Applying quantitative semantics to higher-order quantum computing

Michele Pagani
Université Paris 13, Sorbonne Paris Cité
Villetaneuse, France
michele.pagani@lipn.univ-paris13.fr

Peter Selinger
Dalhousie University
Halifax, Canada
selinger@mathstat.dal.ca

Benoît Valiron
University of Pennsylvania
Philadelphia, U.S.A.
benoit.valiron@monoidal.net

Abstract

Finding a denotational semantics for higher order quantum computation is a long-standing problem in the semantics of quantum programming languages. Most past approaches to this problem fell short in one way or another, either limiting the language to an unusably small finitary fragment, or giving up important features of quantum physics such as entanglement. In this paper, we propose a denotational semantics for a quantum lambda calculus with recursion and an infinite data type, using constructions from quantitative semantics of linear logic.

1. Introduction

Type theory and denotational semantics have been successfully used to model, design, and reason about programming languages for almost half a century. The application of such methods to quantum computing is much more recent, going back only about 10 years [16].

An important problem in the semantics of quantum computing is how to combine quantum computing with higher-order functions, or in other words, how to design a functional quantum programming language. A syntactic answer to this question was arguably given with the design of the quantum lambda calculus [18, 21]. The quantum lambda calculus has a well-defined syntax and operational semantics, with a strong type system and a practical type inference algorithm. However, the question of how to give a *denotational* semantics to the quantum lambda calculus turned out to be difficult, and has remained open for many years [17, 20]. One reason that designing such a semantics is difficult is that quantum computation is inherently defined on *finite dimensional* Hilbert spaces, whereas the semantics of higher-order functional programming languages, including such features as infinite data types and recursion, is inherently infinitary.

In recent years, a number of solutions have been proposed to the problem of finding a denotational semantics of higher-order quantum computation, with varying degrees of success. The first approach [19] was to restrict the language to strict linearity, meaning that each function had to use each argument exactly once, in the spirit of linear logic. In this way, all infinitary concepts (such as infinite types and recursion) were eliminated from the language. Not surprisingly, the resulting finitary language permitted a fully abstract semantics in terms of finite dimensional spaces; this was hardly an acceptable solution to the general problem. The second approach [12] was to construct a semantics of higher-order quantum computation by methods from category theory; specifically, by applying a presheaf construction to a model of first-order quantum computation. This indeed succeeds in yielding a model of the full quantum lambda calculus, albeit without recursion. The main drawback of presheaf models is the absence of recursion, and the fact that such models are relatively difficult to reason about. The third approach [6] was based on the Geometry of Interaction. Starting from a traced monoidal category of basic quantum operations, Hasuo and Hoshino applied a sequence of categorical constructions, which eventually yielded a model of higher-order quantum computation. The problem with this approach is that the tensor product constructed from the geometry-of-interaction construction does not coincide with the tensor product of the underlying physical data types. Therefore, the model drops the possibility of entangled states, and thereby fails to model one of the defining features of quantum computation.

Our contribution. In this paper, we give a novel denotational semantics of higher-order quantum computation, based on methods from *quantitative semantics*. Quantitative semantics refers to a family of semantics of linear logic that interpret proofs as linear mappings between vector spaces (or more generally, modules), and standard lambda-terms as power series. The original idea comes from Girard's normal functor semantics [4]. More recently, quantitative semantics has been used to give a solid, denotational semantics for various algebraic extensions of lambda-calculus, such as probabilistic and differential lambda calculi (e.g. [1], [2]).

One feature of our model is that it can represent *infinite dimensional* structures, and is expressive enough to describe recursive types, such as lists of qubits, and to model recursion. This is achieved by providing an exponential structure *à la* linear logic. Unlike the Hasuo-Hoshino model, our model permits general entanglement. We interpret (a minor variant of) the quantum lambda calculus in this model. Our main result is the adequacy of the model with respect to the operational semantics.

Outline. In Section 2, we briefly review some background. Section 3 presents the version of the quantum lambda calculus that we use in this paper, including its operational semantics. Section 4 recalls the completion of certain categories under infinite biproducts. In Section 5, we apply this construction to a specific category of completely positive maps. Section 6 presents the denotational semantics of the quantum lambda calculus and proves the adequacy theorem. Finally, Section 7 concludes with some properties of the representable elements.

[Paper accepted to POPL 2014 – Unrevised draft.]

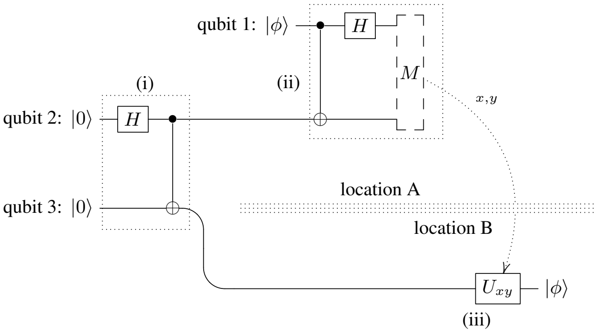

Figure 1: The quantum teleportation protocol.

2. Background

2.1 Quantum computation in a nutshell

Quantum computation is a computational paradigm based on the laws of quantum physics. We briefly recall some basic notions; please see [15] for a more complete treatment. The basic unit of information in quantum computation is a *quantum bit* or *qubit*, whose state is given by a normalized vector in the two-dimensional Hilbert space $\mathbb{C}^2$. It is customary to write the canonical basis of $\mathbb{C}^2$ as $\{|0\rangle, |1\rangle\}$, and to identify these basis vectors with the booleans false and true, respectively. The state of a qubit can therefore be thought of as a complex linear combination of booleans $\alpha|0\rangle + \beta|1\rangle$, called a *quantum superposition*. More generally, the state of n qubits is an element of the n-fold tensor product $\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$.

There are three kinds of basic operations on quantum data: initializations, unitary maps and measurements. Initialization prepares a new qubit in state $|0\rangle$ or $|1\rangle$. A unitary map, or *gate*, is an invertible linear map U such that $U^* = U^{-1}$; here U^* denotes the complex conjugate transpose of U. Finally, the operation of measurement consumes a qubit and returns a classical bit. If n qubits are in state $\alpha|0\rangle \otimes \phi_0 + \beta|1\rangle \otimes \phi_1$, where ϕ_0 and ϕ_1 are normalized states of $n-1$ qubits, then measuring the leftmost qubit will yield false with probability $|\alpha|^2$, leaving the remaining qubits in state ϕ_0, and true with probability $|\beta|^2$, leaving the remaining qubits in state ϕ_1.

Example 1. A small algorithm is the simulation of an unbiased coin toss: initialize one quantum bit to $|0\rangle$, apply the Hadamard gate sending $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, then measure. The result is true with probability $\frac{1}{2}$ and false with probability $\frac{1}{2}$.

Example 2. A slightly more involved algorithm is the *quantum teleportation algorithm* (see [15] for details). The procedure is summarized in Figure 1. Wires represent the path of quantum bits in the computation, and time flows from left to right. The gate $\boxed{H}$ stands for an application of the Hadamard gate, whereas the gate $\overset{\bullet}{\oplus}$ is a controlled-not: it flips the bottom qubit if the upper one is in state $|1\rangle$. The box M is a measurement. The unitaries U_{xy} are

$$U_{00} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \; U_{01} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \; U_{10} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \; U_{11} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right).$$

The goal is to send a quantum bit in an unknown state $|\phi\rangle$ from Location A to Location B using two classical bits. The procedure can be reversed to send two classical bits using a quantum bit. In this case it is called the *dense coding algorithm* [15].

The algorithm consists in three parts. In (i), two quantum bits (qubits 2 and 3) are entangled in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. In (ii), the input qubit 1 in state $|\phi\rangle$ is entangled with qubit 2, then both are measured. The result is sent over location B, where in (iii) an correction U_{xy} is applied on qubit 3, setting it to state $|\phi\rangle$.

2.2 Density matrices and completely positive maps

If we identify $|0\rangle$ and $|1\rangle$ with the standard basis vectors $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$, the state of a qubit can be expressed as a two-dimensional vector $v = \alpha|0\rangle + \beta|1\rangle = \left(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right)$. Similarly, the state of an n-qubit system can be expressed as an 2^n-dimensional column vector. Often, it is necessary to consider *probability distributions* on quantum states; these are also known as *mixed states*. Consider a quantum system that is in one of several states $v_1, \ldots, v_k$ with probabilities $p_1, \ldots, p_k$, respectively. The *density matrix* of this mixed state is defined to be

$$A = \sum_i p_i v_i v_i^*.$$

By a theorem of Von Neumann, the density matrix is a good representation of mixed states, in the following sense: two mixed states are indistinguishable by any physical experiment if and only if they have the same density matrix [15]. Note that $\operatorname{tr} A = p_1 + \ldots + p_k$. For our purposes, it is often convenient to permit sub-probability distributions, so that $p_1 + \ldots + p_k \leqslant 1$.

Let us write $\mathbb{C}^{n\times n}$ for the space of $n \times n$-matrices. Recall that a matrix $A \in \mathbb{C}^{n\times n}$ is called *positive* if $v^*Av \geqslant 0$ for all $v \in \mathbb{C}^n$. Given $A, B \in \mathbb{C}^{n\times n}$, we write $A \sqsubseteq B$ iff $B - A$ is positive; this is the so-called *Löwner partial order*. A linear map $F : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$ is called *positive* if $A \sqsupseteq 0$ implies $F(A) \sqsupseteq 0$, and *completely positive* if $F \otimes \mathrm{id}_k$ is positive for all k, where id_k is the identity function on $\mathbb{C}^{k\times k}$. If F moreover satisfies $\mathrm{tr}(F(A)) \leqslant \operatorname{tr} A$ for all positive A, then it is called a *superoperator*. The density matrices are precisely the positive matrices A of trace $\leqslant 1$. Moreover, the superoperators correspond precisely to those functions from mixed states to mixed states that are physically possible [15, 16].

2.3 The category CPM

The category $\mathbf{CPM}_s$ is defined as follows: the objects are natural numbers, and a morphism $F : n \to m$ is a completely positive map $F : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$. Let **CPM** be the free completion of $\mathbf{CPM}_s$ under finite biproducts; specifically, the objects of **CPM** are sequences $\vec{n} = (n_1, \ldots, n_k)$ of natural numbers, and a morphism $F : \vec{n} \to \vec{m}$ is a matrix (F_{ij}) of morphisms $F_{ij} : n_j \to m_i$ of $\mathbf{CPM}_s$. The categories $\mathbf{CPM}_s$ and **CPM** are symmetric monoidal, and in fact, compact closed [16].

2.4 Limitations of CPM as a model

The category **CPM** can serve as a fully abstract model for a simple, strictly linear, finitary quantum lambda calculus [19]. For example, the type **bit** is interpreted as $(1, 1)$, and the type **qubit** is interpreted as (2). Measurement, as a map from **qubit** to **bit**, sends $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to (a, d). The coin toss is a map $(1) \to (1, 1)$ sending (p) to $(\frac{p}{2}, \frac{p}{2})$. Function spaces are interpreted via the compact closed structure.

As mentioned in the introduction, the semantics of [19] is extremely limited, because it is completely finitary. Thus recursion, infinite data types, and non-linear functions (i.e., those that can use their argument more than once) had to be completely removed from the language in order to fit the model. For example, even the simple squaring function $f \mapsto \lambda x.f(f\,x)$ is not representable in **CPM**. Similarly, **CPM** cannot express infinite types, such as the type of lists of qubits.

