a type, which represents a hole which can be filled with a term M such that $\Gamma \vdash M : \sigma$. Such an observation context will be denoted with letters C, $D\dots$, adding $\Gamma \vdash \sigma$ as superscript for making explicit the typing judgment of the terms to be inserted in the hole of the context. So if C is an observation context with holes $[\ ]^{\Gamma\vdash\sigma}$, this context will often be written $C^{\Gamma\vdash\sigma}$ and the context where all holes have been filled with the term M will be denoted $C[M]$: this is just an ordinary pPCF term. Notice that, in $C[M]$, some (possibly all) free variables of M can be bound by λ's of C. For instance, if $C = \lambda x^\sigma\, [\ \ ]^{x:\sigma\vdash\sigma}$, then $C[x] = \lambda x^\sigma\, x$.

More formally, we give now the typing rules for observation contexts.

$$\frac{}{\Gamma, \Delta \vdash [\ \ ]^{\Delta\vdash\tau} : \tau}$$

$$\frac{}{\Gamma \vdash \underline{n}^{\Delta\vdash\tau} : \iota} \qquad \frac{}{\Gamma, x : \sigma \vdash x^{\Delta\vdash\tau} : \sigma} \qquad \frac{\Gamma \vdash C^{\Delta\vdash\tau} : \iota}{\Gamma \vdash \mathsf{succ}(C)^{\Delta\vdash\tau} : \iota}$$

$$\frac{\Gamma \vdash C^{\Delta\vdash\tau} : \iota \qquad \Gamma \vdash D^{\Delta\vdash\tau} : \sigma \qquad \Gamma, z : \iota \vdash E^{\Delta\vdash\tau} : \sigma}{\Gamma \vdash \mathsf{if}(C, D, z \cdot E)^{\Delta\vdash\tau} : \sigma}$$

$$\frac{\Gamma, x : \sigma \vdash C^{\Delta\vdash\varphi} : \tau}{\Gamma \vdash (\lambda x^\sigma\, C)^{\Delta\vdash\varphi} : \sigma \Rightarrow \tau}$$

$$\frac{\Gamma \vdash C^{\Delta\vdash\varphi} : \sigma \Rightarrow \tau \qquad \Gamma \vdash D^{\Delta\vdash\varphi} : \sigma}{\Gamma \vdash (C)\, D^{\Delta\vdash\varphi} : \tau} \qquad \frac{\Gamma \vdash C^{\Delta\vdash\tau} : \sigma \Rightarrow \sigma}{\Gamma \vdash \mathsf{fix}(C)^{\Delta\vdash\tau} : \sigma}$$

$$\frac{p \in [0,1] \cap \mathbb{Q}}{\Gamma \vdash \mathsf{coin}(p)^{\Delta\vdash\tau} : \iota}$$

Lemma 4 *If* $\Gamma \vdash C^{\Delta\vdash\tau} : \sigma$ *and* $\Delta \vdash M : \tau$, *then* $\Gamma \vdash C[M] : \sigma$.

The proof is a trivial induction on C.

1.2.4 Observational equivalence. Let $M, M' \in \Lambda^\sigma_\Gamma$ (that is, both terms have type σ in the typing context Γ). We say that M and M' are observationally equivalent (notation $M \sim M'$) if, for all observation contexts $C^{\Gamma\vdash\sigma}$ such that $\vdash C^{\Gamma\vdash\sigma} : \iota$, one has

$$\mathsf{Red}(\iota)^\infty_{C[M],\underline{0}} = \mathsf{Red}(\iota)^\infty_{C[M'],\underline{0}}$$

Remark: The choice of testing the probability of reducing to $\underline{0}$ in the definition above of observational equivalence is arbitrary. For instance, we would obtain the same notion of equivalence by stipulating that two terms M and M' typable of type σ in typing context Γ are observationally equivalent if, for all observation context $C^{\Gamma\vdash\sigma}$, one has

$$\sum_{n\in\mathbb{N}} \mathsf{Red}(\iota)^\infty_{C[M],\underline{n}} = \sum_{n\in\mathbb{N}} \mathsf{Red}(\iota)^\infty_{C[M'],\underline{n}}$$

that is, the two closed terms $C[M]$ and $C[M']$ have the same probability of convergence to some value. This is due to the universal quantification on C.

1.3 Basic examples

We give a series of terms written in pPCF which implement natural simple algorithms to illustrate the expressive power of the language. We explain intuitively the behavior of these programs, and one can also have a look at §2.10.1 where the denotational interpretations of these terms in PCS are given, presented as functions.

Given a type σ, we set $\Omega_\sigma = \mathsf{fix}(\lambda x^\sigma\, x)$ so that $\vdash \Omega_\sigma : \sigma$, which is the ever-looping term of type σ.

1.3.1 Arithmetics. The predecessor function, which is usually a basic construction of PCF, is now definable as:

$$\mathsf{pred} = \lambda x^{\iota}\, \mathsf{if}(x, \underline{0}, z \cdot z)$$

it is clear then that $(\mathsf{pred})\,\underline{0} \to_{\mathsf{d}}{}^{*} \underline{0}$ and that $(\mathsf{pred})\,\underline{n+1} \to_{\mathsf{d}}{}^{*} \underline{n}$.

The addition function can be defined as:

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

and it is easily checked that $\vdash \mathsf{add} : \iota \Rightarrow \iota \Rightarrow \iota$. Given $k \in \mathbb{N}$ we set

$$\mathsf{shift}_k = (\mathsf{add})\, \underline{k}$$

so that $\vdash \mathsf{shift}_k : \iota \Rightarrow \iota$.

The exponential function can be defined as:

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

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

In the same line, one defines a comparison function cmp

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

such that $(\mathsf{cmp})\, \underline{n}\, \underline{m}$ reduces to $\underline{0}$ if $n \leq m$ and to $\underline{1}$ otherwise.

1.3.2 More tests. By induction on k, we define a family of terms prob_k such that $\vdash \mathsf{prob}_k : \iota \Rightarrow \iota$:

$$\begin{aligned} \mathsf{prob}_0 &= \lambda x^{\iota}\, \mathsf{if}(x, \underline{0}, z \cdot \Omega_{\iota}) \\ \mathsf{prob}_{k+1} &= \lambda x^{\iota}\, \mathsf{if}(x, \Omega_{\iota}, z \cdot (\mathsf{prob}_k)\, z) \end{aligned}$$

For M such that $\vdash M : \iota$, the term $(\mathsf{prob}_k)\, M$ reduces to $\underline{0}$ with a probability which is equal to the probability of M to reduce to $\underline{k}$.

Similarly, we also define prod_k such that $\vdash \mathsf{prod}_k : \iota^k \Rightarrow \iota$:

$$\begin{aligned} \mathsf{prod}_0 &= \underline{0} \\ \mathsf{prod}_{k+1} &= \lambda x^{\iota}\, \mathsf{if}(x, \mathsf{prod}_k, z \cdot \Omega_{\iota^k \Rightarrow \iota})\,. \end{aligned}$$

Given closed terms $M_1, \dots, M_k$ such that $\vdash M_i : \iota$, the term $(\mathsf{prod}_k)\, M_1 \cdots M_k$ reduces to 0 with probability $\prod_{i=1}^{k} p_i$ where p_i is the probability of M_i to reduce to $\underline{0}$.

Given a type σ and $k \in \mathbb{N}$, we also define a term choose_k such that $\vdash \mathsf{choose}_k : \iota \Rightarrow \sigma^k \Rightarrow \sigma$

$$\begin{aligned} \mathsf{choose}_0 &= \lambda \xi^{\iota}\, \Omega_{\sigma} \\ \mathsf{choose}_{k+1} &= \lambda \xi^{\iota}\, \lambda x_1^{\sigma} \cdots \lambda x_{k+1}^{\sigma}\, \mathsf{if}(\xi, x_1, \zeta \cdot (\mathsf{choose}_k)\, \zeta\, x_2 \cdots x_{k+1})\,. \end{aligned}$$

Given a closed term M such that $\vdash M : \iota$ and terms $N_1, \dots, N_k$ such that $\Gamma \vdash N_i : \sigma$ for each i, the term $(\mathsf{choose}_i)\, M\, N_1 \cdots N_k$ reduces to N_i with the probability that M reduces to $\underline{i}$.

1.3.3 The let construction. This version of PCF, which is globally CBN, offers however the possibility of handling integers in a CBV way. For instance, we can set

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

and this construction can be typed as:

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

One can also check that the following reduction inference holds

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

whereas *it is no true* that

$$\frac{M\xrightarrow{p}M'}{N\left[M/x\right]\xrightarrow{p}N\left[M'/x\right]}$$

(consider cases where x does not occur in N, or occurs twice...). We have of course

$$\frac{}{\mathsf{let}\ x\ \mathsf{be}\ \underline{n}\ \mathsf{in}\ N\rightarrow_{\mathsf{d}} N\left[\theta(n)/x\right]}$$

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.

1.3.4 Random generators. Using these constructions, 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 $0,\dots,2^n-1$:

$$\mathsf{unif}_2=\mathsf{fix}(\lambda u^{\iota\Rightarrow\iota}\,\lambda x^{\iota}\,\mathsf{if}(x,\underline{0},z\cdot\mathsf{if}(\mathsf{coin}(1/2),(u)\,z,z'\cdot(\mathsf{add})\,(\mathsf{exp}_2)\,z\,(u)\,z)))\,.$$

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!).

Using this construction, one can define a function unif which, given an integer n, yields a uniform probability distribution on the integers $0,\dots,n$:

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

One checks easily that $\vdash\mathsf{unif}:\iota\Rightarrow\iota$. Given $n\in\mathbb{N}$, this function applies iteratively unif_2 until the result is $\leq n$. It is not hard to check that the resulting distribution is uniform (with probability $\frac{1}{n+1}$ for each possible result).

Last, let $n\in\mathbb{N}$ and let $\vec{p}=(p_0,\dots,p_n)$ be such that $p_i\in[0,1]\cap\mathbb{Q}$ and $p_0+\cdots+p_n\leq 1$. Then one defines a closed term $\mathsf{ran}(\vec{p})$ which reduces to $\underline{i}$ with probability p_i for each $i\in\{0,\dots,n\}$. The definition is by induction on n.

$$\mathsf{ran}(p_0,\dots,p_n)=\begin{cases}\underline{0} & \text{if } p_0=1 \text{ whatever be the value of } n\\ \mathsf{if}(\mathsf{coin}(p_0),\underline{0},z\cdot\Omega^{\iota}) & \text{if } n=0\\ \mathsf{if}(\mathsf{coin}(p_0),\underline{0},z\cdot\mathsf{succ}(\mathsf{ran}(\frac{p_1}{1-p_0},\dots,\frac{p_n}{1-p_0}))) & \text{otherwise}\end{cases}$$

Observe indeed that in the first case we must have $p_1=\cdots=p_n=0$.

1.3.5 A simple Las Vegas program. Given a function $f : \mathbb{N} \to \mathbb{N}$ and $n \in \mathbb{N}$, find a $k \in \{0, \dots, n\}$ such that $f(k) = 0$. This can be done by iterating random choices of k until we get a value such that $f(k) = 0$: this is probably the simplest example of a Las Vegas algorithm. The following function does the job:

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

with $\vdash M : (\iota \Rightarrow \iota) \Rightarrow \iota \Rightarrow \iota$. Our CBV integers are crucial here since without our version of the conditional, it would not be possible to get a random integer and use this value y both as an argument for f and as a result if the expected condition holds.

We develop now a denotational semantics for this language.

2 Probabilistic coherence spaces

We present shortly a model of probabilistic PCF which is actually a model of classical Linear Logic. For a longer and more detailed account, we refer to [DE11].

Let I be a countable set. Given $u, u' \in (\mathbb{R}^+)^I$, we set

$$\langle u, u' \rangle = \sum_{i \in I} u_i u'_i \in \mathbb{R}^+ \cup \{\infty\}\,.$$

Let $\mathcal{X} \subseteq (\mathbb{R}^+)^I$, we set

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

We have as usual

- $\mathcal{X} \subseteq \mathcal{Y} \Rightarrow \mathcal{Y}^\perp \subseteq \mathcal{X}^\perp$
- $\mathcal{X} \subseteq \mathcal{X}^{\perp\perp}$

and it follows that $\mathcal{X}^{\perp\perp\perp} = \mathcal{X}^\perp$.

2.1 Definition and basic properties of probabilistic coherence spaces

A *probabilistic coherence space* (PCS) is a pair $X = (|X|, \mathsf{P}X)$ where $|X|$ is a countable set and $\mathsf{P}X \subseteq (\mathbb{R}^+)^{|X|}$ satisfies

- $\mathsf{P}X^{\perp\perp} = \mathsf{P}X$ (equivalently, $\mathsf{P}X^{\perp\perp} \subseteq \mathsf{P}X$),
- for each $a \in |X|$ there exists $u \in \mathsf{P}X$ such that $u_a > 0$,
- for each $a \in |X|$ there exists $A > 0$ such that $\forall u \in \mathsf{P}X\ u_a \leq A$.

If only the first of these conditions holds, we say that X is a *pre-probabilistic coherence space* (pre-PCS).

The purpose of the second and third conditions is to prevent infinite coefficients to appear in the semantics. This property in turn will be essential for guaranteeing the morphisms interpreting proofs to be analytic functions, which will be the key property to prove full abstraction. So these conditions, though cosmetics at first sight, are important for our ultimate goal.

Lemma 5 *Let X be a pre-PCS. The following conditions are equivalent:*

- *X is a PCS,*
- $\forall a \in |X|\, \exists u \in \mathsf{P}X\, \exists u' \in \mathsf{P}X^{\perp}\ u_a > 0$ *and* $u'_a > 0$,
- $\forall a \in |X|\, \exists A > 0\, \forall u \in \mathsf{P}X\, \forall u' \in \mathsf{P}X^{\perp}\ u_a \leq A$ *and* $u'_a \leq A$.

The proof is straightforward.

We equip $\mathsf{P}X$ with the most obvious partial order relation: $u \leq v$ if $\forall a \in |X|\ u_a \leq v_a$ (using the usual order relation on $\mathbb{R}$).

Given $u \in (\mathbb{R}^+)^{|X|}$ and $I \subseteq |X|$ we use $u|_I$ for the element v of $(\mathbb{R}^+)^{|X|}$ such that $v_a = u_a$ if $a \in I$ and $v_a = 0$ otherwise. Of course $u \in \mathsf{P}X \Rightarrow u|_I \in \mathsf{P}X$.

Theorem 6 *$\mathsf{P}X$ is an ω-continuous domain. Given $u, v \in \mathsf{P}X$ and $\alpha, \beta \in \mathbb{R}^+$ such that $\alpha + \beta \leq 1$, one has $\alpha u + \beta v \in \mathsf{P}X$.*

Proof. Let us first prove that $\mathsf{P}X$ is complete. Let D be a directed subset of $\mathsf{P}X$. For any $a \in |X|$, the set $\{u_a \mid u \in D\}$ is bounded; let $v_a \in \mathbb{R}^+$ be the lub of that set. In that way we define $v = (v_a)_{a\in|X|} \in (\mathbb{R}^+)^{|X|}$.

We prove that $v \in \mathsf{P}X$. Let $u' \in \mathsf{P}X^{\perp}$, we must prove that $\langle v, u'\rangle \leq 1$. We know that $\{\langle u, u'\rangle \mid u \in D\} \subseteq [0, 1]$ and therefore this set has a lub $A \in [0, 1]$. Let $\varepsilon > 0$, we can find $u \in D$ such that $\langle u, u'\rangle \geq A - \varepsilon$ and since this holds for all ε, we have $\langle v, u'\rangle \geq A$. Let again $\varepsilon > 0$. We can find a finite set $I \subseteq |X|$ such that $\langle v|_I, u'\rangle \geq \langle v, u'\rangle - \frac{\varepsilon}{2}$. Since I is finite we have $\langle v|_I, u'\rangle = \sup_{u\in D}\langle u|_I, u'\rangle$ (it is here that we use our hypothesis that D is directed) and hence we can find $u \in D$ such that $\langle u|_I, u'\rangle \geq \langle v|_I, u'\rangle - \frac{\varepsilon}{2}$ and hence $\langle u, u'\rangle \geq \langle u|_I, u'\rangle \geq \langle v|_I, u'\rangle - \frac{\varepsilon}{2} \geq \langle v, u'\rangle - \varepsilon$. It follows that $A = \sup_{u\in D}\langle u, u'\rangle \geq \langle v, u'\rangle$. So $\langle v, u'\rangle \in [0, 1]$ and hence $v \in \mathsf{P}X$.

It is clear that v is the lub of D in $\mathsf{P}X$ since the order relation is defined pointwise. Therefore $\mathsf{P}X$ is a cpo, which has 0 as least element. Let R be the set of all the elements of $\mathsf{P}X$ which have a finite domain and take only rational values. Then it is clear that for each $u \in \mathsf{P}X$, the elements w of R which are way below u (in the present setting, this simply means that $w_a > 0 \Rightarrow w_a < u_a$) form a directed subset of $\mathsf{P}X$ whose lub is u. Therefore $\mathsf{P}X$ is an ω-continuous domain.

The last statement results from the linearity of the operation $u \mapsto \langle u, u'\rangle$. □

As a consequence, given a family $(u(i))_{i\in\mathbb{N}}$ of elements of $\mathsf{P}X$ and a family $(\alpha_i)_{i\in\mathbb{N}}$ of elements of $\mathbb{R}^+$ such that $\sum_{i\in\mathbb{N}} \alpha_i \leq 1$, one has $\sum_{i\in\mathbb{N}} \alpha_i u(i) \in \mathsf{P}X$.

2.2 Morphisms of PCSs

Let X and Y be PCSs. Let $t \in (\mathbb{R}^+)^{|X|\times|Y|}$ (to be understood as a matrix). Given $u \in \mathsf{P}X$, we define $t\,u \in \overline{\mathbb{R}^+}^{|Y|}$ by $(t\,u)_b = \sum_{a\in|X|} t_{a,b}u_a$ (application of the matrix t to the vector u)[2]. We say that t is a *(linear) morphism* from X to Y if $\forall u \in \mathsf{P}X\ t\,u \in \mathsf{P}Y$, that is

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

[2] This is an unordered sum, which is infinite in general. It makes sense because all its terms are ≥ 0.

The diagonal matrix $\mathsf{Id} \in (\mathbb{R}^+)^{|X|\times|X|}$ given by $\mathsf{Id}_{a,b} = 1$ if $a = b$ and $\mathsf{Id}_{a,b} = 0$ otherwise is a morphism. In that way we have defined a category **Pcoh** whose objects are the PCSs and whose morphisms have just been defined. Composition of morphisms is defined as matrix multiplication: let $s \in \mathbf{Pcoh}(X,Y)$ and $t \in \mathbf{Pcoh}(Y,Z)$, we define $t\,s \in (\mathbb{R}^+)^{|X|\times|Z|}$ by

$$(t\,s)_{a,c} = \sum_{b\in|Y|} s_{a,b}t_{b,c}$$

and a simple computation shows that $t\,s \in \mathbf{Pcoh}(X,Z)$. More precisely, we use the fact that, given $u \in \mathsf{P}X$, one has $(t\,s)\,u = t\,(s\,u)$. Associativity of composition holds because matrix multiplication is associative. Id_X is the identity morphism at X.

2.3 The norm

Given $u \in \mathsf{P}X$, we define $\|u\|_X = \sup\{\langle u,u'\rangle \mid u' \in \mathsf{P}X^\perp\}$. By definition, we have $\|u\|_X \in [0,1]$.

2.4 Multiplicative constructs

We start the description of the category **Pcoh** as a model of Linear Logic. For this purpose, we use Bierman's notion of Linear Category [Bie95], as presented in [Mel09] which is our main reference for this topic.

One sets $X^\perp = (|X|, \mathsf{P}X^\perp)$. It results straightforwardly from the definition of PCSs that $X^\perp$ is a PCS. Given $t \in \mathbf{Pcoh}(X,Y)$, one has $t^\perp \in \mathbf{Pcoh}(Y^\perp, X^\perp)$ if $t^\perp$ is the transpose of t, that is $(t^\perp)_{b,a} = t_{a,b}$.

One defines $X \otimes Y$ by $|X \otimes Y| = |X| \times |Y|$ and

$$\mathsf{P}(X\otimes Y) = \{u \otimes v \mid u \in \mathsf{P}X \text{ and } v \in \mathsf{P}Y\}^{\perp\perp}$$

where $(u\otimes v)_{(a,b)} = u_a v_b$. Then $X \otimes Y$ is a pre-PCS.

We have

$$\mathsf{P}(X\otimes Y^\perp)^\perp = \{u\otimes v' \mid u \in \mathsf{P}X \text{ and } v' \in \mathsf{P}Y^\perp\}^\perp = \mathbf{Pcoh}(X,Y)\,.$$

It follows that $X \multimap Y = (X \otimes Y^\perp)^\perp$ is a pre-PCS. Let $(a,b) \in |X| \times |Y|$. Since X and $Y^\perp$ are PCSs, there is $A > 0$ such that $u_a v'_b < A$ for all $u \in \mathsf{P}X$ and $v' \in \mathsf{P}Y^\perp$. Let $t \in (\mathbb{R}^+)^{|X\multimap Y|}$ be such that $t_{(a',b')} = 0$ for $(a',b') \neq (a,b)$ and $t_{(a,b)} = 1/A$, we have $t \in \mathsf{P}(X \multimap Y)$. This shows that $\exists t \in \mathsf{P}(X \multimap Y)$ such that $t_{(a,b)} > 0$. Similarly we can find $u \in \mathsf{P}X$ and $v' \in \mathsf{P}Y^\perp$ such that $\varepsilon = u_a v'_b > 0$. It follows that $\forall t \in \mathsf{P}(X \multimap Y)$ one has $t_{(a,b)} \leq 1/\varepsilon$. We conclude that $X \multimap Y$ is a PCS, and therefore $X \otimes Y$ is also a PCS.

Lemma 7 *Let X and Y be PCSs. One has $\mathsf{P}(X \multimap Y) = \mathbf{Pcoh}(X,Y)$. That is, given $t \in (\mathbb{R}^+)^{|X|\times|Y|}$, one has $t \in \mathsf{P}(X \multimap Y)$ iff for all $u \in \mathsf{P}X$, one has $t\,u \in \mathsf{P}Y$.*

This results immediately from the definition above of $X \multimap Y$.

Lemma 8 *Let X_1, X_2 and Y be PCSs. Let $t \in (\mathbb{R}^+)^{|X_1\otimes X_2\multimap Y|}$. One has $t \in \mathbf{Pcoh}(X_1 \otimes X_2, Y)$ iff for all $u_1 \in \mathsf{P}X_1$ and $u_2 \in \mathsf{P}X_2$ one has $t\,(u_1 \otimes u_2) \in \mathsf{P}Y$.*

Proof. The condition stated by the lemma is clearly necessary. Let us prove that it is sufficient: under this condition, it suffices to prove that

$$t^\perp \in \mathbf{Pcoh}(Y^\perp, (X_1 \otimes X_2)^\perp)\,.$$

Let $v' \in \mathsf{P}Y^\perp$, it suffices to prove that $t^\perp\, v' \in \mathsf{P}(X_1 \otimes X_2)^\perp$. So let $u_1 \in \mathsf{P}X_1$ and $u_2 \in \mathsf{P}X_2$, it suffices to prove that $\langle t^\perp\, v', u_1 \otimes u_2\rangle \leq 1$, that is $\langle t\,(u_1 \otimes u_2), v'\rangle \leq 1$, which follows from our assumption. □

Let $s_i \in \mathbf{Pcoh}(X_i, Y_i)$ for $i = 1, 2$. Then one defines

$$s_1 \otimes s_2 \in (\mathbb{R}^+)^{|X_1 \otimes X_2 \multimap Y_1 \otimes Y_2|}$$

by $(s_1 \otimes s_2)_{((a_1,a_2),(b_1,b_2))} = (s_1)_{(a_1,b_1)}(s_2)_{(a_2,b_2)}$ and one must check that $s_1 \otimes s_2 \in \mathbf{Pcoh}(X_1 \otimes X_2, Y_1 \otimes Y_2)$. This follows directly from Lemma 8. Let $1 = (\{*\}, [0,1])$. There are obvious choices of natural isomorphisms

$$\begin{aligned}
\lambda_X &\in \mathbf{Pcoh}(1 \otimes X, X)\\
\rho_X &\in \mathbf{Pcoh}(X \otimes 1, X)\\
\alpha_{X_1,X_2,X_3} &\in \mathbf{Pcoh}((X_1 \otimes X_2) \otimes X_3, X_1 \otimes (X_2 \otimes X_3))\\
\gamma_{X_1,X_2} &\in \mathbf{Pcoh}(X_1 \otimes X_2, X_2 \otimes X_1)
\end{aligned}$$

which satisfy the standard coherence properties. This shows that the structure $(\mathbf{Pcoh}, 1, \lambda, \rho, \alpha, \gamma)$ is a symmetric monoidal category.

2.4.1 Internal linear hom.

Given PCSs X and Y, let us define $\mathsf{ev} \in (\mathbb{R}^+)^{|(X \multimap Y) \otimes X \multimap Y|}$ by

$$\mathsf{ev}_{(((a',b'),a),b)} = \begin{cases} 1 & \text{if } (a,b) = (a',b') \\ 0 & \text{otherwise.} \end{cases}$$

Then it is easy to see that $(X \multimap Y, \mathsf{ev})$ is an internal linear hom object in $\mathbf{Pcoh}$, showing that this SMCC is closed. If $t \in \mathbf{Pcoh}(Z \otimes X, Y)$, the corresponding linearly curryfied morphism $\mathsf{cur}(t) \in \mathbf{Pcoh}(Z, X \multimap Y)$ is given by $\mathsf{cur}(t)_{(c,(a,b))} = t_{((c,a),b)}$.

2.4.2 *-autonomy.

Take $\perp = 1$, then one checks readily that the structure $(\mathbf{Pcoh}, 1, \lambda, \rho, \alpha, \gamma, \perp)$ is a *-autonomous category. The duality functor $X \mapsto (X \multimap \perp)$ can be identified with the strictly involutive contravariant functor $X \mapsto X^\perp$.

2.5 Additives

Let $(X_i)_{i\in I}$ be a countable family of PCSs. We define a PCS $\&_{i\in I} X_i$ by $|\&_{i\in I} X_i| = \bigcup_{i\in I}\{i\} \times |X_i|$ and $u \in \mathsf{P}(\&_{i\in I} X_i)$ if, for all $i \in I$, the family $u(i) \in (\mathbb{R}^+)^{|X_i|}$ defined by $u(i)_a = u_{(i,a)}$ belongs to $\mathsf{P}X_i$.

Lemma 9 *Let $u' \in (\mathbb{R}^+)^{|\&_{i\in I} X_i|}$. One has $u' \in \mathsf{P}(\&_{i\in I} X_i)^\perp$ iff*

- $\forall i \in I\ u'(i) \in \mathsf{P}X_i^\perp$
- *and* $\sum_{i\in I} \|u'(i)\|_{X_i^\perp} \leq 1$.

The proof is quite easy. It follows that $\&_{i\in I} X_i$ is a PCS. Moreover we can define $\pi_i \in \mathbf{Pcoh}(\&_{j\in I} X_j, X_i)$ by

$$(\pi_i)_{(j,a),a'} = \begin{cases} 1 & \text{if } j = i \text{ and } a = a' \\ 0 & \text{otherwise.} \end{cases}$$

Then $(\&_{i\in I} X_i, (\pi_i)_{i\in I})$ is the cartesian product of the family $(X_i)_{i\in I}$ in the category **Pcoh**. The coproduct $(\oplus_{i\in I} X_i, (\overline{\pi}_i)_{i\in I})$ is the dual operation, so that

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

and $u \in \mathsf{P}(\oplus_{i\in I} X_i)$ if $\forall i \in I\ u(i) \in \mathsf{P}X_i$ and $\sum_{i\in I} \|u(i)\|_{X_i} \leq 1$. The injections $\overline{\pi}_j \in \mathbf{Pcoh}(X_j, \oplus_{i\in I} X_i)$ are given by

$$(\overline{\pi}_i)_{a',(j,a)} = \begin{cases} 1 & \text{if } j = i \text{ and } a = a' \\ 0 & \text{otherwise.} \end{cases}$$

We define in particular $\mathbf{N} = \oplus_{i\in\mathbb{N}} 1$, that is $|\mathbf{N}| = \mathbb{N}$ and $u \in (\mathbb{R}^+)^{\mathbb{N}}$ belongs to $\mathsf{P}\mathbf{N}$ if $\sum_{n\in\mathbb{N}} u_n \leq 1$.

2.6 Exponentials

Given a set I, a *finite multiset* of elements of I is a function $\mu : I \to \mathbb{N}$ whose *support* $\mathsf{supp}(\mu) = \{a \in I \mid \mu(a) \neq 0\}$ is finite. We use $\mathcal{M}_{\mathrm{fin}}(I)$ for the set of all finite multisets of elements of I. Given a finite family $a_1, \dots, a_n$ of elements of I, we use $[a_1, \dots, a_n]$ for the multiset μ such that $\mu(a) = \#\{i \mid a_i = a\}$. We use additive notations for multiset unions: $\sum_{i=1}^k \mu_i$ is the multiset μ such that $\mu(a) = \sum_{i=1}^k \mu_i(a)$. The empty multiset is denoted as 0 or $[\,]$. If $k \in \mathbb{N}$, the multiset $k\mu$ maps a to $k\mu(a)$.

Let X be a PCS. Given $u \in \mathsf{P}X$ and $\mu \in \mathcal{M}_{\mathrm{fin}}(|X|)$, we define $u^\mu = \prod_{a\in|X|} u_a^{\mu(a)} \in \mathbb{R}^+$. Then we set $u^! = (u^\mu)_{\mu\in\mathcal{M}_{\mathrm{fin}}(|X|)}$ and finally

$$!X = (\mathcal{M}_{\mathrm{fin}}(|X|), \{u^! \mid u \in \mathsf{P}X\}^{\perp\perp})$$

which is a pre-PCS.

We check quickly that $!X$ so defined is a PCS. Let $\mu = [a_1, \dots, a_n] \in \mathcal{M}_{\mathrm{fin}}(|X|)$. Because X is a PCS, and by Theorem 6, for each $i = 1, \dots, n$ there is $u(i) \in \mathsf{P}X$ such that $u(i)_{a_i} > 0$. Let $(\alpha_i)_{i=1}^n$ be a family of strictly positive real numbers such that $\sum_{i=1}^n \alpha_i \leq 1$. Then $u = \sum_{i=1}^n \alpha_i u(i) \in \mathsf{P}X$ satisfies $u_{a_i} > 0$ for each $i = 1, \dots, n$. Therefore $u^!_\mu = u^\mu > 0$. This shows that there is $U \in \mathsf{P}(!X)$ such that $U_\mu > 0$.

Let now $A \in \mathbb{R}^+$ be such that $\forall u \in \mathsf{P}X\, \forall i \in \{1, \dots, n\}\ u_{a_i} \leq A$. For all $u \in \mathsf{P}X$ we have $u^\mu \leq A^n$. We have

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

Let $t \in (\mathbb{R}^+)^{|!X|}$ be defined by $t_\nu = 0$ if $\nu \neq \mu$ and $t_\mu = A^{-n} > 0$; we have $t \in (\mathsf{P}(!X))^\perp$. We have exhibited an element t of $(\mathsf{P}(!X))^\perp$ such that $t_\mu > 0$. By Lemma 5 it follows that $!X$ is a PCS.

2.6.1 Kleisli morphisms as functions.

Let $s \in (\mathbb{R}^+)^{|!X \multimap Y|}$. We define a function $\widehat{s} : \mathsf{P}X \to \overline{\mathbb{R}^+}^{|Y|}$ as follows. Given $u \in \mathsf{P}X$, we set

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

Proposition 10 *One has $s \in \mathsf{P}(!X \multimap Y)$ iff, for all $u \in \mathsf{P}X$, one has $\widehat{s}(u) \in \mathsf{P}Y$.*

Proof. By Lemma 7, the condition is necessary since $u \in \mathsf{P}X \Rightarrow u^! \in \mathsf{P}(!X)$, let us prove that it is sufficient. Given $v' \in \mathsf{P}Y^\perp$, it suffices to prove that $s^\perp\, v' \in \mathsf{P}(!X)^\perp$, that is $\langle s^\perp\, v', u^!\rangle \leq 1$ for all $u \in \mathsf{P}X$. This results from the assumption because $\langle s^\perp\, v', u^!\rangle = \langle \widehat{s}(u), v'\rangle$. □

Theorem 11 *Let $s \in \mathbf{Pcoh}(!X, Y)$. The function $\widehat{s}$ is Scott-continuous. Moreover, given $s, s' \in \mathbf{Pcoh}(!X, Y)$, one has $s = s'$ (as matrices) iff $\widehat{s} = \widehat{s'}$ (as functions $\mathsf{P}X \to \mathsf{P}Y$).*

Proof. Let us first prove that $\widehat{s}$ is Scott continuous. It is clear that this function is monotone. Let D be a directed subset of $\mathsf{P}X$ and let w be its lub, we must prove that $\widehat{s}(w) = \sup_{u \in D} \widehat{s}(u)$. Let $b \in |Y|$. Since multiplication is a Scott-continuous function from $[0,1]^2$ to $[0,1]$, we have $\widehat{s}(w)_b = \sum_{\mu \in |!X|} \sup_{u \in D} s_{\mu,b} u^\mu$. The announced property follows by the monotone convergence theorem.