The purpose of the present paper is to remove all of these restrictions. As an example, consider the following pseudo-code (in ML-style):

```
val qlist : qubit -> qubit list
let rec qlist q = if (cointoss ()) then q
          else let (x,y) = entangle q in x::(f y)
```

$$
\begin{array}{l}
\textit{Terms}\quad M,N,P \quad ::= \\
\qquad x \mid \lambda x^A.M \mid MN \mid \mathtt{skip} \mid M;N \mid \\
\qquad M\otimes N \mid \mathtt{let}\ x^A\otimes y^B \ =\ M\ \mathtt{in}\ N \mid \\
\qquad \mathtt{in}_\ell\ M \mid \mathtt{in}_r\ M \mid \mathtt{match}\ P\ \mathtt{with}\ (x^A : M|y^B : N) \mid \\
\qquad \mathtt{split}^A \mid \mathtt{letrec}\ f^{A\multimap B}x = M\,\mathtt{in}\,N \mid \mathtt{meas} \mid \mathtt{new} \mid U \\
\\
\textit{Values}\quad V,W \quad ::= \\
\qquad x \mid c \mid \lambda x^A.M \mid V\otimes W \mid \mathtt{in}_\ell\ V \mid \mathtt{in}_r\ W \\
\\
\textit{Types}\quad A,B,C \quad ::= \\
\qquad \mathbf{qubit} \mid A{\multimap}B \mid !(A{\multimap}B) \mid 1 \mid A{\otimes}B \mid A{\oplus}B \mid A^\ell.
\end{array}
$$

Table 1: Grammars of terms, values and types.

Here, the function `cointoss` is a fair coin toss, and the function `entangle` sends $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|00\rangle + \beta|11\rangle$.

So if the function `qlist` is applied to a qubit $\alpha|0\rangle + \beta|1\rangle$, the output is $\alpha|0\rangle + \beta|1\rangle$ with probability $\frac{1}{2}$, $\alpha|00\rangle + \beta|11\rangle$ with probability $\frac{1}{4}$, $\alpha|000\rangle + \beta|111\rangle$ with probability $\frac{1}{8}$, and so on. Its semantics should be of type $2 \to (2, 4, 8, \ldots)$, mapping

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\frac{1}{2}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \frac{1}{4}\left(\begin{smallmatrix} a & 0 & 0 & b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ c & 0 & 0 & d \end{smallmatrix}\right), \ldots\right).$$

The category **CPM** is “almost” capable of handling this case, but not quite, because it cannot express infinite tuples of matrices. The model we propose in this paper is essentially an extension of **CPM** to infinite biproducts, using methods developed in [5, 9, 10, 14].

3. A quantum lambda calculus

We define a typed quantum lambda calculus that is a variant of the quantum lambda calculus previously defined in [20]. The main difference is that the language in this present paper is a true extension of linear logic (see the type assignment system of Table 2). In particular, in contrast with [20], $!(A \otimes B) \multimap !A \otimes !B$ is not provable and there is no need for a subtyping relation. The operational semantics implements a call-by-value strategy. An untyped call-by-name variant has been studied in [8].

The classes of *terms*, *values* and *types* are defined in Table 1. The symbol c ranges over the set of term constants $\{\mathtt{skip}, \mathtt{split}^A, \mathtt{meas}, \mathtt{new}, U\}$. The constant U ranges over a set of elementary unitary transformations on quantum bits. In the examples below, we will be using the Hadamard gate H and the controlled-not gate N_c, defined as follows [15]:

$$H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \qquad\qquad N_c = \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right) \qquad (1)$$

Notice that bound variables are given in Church-style, i.e., with a type annotation. This allows Proposition 4, and simplifies the semantic interpretation of the typed terms. We omit such annotations in the sequel if uninteresting or obvious.

We have two kinds of arrows: the linear arrow $A{\multimap}B$, and the intuitionistic arrow $!(A \multimap B)$, which is obtained by the call-by-value translation of the intuitionistic implication into linear logic [3]. Intuitively, only the terms of type $!(A \multimap B)$ represent functions that can be iterated, whereas terms of type $A{\multimap}B$ must be used at most once. A type of the form $!A$ is called a $!$-*type* or *non-linear* type, and all other types are called *linear*. The distinction between linear and non-linear types is crucial for allowing the type system to enforce the no-cloning property of quantum physics.

By convention, $\multimap$ is associative to the right, while application and tensor are associative to the left. We use the notation $A^{\otimes n}$ for A tensored n times. The type A^ℓ denotes finite lists of type A. When doing structural induction on types, we assume that A^ℓ is greater than $A^{\otimes n}$, for any $n \in \mathbb{N}$.

The set of terms and types is somewhat spartan; however it can be easily extended by introducing syntactic sugar. Note that, for technical convenience, we have only allowed types of the form $!A$ when A is an arrow type. However, for an arbitrary type A, the type $!A$ can be simulated by using $!(1 \multimap A)$ instead.

Notation 3. We write $\mathbf{bit} = 1 \oplus 1$, $\mathtt{tt} = \mathtt{in}_r\ \mathtt{skip}$, $\mathtt{ff} = \mathtt{in}_\ell\ \mathtt{skip}$, $\mathtt{nil} = \mathtt{in}_\ell\ \mathtt{skip}$ and $M :: N = \mathtt{in}_r\ (M{\otimes}N)$. We write $\lambda\mathtt{skip}.M$ for the term $\lambda z^1.(z;M)$, where z is a fresh variable, and $\mathtt{if}\ P\ \mathtt{then}\ M\ \mathtt{else}\ N$ for $\mathtt{match}\ P\ \mathtt{with}\ (x^1 : N|y^1 : M)$.

A *context* Δ is a function from a finite set of variables to types. We denote the domain of Δ by $|\Delta|$, and we write $\Delta = x_1 : A_1, \ldots, x_n : A_n$ whenever $|\Delta| = \{x_1, \ldots, x_n\}$ and $\Delta(x_i) = A_i$. We call Δ *exponential* (resp. *linear*) whenever all A_i are $!$-types (resp. no A_i is a $!$-type). We write $!\Delta$ for a context which is exponential. The notation Γ, Σ refers to the union of the two contexts Γ and Σ and assumes that $|\Gamma|$ and $|\Sigma|$ are disjoint.

A *judgement* is a triple $\Gamma \vdash M : A$ of a context Γ, a term M and a type A. A judgement is called *valid* if it can be inferred from the typing rules in Figure 2, using the convention that the contexts Γ and Σ are linear.

Proposition 4. *There is at most one derivation inferring a given typing judgement* $\Gamma \vdash M : A$. □

Example 5. In Section 2.4, we wrote the informal program `qlist`. Our language is expressive enough to represent it. The term `cointoss` can be defined as $\mathtt{meas}(H(\mathtt{new}\,\mathtt{tt}))$, and it has type $\mathbf{bit}$. The term `entangle` is $\lambda x^{\mathbf{qubit}}.N_c(x \otimes (\mathtt{new}\,\mathtt{ff}))$, which has type $\mathbf{qubit} \multimap \mathbf{qubit} \otimes \mathbf{qubit}$. Then, `qlist` is

$$
\begin{array}{l}
\mathtt{letrec}\ f^{\mathbf{qubit}\multimap\mathbf{qubit}^\ell} q = \\
\qquad \mathtt{if}\ \mathtt{cointoss}\ \mathtt{then}\ q :: \mathtt{nil} \\
\qquad \mathtt{else}\ \mathtt{let}\ x^{\mathbf{qubit}} \otimes y^{\mathbf{qubit}} = \mathtt{entangle}\ q\ \mathtt{in}\ x :: fy
\end{array}
$$

which has type $\mathbf{qubit} \multimap \mathbf{qubit}^\ell$. In Examples 9 and 30 we discuss its operational and denotational semantics, respectively.

Example 6. In Example 2 and Figure 1, we sketched the quantum teleportation algorithm. We said that the algorithm can be decomposed in 3 parts. Each of these parts can be described and typed in the quantum lambda-calculus, yielding a higher-order term. This is an adaptation of an example provided in [18].

(i) generates an EPR pair of entangled quantum bits. Its type is therefore $1 \multimap \mathbf{qubit} \otimes \mathbf{qubit}$. The corresponding term is

$$\mathbf{EPR} = \lambda\mathtt{skip}.N_c(H(\mathtt{new}\,\mathtt{ff})) \otimes (\mathtt{new}\,\mathtt{ff}).$$

(ii) performs a Bell measurement on two quantum bits and outputs two classical bits x, y. Its type is thus $\mathbf{qubit} \multimap \mathbf{qubit} \multimap \mathbf{bit} \otimes \mathbf{bit}$, and the term **BellMeasure** is defined as

$$\lambda q_1.\lambda q_2.\left(\begin{array}{l} \mathtt{let}\ x \otimes y = N_c\,(q_1 \otimes q_2) \\ \mathtt{in}\ (\mathtt{meas}\ (H\ x)) \otimes (\mathtt{meas}\ y) \end{array}\right).$$

(iii) performs a correction. It takes one quantum bit, two classical bits, and outputs a quantum bit. It has a type of the form $\mathbf{qubit} \multimap \mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qubit}$. The term is

$$
\begin{array}{rl}
\mathbf{U} = \lambda q.\lambda x \otimes y.\mathtt{if}\ x\ \mathtt{then} & (\mathtt{if}\ y\ \mathtt{then}\ U_{11}\ q\ \mathtt{else}\ U_{10}\ q) \\
& \mathtt{else}\ (\mathtt{if}\ y\ \mathtt{then}\ U_{01}\ q\ \mathtt{else}\ U_{00}\ q).
\end{array}
$$

$$\frac{A \text{ linear}}{!\Delta, x : A \vdash x : A}\;ax \qquad \frac{A \text{ linear}}{!\Delta, x : !A \vdash x : A}\;axd \qquad \frac{!\Delta \vdash V : A \quad V \text{ value}}{!\Delta \vdash V : !A}\;p \qquad \frac{}{!\Delta \vdash \mathtt{skip} : 1}\;1_I$$

$$\frac{\Delta, x : A \vdash M : B}{\Delta \vdash \lambda x^A.M : A \multimap B}\;\multimap_I \quad \frac{!\Delta, \Gamma \vdash M : A \multimap B \quad !\Delta, \Sigma \vdash N : A}{!\Delta, \Gamma, \Sigma \vdash MN : B}\;\multimap_E \quad \frac{!\Delta, \Gamma \vdash M : 1 \quad !\Delta, \Sigma \vdash N : A}{!\Delta, \Gamma, \Sigma \vdash M;N : A}\;1_E$$

$$\frac{!\Delta, \Gamma \vdash M : A \quad !\Delta, \Sigma \vdash N : B}{!\Delta, \Gamma, \Sigma \vdash M \otimes N : A \otimes B}\;\otimes_I \quad \frac{!\Delta, \Gamma \vdash M : A \otimes B \quad !\Delta, \Sigma, x : A, y : B \vdash N : C}{!\Delta, \Gamma, \Sigma \vdash \mathtt{let}\, x^A \otimes y^B \;=\; M \,\mathtt{in}\, N : C}\;\otimes_E$$

$$\frac{!\Delta, \Gamma \vdash M : A}{!\Delta, \Gamma \vdash \mathtt{in}_\ell\, M : A \oplus B}\;\oplus_I^\ell \quad \frac{!\Delta, \Gamma \vdash M : B}{!\Delta, \Gamma \vdash \mathtt{in}_r\, M : A \oplus B}\;\oplus_I^r \quad \frac{\begin{array}{r} !\Delta, \Sigma, y : B \vdash N : C \\ !\Delta, \Gamma \vdash P : A \oplus B \quad !\Delta, \Sigma, x : A \vdash M : C \end{array}}{!\Delta, \Gamma, \Sigma \vdash \mathtt{match}\, P \,\mathtt{with}\, (x^A : M | y^B : N) : C}\;\oplus_E$$

$$\frac{!\Delta, \Gamma \vdash M : 1 \oplus (A \otimes A^\ell)}{!\Delta, \Gamma \vdash M : A^\ell}\;-^\ell_I \quad \frac{}{!\Delta \vdash \mathtt{split}^A : A^\ell \multimap 1 \oplus (A \otimes A^\ell)}\;\mathtt{split} \quad \frac{!\Delta, f : !(A \multimap B), x : A \vdash M : B \quad !\Delta, \Gamma, f : !(A \multimap B) \vdash N : C}{!\Delta, \Gamma \vdash \mathtt{letrec}\, f^{A \multimap B}\, x = M \,\mathtt{in}\, N : C}\;\mathtt{rec}$$

$$\frac{}{!\Delta \vdash \mathtt{meas} : \mathbf{qubit} \multimap \mathbf{bit}}\;\mathtt{meas} \quad \frac{}{!\Delta \vdash \mathtt{new} : \mathbf{bit} \multimap \mathbf{qubit}}\;\mathtt{new} \quad \frac{U \text{ of arity } n}{!\Delta \vdash U : \mathbf{qubit}^{\otimes n} \multimap \mathbf{qubit}^{\otimes n}}\;U$$

Table 2: Typing rules. The contexts Γ and Σ are assumed to be linear. In the p-rule A is assumed to be an arrow type.