Let now $s, s' \in \mathbf{Pcoh}(!X, Y)$ be such that $\widehat{s}(u) = \widehat{s'}(u)$ for all $u \in \mathsf{P}X$. Let $\mu \in |!X|$ and $b \in |Y|$, we prove that $s_{\mu,b} = s'_{\mu,b}$. Let $I = \mathsf{supp}(\mu)$. Given $u \in (\mathbb{R}^+)^I$, let $\eta(u) \in (\mathbb{R}^+)^{|X|}$ be defined by $\eta(u)_a = 0$ for $a \notin u$ and $\eta(u)_a = u_a$ for $a \in I$. Let $A > 0$ be such that $\eta([0,A]^I) \subseteq \mathsf{P}X$ (such an A exists because I is finite and by our definition of PCS). Let $\pi_b : \mathsf{P}Y \to \mathbb{R}$ be defined by $\pi_b(v) = v_b$. Let $f = \pi_b \circ \widehat{s} \circ \eta : [0,A]^I \to \mathbb{R}$ and $f' = \pi_b \circ \widehat{s'} \circ \eta$. Then we have $f = f'$ by our assumption on s and s'. But f and f' are entire functions and we have $f(u) = \sum_{\nu \in \mathcal{M}_{\mathrm{fin}}(I)} s_{\nu,b} \prod_{a \in I} u_a^{\nu(a)}$ and similarly for f' and s'. Since $[0,A]^I$ contains a non-empty open subset of $\mathbb{R}^I$, it follows that $s_{\nu,b} = s'_{\nu,b}$ for all $\nu \in \mathcal{M}_{\mathrm{fin}}(I)$. In particular, $s_{\mu,b} = s'_{\mu,b}$. □

So we can consider the elements of $\mathbf{Pcoh}_!(X, Y)$ (the morphisms of the Kleisli category of the comonad !_ on the category **Pcoh**) as particular Scott continuous functions $\mathsf{P}X \to \mathsf{P}Y$. Of course, not all Scott continuous function are morphisms in $\mathbf{Pcoh}_!$.

Example. Take $X = Y = 1$. A morphism in $\mathbf{Pcoh}_!(1, 1)$ can be seen as a function $f : [0,1] \to [0,1]$ such that $f(u) = \sum_{n=0}^\infty s_n u^n$ where the s_n's are ≥ 0 and satisfy $\sum_{n=0}^\infty s_n \leq 1$. Of course, not all Scott continuous function $[0,1] \to [0,1]$ are of that particular shape! Take for instance the function $f : [0,1] \to [0,1]$ defined by $f(u) = 0$ if $u \leq \frac{1}{2}$ and $f(u) = 2u - 1$ if $u > \frac{1}{2}$; this function f is Scott continuous but has no derivative at $u = \frac{1}{2}$ and therefore cannot be expressed as a power series.

Proposition 12 *Let $s, s' \in \mathbf{Pcoh}_!(X,Y)$ be such that $s \leq s'$ (as elements of $\mathsf{P}(!X \multimap Y)$). Then $\forall u \in \mathsf{P}X$ $\widehat{s}(u) \leq \widehat{s'}(u)$. Let $(s(i))_{i\in\mathbb{N}}$ be a monotone sequence of elements of $\mathbf{Pcoh}_!(X,Y)$ and let $s = \sup_{i\in\mathbb{N}} s(i)$. Then $\forall u \in \mathsf{P}X$ $\widehat{s}(u) = \sup_{i\in I} \widehat{s_i}(u)$.*

Proof. The first statement is obvious. The second one results from the monotone convergence Theorem. □

Remark: We can have $s, s' \in \mathbf{Pcoh}_!(X,Y)$ such that $\forall u \in \mathsf{P}X$ $\widehat{s}(u) \leq \widehat{s'}(u)$ but without having that $s \leq s'$. Take for instance $X = Y = 1$. As in the example above we can see $\widehat{s}$ and $\widehat{s'}$ as functions $[0,1] \to [0,1]$ given by $\widehat{s}(u) = \sum_{n=0}^{\infty} s_n u^n$ and $\widehat{s'}(u) = \sum_{n=0}^{\infty} s'_n u^n$, and $s \leq s'$ means that $\forall n \in \mathbb{N}$ $s_n \leq s'_n$. Then let s be defined by $s_n = 1$ if $n = 2$ and $s_n = 0$ otherwise, and s' be defined by $s'_n = 1$ if $n = 1$ and $s'_n = 0$ otherwise. We have $\widehat{s}(u) = u^2 \leq \widehat{s'}(u) = u$ for all $u \in [0,1]$ whereas s and s' are not comparable in $\mathsf{P}(!1 \multimap 1)$.

Given a multiset $\mu \in \mathcal{M}_{\mathrm{fin}}(I)$, we define its *factorial* $\mu! = \prod_{i\in I} \mu(i)!$ and its *multinomial coefficient* $\mathsf{mn}(\mu) = (\#\mu)!/\mu! \in \mathbb{N}^+$ where $\#\mu = \sum_{i\in I} \mu(i)$ is the cardinality of μ. Remember that, given an I-indexed family $a = (a_i)_{i\in I}$ of elements of a commutative semi-ring, one has the multinomial formula

$$\Big(\sum_{i\in I} a_i\Big)^n = \sum_{\mu\in\mathcal{M}_n(I)} \mathsf{mn}(\mu) a^\mu$$

where $\mathcal{M}_n(I) = \{\mu \in \mathcal{M}_{\mathrm{fin}}(I) \mid \#\mu = n\}$.

Given $\mu \in |!X|$ and $\nu \in |!Y|$ we define $\mathsf{L}(\mu,\nu)$ as the set of all multisets ρ in $\mathcal{M}_{\mathrm{fin}}(|X| \times |Y|)$ such that

$$\forall a \in |X| \sum_{b\in|Y|} \rho(a,b) = \mu(a) \quad \text{and} \quad \forall b \in |Y| \sum_{a\in|X|} \rho(a,b) = \nu(b)\,.$$

Let $t \in \mathbf{Pcoh}(X,Y)$, we define $!t \in (\mathbb{R}^+)^{!X\multimap !Y}$ by

$$(!t)_{\mu,\nu} = \sum_{\rho\in\mathsf{L}(\mu,\nu)} \frac{\nu!}{\rho!} t^\rho\,.$$

Observe that the coefficients in this sum are all non-negative integers.

Lemma 13 *For all $u \in \mathsf{P}X$ one has $!t\,u^! = (t\,u)^!$.*

Proof. Indeed, given $\nu \in |!Y|$, one has

$$\begin{aligned}
(t\,u)^!_\nu &= \prod_{b\in|Y|} \Big(\sum_{a\in|X|} t_{a,b} u_a\Big)^{\nu(b)} \\
&= \prod_{b\in|Y|} \Bigg(\sum_{\substack{\mu\in|!X| \\ \#\mu=\nu(b)}} \mathsf{mn}(\mu) u^\mu \prod_{a\in|X|} t_{a,b}^{\mu(a)}\Bigg) \\
&= \sum_{\substack{\theta\in|!X|^{|Y|} \\ \forall b\ \#\theta(b)=\nu(b)}} u^{\sum_{b\in|Y|}\theta(b)} \Big(\prod_{b\in|Y|} \mathsf{mn}(\theta(b))\Big) \Bigg(\prod_{\substack{a\in|X| \\ b\in|Y|}} t_{a,b}^{\theta(b)(a)}\Bigg)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\mu\in|!X|} u^\mu \sum_{\rho\in\mathsf{L}(\mu,\nu)} t^\rho \prod_{b\in Y} \frac{\nu(b)!}{\prod_{a\in|X|}\rho(a,b)!}\\
&= \sum_{\mu\in|!X|} (!t)_{\mu,\nu} u^\mu
\end{aligned}
$$

since there is a bijective correspondence between the $\theta \in |!X|^{|Y|}$ such that $\forall b \in |Y|\ \#\theta(b) = \nu(b)$ and the $\rho \in \bigcup_{\mu\in|!X|} \mathsf{L}(\mu,\nu)$ (observe that this union of sets is actually a disjoint union): this bijection maps θ to the multiset ρ defined by $\rho(a,b) = \theta(b)(a)$. □

Proposition 14 *For all $t \in \mathbf{Pcoh}(X,Y)$ one has $!t \in \mathbf{Pcoh}(!X,!Y)$ and the operation $t \mapsto !t$ is functorial.*

Proof. Immediate consequences of Lemma 13 and Theorem 11. □

2.6.2 Description of the exponential comonad. We equip now this functor with a structure of comonad: let $\mathsf{der}_X \in (\mathbb{R}^+)^{|!X\multimap X|}$ be given by $(\mathsf{der}_X)_{\mu,a} = \delta_{[a],\mu}$ (the value of the Kronecker symbol $\delta_{i,j}$ is 1 if $i = j$ and 0 otherwise) and $\mathsf{dig}_X \in (\mathbb{R}^+)^{|!X\multimap !!X|}$ be given by $(\mathsf{dig}_X)_{\mu,[\mu_1,\dots,\mu_n]} = \delta_{\sum_{i=1}^n \mu_i,\mu}$. Then we have $\mathsf{der}_X \in \mathbf{Pcoh}(!X,X)$ and $\mathsf{dig}_X \in \mathbf{Pcoh}(!X,!!X)$ simply because

$$\widehat{\mathsf{der}_X}(u) = u \quad\text{and}\quad \widehat{\mathsf{dig}_X}(u) = (u^!)^!$$

for all $u \in \mathsf{P}X$, as easily checked. Using these equations, one also checks easily the naturality of these morphisms, and the fact that $(!\_,\mathsf{der},\mathsf{dig})$ is a comonad.

As to the monoidality of this comonad, we introduce $\mu^0 \in (\mathbb{R}^+)^{|1\multimap !\top|}$ by $\mu^0_{*,[]} = 1$ and $\mu^2_{X,Y} \in (\mathbb{R}^+)^{|!X\otimes !Y\multimap !(X\&Y)|}$ by $(\mu^2_{X,Y})_{\lambda,\rho,\mu} = \delta_{\mu,1\cdot\lambda+2\cdot\rho}$ where $i\cdot[a_1,\dots,a_n] = [(i,a_1),\dots,(i,a_n)]$. It is easily checked that the required commutations hold (again, we refer to [Mel09]).

It follows that we can define a lax symmetric monoidal structure for the functor $!\_$ from the symmetric monoidal category $(\mathbf{Pcoh},\otimes)$ to itself, that is, for each $n \in \mathbb{N}$, a natural morphism

$$\mathsf{m}^{(n)}_{X_1,\dots,X_N} \in \mathbf{Pcoh}(!X_1\otimes\cdots\otimes !X_n, !(X_1\otimes\cdots\otimes X_n))$$

satisfying some coherence conditions.

Given $f \in \mathbf{Pcoh}(!X_1\otimes\cdots\otimes !X_n, Y)$, we define the *promotion* morphism $f^! \in \mathbf{Pcoh}(!X_1\otimes\cdots\otimes !X_n, !Y)$ as the following composition of morphisms in **Pcoh**

$$
\begin{array}{ccc}
!X_1\otimes\cdots\otimes !X_n & & !Y\\
{\scriptstyle \mathsf{dig}_{X_1}\otimes\cdots\otimes\mathsf{dig}_{X_n}}\downarrow & & \uparrow{\scriptstyle !f}\\
!!X_1\otimes\cdots\otimes !!X_n & \xrightarrow{\mathsf{m}^{(n)}_{!X_1,\dots,!X_n}} & !(!X_1\otimes\cdots\otimes !X_n)
\end{array}
\qquad (1)
$$

2.6.3 Cartesian closeness of the Kleisli category. The Kleisli category $\mathbf{Pcoh}_!$ of the comonad $!\_$ has the same objects as **Pcoh**, and $\mathbf{Pcoh}_!(X,Y) = \mathbf{Pcoh}(!X,Y)$. The identity morphism at object X is der_X and given $f \in$

$\mathbf{Pcoh}_!(X, Y)$ and $g \in \mathbf{Pcoh}_!(Y, Z)$ the composition of f and g in $\mathbf{Pcoh}_!$, denoted as $g \circ f$, is given by

$$g \circ f = g\, f^! \,.$$

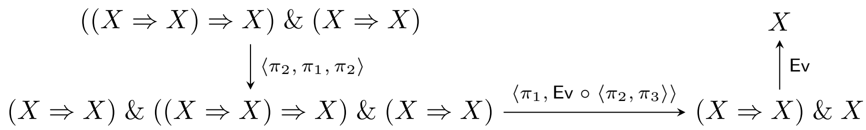
This category is cartesian closed: the terminal object is $\top$, the cartesian product of two objects X and Y is $X \mathbin{\&} Y$ (with projections defined in the obvious way, using $\mathsf{der}_{X \& Y}$ and the projections of the cartesian product in $\mathbf{Pcoh}$), their internal hom object is $X \Rightarrow Y = {!X} \multimap Y$. The corresponding evaluation morphism $\mathsf{Ev} \in \mathbf{Pcoh}_!((X \Rightarrow Y) \mathbin{\&} X, Y)$ is defined as the following composition of morphisms in $\mathbf{Pcoh}$

$$!((X \Rightarrow Y) \mathbin{\&} X) \xrightarrow{(\mu^2)^{-1}} !(X \Rightarrow Y) \otimes {!X} \xrightarrow{\mathsf{der} \otimes !X} (X \Rightarrow Y) \otimes {!X} \xrightarrow{\mathsf{ev}} Y$$

The curryfied version of a morphism $t \in \mathbf{Pcoh}_!(Z \mathbin{\&} X, Y)$ is the morphism $\mathsf{Cur}(t) \in \mathbf{Pcoh}_!(Z, X \Rightarrow Y)$ defined as $\mathsf{Cur}(t) = \mathsf{cur}(t\, \mu^2)$.

2.7 Least fix-point operator in the Kleisli category.

Let X be an object of $\mathbf{Pcoh}$. Let $\mathcal{F} \in \mathbf{Pcoh}_!((X \Rightarrow X) \Rightarrow X, (X \Rightarrow X) \Rightarrow X)$ be $\mathcal{F} = \mathsf{Cur}(\mathcal{F}_0)$ where $\mathcal{F}_0 \in \mathbf{Pcoh}_!(((X \Rightarrow X) \Rightarrow X) \mathbin{\&} (X \Rightarrow X), X)$ is the following composition of morphisms in $\mathbf{Pcoh}_!$

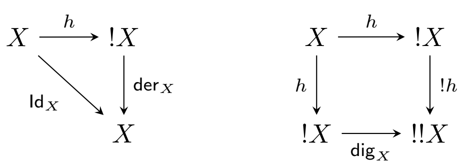


Then, given $F \in \mathsf{P}((X \Rightarrow X) \Rightarrow X)$, that is $F \in \mathbf{Pcoh}(X \Rightarrow X, X)$, one has $\widehat{\mathcal{F}}(F) = \mathsf{Ev} \circ \langle \mathsf{Id}_{X \Rightarrow X}, F \rangle \in \mathbf{Pcoh}(X \Rightarrow X, X)$. Since $\mathcal{F}$ is a morphism in $\mathbf{Pcoh}$, the function $\widehat{\mathcal{F}}$ is Scott continuous and therefore has a least fix-point $\mathsf{Y} \in \mathbf{Pcoh}(X \Rightarrow X, X)$, namely $\mathsf{Y} = \sup_{n \in \mathbb{N}} \widehat{\mathcal{F}}^n(0)$ (the sequence $(\widehat{\mathcal{F}}^n(0))_{n \in \mathbb{N}}$ is monotone in the cpo $\mathsf{P}((X \Rightarrow X) \Rightarrow X)$ because $\widehat{\mathcal{F}}$ is monotone).

If we set $\mathsf{Y}_n = \widehat{\mathcal{F}}^n(0) \in \mathbf{Pcoh}(X \Rightarrow X, X)$, we have $\mathsf{Y}_0 = 0$ and $\mathsf{Y}_{n+1} = \mathsf{Ev} \circ \langle \mathsf{Id}, \mathsf{Y}_n \rangle$ so that, given $f \in \mathbf{Pcoh}(X, X)$, we have $\widehat{\mathsf{Y}_n}(f) = \widehat{f}^n(0)$ and $\widehat{\mathsf{Y}}(f) = \sup_{n \in \mathbb{N}} \widehat{f}^n(0)$. So that Y is the usual least fix-point operator, and this operation turns out to be a morphism in $\mathbf{Pcoh}_!$, namely $\mathsf{Y} \in \mathbf{Pcoh}_!(X \Rightarrow X, X)$. This means that this standard least fix-point operator can be described as a power series, which is not completely obvious at first sight.

2.8 Coalgebras

By definition, a coalgebra of the $!\_$ comonad is a pair (X, h) where X is a PCS and $h \in \mathbf{Pcoh}(X, !X)$ satisfies the following commutations



A morphism from a coalgebra (X_1, h_1) to a coalgebra (X_2, h_2) is an $f \in \mathbf{Pcoh}(X_1, X_2)$ such that the following diagram commutes

$$\begin{array}{ccc} X_1 & \xrightarrow{f} & X_2 \\ {\scriptstyle h_1}\downarrow & & \downarrow{\scriptstyle h_2} \\ !X_1 & \xrightarrow[!f]{} & !X_2 \end{array}$$

Observe that 1 has a natural structure of !-coalgebra $\upsilon \in \mathbf{Pcoh}(1, !1)$ which is obtained as the following composition of morphisms

$$1 \xrightarrow{\mu^0} !\top \xrightarrow{\mathsf{dig}_\top} !!\top \xrightarrow{!(\mu^0)^{-1}} !1$$

Checking that $(1, \upsilon)$ is indeed a !-coalgebra boils down to a simple diagrammatic computation using the general axioms satisfied by the comonadic and monoidal structure of the !_ functor.