We can now write the term

$$\begin{array}{ll} \mathbf{telep} = & \lambda\mathtt{skip}.\mathtt{let}\; x \otimes y = \mathbf{EPR}\;\mathtt{skip}\;\mathtt{in} \\ & \quad \mathtt{let}\; f \quad\; = \mathbf{BellMeasure}\; x\;\mathtt{in} \\ & \quad \mathtt{let}\; g \quad\; = \mathbf{U}\; y \\ & \quad \mathtt{in}\; f \otimes g. \end{array}$$

It can then be shown that

$$\vdash \mathbf{telep} :!(1 \multimap (\mathbf{qubit} \multimap \mathbf{bit} \otimes \mathbf{bit}) \otimes (\mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qubit}))$$

is a valid typing judgement.

In other words, the teleportation algorithm produces a pair of entangled functions $f : \mathbf{qubit} \to \mathbf{bit} \otimes \mathbf{bit}$ and $g : \mathbf{bit} \otimes \mathbf{bit} \to \mathbf{qubit}$. These functions have the property that $g(f(|\phi\rangle)) = |\phi\rangle$ for all qubits $|\phi\rangle$, and $f(g(x \otimes y)) = (x \otimes y)$ for all booleans x and y. These two functions are each other's inverse, but because they contain an embedded qubit each, they can only be used once. They can be said to form a "single-use isomorphism" between the (otherwise non-isomorphic) types $\mathbf{qubit}$ and $\mathbf{bit} \otimes \mathbf{bit}$. However, the whole procedure is duplicable: one can generate as many one-time-use isomorphism pairs as desired.

3.1 Operational semantics

The operational semantics is defined in terms of an abstract machine simulating the behavior of Knill's QRAM model. It is similar to the semantics given in [20].

Definition 7. A *quantum closure* is a triple $[q, \ell, M]$ where

- q is a normalized vector of $\mathbb{C}^{2^n}$, for some integer $n \geqslant 0$. The vector q is called the *quantum state*;
- M is a term, not necessarily closed;
- ℓ is a one-to-one map from the set of free variables of M to the set $\{1, \dots, n\}$. It is called the *linking function*.

We write $|\ell|$ for the domain of ℓ. By abuse of language we may call a closure $[q, \ell, V]$ a *value* when the term V is a value. We denote the set of quantum closures by Cl and the set of quantum closures that are values by Val. We write $\ell|_M$ for the linking function whose domain is restricted to the set of free variables of M. We say that the quantum closure $[q, \ell, M]$ is *total* when $|\ell|$ has cardinality n, the size of the quantum state. In that case, if $|\ell| = \{x_1, \dots, x_n\}$ and $\ell(x_i) = i$, we write ℓ as $|x_1, \dots, x_n\rangle$. A quantum closure $[q, |x_1, \dots, x_n\rangle, M]$ *has a type* A, whenever $x_1 : \mathbf{qubit}, \dots, x_n : \mathbf{qubit} \vdash M : A$. In case $\ell = |x_1, \dots, x_n\rangle$ we can also write $\ell \vdash M : A$.

The purpose of a quantum closure is to provide a mechanism to talk about terms with embedded quantum data. The idea is that a variable $y \in \mathrm{FV}(M)$ is bound in the closure $[q, \ell, M]$ to qubit number $\ell(y)$ of the quantum state q. So for example, the quantum closure

$$[\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |x_1, x_2\rangle, \lambda y^A.yx_1x_2]$$

denotes a term $\lambda y^A.yx_1x_2$ with two embedded qubits x_1, x_2 in the entangled state $|x_1x_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Numbering of qubits in the state starts at 1. The notion of α-equivalence extends naturally to quantum closures, for instance, the states $[q, |x\rangle, \lambda y^A.x]$ and $[q, |z\rangle, \lambda y^A.z]$ are equivalent. From now on, we tacitly identify quantum closures up to renaming of bound variables.

The evaluation of a term is defined as a probabilistic rewriting procedure on quantum closures, using a call-by-value reduction strategy. We use the notation $[q, \ell, M] \xrightarrow{p} [q', \ell', M']$ to mean that the left-hand side closure reduces in one step to the right-hand side with probability $p \in [0, 1]$.

Definition 8. The reduction rules are shown in Table 3. The rules split into three categories: (a) rules handling the classical part of the calculus; (b) rules dealing with quantum data; and (c) congruence rules for the call-by-value strategy. Note that in the statement of the rules, V and W refer to values.

In the rules in Table 3(b), the quantum state q has size n. The quantum state q' in the first rule is obtained by applying the k-ary unitary gate U to the qubits $\ell(x_1), \dots, \ell(x_k)$. Precisely, $q' = (\sigma \circ U \otimes \mathrm{id} \circ \sigma^{-1})(q)$, where σ is the action on $\mathbb{C}^{2^n}$ of any permutation over $\{1, \dots, n\}$ such that $\sigma(i) = \ell(x_i)$ whenever $i \leqslant k$. In the rules about measurements, we assume that if q_0 and q_1 are normalized quantum states of the form

$$\textstyle\sum_j \alpha_j |\phi_j^0\rangle \otimes |0\rangle \otimes |\psi_j^0\rangle, \;\; \sum_j \alpha_j |\phi_j^1\rangle \otimes |1\rangle \otimes |\psi_j^1\rangle, \qquad (2)$$

then q_0' and q_1' are respectively

$$\textstyle\sum_j \alpha_j |\phi_j^0\rangle \otimes |\psi_j^0\rangle, \;\; \sum_j \alpha_j |\phi_j^1\rangle \otimes |\psi_j^1\rangle, \qquad (3)$$

where the vectors ϕ_j^0 and ϕ_j^1 have dimension $\ell(x) - 1$ (so that the measured qubit is $\ell(x)$).

$$\begin{array}{ll}
[q,\ell,(\lambda x^A.M)\,V] \xrightarrow{1} [q,\ell,M\{V/x\}] & [q,\ell,\mathtt{let}\;x^A\otimes y^B \;=\; V\otimes W\;\mathtt{in}\;N] \xrightarrow{1} [q,\ell,N\{V/x,W/y\}] \\
[q,\ell,\mathtt{skip};N] \xrightarrow{1} [q,\ell,N] & [q,\ell,\mathtt{match}\;(\mathtt{in}_\ell\;V)\;\mathtt{with}\;(x^A:M|y^B:N)] \xrightarrow{1} [q,\ell,M\{V/x\}] \\
[q,\ell,\mathtt{split}\,V] \xrightarrow{1} [q,\ell,V] & [q,\ell,\mathtt{match}\;(\mathtt{in}_r\;V)\;\mathtt{with}\;(x^A:M|y^B:N)] \xrightarrow{1} [q,\ell,N\{V/y\}]
\end{array}$$

$$[q,\ell,\mathtt{letrec}\;f^{A\multimap B}\;x=M\;\mathtt{in}\;N] \xrightarrow{1} [q,\ell,N\{(\lambda x^A.\mathtt{letrec}\;f^{A\multimap B}\;x=M\;\mathtt{in}\;M)/f\}]$$

(a) Classical control.

$$[q,\ell,U(x_1\otimes\cdots\otimes x_k)] \xrightarrow{1} [q',\ell,x_1\otimes\cdots\otimes x_k]$$

$$\begin{array}{ll}
[q,\emptyset,\mathtt{new\;ff}] \xrightarrow{1} [q\otimes|0\rangle,\{y\mapsto n+1\},y] & [\alpha q_0+\beta q_1,\{x\mapsto i\},\mathtt{meas}\;x] \xrightarrow{|\beta|^2} [q_1',\emptyset,\mathtt{tt}] \\
[q,\emptyset,\mathtt{new\;tt}] \xrightarrow{1} [q\otimes|1\rangle,\{y\mapsto n+1\},y] & [\alpha q_0+\beta q_1,\{x\mapsto i\},\mathtt{meas}\;x] \xrightarrow{|\alpha|^2} [q_0',\emptyset,\mathtt{ff}]
\end{array}$$

(b) Quantum data. The variable y is fresh.

$$\begin{array}{lll}
[q,\ell,MN] \xrightarrow{p} [q',\ell',M'N] & [q,\ell,M\otimes N] \xrightarrow{p} [q',\ell',M'\otimes N] & [q,\ell,\mathtt{in}_\ell\;M] \xrightarrow{p} [q',\ell',\mathtt{in}_\ell\;M'] \\
[q,\ell,VM] \xrightarrow{p} [q',\ell',VM'] & [q,\ell,V\otimes M] \xrightarrow{p} [q',\ell',V\otimes M'] & [q,\ell,\mathtt{in}_r\;M] \xrightarrow{p} [q',\ell',\mathtt{in}_r\;M']
\end{array}$$

$$[q,\ell,M;N] \xrightarrow{p} [q',\ell',M';N] \qquad [q,\ell,\mathtt{let}\;x^A\otimes y^B \;=\; M\;\mathtt{in}\;N] \xrightarrow{p} [q',\ell',\mathtt{let}\;x^A\otimes y^B \;=\; M'\;\mathtt{in}\;N]$$

$$[q,\ell,\mathtt{match}\;M\;\mathtt{with}\;(x^A:P|y^B:N)] \xrightarrow{p} [q',\ell',\mathtt{match}\;M'\;\mathtt{with}\;(x^A:P|y^B:N)]$$

(c) Congruence rules, under the hypothesis that for some ℓ_0 we have $\ell=\ell_0\uplus\ell|_M$, $\ell'=\ell_0\uplus\ell'|_{M'}$ and $[q,\ell|_M,M]\xrightarrow{p}[q',\ell'|_{M'},M']$.

Table 3: Reduction rules on closures.

Note that the only probabilistic reduction step is the one corresponding to measurement. Also, we underline that the hypothesis associated with a congruence rule $[q,\ell,C[M]]\xrightarrow{p}[q',\ell',C[M']]$ takes into account the whole quantum states q and q'. In fact, because of the entanglement, the evaluation of $[q,\ell|_M,M]$ may have a side-effect on the state of the qubits pointed by the variables occurring in the context $C[\,]$.

The rules assume that the involved closures are well-defined. In particular, whenever $[q,\ell,M] \xrightarrow{p} [q,\ell,M']$, the two terms M and M' have the same free variables. For example, the closure $[|00\rangle,|yz\rangle,(\lambda x.y)z]$ cannot reduce and it represents an error. The type system will prevent such an error as proven in Proposition 12.

Example 9. Recall Example 5. We have $[|\rangle,|\rangle,\mathtt{cointoss}] \xrightarrow{1} [|1\rangle,|x\rangle,\mathtt{meas}(Hx)] \xrightarrow{1} [\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|x\rangle,\mathtt{meas}\;x]$, the latter reducing to either $[|\rangle,|\rangle,\mathtt{tt}]$ or $[|\rangle,|\rangle,\mathtt{ff}]$, with equal probability $\frac{1}{2}$. As for $\mathtt{entangle}$, we have that

$$\begin{array}{ll}
 & [\alpha|0\rangle+\beta|1\rangle,|x\rangle,\mathtt{entangle}\;x] \\
\xrightarrow{1} & [\alpha|0\rangle+\beta|1\rangle,|x\rangle,N_c(x\otimes(\mathtt{new\;ff}))] \\
\xrightarrow{1} & [\alpha|00\rangle+\beta|10\rangle,|xy\rangle,N_c(x\otimes y)] \\
\xrightarrow{1} & [\alpha|00\rangle+\beta|11\rangle,|xy\rangle,x\otimes y].
\end{array}$$

Similarly, one can check that $[\alpha|0\rangle+\beta|1\rangle,|q\rangle,\mathtt{qlist}\,q]$ behaves as described in Section 2.4, reducing to $[\alpha|0\rangle+\beta|1\rangle,|q\rangle,q::\mathtt{nil}]$ with probability $\frac{1}{2}$, to $[\alpha|00\rangle+\beta|11\rangle,|qq'\rangle,q'::q::\mathtt{nil}]$ with probability $\frac{1}{4}$, etc. In particular, notice that in any single reduction sequence the variable q has not been duplicated, as correctly asserted by the type of $\mathtt{qlist}$.