A simple computation shows that $\upsilon_{*,n} = 1$ for all $n \in |!1|$ (remember that $|!1| = \mathbb{N}$).

Let $(X_i, h_i)_{i \in I}$ be a countable family of coalgebras. Then we can endow $X = \bigoplus_{i \in I} X_i$ with a structure of coalgebra $h \in \mathbf{Pcoh}(X, !X)$. By the universal property of the coproduct, it suffices to define for each $i \in I$ a morphism $h'_i : X_i \to !X$. We set $h'_i = !\overline{\pi}_i \, h_i$ where we record that $\overline{\pi}_i : X_i \to X$ is the ith canonical injection into the coproduct. It is then quite easy to check that (X, h) so defined is a coalgebra using the fact that each (X_i, h_i) is a coalgebra.

2.8.1 Natural numbers. Consider the case where $I = \mathbb{N}$, $X_i = 1$ and $h_i = \upsilon$ for each $i \in \mathbb{N}$. Then we use N to denote the corresponding object X and h_N for the corresponding coalgebra structure, $h_\mathsf{N} \in \mathbf{Pcoh}(\mathsf{N}, !\mathsf{N})$. We use $\overline{n} \in \mathbf{Pcoh}(1, \mathsf{N})$ for the nth injection that we consider also as the element of PN defined by $\overline{n}_k = \delta_{n,k}$.

An easy computation shows that

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

Let $t \in \mathbf{Pcoh}_!(\mathsf{N}, X)$ for some object X of $\mathbf{Pcoh}$. Then $t \, h_\mathsf{N} \in \mathbf{Pcoh}(\mathsf{N}, X)$ is a linearized[3] version of t. Given $u \in \mathsf{PN}$, an easy computation shows that

$$t \, h_\mathsf{N} \, u = \sum_{n=0}^{\infty} u_n \widehat{t}(\overline{n}) \, .$$

The objects N and $1 \oplus \mathsf{N}$ are obviously isomorphic, through the morphisms $p \in \mathbf{Pcoh}(\mathsf{N}, 1 \oplus \mathsf{N})$ and $s \in \mathbf{Pcoh}(1 \oplus \mathsf{N}, \mathsf{N})$ given by

$$p_{n,(1,*)} = s_{(1,*),n} = \delta_{n,0} \text{ and } p_{n,(2,n')} = s_{(2,n'),n} = \delta_{n,n'+1}$$

We set $\overline{\mathsf{suc}} = s \, \overline{\pi}_2 \in \mathbf{Pcoh}(\mathsf{N}, \mathsf{N})$, so that $\overline{\mathsf{suc}}_{n,n'} = \delta_{n+1,n'}$ represents the successor function.

[3]This is not at all the same kind of linearization as the one introduced by Differential Linear Logic [Ehr15b].

2.9 Conditional

Given an object X of $\mathbf{Pcoh}$, we define a morphism

$$\overline{\mathsf{if}} \in \mathbf{Pcoh}(\mathsf{N} \otimes !X \otimes !(!\mathsf{N} \multimap X), X)\,.$$

For this, we define first $\overline{\mathsf{if}}_0 \in \mathbf{Pcoh}(1 \otimes !X \otimes !(!\mathsf{N} \multimap X), X)$ as the following composition of morphisms (without mentioning the isomorphisms associated with the monoidality of $\otimes$)

$$!X \otimes !(!\mathsf{N} \multimap X) \xrightarrow{!X \otimes \mathsf{w}} !X \xrightarrow{\mathsf{der}_X} X$$

and next $\overline{\mathsf{if}}_+ \in \mathbf{Pcoh}(\mathsf{N} \otimes !X \otimes !(!\mathsf{N} \multimap X), X)$ (with the same conventions as above)

$$\mathsf{N} \otimes !X \otimes !(!\mathsf{N} \multimap X) \xrightarrow{h_{\mathsf{N}} \otimes \mathsf{w} \otimes \mathsf{der}} !\mathsf{N} \otimes (!\mathsf{N} \multimap X) \xrightarrow{\mathsf{ev}\ \gamma} X$$

where γ is the isomorphism associated with the symmetry of the functor $\otimes$, see Section 2.4.

The universal property of $\oplus$ and the fact that $\_ \otimes Y$ is a left adjoint for each object Y allows therefore to define $\overline{\mathsf{if}}' \in \mathbf{Pcoh}((1 \oplus \mathsf{N}) \otimes !X \otimes !(!\mathsf{N} \multimap X), X)$. Finally our conditional morphism is $\overline{\mathsf{if}} = \overline{\mathsf{if}}'\,(p \otimes !X \otimes !(!\mathsf{N} \multimap X)) \in \mathbf{Pcoh}(\mathsf{N} \otimes !X \otimes !(!\mathsf{N} \multimap X), X)$. The isomorphism $p \in \mathbf{Pcoh}(\mathsf{N}, 1 \oplus \mathsf{N})$ is defined at the end of Section 2.8.

It is important to notice that the two following diagrams commute

$$\begin{array}{ccc}
1 \otimes !X \otimes !(!\mathsf{N} \multimap X) & \xrightarrow{\overline{0} \otimes \mathsf{Id}} & \mathsf{N} \otimes !X \otimes !(!\mathsf{N} \multimap X) \\
 & \searrow^{\mathsf{der} \otimes \mathsf{w}} & \downarrow \overline{\mathsf{if}} \\
 & & X
\end{array}$$

$$\begin{array}{ccc}
1 \otimes !X \otimes !(!\mathsf{N} \multimap X) & \xrightarrow{\overline{n+1} \otimes \mathsf{Id}} & \mathsf{N} \otimes !X \otimes !(!\mathsf{N} \multimap X) \\
\downarrow \overline{n}^! \otimes \mathsf{w} & & \downarrow \overline{\mathsf{if}} \\
!\mathsf{N} \otimes (!\mathsf{N} \multimap X) & \xrightarrow{\mathsf{ev}\ \gamma} & X
\end{array}$$

This second commutation boils down to the following simple property: $\forall n \in \mathbb{N}\ h_{\mathsf{N}}\,\overline{n} = \overline{n}^!$. Observe that it is not true however that $\forall u \in \mathsf{PN}\ h_{\mathsf{N}}\,u = u^!$. This means that h_{N} allows to duplicate and erase "true" natural numbers $\overline{n}$ but not general elements of PN which can be considered as "computations" and not as "values".

2.10 Interpreting terms

Given a type σ, we define an object $[\![\sigma]\!]$ of $\mathbf{Pcoh}$ as follows: $[\![\iota]\!] = \mathsf{N}$ and $[\![\sigma \Rightarrow \tau]\!] = [\![\sigma]\!] \Rightarrow [\![\tau]\!]$.

Given a context $\Gamma = (x_1 : \sigma_1, \ldots, x_k : \sigma_k)$, a type σ and a term M such that $\Gamma \vdash M : \sigma$, we define a morphism $[\![M]\!]_\Gamma \in \mathbf{Pcoh}_!([\![\Gamma]\!], [\![\sigma]\!])$ where $[\![\Gamma]\!] = [\![\sigma_1]\!] \mathbin{\&} \cdots \mathbin{\&} [\![\sigma_k]\!]$. Equivalently, we can see $[\![M]\!]_\Gamma$ as a morphism in

$\mathbf{Pcoh}(\llbracket\Gamma\rrbracket^!, \llbracket\sigma\rrbracket)$ where $\llbracket\Gamma\rrbracket^! = !\llbracket\sigma_1\rrbracket \otimes \cdots \otimes !\llbracket\sigma_k\rrbracket$. By Theorem 11, this morphism can be fully described as a function $\widehat{\llbracket M\rrbracket_\Gamma} : \prod_{i=1}^k \mathsf{P}\llbracket\sigma_i\rrbracket \to \mathsf{P}\llbracket\sigma\rrbracket$. The definition is by induction on the typing derivation of $\Gamma \vdash M : \sigma$, or, equivalently, on M.

If $M = x_i$, then $\llbracket M\rrbracket_\Gamma = \pi_i$, that is $\widehat{\llbracket M\rrbracket_\Gamma}(u_1, \dots, u_k) = u_i$.

If $M = \underline{n}$, then $\llbracket M\rrbracket_\Gamma = \overline{n} \circ \tau$ where τ is the unique morphism in $\mathbf{Pcoh}_!(\llbracket\Gamma\rrbracket, \top)$. That is $\widehat{\llbracket M\rrbracket_\Gamma}(\vec{u}) = \overline{n}$.

If $M = \mathsf{coin}(p)$ for some $p \in [0,1] \cap \mathbb{Q}$ then $\llbracket M\rrbracket_\Gamma = p\overline{0} + (1-p)\overline{1}$.

If $M = \mathsf{succ}(P)$ with $\Gamma \vdash P : \iota$, we have $\llbracket P\rrbracket_\Gamma \in \mathbf{Pcoh}(\llbracket\Gamma\rrbracket^!, \mathsf{N})$ and we set $\llbracket M\rrbracket_\Gamma = \overline{\mathsf{suc}}\, \llbracket P\rrbracket_\Gamma$, which is characterized by $\widehat{\llbracket M\rrbracket_\Gamma}(\vec{u}) = \sum_{n=0}^{\infty} (\widehat{\llbracket P\rrbracket_\Gamma}(\vec{u}))_n \overline{n+1}$.

If $M = \mathsf{if}(P, Q, z \cdot R)$, $\Gamma \vdash P : \iota$, $\Gamma \vdash Q : \sigma$ and $\Gamma, z : \iota \vdash R : \sigma$ then by inductive hypothesis we have $\llbracket P\rrbracket_\Gamma \in \mathbf{Pcoh}(\llbracket\Gamma\rrbracket^!, \mathsf{N})$, $\llbracket Q\rrbracket_\Gamma \in \mathbf{Pcoh}(\llbracket\Gamma\rrbracket^!, \llbracket\sigma\rrbracket)$ and $\llbracket R\rrbracket_{\Gamma,z:\iota} \in \mathbf{Pcoh}(\llbracket\Gamma\rrbracket^! \otimes !\mathsf{N}, \llbracket\sigma\rrbracket)$. We have $\mathsf{cur}(\llbracket R\rrbracket_{\Gamma,z:\iota}) \in \mathbf{Pcoh}(\llbracket\Gamma\rrbracket^!, !\mathsf{N} \multimap \llbracket\sigma\rrbracket)$ and hence we define $\llbracket M\rrbracket_\Gamma$ as the following composition of morphisms in $\mathbf{Pcoh}$

$$\begin{array}{ccc} \llbracket\Gamma\rrbracket^! & & \llbracket\sigma\rrbracket \\ \downarrow \scriptstyle{\mathsf{contr}_\Gamma} & & \uparrow \scriptstyle{\overline{\mathsf{if}}} \\ \llbracket\Gamma\rrbracket^! \otimes \llbracket\Gamma\rrbracket^! \otimes \llbracket\Gamma\rrbracket^! & \xrightarrow{\llbracket M\rrbracket_\Gamma \otimes \llbracket P\rrbracket^!_\Gamma \otimes \mathsf{cur}(\llbracket R\rrbracket_{\Gamma,z:\iota})^!} & \mathsf{N} \otimes !\llbracket\sigma\rrbracket \otimes !(!\mathsf{N} \multimap \llbracket\sigma\rrbracket) \end{array}$$

where contr_Γ is an obvious composition of contraction morphisms and associativity and symmetry isomorphisms associated with the $\otimes$ functor (we also use promotion (1)). Seen as a function, this morphism is completely characterized by

$$\widehat{\llbracket M\rrbracket_\Gamma}(\vec{u}) = (\widehat{\llbracket P\rrbracket_\Gamma}(\vec{u}))_0 \widehat{\llbracket Q\rrbracket_\Gamma}(\vec{u}) + \sum_{n=0}^{\infty} (\widehat{\llbracket P\rrbracket_\Gamma}(\vec{u}))_{n+1} \widehat{\llbracket R\rrbracket_{\Gamma,z:\iota}}(\vec{u}, \overline{n})\,.$$

If $M = (P)\,Q$ with $\Gamma \vdash P : \sigma \Rightarrow \tau$ and $\Gamma \vdash Q : \sigma$ then we have $\llbracket P\rrbracket_\Gamma \in \mathbf{Pcoh}_!(\llbracket\Gamma\rrbracket^!, !\llbracket\sigma\rrbracket \multimap \llbracket\tau\rrbracket)$ and $\llbracket Q\rrbracket_\Gamma \in \mathbf{Pcoh}_!(\llbracket\Gamma\rrbracket^!, \llbracket\sigma\rrbracket)$ and we define $\llbracket M\rrbracket_\Gamma$ as the following composition of morphisms

$$\llbracket\Gamma\rrbracket^! \xrightarrow{\mathsf{contr}_\Gamma} \llbracket\Gamma\rrbracket^! \otimes \llbracket\Gamma\rrbracket^! \xrightarrow{\llbracket P\rrbracket_\Gamma \otimes \llbracket Q\rrbracket^!_\Gamma} (!\llbracket\sigma\rrbracket \multimap \llbracket\tau\rrbracket) \otimes !\llbracket\sigma\rrbracket \xrightarrow{\mathsf{ev}} \llbracket\tau\rrbracket$$

so that $\llbracket M\rrbracket_\Gamma$ is characterized by $\widehat{\llbracket M\rrbracket_\Gamma}(\vec{u}) = \widehat{\llbracket P\rrbracket_\Gamma}(\vec{u})(\widehat{\llbracket Q\rrbracket_\Gamma}(\vec{u}))$.

If $M = \lambda x^\sigma\, P$ with $\Gamma, x : \sigma \vdash P : \tau$ then we have $\llbracket P\rrbracket_{\Gamma,x:\sigma} \in \mathbf{Pcoh}(\llbracket\Gamma\rrbracket^! \otimes !\llbracket\sigma\rrbracket, \llbracket\tau\rrbracket)$ and we set $\llbracket M\rrbracket_\Gamma = \mathsf{cur}(\llbracket P\rrbracket_{\Gamma,x:\sigma}) \in \mathbf{Pcoh}(\llbracket\Gamma\rrbracket^!, !\llbracket\sigma\rrbracket \multimap \llbracket\tau\rrbracket)$ so that, given $\vec{u} \in \prod_{i=1}^k \mathsf{P}\llbracket\sigma_i\rrbracket$ (remember that $\Gamma = (x_1 : \sigma_1, \dots, x_k : \sigma_k)$), the semantics $\llbracket M\rrbracket_\Gamma(\vec{u})$ of M is the element of $\mathsf{P}(!\llbracket\sigma\rrbracket \multimap \llbracket\tau\rrbracket)$ which, as a function $\mathsf{P}\llbracket\sigma\rrbracket \to \mathsf{P}\llbracket\tau\rrbracket$, is characterized by $\widehat{\llbracket M\rrbracket_\Gamma}(\vec{u})(u) = \widehat{\llbracket P\rrbracket_{\Gamma,x:\sigma}}(\vec{u}, u)$.

If $M = \mathsf{fix}(P)$ with $\Gamma \vdash P : \sigma \Rightarrow \sigma$ then we have $\llbracket P\rrbracket_\Gamma \in \mathbf{Pcoh}(\llbracket\Gamma\rrbracket^!, !\llbracket\sigma\rrbracket \multimap \llbracket\sigma\rrbracket)$ and we set $\llbracket M\rrbracket_\Gamma = \mathsf{Y}\,\llbracket P\rrbracket^!_\Gamma$. This means that $\widehat{\llbracket M\rrbracket_\Gamma}(\vec{u}) = \sup_{n\in\mathbb{N}} f^n(0)$ where $f \in \mathbf{Pcoh}_!(\llbracket\sigma\rrbracket, \llbracket\sigma\rrbracket)$ is given by $f(u) = \widehat{\llbracket P\rrbracket_\Gamma}(\vec{u})(u)$.

Lemma 15 (Substitution) *Assume that* $\Gamma, x : \sigma \vdash M : \tau$ *and that* $\Gamma \vdash P : \sigma$. *Then* $\llbracket M\,[P/x]\rrbracket_\Gamma = \llbracket M\rrbracket_{\Gamma,x:\sigma} \circ \langle \mathsf{Id}_{\llbracket\Gamma\rrbracket}, \llbracket P\rrbracket_\Gamma\rangle$ *in* $\mathbf{Pcoh}_!$. *In other words, for any* $\vec{u} \in \mathsf{P}\llbracket\Gamma\rrbracket$, *we have* $\widehat{\llbracket M\,[P/x]\rrbracket_\Gamma}(\vec{u}) = \widehat{\llbracket M\rrbracket_{\Gamma,x:\sigma}}(\vec{u}, \widehat{\llbracket P\rrbracket_\Gamma}(\vec{u}))$.

The proof is a simple induction on M, the simplest way to write it is to use the functional characterization of the semantics.

For the notations Λ^σ_Γ and Λ^σ_0 used below, we refer to §1.2.2. We formulate the invariance of the interpretation of terms under weak-reduction, using the stochastic reduction matrix introduced in §1.2.2.