Lemma 10 (Substitution)**.** *Suppose $!\Delta,\Gamma,x:A\vdash M:B$ and $!\Delta,\Sigma\vdash V:A$, where Γ and Σ are linear contexts with disjoint domain. Then $!\Delta,\Gamma,\Sigma\vdash M\{V/x\}:B$.*

Proof. By induction on the derivation of $!\Delta,\Gamma,x:A\vdash M:B$ (which is unique by Proposition 4). □

Proposition 11 (Subject reduction)**.** *When $[q,|y_1\dots y_n\rangle,M] \xrightarrow{p} [q',|x_1\dots x_{n'}\rangle,M']$ and $y_1:\mathbf{qubit},\dots,y_n:\mathbf{qubit}\vdash M:A$, then $x_1:\mathbf{qubit},\dots,x_{n'}:\mathbf{qubit}\vdash M':A$.*

Proof. The proof is done by structural induction on the reduction $[q,|y_1\dots y_n\rangle,M] \xrightarrow{p} [q',|x_1\dots x_{n'}\rangle,M']$, using Lemma 10 for the cases where substitution occurs. □

Proposition 12 (Type safety)**.** *If $[q,\ell,M]$ is typable then either M is a value or there is a closure $[q',\ell',M']$ such that $[q,\ell,M] \xrightarrow{p} [q',\ell',M']$. Moreover, if M is not a value, the total probability of all possible single-step reductions from $[q,\ell,M]$ is* 1*.*

Proof. By induction on a typing derivation of M. □

Lemma 13 (Totality)**.** *If $[q,\ell,M] \xrightarrow{p} [q',\ell',M']$ and $[q,\ell,M]$ is total, then $[q',\ell',M']$ is total too.*

Proof. By induction on a derivation of $[q,\ell,M] \xrightarrow{p} [q',\ell',M']$, one proves that

$$\dim(q')=\dim(q)+\dim(\ell')-\dim(\ell)$$

where $\dim(q)$ is the size of the quantum state q and $\dim(\ell)$ is the cardinality of the domain set of the linking function ℓ. Then, one gets the statement, since $[q,\ell,M]$ is total iff $\dim(q)=\dim(\ell)$. □

3.2 Reduction system as a Markov chain

The reduction relation $\to$ defines the probability that a closure reduces to another one in a single step. In order to extend it to an arbitrary large (but finite) number of reduction steps, we present the reduction relation as a Markov process over the set of closures, following the spirit of [1].

Definition 14. We define an infinite matrix Red $\in [0,1]^{\mathrm{Cl}\times\mathrm{Cl}}$ componentwise:

$$\mathrm{Red}_{[q,\ell,M],[q',\ell',M']} := \begin{cases} p & \text{if } [q,\ell,M] \xrightarrow{p} [q',\ell',M'], \\ 1 & \text{if } [q,\ell,M] = [q',\ell',M'] \text{ and} \\ & M \text{ is a value,} \\ 0 & \text{otherwise.} \end{cases}$$

Note that Red is well-defined: for any two quantum closures $[q,\ell,M]$ and $[q',\ell',M']$ there is at most one p such that $[q,\ell,M] \xrightarrow{p} [q',\ell',M']$. Red is a *stochastic matrix*: for all closures $[q,\ell,M]$, $0 \leqslant \sum_{[q',\ell',M']\in\mathrm{Cl}} \mathrm{Red}_{[q,\ell,M],[q',\ell',M']} \leqslant 1$.

Intuitively, the value of $\mathrm{Red}_{[q,\ell,M],[q',\ell',M']}$ describes the probability of evolving from the state $[q,\ell,M]$ to the state $[q',\ell',M']$ in one step.

A closure $[q,\ell,M]$ is *absorbing* whenever $\mathrm{Red}_{[q,\ell,M],[q,\ell,M]} = 1$: the absorbing states are those which are invariant under the transition matrix. In particular, values are all absorbing. (Note that there are absorbing terms which are not values, such as $[|\rangle, |\rangle, \mathbf{\Omega}]$, with $\mathbf{\Omega}$ the total diverging term $\mathtt{letrec}\ f\, x = f x\ \mathtt{in}\ f\ \mathtt{skip}$).

The n-th power Red^n of the matrix Red is a stochastic matrix on Cl (in case $n = 0$, we have the identity matrix on Cl). Intuitively, the value of $\mathrm{Red}^n_{[q,\ell,M],[q',\ell',M']}$ is the probability of evolving from the state $[q,\ell,M]$ to the state $[q',\ell',M']$ in exactly n steps. In particular, if $[q',\ell',V]$ is a value then the sequence $\{\mathrm{Red}^n_{[q,\ell,M],[q',\ell',V]}\}_{n\in\mathbb{N}}$ is monotonically increasing.

We then can define the matrix Red^∞ in $[0,1]^{\mathrm{Cl}\times\mathit{Val}}$ as follows:

$$\mathrm{Red}^\infty_{[q,\ell,M],[q',\ell',V]} := \sup_{n=0}^{\infty} \left(\mathrm{Red}^n_{[q,\ell,M],[q',\ell',V]}\right). \tag{4}$$

The element $\mathrm{Red}^\infty_{[q,\ell,M],[q',\ell',V]}$ is the probability that $[q,\ell,M]$ reaches a value $[q',\ell',V]$ in an arbitrary number of steps. Finally, we define the probability that $[q,\ell,M]$ reduces to some value as

$$\mathrm{Halt}_{[q,\ell,M]} := \sum_{[q',\ell',V]\in\mathrm{Val}} \mathrm{Red}^\infty_{[q,\ell,M],[q',\ell',V]}. \tag{5}$$

4. Infinite biproduct completion

In this section, we recall the definition of the infinite biproduct completion $\mathbf{C}^\oplus$ of a symmetric monoidal closed linear continuous $\mathcal{R}$-category $\mathbf{C}$ (Definition 15). We also recall how $\mathbf{C}$ gives (under certain hypotheses) a Lafont category, which is a model of intuitionistic linear logic (Proposition 18). This construction is known: it was sketched in [5] and detailed in [9, 10, 13, 14]. In particular, [10] gives the definition of linear continuous $\mathcal{R}$-category that we use here. Our contribution is in applying such a construction to a category useful for interpreting quantum data types (Section 5).

Consider a *continuous commutative semiring* $\mathcal{R}$. This is a commutative semiring $(|\mathcal{R}|, 0, 1, +, \cdot)$ equipped with an order relation $\prec$ such that 0 is the minimum, any directed set $D \subseteq |\mathcal{R}|$ has a sup $\bigvee$, and $+$ and $\cdot$ are continuous, i.e., monotone and $\bigvee(r + D) = r + \bigvee D$ and $\bigvee(r \cdot D) = r \cdot \bigvee D$. The letters p, q, r range over $|\mathcal{R}|$.

We say that a symmetric monoidal closed category $\mathbf{C}$ is a *linear continuous $\mathcal{R}$-category* whenever: (i) every homset is endowed with a structure of module over the semiring $\mathcal{R}$; (ii) composition and tensor are bilinear, that is $(pf + p'f')\,;(qg + q'g')$ is equal to

$$(p\cdot q)(f\,;g) + (p\cdot q')(f\,;g') + (p'\cdot q)(f'\,;g) + (p'\cdot q')(f'\,;g'),$$

and the same for $\otimes$; (iii) every homset is endowed with a structure of complete partial order with $\mathbf{0}$ as the minimum and composition, $\otimes$, addition and scalar multiplication continuous.

From now on, $\mathbf{C}$ denotes a symmetric monoidal closed linear continuous $\mathcal{R}$-category. In that case, notice that we can define the indexed sum over a homset $\mathbf{C}(A,B)$ as

$$\sum_{f\in S} f := \bigvee_{F\subseteq_{\mathrm{fin}} S}\Big(\sum_{f\in F} f\Big). \tag{6}$$

Definition 15. An *object* $\mathfrak{A}$ of $\mathbf{C}^\oplus$ is a pair $(|\mathfrak{A}|, (\mathfrak{A}_a)_{a\in|\mathfrak{A}|})$ of a (possibly infinite) set of indexes $|\mathfrak{A}|$, called the *web* of $\mathfrak{A}$, and a $|\mathfrak{A}|$-family of objects in $\mathbf{C}$. The *homset* $\mathbf{C}^\oplus(\mathfrak{A},\mathfrak{B})$ is the set of the $|\mathfrak{A}| \times |\mathfrak{B}|$ matrices of morphisms $\phi = (\phi_{a,b})_{(a,b)\in|\mathfrak{A}|\times|\mathfrak{B}|}$ in $\mathbf{C}$. Given $\phi \in \mathbf{C}^\oplus(\mathfrak{A},\mathfrak{B})$ and $\psi \in \mathbf{C}^\oplus(\mathfrak{B},\mathfrak{C})$, the (diagrammatic) *composition* $\phi\,;\psi$ is the matrix product: $(\phi\,;\psi)_{a,c} = \sum_{b\in|\mathfrak{B}|} \phi_{a,b}\,;\psi_{b,c}$. The identity is the diagonal matrix $\mathrm{id}_{a,a'} := \mathrm{id}_{\mathfrak{A}_a}$ if $a = a'$, and $\mathrm{id}_{a,a'} := \mathbf{0}$ if $a \neq a'$.

4.1 The linear structure

4.1.1 Biproduct

The category $\mathbf{C}^\oplus$ is the free biproduct completion of $\mathbf{C}$. The biproduct $\bigoplus_{i\in I} \mathfrak{A}_i$ of a family $(\mathfrak{A}_i)_{i\in I}$ of objects in $\mathbf{C}^\oplus$ is defined by $|\bigoplus_{i\in I} \mathfrak{A}_i| := \bigcup_{i\in I} \{i\} \times |\mathfrak{A}_i|$ and $\left(\bigoplus_{i\in I} \mathfrak{A}_i\right)_{(j,a)} := (\mathfrak{A}_j)_a$. The corresponding projections and injections are denoted respectively by π^j and ι^j. The tupling $\langle\phi_i\rangle_{i\in I}$ (resp. (co)-tupling $[\psi_i]_{i\in I}$) of a family of morphisms ϕ_i elements of $\mathbf{C}^\oplus(\mathfrak{A},\mathfrak{B}_i)$ (resp. ψ_i elements of $\mathbf{C}^\oplus(\mathfrak{A}_i,\mathfrak{B})$) is defined by $(\langle\phi_i\rangle_{i\in I})_{a,(i,b)} := (\phi_i)_{a,b}$ and $([\psi_i]_{i\in I})_{(i,a),b} := (\psi_i)_{a,b}$.

4.1.2 Monoidal product

The bifunctor $\otimes : \mathbf{C}^\oplus \times \mathbf{C}^\oplus \to \mathbf{C}^\oplus$ is defined on objects $\mathfrak{A}, \mathfrak{B}$ by $|\mathfrak{A}\otimes\mathfrak{B}| := |\mathfrak{A}| \times |\mathfrak{B}|$ and $(\mathfrak{A}\otimes\mathfrak{B})_{(a,b)} := \mathfrak{A}_a \otimes \mathfrak{B}_b$, where the $\otimes$ in the right-hand side of the second equation is that of the category $\mathbf{C}$. The tensor unit is the singleton web space $(\{*\}, \mathbf{1})$, where $\mathbf{1}$ is the tensor unit of $\mathbf{C}$. By abuse of notation we will also denote the unit of $\mathbf{C}^\oplus$ by $\mathbf{1}$. The action of $\otimes$ on morphisms is defined componentwise, and similarly for the associativity, unit, and symmetry isomorphisms. E.g., the associator is $\alpha^{\mathfrak{A},\mathfrak{B},\mathfrak{C}}_{((a,b),c),(a',(b',c'))} = \delta_{a,a'}\delta_{b,b'}\delta_{c,c'}\alpha^{\mathfrak{A}_a,\mathfrak{B}_b,\mathfrak{C}_c}$, where $\alpha^{\mathfrak{A}_a,\mathfrak{B}_b,\mathfrak{C}_c}$ is the associator in $\mathbf{C}$ and $\delta_{a,a'}$ is the Kronecker delta.