Theorem 16 *Assume that* $\Gamma \vdash M : \sigma$. *One has*

$$[\![M]\!]_\Gamma = \sum_{M' \in \Lambda^\sigma_\Gamma} \mathsf{Red}(\Gamma, \sigma)_{M,M'} [\![M']\!]_\Gamma$$

Proof. Simple case analysis, on the shape of M, and using the Substitution Lemma. □

As a corollary we get the following inequality.

Theorem 17 *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 16 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. □

2.10.1 Examples. We refer to the various terms introduced in Section 1.3 and describe as functions the interpretation of some of them.

We have $\vdash \mathsf{pred} : \iota \Rightarrow \iota$ so $[\![\mathsf{pred}]\!] \in \mathsf{P}(\mathsf{N} \Rightarrow \mathsf{N})$, and one checks easily that $\widehat{[\![\mathsf{pred}]\!]}(u) = (u_0 + u_1)\overline{0} + \sum_{n=1}^{\infty} u_{n+1}\overline{n}$.

Similarly, we have

$$\begin{aligned}
\widehat{[\![\mathsf{add}]\!]}(u)(v) &= \sum_{n=0}^{\infty} \Big(\sum_{i=0}^{n} u_i v_{n-i}\Big)\overline{n} \\
\widehat{[\![\mathsf{exp}_2]\!]}(u) &= \sum_{n=0}^{\infty} u_n \overline{2^n} \\
\widehat{[\![\mathsf{shift}_k]\!]}(u) &= \sum_{n=0}^{\infty} u_n \overline{k+n} \\
\widehat{[\![\mathsf{cmp}]\!]}(u)(v) &= \Big(\sum_{i \leq j} u_i v_j\Big)\overline{0} + \Big(\sum_{i > j} u_i v_j\Big)\overline{1} \\
\widehat{[\![\mathsf{prob}_k]\!]}(u) &= u_k \overline{0} \\
\widehat{[\![\mathsf{prod}_k]\!]}(u^1, \dots, u^k) &= \Big(\prod_{i=1}^{k} u^i_0\Big)\overline{0} \\
\widehat{[\![\mathsf{choose}_k]\!]}(u)(w^1, \dots, w^k) &= \sum_{i=0}^{k-1} u_i w^{i+1}
\end{aligned}$$

$$\widehat{[\![\mathsf{unif}]\!]}(u) = \sum_{n=0}^{\infty} \frac{u_n}{n+1}\Big(\sum_{i=0}^{n} \bar{i}\Big) = \sum_{i=0}^{\infty}\Big(\sum_{n=i}^{\infty}\frac{u_n}{n+1}\Big)\bar{i}$$

$$[\![\mathsf{ran}(p_0,\dots,p_n)]\!] = \sum_{i=0}^{n} p_i \bar{i}$$

3 Adequacy

We want now to prove the converse inequality to that of Theorem 17.

For any type σ we define a binary relation $\mathcal{R}^\sigma \subseteq \Lambda_0^\sigma \times \mathsf{P}[\![\sigma]\!]$ by induction on types as follows:

- $M\ \mathcal{R}^\iota\ u$ if $\forall n \in \mathbb{N}\ u_n \leq \mathsf{Red}(\iota)^\infty_{M,\underline{n}}$
- $M\ \mathcal{R}^{\sigma\Rightarrow\tau}\ t$ if $\forall P \in \Lambda_0^\sigma\, \forall u \in \mathsf{P}[\![\sigma]\!]\ P\ \mathcal{R}^\sigma\ u \Rightarrow (M)\,P\ \mathcal{R}^\tau\ \widehat{t}(u)$. Here we have $t \in \mathsf{P}[\![\sigma \Rightarrow \tau]\!]$ and hence $\widehat{t} : \mathsf{P}[\![\sigma]\!] \to \mathsf{P}[\![\tau]\!]$

So $\mathcal{R}^\sigma$ is a logical relation.

Lemma 18 *If $M \in \Lambda_0^\sigma$ then $M\ \mathcal{R}^\sigma\ 0$. If $(u(i))_{i\in\mathbb{N}}$ is an increasing sequence in $\mathsf{P}[\![\sigma]\!]$ such that $\forall i \in \mathbb{N}\ M\ \mathcal{R}^\sigma\ u(i)$, then $M\ \mathcal{R}^\sigma\ \sup_{i\in\mathbb{N}} u(i)$.*

Proof. Simple induction on types, using Proposition 12. □

Lemma 19 *Assume that $\vdash M : \iota$, $\vdash P : \sigma$ and $z : \iota \vdash Q : \sigma$ where $\sigma = \sigma_1 \Rightarrow \cdots \sigma_k \Rightarrow \iota$. Let $N_1, \dots, N_k$ be terms such that $\vdash N_i : \sigma_i$ for $i = 1, \dots, k$.*

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

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

This is a straightforward consequence of the definition of weak-reduction, and of Lemma 3.

Lemma 20 *Let σ be a type. Let $M, M' \in \Lambda_0^\sigma$ and let $u \in \mathsf{P}[\![\sigma]\!]$. Then*

$$M'\ \mathcal{R}^\sigma\ u \Rightarrow M\ \mathcal{R}^\sigma\ \mathsf{Red}(\sigma)_{M,M'}u\,.$$

Proof. By induction on σ. Assume first that $\sigma = \iota$.

Assume that $M'\ \mathcal{R}^\iota\ u$. This means that, for all $n \in \mathbb{N}$, one has $u_n \leq \mathsf{Red}(\iota)^\infty_{M',\underline{n}}$. Let $n \in \mathbb{N}$, we want to prove that

$$\mathsf{Red}(\iota)^\infty_{M,\underline{n}} \geq \mathsf{Red}(\iota)_{M,M'}u_n$$

This results from the fact that $\mathsf{Red}(\iota)^\infty_{M,\underline{n}} = \sum_{M''\in\Lambda_0^\iota} \mathsf{Red}(\iota)_{M,M''}\mathsf{Red}(\iota)^\infty_{M'',\underline{n}}$ and from our hypothesis about M'.

Assume now that $\sigma = \tau \Rightarrow \varphi$ and let $f \in \mathsf{P}[\![\sigma]\!]$. Assume that $M'\ \mathcal{R}^{\tau\Rightarrow\varphi}\ f$, we want to prove that

$$M\ \mathcal{R}^{\tau\Rightarrow\varphi}\ \mathsf{Red}(\tau\Rightarrow\varphi)_{M,M'}f$$

If M is weak-normal then either $M' = M$ and then $\mathsf{Red}(\tau \Rightarrow \varphi)_{M,M'} = 1$ and we can directly apply our hypothesis that $M' \mathcal{R}^{\tau \Rightarrow \varphi} f$, or $M' \neq M$ and then $\mathsf{Red}(\tau \Rightarrow \varphi)_{M,M'} = 0$, and we can apply Lemma 18. So assume that M is not weak-normal.

Let $P \in \Lambda_0^\tau$ and $u \in \mathsf{P}[\![\tau]\!]$ be such that $P \mathcal{R}^\tau u$. We need to prove that

$$(M)\, P\, \mathcal{R}^\varphi\, \mathsf{Red}(\varphi)_{M,M'} f(u)\,.$$

This results from the inductive hypothesis and from the fact that, due to our definition of weak-reduction, it holds that $\mathsf{Red}(\tau \Rightarrow \varphi)_{M,M'} = \mathsf{Red}(\varphi)_{(M)P,(M')P}$ because M is not weak-normal. □

Remark: From now on, and for the purpose of avoiding too heavy notations, we often consider implicitly morphisms of $\mathbf{Pcoh}_!$ as functions. Typically, if $f \in \mathbf{Pcoh}_!(X,Y)$ and $u \in \mathsf{P}X$, we write as above $f(u)$ instead of $\widehat{f}(u)$.

Theorem 21 *Assume that $\Gamma \vdash M : \sigma$ where $\Gamma = (x_1 : \sigma_1, \dots, x_l : \sigma_l)$. For all families $(P_i)_{i=1}^l$ and $(u_i)_{i=1}^l$ one has*

$$(\forall i\ P_i\, \mathcal{R}^{\sigma_i}\, u_i) \Rightarrow M\,[P_1/x_1, \dots, P_l/x_l]\ \mathcal{R}^\sigma\ [\![M]\!]_\Gamma(u_1, \dots, u_l)$$

Proof. By induction on the derivation of $\Gamma \vdash M : \sigma$ (that is, on M).

The cases $M = x_i$ and $M = \underline{n}$ are straightforward.

Assume that $M = \mathsf{coin}(p)$ where $p \in [0,1] \cap \mathbb{Q}$. Then $\sigma = \iota$ and $[\![M]\!]_\Gamma(u_1, \dots, u_l) = p\overline{0} + (1-p)\overline{1}$. On the other hand

$$\mathsf{Red}(\iota)_{M[P_1/x_1,\dots,P_l/x_l],\underline{n}} = \begin{cases} p & \text{if } n = 0 \\ 1-p & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

and hence $(\forall i\ P_i\, \mathcal{R}^{\sigma_i}\, u_i) \Rightarrow M\,[P_1/x_1, \dots, P_l/x_l]\ \mathcal{R}^\sigma\ [\![M]\!]_\Gamma(u_1, \dots, u_l)$ by definition of $\mathcal{R}^\iota$.

Assume that $M = \mathsf{succ}(N)$. Assume that $\forall i\ P_i\, \mathcal{R}^{\sigma_i}\, u_i$. By inductive hypothesis we have $N\,[P_1/x_1, \dots, P_l/x_l]\ \mathcal{R}^\iota\ [\![N]\!]_\Gamma(u_1, \dots, u_l)$. This means that, for all $n \in \mathbb{N}$, one has

$$[\![N]\!]_\Gamma(u_1, \dots, u_l)_n \le \mathsf{Red}(\iota)^\infty_{N[P_1/x_1,\dots,P_l/x_l],\underline{n}}$$

It follows that, for all $n \in \mathbb{N}$,

$$[\![\mathsf{succ}(N)]\!]_\Gamma(u_1, \dots, u_l)_{n+1} \le \mathsf{Red}(\iota)^\infty_{\mathsf{succ}(N)[P_1/x_1,\dots,P_l/x_l],\underline{n+1}}$$

that is

$$\forall n \in \mathbb{N} \quad [\![\mathsf{succ}(N)]\!]_\Gamma(u_1, \dots, u_l)_n \le \mathsf{Red}(\iota)^\infty_{\mathsf{succ}(N)[P_1/x_1,\dots,P_l/x_l],\underline{n}}$$

since the inequality is obvious for $n = 0$.

Assume that $M = \mathsf{if}(P, Q, z \cdot R)$ with $\Gamma \vdash P : \iota$, $\Gamma \vdash Q : \sigma$ and $\Gamma, z : \iota \vdash R : \sigma$ with $\sigma = \tau_1 \Rightarrow \cdots \tau_h \Rightarrow \iota$. Assume that $\forall i\ P_i\, \mathcal{R}^{\sigma_i}\, u_i$. By inductive hypothesis, applying the definition of $\mathsf{Red}(\iota)$, we get

$$\forall n \in \mathbb{N} \quad \mathsf{Red}(\iota)^\infty_{P[P_1/x_1,\dots,P_l/x_l],\underline{n}} \ge [\![P]\!]_\Gamma(u_1, \dots, u_l)_n \tag{2}$$

$$Q\,[P_1/x_1,\dots,P_l/x_l]\;\mathcal{R}^\sigma\;[\![Q]\!]_\Gamma(u_1,\dots,u_l) \tag{3}$$
$$\forall n\in\mathbb{N}\quad R\,[P_1/x_1,\dots,P_l/x_l,\underline{n}/z]\;\mathcal{R}^\sigma\;[\![R]\!]_{\Gamma,z:\iota}(u_1,\dots,u_l,\overline{n}) \tag{4}$$

Observe that, in the last equation, we use the inductive hypothesis with $l+1$ parameters, and we use the fact that, obviously, $\underline{k}\;\mathcal{R}^\iota\;\overline{k}$. On the other hand, we have

$$\begin{aligned}[\![M]\!]_\Gamma(u_1,\dots,u_l) &= [\![P]\!]_\Gamma(u_1,\dots,u_l)_0[\![Q]\!]_\Gamma(u_1,\dots,u_l)\\ &\quad+\sum_{k=0}^{\infty}[\![P]\!]_\Gamma(u_1,\dots,u_l)_{k+1}[\![R]\!]_{\Gamma,z:\iota}(u_1,\dots,u_l,\overline{k})\end{aligned}$$

and we must prove that $M\,[P_1/x_1,\dots,P_l/x_l]\;\mathcal{R}^\sigma\;[\![M]\!]_\Gamma(u_1,\dots,u_l)$. So, for $j=1,\dots,h$, let R_j and v_j be such that $\vdash R_j:\tau_j$, $v_j\in\mathsf{P}[\![\tau_j]\!]$ and $R_j\;\mathcal{R}^{\tau_j}\;v_j$. We must prove that $(M\,[P_1/x_1,\dots,P_l/x_l])\,R_1\cdots R_h\;\mathcal{R}^\iota\;[\![M]\!]_\Gamma(u_1,\dots,u_l)(v_1)\cdots(v_h)$. Let $n\in\mathbb{N}$. By Lemma 19 we have

$$\begin{aligned}&\mathsf{Red}(\iota)^\infty_{(M[P_1/x_1,\dots,P_l/x_l])R_1\cdots R_h,\underline{n}}\\ &\quad=\mathsf{Red}(\iota)^\infty_{P[P_1/x_1,\dots,P_l/x_l],\underline{0}}\mathsf{Red}(\iota)^\infty_{(Q[P_1/x_1,\dots,P_l/x_l])R_1\cdots R_h,\underline{n}}\\ &\qquad+\sum_{k=0}^{\infty}\mathsf{Red}(\iota)^\infty_{P[P_1/x_1,\dots,P_l/x_l],\underline{k+1}}\mathsf{Red}(\iota)^\infty_{(R[P_1/x_1,\dots,P_l/x_l,\underline{k}/z])R_1\cdots R_h,\underline{n}}\end{aligned}$$

By (2), (3) and (4), and by definition of $\mathcal{R}^\sigma$, we have therefore

$$\begin{aligned}&\mathsf{Red}(\iota)^\infty_{(M[P_1/x_1,\dots,P_l/x_l])R_1\cdots R_h,\underline{n}}\\ &\quad\geq[\![P]\!]_\Gamma(u_1,\dots,u_l)_0[\![Q]\!]_\Gamma(u_1,\dots,u_l)(v_1)\cdots(v_h)_{\underline{n}}\\ &\qquad+\sum_{k=0}^{\infty}[\![P]\!]_\Gamma(u_1,\dots,u_l)_{\underline{k+1}}[\![R]\!]_\Gamma(u_1,\dots,u_l,\underline{k}/z)(v_1)\cdots(v_h)_{\underline{n}}\\ &\quad=[\![M]\!]_\Gamma(u_1,\dots,u_l)(v_1)\cdots(v_h)_{\underline{n}}\end{aligned}$$

that is $(M\,[P_1/x_1,\dots,P_l/x_l])\,R_1\cdots R_h\;\mathcal{R}^\iota\;[\![M]\!]_\Gamma(u_1,\dots,u_l)(v_1)\cdots(v_h)$ as contended.

Assume that $M=(P)\,Q$ with $\Gamma\vdash P:\tau\Rightarrow\sigma$ and $\Gamma\vdash Q:\tau$. Let $t=[\![P]\!]_\Gamma(u_1,\dots,u_l)$. Assume that $\forall i\;P_i\;\mathcal{R}^{\sigma_i}\;u_i$. By inductive hypothesis we have

$$P\,[P_1/x_1,\dots,P_l/x_l]\;\mathcal{R}^{\tau\Rightarrow\sigma}\;t$$

and $Q\,[P_1/x_1,\dots,P_l/x_l]\;\mathcal{R}^\tau\;[\![Q]\!]_\Gamma(u_1,\dots,u_l)$. Hence we have

$$((P)\,Q)\,[P_1/x_1,\dots,P_l/x_l]\;\mathcal{R}^\tau\;\widehat{t}([\![Q]\!]_\Gamma(u_1,\dots,u_l))$$

which is the required property since $\widehat{t}([\![Q]\!]_\Gamma(u_1,\dots,u_l))=[\![(P)\,Q]\!]_\Gamma(u_1,\dots,u_l)$ by definition of the interpretation of terms.

Assume that $\sigma=(\tau\Rightarrow\varphi)$, $M=\lambda x^\tau\,P$ with $\Gamma,x:\tau\vdash P:\varphi$. Let $t=[\![\lambda x^\tau\,P]\!]_\Gamma(u_1,\dots,u_l)$. Assume also that $\forall i\;P_i\;\mathcal{R}^{\sigma_i}\;u_i$. We must prove that

$$\lambda x^\tau\,(P\,[P_1/x_1,\dots,P_l/x_l])\;\mathcal{R}^{\tau\Rightarrow\varphi}\;t\,.$$

To this end, let Q be such that $\vdash Q : \tau$ and $v \in \mathsf{P}[\![\tau]\!]$ be such that $Q\ \mathcal{R}^\tau\ v$, we have to make sure that

$$(\lambda x^\tau\ (P\,[P_1/x_1,\ldots,P_l/x_l]))\,Q\ \mathcal{R}^\varphi\ \widehat{t}(v)\,.$$

By Lemma 20, it suffices to prove that $P\,[P_1/x_1,\ldots,P_l/x_l,Q/x]\ \mathcal{R}^\varphi\ \widehat{t}(v)$. This results from the inductive hypothesis since we have $\widehat{t}(v) = [\![P]\!]_{\Gamma,x:\tau}(u_1,\ldots,u_n,v)$ by cartesian closeness.

Last assume that $M = \mathsf{fix}(P)$ with $\Gamma \vdash P : \sigma \Rightarrow \sigma$. Assume also that $\forall i\ P_i\ \mathcal{R}^{\sigma_i}\ u_i$. We must prove that

$$\mathsf{fix}(P\,[P_1/x_1,\ldots,P_l/x_l])\ \mathcal{R}^\sigma\ [\![\mathsf{fix}(P)]\!]_\Gamma(u_1,\ldots,u_l) = \sup_{k=0}^{\infty} \widehat{t}^k(0)$$

where $t = [\![P]\!]_\Gamma(u_1,\ldots,u_l) \in \mathsf{P}([\![\sigma]\!] \Rightarrow [\![\sigma]\!])$. By Lemma 18, it suffices to prove that

$$\forall k \in \mathbb{N}\quad \mathsf{fix}(P\,[P_1/x_1,\ldots,P_l/x_l])\ \mathcal{R}^\sigma\ \widehat{t}^k(0)$$

and we proceed by induction on k. The base case $k = 0$ results from Lemma 18. Assume now that $\mathsf{fix}(P\,[P_1/x_1,\ldots,P_l/x_l])\ \mathcal{R}^\sigma\ \widehat{t}^k(0)$ and let us prove that

$$\mathsf{fix}(P\,[P_1/x_1,\ldots,P_l/x_l])\ \mathcal{R}^\sigma\ \widehat{t}^{k+1}(0)\,.$$

By Lemma 20, it suffices to prove that

$$(P\,[P_1/x_1,\ldots,P_l/x_l])\,\mathsf{fix}(P\,[P_1/x_1,\ldots,P_l/x_l])\ \mathcal{R}^\sigma\ \widehat{t}^{k+1}(0) = \widehat{t}(\widehat{t}^k(0))\,.$$

which results from the "internal" inductive hypothesis

$$\mathsf{fix}(P\,[P_1/x_1,\ldots,P_l/x_l])\ \mathcal{R}^\sigma\ \widehat{t}^k(0)$$

and from the "external" inductive hypothesis

$$P\,[P_1/x_1,\ldots,P_l/x_l]\ \mathcal{R}^{\sigma\Rightarrow\sigma}\ t\,.$$

□

In particular, if $\vdash M : \iota$ we have $\forall n \in \mathbb{N}\ \mathsf{Red}(\iota)^\infty_{M,\underline{n}} \geq ([\![M]\!])_n$. By Theorem 17 we have therefore the following operational interpretation of the semantics of ground type closed terms.

Theorem 22 *If $\vdash M : \iota$ then, for all $n \in \mathbb{N}$ we have $\forall n \in \mathbb{N}\ \mathsf{Red}(\iota)^\infty_{M,\underline{n}} = ([\![M]\!])_n$.*

As usual, the Adequacy Theorem follows straightforwardly. The observational equivalence relation on terms is defined in Section 1.2.

Lemma 23 *Given an observation context $C^{\Gamma\vdash\iota}$, there is a function f_C such that, for any term $M \in \Lambda^\sigma_\Gamma$, one has $[\![C[M]]\!]{=}f_C([\![M]\!]_\Gamma)$.*

The proof is a simple induction on C.

Theorem 24 (Adequacy) *Let $M, M' \in \Lambda^\sigma_\Gamma$ be terms of* pPCF. *If $[\![M]\!]_\Gamma = [\![M']\!]_\Gamma$ then $M \sim M'$.*

Proof. Assume that $[\![M]\!]_\Gamma = [\![M']\!]_\Gamma$. Let $C^{\Gamma\vdash\sigma}$ be an observation context such that $\vdash C^{\Gamma\vdash\sigma} : \iota$, we have

$$\begin{aligned}\mathsf{Red}(\iota)^\infty_{C[M],\underline{0}} &= [\![C[M]]\!]_0 \quad \text{by Theorem 22}\\ &= f_C([\![M]\!]_\Gamma)_0 \quad \text{by Lemma 23}\\ &= f_C([\![M']\!]_\Gamma)_0\\ &= \mathsf{Red}(\iota)^\infty_{C[M'],\underline{0}}\,.\end{aligned}$$

□

4 Full abstraction

We want now to prove the converse of Theorem 24, that is: given two terms M and M' such that $\Gamma \vdash M : \sigma$ and $\Gamma \vdash M' : \sigma$, if $M \sim M'$ then $[\![M]\!]_\Gamma = [\![M']\!]_\Gamma$. This means that **Pcoh** provides an equationally fully abstract model of pPCF.

4.1 Intuition

Let us first convey some intuitions about our approach to Full Abstraction. The first thing to say is that the usual method, which consists in proving that the model contains a collection of definable elements which is "dense" in a topological sense, does not apply here because definable elements are very sparse in **Pcoh**. For instance, in $\mathsf{P}[\![\iota \Rightarrow \iota]\!]$, there is an element t which is characterized by $\widehat{t}(u) = 4u_0u_1\overline{0}$. We have $t \in \mathsf{P}[\![\iota \Rightarrow \iota]\!]$ because, for any $u \in \mathsf{PN}$ we have $u_0 + u_1 \leq 1$ and hence $u_0u_1 \leq u_0(1-u_0) \leq 1/4$, and therefore $\widehat{t}(u) \in [0,1]$. It is easy to see that t is not definable in pPCF. The "best" definable approximation of t is obtained by means of the term $\lambda x^\iota\, \mathsf{if}(x, \mathsf{if}(x, \Omega^\iota, z' \cdot \mathsf{if}(z', \underline{0}, z'' \cdot \Omega^\iota)), z \cdot \Omega^\iota)$ whose interpretation s satisfies $\widehat{s}(u) = 2u_0u_1\overline{0}$.

Let M and M' be terms (that we suppose closed for simplifying and without loss of generality) such that $\vdash M : \sigma$ and $\vdash M' : \sigma$. Assume that $[\![M]\!] \neq [\![M']\!]$, we have to prove that $M \not\sim M'$. Let $a \in |[\![\sigma]\!]|$ be such that $[\![M]\!]_a \neq [\![M']\!]_a$. We define a term F such that $\vdash F : \sigma \Rightarrow \iota$ and $[\![(F)\,M]\!]_0 \neq [\![(F)\,M']\!]_0$. Then we use the observation context $C = (F)\,[\ \ ]^{\vdash\sigma}$ to separate M and M'. For defining F, *independently of* M *and* M', we associate with a a closed term a^- such that $\vdash a^- : \iota \Rightarrow \sigma \Rightarrow \iota$ and which has the following essential property:

> There is an $n \in \mathbb{N}$ – depending only on a – such that, given $w, w' \in \mathsf{P}[\![\sigma]\!]$ such that $w_a \neq w'_a$ there are rational numbers $p_0, \dots, p_{n-1} \in [0,1]$ such that $\widehat{[\![a^-]\!]}(u)(w)_0 \neq \widehat{[\![a^-]\!]}(u)(w')_0$ where $u = p_0\overline{0} + \cdots + p_{n-1}\overline{n-1}$.

Applying this property to $w = [\![M]\!]$ and $w' = [\![M']\!]$, we obtain the required term F by setting $F = (a^-)\,\mathsf{ran}(p_0, \dots, p_{n-1})$.

In order to prove this crucial property of a^-, we consider the map $\varphi_w : u \mapsto \widehat{[\![a^-]\!]}(u)(w)_0$ which is an entire function depending only on the n first components $u_0, \dots, u_{n-1}$ of $u \in \mathsf{PN}$ (again, n is a non-negative integer which depends only on a).

In Lemma 26, we prove that the coefficient in φ_w of the particular monomial $u_0 u_1 \dots u_{n-1}$ is w_a.

It follows that the functions φ_w and $\varphi_{w'}$ are different, and therefore take different values on an argument of shape $p_0\overline{0} + \cdots + p_{n-1}\overline{n-1}$ where all p_is are rational, because φ_w and $\varphi_{w'}$ are continuous functions.

4.2 Useful notions and constructs

We introduce some elementary material used in the proof.

- First, for a morphism $t \in \mathbf{Pcoh}_!(\mathsf{N}, X)$, we explain what it means to depend on finitely many parameters, considering t as a function from a subset of $(\mathbb{R}^+)^{\mathbb{N}}$ to $\mathsf{P}X$.
- Then we give the construction of the term a^- (testing term) and of the auxiliary term a^+. The interpretations of these terms are morphisms depending on a finite number of parameters; we define explicitly $|a|^-, |a|^+ \in \mathbb{N}$ which are the number of relevant parameters. We also give the interpretation of these morphisms as functions in the category $\mathbf{Pcoh}_!$.
- We introduce next useful notations which will be used in the proof of the main lemma.

4.2.1 Morphisms depending on a finite number of parameters. Let $k \in \mathbb{N}$. Let $\Delta_k = \overbrace{1 \oplus \cdots \oplus 1}^{k}$ so that $|\Delta_k| = \{0, \dots, k-1\}$ and $\mathsf{P}\Delta_k = \{x \in (\mathbb{R}^+)^k \mid x_0 + \cdots + x_{k-1} \leq 1\}$. We have two morphisms $\eta^+(k) \in \mathbf{Pcoh}_!(\Delta_k, \mathbf{N})$ and $\eta^-(k) \in \mathbf{Pcoh}_!(\mathbf{N}, \Delta_k)$ defined by

$$\eta^+(k)_{m,j} = \eta^-(k)_{m,j} = \begin{cases} 1 & \text{if } m = [j] \text{ and } j < k \\ 0 & \text{otherwise.} \end{cases}$$

Given $t \in \mathbf{Pcoh}_!(\mathbf{N}, X)$, the morphism $s = t \circ \eta^+(k) \circ \eta^-(k) \in \mathbf{Pcoh}_!(\mathbf{N}, X)$ satisfies

$$s(u) = t(u_0, \dots, u_{k-1}, 0, 0, \dots)$$

if we consider PN as a subset of $(\mathbb{R}^+)^{\mathbb{N}}$. We say that t *depends on at most k parameters* if $t = t \circ \eta^+(k) \circ \eta^-(k)$, which simply means that, for any $(m, a) \in |!\mathbf{N} \multimap X| = \mathcal{M}_{\mathrm{fin}}(\mathbb{N}) \times |X|$, if $t_{m,a} \neq 0$ then $m \in \mathcal{M}_{\mathrm{fin}}(\{0, \dots, k-1\})$.

If $t \in \mathbf{Pcoh}_!(\mathbf{N}, X)$, t is considered here as a function with infinitely many real parameters. Given $k \in \mathbb{N}$ and $u \in (\mathbb{R}^+)^{\mathbb{N}}$, we define $u\{k\} \in (\mathbb{R}^+)^{\mathbb{N}}$ by $u\{k\}_i = u_{i+k}$. Observe that $s = t \circ [\![\mathsf{shift}_k]\!]$ is characterized by $s(u) = t(u\{k\})$.

The term shift_k, as well as the other terms used below, is defined in Section 1.3.

4.2.2 Testing term associated with a point of the web. Given a type σ and an element a of $|[\![\sigma]\!]|$, we define two pPCF closed terms a^+ and a^- such that

$$\vdash a^+ : \iota \Rightarrow \sigma \quad \text{and} \quad \vdash a^- : \iota \Rightarrow \sigma \Rightarrow \iota\,.$$

The definition is by mutual induction on σ. We first associate with a two natural numbers $|a|^+$ and $|a|^-$.

If $\sigma = \iota$, and hence $a = n \in \mathbb{N}$, we set $|a|^+ = |a|^- = 0$.

If $\sigma = (\varphi \Rightarrow \psi)$ so that $a = ([b_1, \ldots, b_k], c)$ with $b_i \in |[\![\varphi]\!]|$ for each $i = 1, \ldots, k$ and $c \in |[\![\psi]\!]|$, we set

$$|a|^+ = |c|^+ + \sum_{i=1}^{k} |b_i|^-$$

$$|a|^- = |c|^- + k + \sum_{i=1}^{k} |b_i|^+$$

Assume that $\sigma = \iota$, then $a = n$ for some $n \in \mathbb{N}$. We set

$$a^+ = n^+ = \lambda \xi^\iota \, \underline{n} \quad \text{and} \quad a^- = n^- = \lambda \xi^\iota \, \mathsf{prob}_n$$

so that $[\![n^+]\!](u) = n$ and $[\![n^-]\!](u)(w) = w_n \overline{0}$.

Assume that $\sigma = (\varphi \Rightarrow \psi)$ so that $a = ([b_1, \ldots, b_k], c)$ with $b_i \in |[\![\varphi]\!]|$ for each $i = 1, \ldots, k$ and $c \in |[\![\psi]\!]|$. Then we define a^+ such that $\vdash a^+ : \iota \Rightarrow \varphi \Rightarrow \psi$ by

$$\begin{aligned} a^+ = \lambda \xi^\iota \, \lambda x^\varphi \, \mathsf{if}(\; & (\mathsf{prod}_k) \\ & \quad (b_1{}^-) \, \xi \, x \\ & \quad (b_2{}^-) \, (\mathsf{shift}_{|b_1|^-}) \, \xi \, x \\ & \quad \cdots \\ & \quad (b_k{}^-) \, (\mathsf{shift}_{|b_1|^- + \cdots + |b_{k-1}|^-}) \, \xi \, x, \\ & (c^+) \, (\mathsf{shift}_{|b_1|^- + \cdots + |b_k|^-}) \, \xi, \\ & [z]\Omega_\psi \;) \end{aligned}$$

Therefore we have, given $u \in \mathsf{P}\mathbf{N}$ and $w \in \mathsf{P}[\![\varphi]\!]$

$$[\![a^+]\!](u)(w) = \Big(\prod_{i=1}^{k} [\![b_i{}^-]\!] \Big(u \Big\{ \sum_{j=1}^{i-1} |b_j|^- \Big\} \Big)(w) \Big)_0 [\![c^+]\!] \Big(u \Big\{ \sum_{j=1}^{k} |b_j|^- \Big\} \Big) .$$

The term a^- is such that $\vdash a^- : \iota \Rightarrow (\varphi \Rightarrow \psi) \Rightarrow \iota$ and is defined by

$$\begin{aligned} a^- = \lambda \xi^\iota \, \lambda f^{\varphi \Rightarrow \psi} \; & (c^-) \, (\mathsf{shift}_{k + |b_1|^+ + \cdots + |b_k|^+}) \, \xi \\ & (f) \, (\mathsf{choose}_k) \, \xi \\ & \quad (b_1{}^+) \, (\mathsf{shift}_k) \, \xi \\ & \quad \cdots \\ & \quad (b_k{}^+) \, (\mathsf{shift}_{k + |b_1|^+ + \cdots + |b_{k-1}|^+}) \, \xi \, . \end{aligned}$$

Therefore we have, given $u \in \mathsf{P}\mathbf{N}$ and $t \in \mathsf{P}(\varphi \Rightarrow \psi)$

$$[\![a^-]\!](u)(t) = [\![c^-]\!](u\Big\{ k + \sum_{j=1}^{k} |b_j|^+ \Big\})(t\Big(\sum_{i=1}^{k} u_{i-1} [\![b_i{}^+]\!](u\Big\{ k + \sum_{j=1}^{i-1} |b_j|^+ \Big\}) \Big)) \, .$$

Lemma 25 *Let σ be a type and $a \in |[\![\sigma]\!]|$. Seen as an element of $\mathbf{Pcoh}_!(\mathbf{N}, [\![\sigma]\!])$ (resp. of $\mathbf{Pcoh}_!(\mathbf{N}, [\![\sigma \Rightarrow \iota]\!])$), $[\![a^+]\!]$ (resp. $[\![a^-]\!]$) depends on at most $|a|^+$ (resp. $|a|^-$) parameters.*

The proof is a simple induction on σ, based on an inspection of the expressions above for $[\![a^+]\!]$ and $[\![a^-]\!]$.

4.2.3 More notations. Let $I = \{n_1 < \cdots < n_k\}$ be a finite subset of $\mathbb{N}$, we use $\mathsf{o}(I)$ for the multiset $[n_1, \dots, n_k]$ where each element of I appears exactly once. Given $p, q \in \mathbb{N}$, we set

$$\mathsf{o}(p,q) = \mathsf{o}(\{p, p+1, \dots, p+q-1\})$$
$$\mathcal{M}_{\text{fin}}(p,q) = \mathcal{M}_{\text{fin}}(\{p, p+1, \dots, p+q-1\})\,.$$

These specific multisets, where each elements appears exactly once, play an essential role in Lemma 26.