Notice the n-fold tensor product $\mathfrak{A}^{\otimes n}$ of an object $\mathfrak{A}$ can be represented by $|\mathfrak{A}^{\otimes n}| := \{(a_1,\dots,a_n) \mid \forall i \leqslant n, a_i \in |\mathfrak{A}|\}$ and $\mathfrak{A}^{\otimes n}_{(a_1,\dots,a_n)} := \mathfrak{A}_{a_1} \otimes\cdots\otimes \mathfrak{A}_{a_n}$. The group S_n of permutations on $\{1,\dots,n\}$ gives the $n!$ symmetries of $\mathfrak{A}^{\otimes n}$, namely $\sigma \in S_n$ can be seen as the symmetry

$$\sigma_{(a_1,\dots,a_n),(a'_1,\dots,a'_n)} := \delta_{a_1,a'_{\sigma(1)}} \cdots \delta_{a_n,a'_{\sigma(n)}} \sigma^{\mathfrak{A}_{a_1},\dots,\mathfrak{A}_{a_n}},$$

where $\sigma^{\mathfrak{A}_{a_1},\dots,\mathfrak{A}_{a_n}}$ is the symmetry in $\mathbf{C}$ between $\mathfrak{A}_{a_1} \otimes\cdots\otimes \mathfrak{A}_{a_n}$ and $\mathfrak{A}_{a_{\sigma(1)}} \otimes\cdots\otimes \mathfrak{A}_{a_{\sigma(n)}}$.

Tensor product distributes over biproducts. The isomorphism between $(\bigoplus_{i\in I} \mathfrak{A}_i) \otimes \mathfrak{B}$ and $\bigoplus_{i\in I} (\mathfrak{A}_i \otimes \mathfrak{B})$ is

$$\mathtt{distr}_{((i,a),b),(i',(a',b'))} := \delta_{i,i'}\delta_{a,a'}\delta_{b,b'}\,\mathrm{id}^{\mathfrak{A}_a\otimes\mathfrak{B}_b}.$$

4.1.3 Monoidal closure

The internal hom object is defined as $|\mathfrak{A} \multimap \mathfrak{B}| := |\mathfrak{A}| \times |\mathfrak{B}|$ and $(\mathfrak{A} \multimap \mathfrak{B})_{(a,b)} := \mathfrak{A}_a \multimap \mathfrak{B}_b$, where $\mathfrak{A}_a \multimap \mathfrak{B}_b$ is the internal hom in $\mathbf{C}$. For every pair of objects $\mathfrak{A}, \mathfrak{B}$, the evaluation morphism $\mathrm{Eval}^{\mathfrak{A},\mathfrak{B}} : \mathbf{C}^\oplus((\mathfrak{A} \multimap \mathfrak{B})\otimes\mathfrak{A}, \mathfrak{B})$ is defined componentwise, using the evaluation morphism $\mathrm{eval}^{\mathfrak{A}_a,\mathfrak{B}_b}$ in $\mathbf{C}((\mathfrak{A}_a \multimap \mathfrak{B}_b) \otimes \mathfrak{A}_a, \mathfrak{B}_b)$. The isomorphism from $\mathbf{C}^\oplus(\mathfrak{C} \otimes \mathfrak{A}, \mathfrak{B})$ to $\mathbf{C}^\oplus(\mathfrak{C}, \mathfrak{A} \multimap \mathfrak{B})$ is denoted by $\Lambda(-)$ and its inverse by $\mathrm{App}(-)$.

Proposition 16. *The category $\mathbf{C}^\oplus$ endowed with the above structure is symmetric monoidal closed.*

Similarly, it is easy to check that $\mathbf{C}^\oplus$ also inherits the $\star$-autonomous (resp. compact closed) structure of $\mathbf{C}$.

Proposition 17. $\mathbf{C}^{\oplus}$ *is a linear continuous $\mathcal{R}$-category with the pointwise $\mathcal{R}$-module operations and order, e.g.,* $(\phi + \psi)_{a,b} = \phi_{a,b} + \psi_{a,b}$.

4.2 Exponential structure

A symmetric monoidal closed category with finite products, such that each object has a corresponding free commutative comonoid, is called a *Lafont category*, which is known to be a model of intuitionistic linear logic [7, 13].

We say that the *n-th (symmetric) power* (A^n, eq^{A^n}) of an object A of a symmetric monoidal category is the equalizer of the $n!$ symmetries of the n-ary tensor $A^{\otimes n}$, provided that such an equalizer exists. That is, eq^{A^n} is a morphism from A^n to $A^{\otimes n}$ equalizing the symmetries of $A^{\otimes n}$ (i.e., for every permutation $\sigma \in S_n$, $eq^{A^n}; \sigma = eq^{A^n}$), enjoying the following universal property: for every object D and morphism f from D to $A^{\otimes n}$ equalizing the symmetries of $A^{\otimes n}$, there exists a unique morphism $f^\dagger$ such that $f^\dagger \,;\, eq^{A^n} = f$.

$$\begin{tikzcd}
A^n \arrow[r, "eq^{A^n}"] & A^{\otimes n} \arrow[r, shift left, "\sigma_1"] \arrow[r, shift right, "\sigma_{n!}"'] & A^{\otimes n} \\
D \arrow[u, dotted, "\text{unique } f^\dagger"] \arrow[ur, "f"] & &
\end{tikzcd} \tag{7}$$

Moreover, we say that (A^n, eq^{A^n}) *preserves the monoidal product* whenever for every object B, the pair $(A^n \otimes B, eq^{A^n} \otimes \mathrm{id}^B)$ is the equalizer of the diagram obtained from the diagram equalized by (A^n, eq^{A^n}) by replacing each object A with $A \otimes B$ and each arrow f by $f \otimes \mathrm{id}^B$.

Proposition 18 (Folklore, cf. [5, 14])**.** $\mathbf{C}^{\oplus}$ *is a Lafont category whenever the category* $\mathbf{C}$ *has the n-th power for every $n \in \mathbb{N}$ and object A, and this power preserves the monoidal product.*

Namely, one proves that $\mathbf{C}^{\oplus}$ inherits the n-th powers $(\mathfrak{A}^n, eq^{\mathfrak{A}^n})$ from $\mathbf{C}$. Then, the free commutative comonoid $!\mathfrak{A}$ of an object $\mathfrak{A}$ is defined as $\bigoplus_n \mathfrak{A}^n$.

For later reference, we give a concrete presentation of $!\mathfrak{A}$:

$$|!\mathfrak{A}| := \mathcal{M}_f(|\mathfrak{A}|), \quad (!\mathfrak{A})_\mu := \bigotimes_{a \in |\mu|} \mathfrak{A}_a^{\mu(a)}, \tag{8}$$

where $\mathcal{M}_f(|\mathfrak{A}|)$ is the set of the finite multisets of $|\mathfrak{A}|$, $\mu(a)$ is the number of occurrences of a in μ, $|\mu|$ is the support of the multiset μ, i.e., $|\mu| := \{a \in |\mathfrak{A}| \;;\; \mu(a) \neq 0\}$, the object $\mathfrak{A}_a^{\mu(a)}$ is the $\mu(a)$-th power in $\mathbf{C}$ of $\mathfrak{A}_a$. Finally, the object $\bigotimes_{a \in |\mu|} \mathfrak{A}_a^{\mu(a)}$ denotes the tensor of the spaces $\mathfrak{A}_a^{\mu(a)}$. This is well-defined up to isomorphism; for example, it can be defined by arbitrarily fixing an order on the elements of $|\mathfrak{A}|$. The counit, here called *weakening* $\mathtt{w} \in \mathbf{C}^{\oplus}(!\mathfrak{A}, \mathbf{1})$, is $\mathtt{w}_{\mu,*} := \delta_{\mu,[\,]}\, \mathrm{id}^{\mathbf{1}}$, where $\mathrm{id}^{\mathbf{1}}$ is the identity of $\mathbf{1}$ in $\mathbf{C}$. The co-multiplication, here called *contraction* $\mathtt{c} \in \mathbf{C}^{\oplus}(!\mathfrak{A}, !\mathfrak{A} \otimes !\mathfrak{A})$, is given by $\mathtt{c}_{\mu,(\mu',\mu'')} = \delta_{\mu,\mu'+\mu''} \overline{\mathtt{c}}^{\mu',\mu''}$, where $\overline{\mathtt{c}}^{\mu',\mu''}$ is the unique morphism in $\mathbf{C}$ satisfying the equation $\overline{\mathtt{c}}^{\mu',\mu''} \,;\, eq^{\mathfrak{A}^{\mu'}} \otimes eq^{\mathfrak{A}^{\mu''}} = eq^{\mathfrak{A}^{\mu}} ;\sigma$, with $eq^{\mathfrak{A}^{\mu}}$ be the equalizer of the symmetries of $\bigotimes_{a \in |\mu|} \mathfrak{A}_a^{\otimes \mu(a)}$ of the shape $\bigotimes_{a \in |\mu|} \sigma^a$ with $\sigma^a \in S_{\mu(a)}$ (and similarly for $eq^{\mathfrak{A}^{\mu'}}$ and $eq^{\mathfrak{A}^{\mu''}}$). Notice that such equalizers exist by the hypothesis that the powers of $\mathbf{C}$ preserve the monoidal product. Last, the *dereliction* $\mathtt{d} \in \mathbf{C}^{\oplus}(!\mathfrak{A}, \mathfrak{A})$ is $\mathtt{d}_{\mu,a} := \delta_{\mu,[a]}\, \mathrm{id}^{\mathfrak{A}_a}$.

The linear exponential comonad is given as usual for Lafont categories. The functorial promotion maps an object $\mathfrak{A}$ to $!\mathfrak{A}$ and a morphism $\phi \in \mathbf{C}^{\oplus}(\mathfrak{A}, \mathfrak{B})$ to the unique comonoid morphism $!\phi \in \mathbf{C}^{\oplus}(!\mathfrak{A}, !\mathfrak{B})$ satisfying the equation $\mathtt{d} \,;\, \phi = !\phi \,;\, \mathtt{d}$, which has exactly one solution by the freeness of the exponential comonoid on $\mathfrak{B}$. Weakening gives the counit. The co-multiplication (also called *digging*) is the unique comonoid morphism $\mathtt{dig} \in \mathbf{C}^{\oplus}(!\mathfrak{A}, !!\mathfrak{A})$ such that $\mathtt{dig} \,;\, \mathtt{d} = \mathrm{id}$. Finally, the last two morphisms which are essential to interpret our calculus are Bierman's $\mathtt{m}^{\otimes} \in \mathbf{C}^{\oplus}(!\mathfrak{A} \otimes !\mathfrak{B}, !(\mathfrak{A} \otimes \mathfrak{B}))$ and $\mathtt{m}^{\mathbf{1}} \in \mathbf{C}^{\oplus}(\mathbf{1}, !\mathbf{1})$ which are the unique comonoid morphisms such that $\mathtt{m}^{\otimes} \,;\, \mathtt{d} = \mathtt{d} \otimes \mathtt{d}$ and $\mathtt{m}^{\mathbf{1}} \,;\, \mathtt{d} = \mathrm{id}^{\mathbf{1}}$.

5. Completing CPM

We want to apply the general construction $\mathbf{C}^{\oplus}$ to a category $\mathbf{C}$ which is useful for interpreting quantum data types. One natural choice would be to consider the category **CPM** of completely positive maps [16]. However, **CPM** misses two essential requirements for producing $\mathbf{CPM}^{\oplus}$. First, **CPM** does not have the equalizers of the tensor symmetries. Second, the homsets of **CPM** are not continuous with respect to the Löwner order, i.e., not every directed subset has a sup.

We will therefore recast this category into $\overline{\mathbf{CPMs}}$, the category of completely positive maps on positive matrices with symmetries and a ∞ morphism completing the Löwner order on completely positive maps.

5.1 Complete positive maps with symmetries and top

Any permutation $g \in S_n$ gives rise to a matrix $P_g \in \mathbb{C}^{n \times n}$, defined by $P_g(e_i) = e_{g(i)}$, where e_i is the ith standard basis vector. We define an action of g on $\mathbb{C}^{n \times n}$ by $g \cdot A := P_g A P_g^{-1}$. Moreover, for a subgroup $G \subseteq S_n$, we define $G \cdot A := \frac{1}{\#G} \sum_{g \in G} g \cdot A$, where $\#G$ is the number of elements of G.

Lemma 19. *Given a subgroup $G \subseteq S_n$, its action on $\mathbb{C}^{n \times n}$ is idempotent (i.e., $G \,;\, G = G$) and completely positive.*

Proof. For the idempotence, notice that for every $g \in G$, $Gg = G$, therefore: $G \cdot G \cdot A = \frac{1}{\#G} \sum_{g \in G} Gg \cdot A = G \cdot A$ The complete positivity of G is derived from the complete positivity of each element $g \in G$, when considered as a morphism. Indeed, any map of the form $A \mapsto SAS^{-1}$ is completely positive, and therefore so is $A \mapsto g \cdot A = P_g A P_g^{-1}$. Moreover, non-negative linear combination of completely positive maps is completely positive, and therefore $G = \frac{1}{\#G} \sum_{g \in G} g$ is completely positive. □

In the sequel, we use the notation G both for a subgroup of S_n and for the completely positive map defined by it.

We can now define the category $\overline{\mathbf{CPMs}}$ which is essentially a sub-category of the Karoubi envelope of the completion of $\mathbf{CPM}_s$, continuous with respect to the Löwner ordering on positive matrices. In fact, the idea of using the Karoubi construction for getting the tensor powers follows [9].

Definition 20. The category $\overline{\mathbf{CPMs}}$ of *completely positive maps with symmetries and top* has as objects pairs (n, G) where $n \in \mathbb{N}$ and G is a subgroup of S_n. A morphism f from (n, G) to (m, H) is either a completely positive map from $\mathbb{C}^{n \times n}$ to $\mathbb{C}^{m \times m}$ such that $G \,;\, f \,;\, H = f$, or the constant ∞. The identity of (n, G) is G and the composition is the functional composition on completely positive maps, or is given by the equations $\infty \,;\, g = \infty = f \,;\, \infty$ if $f, g \neq \mathbf{0}$, and $\infty \,;\, \mathbf{0} = \mathbf{0} = \mathbf{0} \,;\, \infty$.

Let $\overline{\mathbb{R}^+} = \mathbb{R}^+ \cup \{\infty\}$ be the continuous completion of the semiring $\mathbb{R}^+$ with respect to the canonical ordering on reals, with $0 \cdot \infty = 0$. Note that $\overline{\mathbb{R}^+}$ is a continuous semiring.

Remark 21. The category $\overline{\mathbf{CPMs}}$ is a linear continuous $\overline{\mathbb{R}^+}$-category, continuous with respect to the Löwner order $\sqsubseteq$ on positive maps enriched with ∞ as the maximum element.

Proposition 22. *The category* $\overline{\mathbf{CPMs}}$ *inherits the symmetric monoidal closed structure of* **CPM**.

Proof. The object $(n, G) \otimes (m, H)$ is defined as $(nm, G \otimes H)$, where we use the isomorphism $\mathbb{C}^{nm,nm} = \mathbb{C}^{n\times m, n\times m}$ obtained by the lexicographic order on the pairs $(i, j) \in n \times m$, and $G \otimes H$ is intended to be the subgroup of S_{nm} of the permutations of the form $g \otimes h$, with $g \in G, h \in H$ acting as $(i, j) \mapsto (g(i), h(j))$. The tensor unit is $\mathbf{1} = (1, \{\mathrm{id}\})$. Symmetry, unit, and associativity maps are obtained from those of **CPM** by pre-composing and post-composing with the actions of the groups of the objects. The homset $(n, G) \multimap (m, H)$ is equal to the tensor $(nm, G \otimes H)$ and the morphism eval is again inherited from **CPM**. Concretely, given $F \in \mathbb{C}^{n\times m, n\times m}$ and $N \in \mathbb{C}^{n\times n}$, $\mathrm{eval}(F \otimes N)$ is the matrix in $\mathbb{C}^{m\times m}$ defined at the coordinate $(j, j') \in m \times m$ by

$$\frac{1}{\#G\#H} \sum_{g\in G} \sum_{h\in H} \sum_{(i,i')\in n\times n} F_{(i,h(j)),(i',h(j'))} N_{g(i),g(i')}. \quad \square$$

In fact, one can prove that $\overline{\mathbf{CPMs}}$ inherits the compact closed structure of **CPM**.

Lemma 23. *The category* $\overline{\mathbf{CPMs}}$ *has the* n*-th powers for any* $n \in \mathbb{N}$*. Moreover, such powers preserve the monoidal product.*

Proof. Notice that the group of the $n!$ symmetries of $(m, G)^{\otimes n}$ can be seen as a group H of permutations on m^n, each element σ acting as follows on m^n seen as the set of n-tuples of elements in $\{1, \dots, m\}$ lexicographically ordered: $(i_1, \dots, i_n) \mapsto (i_{\sigma(1)}, \dots, i_{\sigma(n)})$. Let us denote by $\langle G^{\otimes n} \cup H\rangle$ the smallest subgroup of S_{m^n} containing $G^{\otimes n} \cup H$. Notice that all elements of $\langle G^{\otimes n} \cup H\rangle$ are of the form $(g_1, \dots, g_n)\ ;\ \sigma$ for $g_i \in G$ and $\sigma \in H$. In fact, such a permutation can also be expressed as $\sigma\ ;\ (g_{\sigma(1)}, \dots, g_{\sigma(n)})$. In particular, the morphism induced by $\langle G^{\otimes n} \cup H\rangle$ is equal to $G^{\otimes n}\ ;\ H$. Define the equalizer of the symmetries of $(m, G)^{\otimes n}$ by $(m, G)^n := (m^n, \langle G^{\otimes n} \cup H\rangle)$ with $eq^{(m,G)^n} := \langle G^{\otimes n} \cup H\rangle$. $\square$

5.2 The biproduct completion of $\overline{\mathbf{CPMs}}$.

The category $\overline{\mathbf{CPMs}}$ is a linear continuous $\overline{\mathbb{R}^+}$-category (Remark 21), so we can apply the construction of Section 4 to obtain its infinite biproduct completion $\overline{\mathbf{CPMs}}^{\oplus}$. To sum up, the category $\overline{\mathbf{CPMs}}^{\oplus}$ is given as follows.

Objects are given by indexed families $\{(n_a, G_a)\}_{a\in|\mathfrak{A}|}$, where the index set $|\mathfrak{A}|$ is called the web of $\mathfrak{A}$ and, for every $a \in |\mathfrak{A}|$, n_a is a natural non-negative integer and G_a a group of permutations over n_a.

Morphisms from $\{(n_a, G_a)\}_{a\in|\mathfrak{A}|}$ to $\{(m_b, H_b)\}_{b\in|\mathfrak{B}|}$ are matrices ϕ indexed by $|\mathfrak{A}| \times |\mathfrak{B}|$ and such that $\phi_{a,b}$ is either a completely positive map from $\mathbb{C}^{n_a\times n_a}$ to $\mathbb{C}^{m_b\times m_b}$ invariant under the actions of G_a and H_b, or the top ∞.

From Propositions 18 and 22 and Lemma 23, we can conclude:

Corollary 24. *The category* $\overline{\mathbf{CPMs}}^{\oplus}$ *is a Lafont category.*

Example 25. The unit of the monoidal product $\otimes$ is given by the singleton web object $\mathbf{1} = \{(1, \{\mathrm{id}\})_*\}$. The biproduct $\mathbf{1} \oplus \mathbf{1}$ will be used to interpret the **bit** type and it is defined as the two-element family $\{(1, \{\mathrm{id}\})_{\mathtt{tt}}, (1, \{\mathrm{id}\})_{\mathtt{ff}}\}$. The free commutative comonoids associated with $\mathbf{1}$ and $\mathbf{1}\oplus\mathbf{1}$ are infinite families that can be concretely defined as (see Equation 8): $!\mathbf{1} = \{(1, \{\mathrm{id}\})_n\}_{n\in\mathbb{N}}$ and $!(\mathbf{1} \oplus \mathbf{1}) = \{(1, \{\mathrm{id}\})_{(n,m)}\}_{n,m\in\mathbb{N}}$, where we use the isomorphisms between $\mathcal{M}_f(\{*\})$ (resp. $\mathcal{M}_f(\{\mathtt{tt}, \mathtt{ff}\})$) and $\mathbb{N}$ (resp. $\mathbb{N} \times \mathbb{N}$). In general, notice that all constructions of the Lafont category preserve the underlined **CPMs** space $(1, \{\mathrm{id}\})$ and act only at the level of webs.

For more involved examples, one should look for objects with larger dimensions, like $\mathbf{qubit} := \{(2, \{\mathrm{id}\})_*\}$. In fact, we have $\mathbf{qubit}^{\otimes 2} := \{(4, \{\mathrm{id}\})_*\}$, while the 2-power $\mathbf{qubit}^2$ is $\{(4, \{\mathrm{id}, \sigma\})_*\}$, where 4 is represented as the lexicographically ordered set $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$ and the permutation σ acts on it by $(b, b') \mapsto (b', b)$ (cf. the proof of Lemma 23). The group of permutations $\{\mathrm{id}, \sigma\}$ shrinks the set of possible morphisms to or from $\mathbf{qubit}^2$. For example, the matrix N_c associated with the controlled-not gate (Equation (1)) defines a complete positive endomap of $\mathbb{C}^{4\times 4}$, which is an endo-morphism of $\mathbf{qubit}^{\otimes 2}$ but not of $\mathbf{qubit}^2$, because N_c is not invariant under the action of $\{\mathrm{id}, \sigma\}$:

$$\{\mathrm{id}, \sigma\}(N_c) = \frac{1}{2}(\mathrm{id}(N_c) + \sigma(N_c)) = \frac{1}{2}\begin{pmatrix} 2&0&0&0\\ 0&1&0&1\\ 0&0&1&1\\ 0&1&1&0 \end{pmatrix} \neq N_c.$$

Concerning biproducts, the object $\mathbf{qubit} \oplus \mathbf{qubit}$ is given by $\{(2, \{\mathrm{id}\})_{\mathtt{tt}}, (2, \{\mathrm{id}\})_{\mathtt{ff}}\}$, while its 2-power $(\mathbf{qubit} \oplus \mathbf{qubit})^2$ is $\{(4, \{\mathrm{id}, \sigma\})_{[\mathtt{tt},\mathtt{tt}]}, (4, \{\mathrm{id}\})_{[\mathtt{tt},\mathtt{ff}]}, (4, \{\mathrm{id}, \sigma\})_{[\mathtt{ff},\mathtt{ff}]}\}$. Notice the difference between the **CPMs** object $(4, \{\mathrm{id}\})$ associated with $[\mathtt{tt}, \mathtt{ff}]$ and the object $(4, \{\mathrm{id}, \sigma\})$ associated with the two multisets of singleton support.

The description of the objects and the morphisms of $\overline{\mathbf{CPMs}}^{\oplus}$ as indexed families is crucial for inferring the structure of a Lafont category from the more basic categories underlying $\overline{\mathbf{CPMs}}^{\oplus}$. However, it is worthwhile to notice that $\overline{\mathbf{CPMs}}^{\oplus}$ can also be presented as a concrete category of modules and linear maps between modules. The rest of the section sketches such an alternative presentation.