Given $m \in \mathcal{M}_{\text{fin}}(\mathbb{N})$ and p and q as above, we use the notation $\mathsf{W}(m,p,q)$ for the element m' of $\mathcal{M}_{\text{fin}}(\mathbb{N})$ defined by

$$m'(i) = \begin{cases} m(i+p) & \text{if } 0 \leq i \leq q-1 \\ 0 & \text{otherwise} \end{cases}$$

and the notation $\mathsf{S}(m,p)$ for the element m' of $\mathcal{M}_{\text{fin}}(\mathbb{N})$ defined by $m'(i) = m(i+p)$ for each $i \in \mathbb{N}$.

So $\mathsf{W}(m,p,q)$ is obtained by selecting in m a "window" starting at index p and ending at index $p+q-1$ and by shifting this window by p to the left. Similarly $\mathsf{S}(m,p)$ is obtained by shifting m by p to the left.

Given a set I and an element i of I, we use e_i for the element of $(\mathbb{R}^+)^I$ defined by $(\mathsf{e}_i)_j = \delta_{i,j}$.

4.2.4 Expression of the semantics of testing terms. We write now the functions $[\![a^-]\!]$ and $[\![a^+]\!]$ in a form which makes explicit their dependency on their first argument $u \in \mathsf{P}\mathsf{N}$. This also allows to make explicit their dependency on a finite number of parameters.

Let σ be a type and let $a \in |[\![\sigma]\!]|$. By Lemma 25, for each $m \in \mathcal{M}_{\text{fin}}(0, |a|^+)$, there are uniquely defined $\pi(a,m) \in (\mathbb{R}^+)^{|[\![\sigma]\!]|}$ and $\mu(a,m) \in (\mathbb{R}^+)^{|([\![\sigma]\!] \Rightarrow \perp)|}$ such that we can write

$$[\![a^+]\!](u) = \sum_{m \in \mathcal{M}_{\text{fin}}(0,|a|^+)} u^m \pi(a,m) \tag{5}$$

for all $u \in \mathsf{P}\mathsf{N}$ and, for each $w \in \mathsf{P}[\![\sigma]\!]$,

$$[\![a^-]\!](u)(w)_0 = \sum_{m \in \mathcal{M}_{\text{fin}}(0,|a|^-)} u^m \mu(a,m)(w) \tag{6}$$

for all $u \in \mathsf{P}\mathsf{N}$.

Observe that, for any $w \in \mathsf{P}[\![\sigma]\!]$, we have

$$\mu(a,m)(w) = \sum_{h \in \mathcal{M}_{\text{fin}}(|[\![\sigma]\!]|)} \mu(a,m)_{(h,*)} w^h\,. \tag{7}$$

4.3 Proof of Full Abstraction

We can now state and prove the main lemma in the proof of full abstraction. This lemma uses notations introduced in Section 4.2.

Lemma 26 *Let σ be a type and let $a \in |[\![\sigma]\!]|$. We have*

$$\pi(a, \mathsf{o}(0, |a|^+)) = \mathsf{e}_a$$
$$\mu(a, \mathsf{o}(0, |a|^-)) = \mathsf{e}_{([a],*)}$$

that is, $\mu(a, \mathsf{o}(0, |a|^-))(w) = w_a$ for each $w \in \mathsf{P}[\![\sigma]\!]$.

Proof. By induction on σ. Assume that $\sigma = \iota$ so that $a = n \in \mathbb{N}$ and we have $|n|^+ = |n|^- = 0$. We have $[\![n^+]\!](u) = \mathsf{e}_n$ and $[\![n^-]\!](u)(w) = w_n$ as expected.

Assume now that $\sigma = \varphi \Rightarrow \psi$ so that a can be written

$$a = ([b_1, \dots, b_k], c)$$

for some $b_1, \dots, b_k \in |[\![\varphi]\!]|$ and $c \in |[\![\psi]\!]|$.

For each $u \in \mathsf{PN}$ and $w \in \mathsf{P}[\![\varphi]\!]$, we have

$$\begin{aligned}
[\![a^+]\!](u)(w) &= \prod_{i=1}^{k} \Big([\![{b_i}^-]\!](u\Big\{\sum_{j=1}^{i-1} |b_j|^-\Big\})(w)\Big)_0 [\![c^+]\!](u\Big\{\sum_{j=1}^{k} |b_j|^-\Big\}) \quad \text{see §4.2.2} \\
&= \prod_{i=1}^{k} \Big(\sum_{m \in \mathcal{M}_{\mathrm{fin}}(\sum_{j=1}^{i-1} |b_j|^-, |b_i|^-)} u^m \mu(b_i, \mathsf{S}(m, \sum_{j=1}^{i-1} |b_j|^-))(w)\Big) \\
&\qquad \Big(\sum_{m \in \mathcal{M}_{\mathrm{fin}}(\sum_{j=1}^{k} |b_j|^-, |c|^+)} u^m \pi(c, \mathsf{S}(m, \sum_{i=1}^{k} |b_i|^-))\Big) \quad \text{see §4.2.4} \\
&= \sum_{m \in \mathcal{M}_{\mathrm{fin}}(0, |a|^+)} u^m \Big(\prod_{i=1}^{k} \mu(b_i, \mathsf{W}(m, \sum_{j=1}^{i-1} |b_j|^-, |b_i|^-))(w)\Big) \\
&\qquad \pi(c, \mathsf{W}(m, \sum_{j=1}^{k} |b_j|^-, |c|^+))\,,
\end{aligned}$$

using the fact that $|a|^+ = \sum_{j=1}^{k} |b_i|^- + |c|^+$ and distributing products over sums. We also use the fact that there is a bijection

$$\begin{aligned}
\mathcal{M}_{\mathrm{fin}}(0, |a|^+) &\to \Big(\prod_{i=1}^{k} \mathcal{M}_{\mathrm{fin}}(\sum_{j=1}^{i-1} |b_j|^-, |b_i|^-)\Big) \times \mathcal{M}_{\mathrm{fin}}(\sum_{j=1}^{k} |b_j|^-, |c|^+) \\
m &\mapsto ((\mathsf{W}(m, \sum_{j=1}^{i-1} |b_j|^-, |b_i|^-))_{i=1}^{k}, \mathsf{W}(m, \sum_{j=1}^{k} |b_j|^-, |c|^+))\,.
\end{aligned}$$

Again we refer to §4.2.3 for the notations used in these expressions.

Therefore, given $m \in \mathcal{M}_{\mathrm{fin}}(0, |a|^+)$ and $w \in \mathsf{P}[\![\varphi]\!]$, the element $\pi(a, m)(w)$ of $\mathbb{R}^+$ satisfies

$$\pi(a, m)(w) = \Big(\prod_{i=1}^{k} \mu(b_i, \mathsf{W}(m, \sum_{j=1}^{i-1} |b_j|^-, |b_i|^-))(w)\Big) \pi(c, \mathsf{W}(m, \sum_{j=1}^{k} |b_j|^-, |c|^+))\,.$$

In this expression, we take now $m = \mathsf{o}(0, |a|^+)$. Since clearly $\mathsf{W}(m, p, q) = \mathsf{o}(0, q)$ for all $p, q \in \mathbb{N}$ such that $p + q \leq |a|^+$, we get, by inductive hypothesis:

$$\pi(a, \mathsf{o}(0, |a|^+))(w) = \Big(\prod_{i=1}^{k} w_{b_i}\Big)\mathsf{e}_c$$

and hence $\pi(a, \mathsf{o}(0, |a|^+)) = \mathsf{e}_a$ as contended.

Concerning a^-, for each $u \in \mathsf{PN}$ and $t \in \mathsf{P}[\![\varphi \Rightarrow \psi]\!]$, we have

$$
\begin{aligned}
[\![a^-]\!](u)(t)_0 &= [\![c^-]\!](u\Big\{k + \sum_{i=1}^{k} |b_i|^+\Big\})(t\Big(\sum_{i=1}^{k} u_{i-1}[\![{b_i}^+]\!](u\Big\{k + \sum_{j=1}^{i-1} |b_i|^+\Big\})\Big))_0 \\
&\qquad\qquad \text{see §4.2.2} \\
&= [\![c^-]\!](u\Big\{k + \sum_{i=1}^{k} |b_i|^+\Big\}) \\
&\quad (t\Big(\sum_{i=1}^{k} u_{i-1} \sum_{r \in \mathcal{M}_{\mathrm{fin}}(k+\sum_{j=1}^{i-1}|b_j|^+, |b_i|^+)} u^r \pi(b_i, \mathsf{S}(r, k + \sum_{j=1}^{i-1} |b_j|^+))\Big))_0 \\
&\qquad\qquad \text{see §4.2.4} \\
&= \sum_{\substack{l \in \mathcal{M}_{\mathrm{fin}}(k+\sum_{i=1}^{k}|b_i|^+, |c|^-) \\ h \in \mathcal{M}_{\mathrm{fin}}(|[\![\psi]\!]|)}} u^l \mu(c, \mathsf{S}(l, k + \sum_{i=1}^{k} |b_i|^+))_{(h,*)} \\
&\quad \Bigg(\sum_{(m',c') \in |[\![\varphi \Rightarrow \psi]\!]|} t_{m',c'} \Big(\sum_{i=1}^{k} u_{i-1} \\
&\qquad \sum_{r \in \mathcal{M}_{\mathrm{fin}}(k+\sum_{j=1}^{i-1}|b_j|^+, |b_i|^+)} u^r \pi(b_i, \mathsf{S}(r, k + \sum_{j=1}^{i-1} |b_j|^+))\Big)^{m'} \mathsf{e}_{c'}\Bigg)^h \\
&\qquad \text{by §4.2.4, (6), (7) and by definition of application in } \mathbf{Pcoh}_! \\
&= \sum_{\substack{l \in \mathcal{M}_{\mathrm{fin}}(k+\sum_{i=1}^{k}|b_i|^+, |c|^-) \\ h \in \mathcal{M}_{\mathrm{fin}}(|[\![\psi]\!]|)}} u^l \mu(c, \mathsf{S}(l, k + \sum_{i=1}^{k} |b_i|^+))_{(h,*)} \prod_{c' \in |[\![\psi]\!]|} A(c')^{h(c')}
\end{aligned}
$$

where, for each $c' \in |[\![\psi]\!]|$,

$$
\begin{aligned}
A(c') = & \sum_{m' \in \mathcal{M}_{\mathrm{fin}}(|[\![\varphi]\!]|)} t_{m',c'} \prod_{b \in |[\![\varphi]\!]|} \Big(\sum_{i=1}^{k} u^{[i-1]} \\
& \sum_{r \in \mathcal{M}_{\mathrm{fin}}(k+\sum_{j=1}^{i-1}|b_j|^+, |b_i|^+)} u^r \pi(b_i, \mathsf{S}(r, k + \sum_{j=1}^{i-1} |b_j|^+))_b\Big)^{m'(b)}
\end{aligned}
$$

where we recall that $[i-1]$ is the multiset which has $i-1$ as unique element. We can write $A(c') = \sum_{r \in \mathcal{M}_{\mathrm{fin}}(\mathbb{N})} u^r B(c')_r$ where u does not occur in the expression $B(c')_r$. For any $c' \in |[\![\psi]\!]|$, all the $r \in \mathcal{M}_{\mathrm{fin}}(\mathbb{N})$ such that $B(c')_r \neq 0$ satisfy $r \in \mathcal{M}_{\mathrm{fin}}(0, k + \sum_{i=1}^{k} |b_i|^+)$: this results from a simple inspection of the exponents of u in the expression $A(c')$. It follows that, for any $h \in \mathcal{M}_{\mathrm{fin}}(|[\![\psi]\!]|)$, we can write

$$\prod_{c' \in |[\![\psi]\!]|} A(c')^{h(c')} = \sum_{r \in \mathcal{M}_{\mathrm{fin}}(0, k+\sum_{i=1}^{k} |b_i|^+)} u^r D(r)_h \qquad (8)$$

where u does not occur in the expressions $D(r)_h$. With these notations, we have therefore

$$\begin{aligned}
[\![a^-]\!](u)(t)_0 &= \sum_{\substack{l \in \mathcal{M}_{\mathrm{fin}}(k+\sum_{i=1}^{k} |b_i|^+, |c|^-) \\ h \in \mathcal{M}_{\mathrm{fin}}(|[\![\psi]\!]|)}} u^l \mu(c, \mathsf{S}(l, k + \sum_{i=1}^{k} |b_i|^+))_{(h,*)} \prod_{c' \in |[\![\psi]\!]|} A(c')^{h(c')} \\
&= \sum_{\substack{m \in \mathcal{M}_{\mathrm{fin}}(0,|a|^-) \\ h \in \mathcal{M}_{\mathrm{fin}}(|[\![\psi]\!]|)}} u^m \mu(c, \mathsf{S}(m, k + \sum_{i=1}^{k} |b_i|^+))_h D(\mathsf{W}(m, 0, k + \sum_{i=1}^{k} |b_i|^+))_h
\end{aligned}$$

In the second line, the u^m results from the product of the u^l of the first line with the u^r arising from (8). Remember indeed that $|a|^- = k + \sum_{i=1}^{k} |b_i|^+ + |c|^-$. We are interested in the coefficient

$$\alpha = \mu(a, \mathsf{o}(0, |a|^-))(t) \qquad (9)$$

of $u^{\mathsf{o}(0,|a|^-)}$ in the sum above. We have

$$\alpha = \sum_{h \in \mathcal{M}_{\mathrm{fin}}(|[\![\psi]\!]|)} \mu(c, \mathsf{S}(\mathsf{o}(0, |a|^-), k + \sum_{i=1}^{k} |b_i|^+))_h \; D(\mathsf{W}(\mathsf{o}(0, |a|^-), 0, k + \sum_{i=1}^{k} |b_i|^+))_h \, .$$

But $\mathsf{S}(\mathsf{o}(0, |a|^-), k + \sum_{i=1}^{k} |b_i|^+) = \mathsf{o}(0, |c|^-)$ and hence, applying the inductive hypothesis to c, we get

$$\alpha = D(\mathsf{o}(0, k + \sum_{i=1}^{k} |b_i|^+))_{[c]} \, .$$

Coming back to (8), we see that α is the coefficient of $u^{\mathsf{o}(0,k+\sum_{i=1}^{k} |b_i|^+)}$ in $A(c)$ (indeed, in the present situation $h = [c]$ and so the product which appears on the left side of (8) has only one factor, namely $A(c)$).

So we focus our attention on $A(c)$, remember that

$$A(c) = \sum_{m' \in \mathcal{M}_{\mathrm{fin}}(|[\![\varphi]\!]|)} t_{m',c} \prod_{b \in |[\![\varphi]\!]|} \Big(\sum_{i=1}^{k} u^{[i-1]} \sum_{r \in \mathcal{M}_{\mathrm{fin}}(k+\sum_{j=1}^{i-1} |b_j|^+, |b_i|^+)} u^r \pi(b_i, \mathsf{S}(r, k + \sum_{j=1}^{i-1} |b_j|^+))_b \Big)^{m'(b)} \, .$$

Let

$$J = \Big\{(i,r) \mid i \in \{1,\dots,k\} \text{ and } r \in \mathcal{M}_{\mathrm{fin}}(k + \sum_{j=1}^{i-1} |b_j|^+, |b_i|^+)\Big\}.$$

Observe that, given $(i,r),(i',r') \in J$, either $(i,r) = (i',r')$, or $i \neq i'$ and r and r' have disjoint supports.