Let $\mathfrak{A}$ be an object of $\overline{\mathbf{CPMs}}^{\oplus}$. We define a module $\mathrm{Pos}(\mathfrak{A})$ over $\overline{\mathbb{R}^+}$ as follows. For every a in $|\mathfrak{A}|$ consider the quotient $\mathbb{C}^{n_a\times n_a}/\!\sim_{G_a}$ of the set of square matrices, where $M \sim_{G_a} M'$ whenever there exists $g \in G_a$ such that $g(M) = M'$. Notice that the image of $\mathbb{C}^{n_a\times n_a}$ under the action of G_a yields a set $\mathrm{Mat}(a) \subseteq \mathbb{C}^{n_a\times n_a}$ of canonical representatives for $\mathbb{C}^{n_a\times n_a}/\!\sim_{G_a}$. Let us write $\mathrm{Pos}(a)$ for its associated cone of positive matrices. This positive cone is an $\mathbb{R}^+$-module. Since group actions are completely positive maps, complete positivity naturally extends to complex linear maps $f : \mathrm{Mat}(a) \to \mathrm{Mat}(b)$: f can be regarded as the map $G_a\ ;\ f : \mathbb{C}^{n_a\times n_a} \to \mathbb{C}^{n_b\times n_b}$. We define f to be *completely positive* if and only if $G_a\ ;\ f$ is. Since the positive matrices span the complex vector space of square matrices (of corresponding size), one can canonically extend the definition of complete positivity to $\mathbb{R}^+$-module homomorphisms $\mathrm{Pos}(a) \to \mathrm{Pos}(b)$. We then define:

$$\mathrm{Pos}(\mathfrak{A}) := \bigoplus_{a\in|\mathfrak{A}|} (\mathrm{Pos}(a) \cup \{\infty_a\}) \tag{9}$$

The operations are defined pointwise, and ∞_a is absorbing for addition and scalar multiplication with respect to $\mathrm{Pos}(a)$, except for the rule $0 \cdot \infty_a = \mathbf{0}$. The Löwner order $\sqsubseteq$ on positive matrices can be extended to $\mathrm{Pos}(\mathfrak{A})$ componentwise: $v \sqsubseteq u$ if for all $a \in |\mathfrak{A}|$, $v_a \sqsubseteq u_a$ or $u_a = \infty_a$. In particular, notice that $\mathrm{Pos}(\mathfrak{A})$ is complete with respect to this order, where the maximum is the vector whose value is ∞_a in every $a \in |\mathfrak{A}|$, and the directed sup is defined componentwise. This makes $\mathrm{Pos}(\mathfrak{A})$ into a continuous module over $\overline{\mathbb{R}^+}$: addition and scalar multiplication are continuous operations with respect to the order.

Example 26. Let us define the modules associated with the objects discussed in Example 25. Clearly we have: $\mathrm{Pos}(\mathbf{1}) = \overline{\mathbb{R}^+}$, $\mathrm{Pos}(\mathbf{1}\oplus\mathbf{1}) = \overline{\mathbb{R}^+}^2$, $\mathrm{Pos}(!\mathbf{1}) = \overline{\mathbb{R}^+}^{\mathbb{N}}$ and $\mathrm{Pos}(!(\mathbf{1} \oplus \mathbf{1})) = \overline{\mathbb{R}^+}^{\mathbb{N}\times\mathbb{N}}$.

Concerning the examples on **qubit**, we have that $\mathrm{Pos}(\mathbf{qubit})$ (resp. $\mathrm{Pos}(\mathbf{qubit}^{\otimes 2})$) is the cone of positive matrices of dimension

2×2 (resp. 4×4) plus the top element ∞. More interestingly, the module associated with $\mathbf{qubit}^2$ is

$$\left\{ \left(\begin{smallmatrix} a & b & b & c \\ d & e & f & g \\ d & f & e & g \\ h & i & i & l \end{smallmatrix} \right) \text{ positive ; } a,b,c,d,e,f,g,h,i,l \in \mathbb{C} \right\}$$

which is a subcone of $\mathrm{Pos}(\mathbf{qubit}^{\otimes 2})$ of dimension 10. Finally, $\mathrm{Pos}(\mathbf{qubit} \oplus \mathbf{qubit})^2$ is equal to the direct sum $\mathrm{Pos}(\mathbf{qubit}^2) \oplus \mathrm{Pos}(\mathbf{qubit}^{\otimes 2}) \oplus \mathrm{Pos}(\mathbf{qubit}^2)$.

Let $f : \mathrm{Pos}(\mathfrak{A}) \to \mathrm{Pos}(\mathfrak{B})$ be a continuous module homomorphism. We say that f is *quantum-compatible* if for all $a \in |\mathfrak{A}|$ and $b \in |\mathfrak{B}|$, $f_{a,b} = \iota^a ; f ; \pi^b$ is either the map ∞ sending all non-zero elements to ∞_b and $\mathbf{0}$ to $\mathbf{0}$, or a module homomorphism $\mathrm{Pos}(a) \to \mathrm{Pos}(b)$. We say that f is *completely positive* if all the module homomorphisms $f_{a,b}$ are completely positive maps.

Proposition 27. *There is an isomorphism between the homset* $\overline{\mathbf{CPMs}}^{\oplus}(\mathfrak{A}, \mathfrak{B})$ *and the continuous module homomorphisms from* $\mathrm{Pos}(\mathfrak{A})$ *to* $\mathrm{Pos}(\mathfrak{B})$ *that are quantum compatible and completely positive.*

Proof. Take $\phi \in \overline{\mathbf{CPMs}}^{\oplus}(\mathfrak{A}, \mathfrak{B})$. We define the map f_ϕ from $\mathrm{Pos}(\mathfrak{A})$ to $\mathrm{Pos}(\mathfrak{B})$ by $f_\phi(v)_b := \sum_a \phi_{a,b}(v_a)$. Here, we set $\phi_{a,b}(v_a) = \infty_b$ when $\phi_{a,b} = \infty$ and $v_a \neq 0$, or when $\phi_{a,b} \neq 0$ and $v_a = \infty_a$. We set $\phi_{a,b}(v_a) = 0$ when one of $\phi_{a,b}$ and v_a is zero. In all other cases, $\phi_{a,b}(v_a)$ is a well-defined positive matrix in the space $\mathbb{C}^{n_b \times n_b}$. The infinite sum in the definition of $f_\phi(v)_b$ converges since $\{\sum_{a \in F} \phi_{a,b}(v_a) \mid F \subseteq_{fin} |\mathfrak{A}|\}$ is directed. One then proves that $\phi \mapsto f_\phi$ is a bijection. □

6. Interpretation of the quantum lambda calculus

6.1 Denotational semantics

We interpret the quantum λ-calculus into $\overline{\mathbf{CPMs}}^{\oplus}$, extending the standard interpretation of intuitionistic linear logic to also include the quantum features of the calculus. Section 7 will show that the denotation of a quantum λ-term is a true family of complete positive maps, not containing the ∞ morphism.

The denotation $\llbracket A \rrbracket$ of a type A is an object of $\overline{\mathbf{CPMs}}^{\oplus}$, i.e., an indexed sequence of objects of $\overline{\mathbf{CPMs}}$, defined by structural induction on A, as follows. $\llbracket \mathbf{qubit} \rrbracket$ is the singleton web object $\{(2, \{\mathrm{id}\})_*\}$; $\llbracket 1 \rrbracket$ is the tensor unit $\mathbf{1} = \{(1, \{\mathrm{id}\})_*\}$ of $\overline{\mathbf{CPMs}}^{\oplus}$; $\llbracket A \multimap B \rrbracket = \llbracket A \otimes B \rrbracket$ is the tensor product of $\llbracket A \rrbracket$ and $\llbracket B \rrbracket$; $\llbracket A \oplus B \rrbracket$ is the biproduct of $\llbracket A \rrbracket$ and $\llbracket B \rrbracket$; $\llbracket !A \rrbracket$ is the free commutative comonoid over $\llbracket A \rrbracket$; $\llbracket A^\ell \rrbracket$ is the infinite biproduct $\oplus_{i=0}^{\infty} \llbracket A \rrbracket^{\otimes n}$.

Notice the difference between $\llbracket !A \rrbracket = \oplus_{i=0}^{\infty} \llbracket A \rrbracket^n$ and $\llbracket A^\ell \rrbracket$. Recalling Notation 3, we have that $\llbracket \mathbf{bit} \rrbracket$ is defined as $\llbracket 1 \oplus 1 \rrbracket = \{(1, \{\mathrm{id}\})_{\mathtt{ff}}, (1, \{\mathrm{id}\})_{\mathtt{tt}}\}$. By abuse of notation, we can omit the $\llbracket\ \rrbracket$ brackets, i.e., in the following, the simple letter A will denote both the type and its interpretation in $\overline{\mathbf{CPMs}}^{\oplus}$.

Let $\Gamma = x_1 : A_1, \ldots, x_n : A_n$. We define the denotation of a typing judgement $\Gamma \vdash M : A$ as a morphism $\llbracket M \rrbracket^{\Gamma \vdash A}$ in $\overline{\mathbf{CPMs}}^{\oplus}(\bigotimes_i \llbracket A_i \rrbracket, \llbracket A \rrbracket)$. The definition is by structural induction on the unique type derivation π of $\Gamma \vdash M : A$ (Proposition 4). In Table 5, we recall the definition regarding the usual linear logic rules: the morphisms $\phi, \psi, \phi_A, \phi_B$ refer to the denotation of the premises of the last rule of π, which are uniquely defined given $\Gamma \vdash M : A$.

$$\llbracket \mathtt{meas} \rrbracket^{!\Delta \vdash \mathbf{qubit} \multimap \mathbf{bit}}_{\vec{m},(*,b)} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \mapsto \begin{cases} a & \text{if } \vec{m} = \vec{[\,]} \text{ and } b = \mathtt{ff}, \\ d & \text{if } \vec{m} = \vec{[\,]} \text{ and } b = \mathtt{tt}, \\ 0 & \text{otherwise.} \end{cases}$$

$$\llbracket \mathtt{new} \rrbracket^{!\Delta \vdash \mathbf{bit} \multimap \mathbf{qubit}}_{\vec{m},(b,*)} = a \mapsto \begin{cases} \left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix} \right) & \text{if } \vec{m} = \vec{[\,]} \text{ and } b = \mathtt{ff}, \\ \left(\begin{smallmatrix} 0 & 0 \\ 0 & a \end{smallmatrix} \right) & \text{if } \vec{m} = \vec{[\,]} \text{ and } b = \mathtt{tt}, \\ \mathbf{0} & \text{otherwise.} \end{cases}$$

$$\llbracket U \rrbracket^{!\Delta \vdash \mathbf{qubit}^{\otimes n} \multimap \mathbf{qubit}^{\otimes n}}_{\vec{m},(\vec{*},\vec{*})} = M \mapsto \begin{cases} UMU^{-1} & \text{if } \vec{m} = \vec{[\,]}, \\ \mathbf{0} & \text{otherwise.} \end{cases}$$

Table 4: Interpretation of the quantum constants. U and M have the same dimension $\mathbb{C}^{2^n \times 2^n}$, U being unitary.

In the interpretation of the `letrec` constructor, the fixed point operator Y is defined as follows. Let ϕ be a morphism in $\overline{\mathbf{CPMs}}^{\oplus}(!C \otimes !A, !A)$. By induction on n, we define the morphism $\phi^n \in \overline{\mathbf{CPMs}}^{\oplus}(!C, !A)$:

$$\phi^0 := !C \xrightarrow{\mathsf{w};!\mathbf{0}} !A, \tag{10}$$

$$\phi^{n+1} := !C \xrightarrow{\mathsf{c}} !C \otimes !C \xrightarrow{\mathrm{id} \otimes \phi^n} !C \otimes !A \xrightarrow{\phi} !A. \tag{11}$$

Since ϕ can be regarded as a continuous module homomorphism (in particular it is monotone), the set $\{\phi^n\}$ is directed complete. We define $\mathrm{Y}(\phi)$ as its least upper bound.