Given $(i,r) \in J$, we set

$$\theta(i,r) = \pi(b_i, \mathsf{S}(r, k + \sum_{j=1}^{i-1} |b_j|^+)) \tag{10}$$

so that $\theta(i,r) \in (\mathbb{R}^+)^{|[\![\varphi]\!]|}$ for each $(i,r) \in J$. With these notations, we have

$$\begin{aligned} A(c) &= \sum_{m' \in \mathcal{M}_{\mathrm{fin}}(|[\![\varphi]\!]|)} t_{m',c} \prod_{b \in |[\![\varphi]\!]|} \left(\sum_{(i,r)\in J} u^{[i-1]+r} \theta(i,r)_b \right)^{m'(b)} \\ &= \sum_{m' \in \mathcal{M}_{\mathrm{fin}}(|[\![\varphi]\!]|)} t_{m',c} \prod_{b \in |[\![\varphi]\!]|} \left(\sum_{\substack{p \in \mathcal{M}_{\mathrm{fin}}(J) \\ \#p = m'(b)}} u^{\sigma(p)} \mathsf{mn}(p) \theta_b^p \right) \end{aligned}$$

where we recall that $\mathsf{mn}(p) = (\#p)!/\prod_{b\in|[\![\varphi]\!]|} p(b)!$ is the multinomial coefficient associated with the finite multiset p by the multinomial formula. In this expression, for each $b \in |[\![\varphi]\!]|$, θ_b is the J-indexed family of real numbers defined by $\theta_b(i,r) = \theta(i,r)_b$ and $\sigma(p) \in \mathcal{M}_{\mathrm{fin}}(\mathbb{N})$ is defined as

$$\sigma(p) = \sum_{(i,r)\in J} p(i,r) \cdot ([i-1] + r). \tag{11}$$

Distributing the product over the sum and rearranging the sums, we get

$$\begin{aligned} A(c) &= \sum_{m' \in \mathcal{M}_{\mathrm{fin}}(|[\![\varphi]\!]|)} t_{m',c} \sum_{\substack{\rho \in \mathcal{M}_{\mathrm{fin}}(J)^{|[\![\varphi]\!]|} \\ \forall b\ \#\rho(b) = m'(b)}} u^{\sum_{b\in|[\![\varphi]\!]|} \sigma(\rho(b))} \prod_{b\in|[\![\varphi]\!]|} \mathsf{mn}(\rho(b)) \theta_b^{\rho(b)} \\ &= \sum_{m \in \mathcal{M}_{\mathrm{fin}}(0, k + \sum_{i=1}^k |b_i|^+)} u^m \sum_{\substack{\rho \in \mathcal{M}_{\mathrm{fin}}(J)^{|[\![\varphi]\!]|} \\ \sum_{b\in|[\![\varphi]\!]|} \sigma(\rho(b)) = m}} t_{\rho_1,c} \prod_{b\in|[\![\varphi]\!]|} \mathsf{mn}(\rho(b)) \theta_b^{\rho(b)} \end{aligned}$$

where $\rho_1 \in \mathcal{M}_{\mathrm{fin}}(|[\![\varphi]\!]|)$ is defined by

$$\rho_1(b) = \#\rho(b) = \sum_{(i,r)\in J} \rho(b)(i,r) \tag{12}$$

for each $\rho \in \mathcal{M}_{\mathrm{fin}}(J)^{|[\![\varphi]\!]|}$. For $m \in \mathcal{M}_{\mathrm{fin}}(0, k + \sum_{i=1}^k |b_i|^+)$, let

$$\zeta(m) = \sum_{\substack{\rho \in \mathcal{M}_{\mathrm{fin}}(J)^{|[\![\varphi]\!]|} \\ \sum_{b\in|[\![\varphi]\!]|} \sigma(\rho(b)) = m}} t_{\rho_1,c} \prod_{b\in|[\![\varphi]\!]|} \mathsf{mn}(\rho(b)) \theta_b^{\rho(b)} \tag{13}$$

be the coefficient of u^m in $A(c)$.

Since we want to compute $\alpha = \zeta(\mathsf{o}(0, k + \sum_{i=1}^{k} |b_i|^+))$ defined in (9), we consider the particular case where $m = \mathsf{o}(0, k + \sum_{i=1}^{k} |b_i|^+)$. The elements ρ of $\mathcal{M}_{\mathrm{fin}}(J)^{|[\![\varphi]\!]|}$ which index the sum (13) satisfy the condition $\sum_{b\in|[\![\varphi]\!]|} \sigma(\rho(b)) = \mathsf{o}(0, k + \sum_{i=1}^{k} |b_i|^+)$, that is, coming back to the definition (11) of σ,

$$\sum_{\substack{(i,r)\in J\\ b\in|[\![\varphi]\!]|}} \rho(b)(i,r)\cdot([i-1]+r) = \mathsf{o}(0, k + \sum_{i=1}^{k} |b_i|^+)\,. \tag{14}$$

Since $\mathsf{o}(0, k+\sum_{i=1}^{k} |b_i|^+) = [0, \dots, k + \sum_{i=1}^{k} |b_i|^+ - 1]$ (see §4.2.3), condition (14) implies that, for each $i \in \{1, \dots, k\}$, there is exactly one $b_\rho(i) \in |[\![\varphi]\!]|$ and exactly one $r_\rho(i) \in \mathcal{M}_{\mathrm{fin}}(k + \sum_{j=1}^{i-1} |b_j|^+, |b_i|^+)$ such that

$$\rho(b_\rho(i))(i, r_\rho(i)) \neq 0\,,$$

and we know moreover that $\rho(b_\rho(i))(i, r_\rho(i)) = 1$ because $i-1$ occurs exactly once in $[i-1]+r_\rho(i)$ (since the multisets $[i-1]$ and $r_\rho(i)$ have disjoint supports for $i = 1, \dots, k$). Moreover, since $r_\rho(i)$ and $r_\rho(i')$ have disjoint supports when i and i' are distinct elements of $\{1, \dots, k\}$, we must have

$$r_\rho(i) = \mathsf{o}(k + \sum_{j=1}^{i-1} |b_j|^+, |b_i|^+) \tag{15}$$

by (14) again.

From the first part of these considerations (existence and uniqueness of $b_\rho(i)$ and $r_\rho(i)$), it follows that if $b \in |[\![\varphi]\!]|$ and $(i,r) \in J$ are such that $\rho(b)(i,r) \neq 0$ then we have $b = b_\rho(i)$ and $r = r_\rho(i)$, and hence $\rho(b)(i,r) = 1$. In particular, $\mathsf{mn}(\rho(b)) = 1$ for each b. It follows that

$$\begin{aligned}
\prod_{b\in|[\![\varphi]\!]|} \mathsf{mn}(\rho(b))\theta_b^{\rho(b)} &= \prod_{b\in|[\![\varphi]\!]|} \prod_{\substack{(i,r)\in J\\ b_\rho(i)=b,\ r_\rho(i)=r}} \theta(i,r)_b \\
&= \prod_{i=1}^{k} \pi(b_i, \mathsf{S}(r_\rho(i), k + \sum_{j=1}^{i-1} |b_j|^+))_{b_\rho(i)}
\end{aligned}$$

coming back to the definition of θ, see (10). Let H be the set of all ρ's satisfying (14), we have therefore

$$\begin{aligned}
\alpha = \zeta(\mathsf{o}(0, k + \sum_{i=1}^{k} |b_i|^+)) &= \sum_{\rho\in H} t_{\rho_1,c} \prod_{b\in|[\![\varphi]\!]|} \mathsf{mn}(\rho(b))\theta_b^{\rho(b)} \\
&= \sum_{\rho\in H} t_{\rho_1,c} \prod_{i=1}^{k} \pi(b_i, \mathsf{S}(r_\rho(i), k + \sum_{j=1}^{i-1} |b_j|^+))_{b_\rho(i)} \\
&\qquad \text{by the observations above} \\
&= \sum_{\rho\in H} t_{\rho_1,c} \prod_{i=1}^{k} \pi(b_i, \mathsf{o}(0, |b_i|^+))_{b_\rho(i)} \quad \text{by (15).}
\end{aligned}$$

By our inductive hypothesis about $\pi(b_i, \mathsf{o}(0, |b_i|^+))$, all the terms of this sum vanish, but the one corresponding to the unique element ρ of H such that $b_\rho(i) = b_i$ for $i = 1, \dots, k$. For this specific ρ, coming back to the definition (12) of ρ_1, we have $\rho_1 = [b_1, \dots, b_k]$. It follows that

$$\alpha = \zeta(\mathsf{o}(0, k + \sum_{i=1}^{k} |b_i|^+)) = t_{[b_1,\dots,b_k],c}$$

as contended, and this ends the proof of the lemma. □

4.3.1 Main statements. We first state a separation theorem which seems interesting on its own right and expresses that our testing terms a^-, when fed with suitable rational probability distributions, are able to separate any two distinct elements of the interpretation of a type.

Theorem 27 (Separation) *Let σ be a type and let $a \in |[\![\sigma]\!]|$. Let $w, w' \in \mathsf{P}[\![\sigma]\!]$ be such that $w_a \neq w'_a$. Let $n = |a|^-$. There is a sequence $(q_i)_{i=0}^{n-1}$ of rational numbers such that the element $u = \sum_{i=0}^{n-1} q_i \mathsf{e}_i$ of PN satisfies $[\![a^-]\!](u)(w) \neq [\![a^-]\!](u)(w')$.*

Proof. With the notations of the statement of the proposition, we consider the functions $\varphi, \varphi' : \mathsf{PN} \to \mathbb{R}^+$ defined by $\varphi(u) = [\![a^-]\!](u)(w)_0$ and $\varphi'(u) = [\![a^-]\!](u)(w')_0$. By Lemma 25, the morphisms φ and φ' depend on at most $n = |a|^-$ parameters. In other words, there are $t, t' \in \mathbf{Pcoh}_!(\Delta_n, \bot)$ such that

$$\forall u \in \mathsf{PN} \quad \varphi(u) = t\Big(\sum_{i=0}^{n-1} u_i \mathsf{e}_i\Big) \text{ and } \varphi'(u) = t'\Big(\sum_{i=0}^{n-1} u_i \mathsf{e}_i\Big)$$

Coming back to (6), we see that the coefficient of $u^{[0,\dots,n-1]}$ in the expression of $\varphi(u)$ is $\mu(a, [0, \dots, n-1])(w)$, whose value is w_a by Lemma 26. In other words $t_{[0,\dots,n-1],*} = w_a$ and similarly $t'_{[0,\dots,n-1],*} = w'_a$. From this, it results that the functions t and t' from $\mathsf{P}\Delta_n$ to $\mathbb{R}$ are distinct (because these are entire functions with distinct power series, which are defined on the subset $\mathsf{P}\Delta_n$ of $(\mathbb{R}^+)^n$, which contains a non-empty subset of $\mathbb{R}^n$ which is open for the usual topology). Since these functions are continuous (again, for the usual topology), there is an $u \in \mathsf{P}\Delta_n$ such that $u_0, \dots, u_{n-1} \in \mathbb{Q}$ and $t(u) \neq t'(u)$. □

Theorem 28 (Full Abstraction) *Let σ be a type, Γ be a typing context and let M and M' be terms such that $\Gamma \vdash M : \sigma$ and $\Gamma \vdash M' : \sigma$. If $M \sim M'$ then $[\![M]\!]_\Gamma = [\![M']\!]_\Gamma$.*

Proof. Assume that $[\![M]\!]_\Gamma \neq [\![M']\!]_\Gamma$.

Let $(x_1 : \sigma_1, \dots, x_k : \sigma_k)$ be the typing context Γ. Let $N = \lambda x_1^{\sigma_1} \cdots \lambda x_k^{\sigma_k}\, M$ and $N' = \lambda x_1^{\sigma_1} \cdots \lambda x_k^{\sigma_k}\, M'$ be closures of M and M'. Let $\tau = \sigma_1 \Rightarrow \cdots \sigma_k \Rightarrow \sigma$.

Let $w = [\![N]\!]$ and $w' = [\![N']\!]$, we have $w \neq w'$ so there is $a \in |[\![\tau]\!]|$ such that $w_a \neq w'_a$. By Theorem 27, we can find a sequence $(q_i)_{i=0}^{n-1}$ of rational numbers such that for all $i \in \{0, \dots, n-1\}$ one has $q_i \geq 0$ and $\sum_{i=0}^{n-1} q_i \leq 1$, and $u = \sum_{i=0}^{n-1} q_i \mathsf{e}_i \in \mathsf{PN}$ satisfies $[\![a^-]\!](u)(w)_0 \neq [\![a^-]\!](u)(w')_0$.

Observe that $u = [\![\mathsf{ran}(q_0, \ldots, q_{n-1})]\!]$.

Let C be the following observation context:

$$C^{\Gamma\vdash\sigma} = \left(a^-\right) \mathsf{ran}(q_0, \ldots, q_{n-1})\, \lambda x_1^{\sigma_1} \cdots \lambda x_k^{\sigma_k}\, [\ \ ]^{\Gamma\vdash\sigma}$$

which satisfies $\vdash C^{\Gamma\vdash\sigma} : \iota$, $[\![C[M]]\!] = [\![a^-]\!](u)(w)$ and $[\![C[M']]\!] = [\![a^-]\!](u)(w')$.

Applying Theorem 22, we get that

$$\mathsf{Red}(\iota)^{\infty}_{C[M],\underline{0}} \neq \mathsf{Red}(\iota)^{\infty}_{C[M'],\underline{0}}$$

which shows that $M \not\sim M'$. □

4.3.2 Failure of inequational full abstraction. We can define an observational preorder on closed terms: given terms M and M' such that $\vdash M : \sigma$ and $\vdash M' : \sigma$, let us write $M \lesssim M'$ if, for all closed C such that $\vdash C : \sigma \Rightarrow \iota$, one has $\mathsf{Red}(\iota)^{\infty}_{(C)M,\underline{0}} \leq \mathsf{Red}(\iota)^{\infty}_{(C)M',\underline{0}}$. Then it is easy to see that $[\![M]\!] \leq [\![M']\!] \Rightarrow M \lesssim M'$ (just as in the proof of Theorem 24).

The converse implication however is far from being true. A typical counter-example (which is essentially the same as the example of the Remark following Proposition 12) is provided by the two terms

$$M_1 = \lambda x^{\iota}\, \mathsf{if}(x, \underline{0}, z \cdot \Omega^{\iota})$$
$$M_2 = \lambda x^{\iota}\, \mathsf{if}(x, \mathsf{if}(x, \underline{0}, z' \cdot \Omega^{\iota}), z \cdot \Omega^{\iota})$$

One has $\vdash M_i : \iota \Rightarrow \iota$ for $i = 1, 2$ and the functional behavior of the interpretations of these terms is given by

$$[\![M_1]\!](u) = u_0\, \overline{0}$$
$$[\![M_2]\!](u) = u_0^2\, \overline{0}$$

for all $u \in \mathsf{PN}$ so $[\![M_1]\!]$ and $[\![M_2]\!]$ are not comparable in $\mathsf{P}[\![\iota \Rightarrow \iota]\!]$ and nevertheless one can check that $M_2 \lesssim M_1$. The proof boils down to the observation that, for each $u \in \mathsf{PN}$, one has $[\![M_2]\!](u) \leq [\![M_1]\!](u)$.

Conclusion

We have studied an operationally meaningful probabilistic extension of PCF and, in particular, we have proven a full abstraction result for the probabilistic coherence spaces model of Linear Logic, with respect to a natural notion of observational equivalence on the terms of this language.

This observational equivalence can be considered as too restrictive however since it is based on a strict equality of probabilities of convergence. In the present probabilistic setting, a suitable *distance* on terms could certainly be more relevant, and provide more interesting information on the behavior of programs, than our observational equivalence relation. The study of such notions of distance and of their connections with PCSs, based on earlier works by various authors, will be the purpose of our next investigations. We also plan to extend our adequacy and, if possible, full abstraction results to richer type structures, in a call-by-push-value flavored setting.

References

[Bie95] Gavin Bierman. What is a categorical model of intuitionistic linear logic? In Mariangiola Dezani-Ciancaglini and Gordon D. Plotkin, editors, *Proceedings of the second Typed Lambda-Calculi and Applications conference*, volume 902 of *Lecture Notes in Computer Science*, pages 73–93. Springer-Verlag, 1995.

[DE11] Vincent Danos and Thomas Ehrhard. Probabilistic coherence spaces as a model of higher-order probabilistic computation. *Information and Computation*, 152(1):111–137, 2011.

[Ehr02] Thomas Ehrhard. On Köthe sequence spaces and linear logic. *Mathematical Structures in Computer Science*, 12:579–623, 2002.

[Ehr15a] Thomas Ehrhard. A Call-By-Push-Value FPC and its interpretation in Linear Logic. Technical report, University Paris Diderot, PPS Laboratory, 2015.

[Ehr15b] Thomas Ehrhard. A semantical introduction to differential linear logic. *Mathematical Structures in Computer Science*, 2015. To appear.

[EPT11] Thomas Ehrhard, Michele Pagani, and Christine Tasson. The computational meaning of probabilistic coherent spaces. In *Proceedings of the 26th Annual IEEE Symposium on Logic in Computer Science, LICS 2011, June 21-24, 2011, Toronto, Ontario, Canada*, pages 87–96. IEEE Computer Society, 2011.

[ETP14] Thomas Ehrhard, Christine Tasson, and Michele Pagani. Probabilistic coherence spaces are fully abstract for probabilistic PCF. In Suresh Jagannathan and Peter Sewell, editors, *POPL*, pages 309–320. ACM, 2014.

[Gir88] Jean-Yves Girard. Normal functors, power series and the λ-calculus. *Annals of Pure and Applied Logic*, 37:129–177, 1988.

[Gir99] Jean-Yves Girard. Coherent Banach spaces: a continuous denotational semantics. *Theoretical Computer Science*, 227(1-2):275–297, 1999.

[Gir04] Jean-Yves Girard. Between logic and quantic: a tract. In Thomas Ehrhard, Jean-Yves Girard, Paul Ruet, and Philip Scott, editors, *Linear Logic in Computer Science*, volume 316 of *London Mathematical Society Lecture Notes Series*, pages 346–381. Cambridge University Press, 2004.

[JT98] Achim Jung and Regina Tix. The troublesome probabilistic powerdomain. *Electronic Notes in Theoretical Computer Science*, 13:70–91, 1998.

[Lev06] Paul Blain Levy. Call-by-push-value: Decomposing call-by-value and call-by-name. *Higher-Order and Symbolic Computation*, 19(4):377–414, 2006.

[Mel09] Paul-André Melliès. Categorical semantics of linear logic. *Panoramas et Synthèses*, 27, 2009.

[Plo77] Gordon Plotkin. LCF considered as a programming language. *Theoretical Computer Science*, 5:223–256, 1977.