The denotations of the constants `meas`, `new` and the unitary transformations are given in Table 4

Given a linking $\ell = |y_1, \ldots, y_m\rangle$, we write $\ell \vdash M : A$ for the judgement $y_1 : \mathbf{qubit}, \ldots, y_m : \mathbf{qubit} \vdash M : A$.

Proposition 28 (Invariance of the interpretation)**.** *Let ℓ be the linking $|y_1, \ldots, y_m\rangle$ and $\ell \vdash M : A$. If M is not a value, then for all quantum states $q \in \mathbb{C}^{2^m}$,*

$$\llbracket M \rrbracket^{\ell \vdash A}(qq^*) = \sum_{[q,\ell,M] \xrightarrow{p} [q',\ell',N]} p \cdot \llbracket N \rrbracket^{\ell' \vdash A}(q'q'^*). \tag{12}$$

Proof. By hypothesis, $[q, \ell, M]$ is a typable total closure, and so, by Proposition 11 and Lemma 13, any of its reduct $[q', \ell', N]$ is a typable total closure, so that $\llbracket N \rrbracket^{\ell' \vdash A}(q'q'^*)$ is well-defined.

Equation 12 is proven by cases, depending on the rule applied to $[q, \ell, M]$. The cases of Table 3(a) follows from the fact that $\overline{\mathbf{CPMs}}^{\oplus}$ is a continuous model of linear logic. The quantum rules (Table 3(b)) are trivial consequences of Table 4, and the congruence rules of Table 3(c) are done by induction on M, using the fact that the category $\overline{\mathbf{CPMs}}^{\oplus}$ is linear. □

Corollary 29. *We have* $\llbracket M \rrbracket^{\vdash 1}_{*} \geqslant \mathrm{Halt}_{[|\,\rangle,|\,\rangle,M]}$.

Proof. By induction on n, we can show that $\llbracket M \rrbracket^{\vdash 1}_{*}$ is equal to $\sum_{[q',\ell',N]} \mathrm{Red}^n_{[|\,\rangle,|\,\rangle,M],[q',\ell',N]} \llbracket N \rrbracket^{\ell' \vdash 1}(q'q'^*)$. Then the claim follows by taking the limit as $n \to \infty$, and invoking the monotonicity of $\{\mathrm{Red}^n\}_n$. □

6.2 Examples

In this section, we discuss the denotations of the two examples of programs that we already encountered.

Example 30. Recall the terms of Example 5. The web of $\llbracket \mathbf{qubit}^\ell \rrbracket$ is $\mathbb{N}$, while $\llbracket \mathbf{qubit}^\ell \rrbracket_n = (2^n, \{\mathrm{id}\})$. Notice that $\mathrm{Pos}(\llbracket \mathbf{qubit}^\ell \rrbracket)$ is equivalent to $\bigoplus_n P(\mathbb{C}^{2^n \times 2^n})$ where $P(\mathbb{C}^{2^n \times 2^n})$ is the cone of $2^n \times 2^n$ positive matrices. The denotation of the term `qlist` is a morphism in $\overline{\mathbf{CPMs}}^{\oplus}(\mathbf{qubit}, \mathbf{qubit}^\ell)$, that is, a map sending a 2×2 positive matrix onto $\bigoplus_n P(\mathbb{C}^{2^n \times 2^n})$. The program `qlist`

$$!\Delta\otimes A \xrightarrow{\mathtt{w}\otimes\mathrm{id}} 1\otimes A \simeq A$$

(a) $!\Delta, x : A \vdash x : A$

$$!\Delta\otimes !A \xrightarrow{\mathtt{w}\otimes\mathtt{d}} 1\otimes A \simeq A$$

(b) $!\Delta, x : !A \vdash x : A$

$$!\Delta \xrightarrow{\mathtt{dig}} !!\Delta \xrightarrow{\mathtt{m}} !(!\Delta) \xrightarrow{!\phi} !A$$

(c) $!\Delta, \vdash V : !A$

$$!\Delta\otimes\Gamma \xrightarrow{\Lambda(\phi)} A \multimap B$$

(d) $!\Delta, \Gamma \vdash \lambda x^A.M : A \multimap B$

$$!\Delta\otimes\Gamma\otimes\Sigma \xrightarrow{\mathtt{c}\otimes\mathrm{id}} !\Delta\otimes\Gamma\otimes!\Delta\otimes\Sigma \xrightarrow{\phi\otimes\psi} A\otimes A\multimap B \xrightarrow{\mathrm{eval}} B$$

(e) $!\Delta, \Gamma, \Sigma \vdash MN : B$

$$!\Delta \xrightarrow{\mathtt{w}} 1$$

(f) $!\Delta \vdash \mathtt{skip} : 1$

$$!\Delta\otimes\Gamma\otimes\Sigma \xrightarrow{\mathtt{c}\otimes\mathrm{id}} !\Delta\otimes\Gamma\otimes!\Delta\otimes\Sigma \xrightarrow{\phi\otimes\mathrm{id}} 1\otimes!\Delta\otimes\Sigma \simeq !\Delta\otimes\Sigma \xrightarrow{\psi} A$$

(g) $!\Delta, \Gamma, \Sigma \vdash M;N : A$

$$!\Delta\otimes\Gamma\otimes\Sigma \xrightarrow{\mathtt{c}\otimes\mathrm{id}} !\Delta\otimes\Gamma\otimes!\Delta\otimes\Sigma \xrightarrow{\phi\otimes\psi} A\otimes B$$

(h) $!\Delta, \Gamma, \Sigma \vdash M\otimes N : A\otimes B$

$$!\Delta\otimes\Gamma\otimes\Sigma \xrightarrow{\mathtt{c}\otimes\mathrm{id}} !\Delta\otimes\Gamma\otimes!\Delta\otimes\Sigma \xrightarrow{\phi\otimes\mathrm{id}} A\otimes B\otimes!\Delta\otimes\Sigma \xrightarrow{\psi} C$$

(i) $!\Delta, \Gamma, \Sigma \vdash \mathtt{let}\, x^A\otimes y^B \;=\; M\,\mathtt{in}\,N : C$

$$!\Delta\otimes\Gamma \xrightarrow{\phi} A \xrightarrow{\iota^\ell} A\oplus B$$

(j) $!\Delta, \Gamma \vdash \mathtt{in}_\ell\, M : A\oplus B$

$$!\Delta\otimes\Gamma \xrightarrow{\phi} B \xrightarrow{\iota^r} A\oplus B$$

(k) $!\Delta, \Gamma \vdash \mathtt{in}_r\, M : A\oplus B$

$$!\Delta\otimes\Gamma\otimes\Sigma \xrightarrow{\mathtt{c}\otimes\mathrm{id}} !\Delta\otimes\Gamma\otimes!\Delta\otimes\Sigma \xrightarrow{\psi\otimes\mathrm{id}} (A\oplus B)\otimes!\Delta\otimes\Sigma \xrightarrow{\mathtt{distr}} (A\otimes!\Delta\otimes\Sigma)\oplus(B\otimes!\Delta\otimes\Sigma) \xrightarrow{\phi_A\oplus\phi_B} C$$

(l) $!\Delta, \Gamma, \Sigma \vdash \mathtt{match}\, M\, \mathtt{with}\, (x^A : N | y^B : L) : C$

$$!\Delta\otimes\Gamma \xrightarrow{\phi} 1\oplus(A\otimes A^\ell) \xrightarrow{\mathrm{id}\oplus\mathtt{distr}} 1\oplus(\textstyle\bigoplus_{n=1}^{\infty} A^{\otimes n}) = A^\ell$$

(m) $!\Delta, \Gamma \vdash M : A^\ell$

$$!\Delta\otimes\Gamma \xrightarrow{\mathtt{c}} !\Delta\otimes\Gamma\otimes!\Delta \xrightarrow{\mathrm{id}\otimes\mathrm{Y}(\mathtt{dig};\mathtt{m};!(\Lambda\phi))} !\Delta\otimes\Gamma\otimes!(A\multimap B) \xrightarrow{\psi} C$$

(n) $!\Delta, \Gamma \vdash \mathtt{letrec}\, f\, x = M\, \mathtt{in}\, N : C$

Table 5: Sketch of the interpretation of the typing judgements. The morphisms ϕ, ψ, ϕ_A, ϕ_B refer to the denotation of the premises of the unique derivation concluding a typing judgement. In (c) and (n), the morphism $\mathtt{m}$ stands for $\mathtt{m}^1$ or the suitable sequence of $\mathtt{m}^\otimes$, depending on the context $!!\Delta$.

is defined using recursion: its semantics is the the limit of the morphisms f_n sending $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to $(\mathbf{0}, \frac{1}{2}e_1, \ldots, \frac{1}{2^n}e_n, \mathbf{0}, \mathbf{0}, \ldots)$ where e_i is the $2^i \times 2^i$ positive matrix of the form

$$\begin{pmatrix} a & 0 & \cdots & 0 & b \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ c & 0 & \cdots & 0 & d \end{pmatrix}.$$

This limit is the map sending $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to the sequence of infinitely increasing matrices $(\mathbf{0}, \frac{1}{2}e_1, \ldots, \frac{1}{2^n}e_n, \ldots)$. Note that the first element of the sequence is $\mathbf{0}$, as the program `qlist` never return the empty list. Also note that all the positive matrices in the sequence represent *entangled states of arbitrary sizes*. Our semantics is the first one to be able to account for such a case: in [6], only fixed sizes were allowed for entangled states.

Example 31. We claim in the introduction that the model is expressive enough to describe entanglement at higher-order types. As we discuss in Example 6, the encoding of the quantum teleportation algorithm produces two entangled, mutually inverse functions: $f : \mathbf{qubit} \to \mathbf{bit} \otimes \mathbf{bit}$ and $g : \mathbf{bit} \otimes \mathbf{bit} \to \mathbf{qubit}$.

The term $(\mathbf{teleport}\, \mathtt{skip})$ of type $(\mathbf{qubit} \multimap \mathbf{bit} \otimes \mathbf{bit}) \otimes (\mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qubit})$ is one instance of such a pair of functions. Its denotation is a finite sequence of 16 square matrices of size 4×4. Using a lexicographic convention, we can lay them out as follows:

$$\begin{array}{rcllll} A & = & \frac{1}{4}(& A_{00,00}, & A_{00,01}, & A_{00,10}, & A_{00,11}, \\ & & & A_{01,00}, & A_{01,01}, & A_{01,10}, & A_{01,11}, \\ & & & A_{10,00}, & A_{10,01}, & A_{10,10}, & A_{10,11}, \\ & & & A_{11,00}, & A_{11,01}, & A_{11,10}, & A_{11,11} &). \end{array}$$

Because of the convention, morally each row corresponds to an element of type $\mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qubit}$ whereas each column corresponds to an element of type $\mathbf{qubit} \multimap \mathbf{bit} \otimes \mathbf{bit}$. Picking a row, i.e. a choice of two left-sided booleans, amounts to choosing the two booleans that will be fed to the function g. Picking a column, i.e. a choice of two right-sided booleans, amounts to deciding on the probabilistic result we get from the function f. The intersection of a column and a row is therefore the representation of a map $\mathbf{qubit} \multimap \mathbf{qubit}$. This map is a description of a possible path in the control flow of the algorithm.

Indeed, consider again Figure 1. In (ii), i.e., in the function f, qubit 1 and qubit 2 are entangled and measured, generating two classical bits. This pair of bits (x, y) is picked probabilistically: a column was chosen by this choice. Now, in (iii), i.e. in the function g, two bits are used to decide on the matrix U_{xy} that should be used: this is the choice of a matrix in the column. This matrix is the composition of these two operations, yielding a function from $\mathbf{qubit}$ to $\mathbf{qubit}$. The 4 matrices in the column record all the possible choices of inputs to g.

The matrices on the diagonal corresponds to a run of the algorithm as it was intended: feeding g with the result from f. Since they are supposed to be the identity on $\mathbf{qubit}$, we can therefore deduce that the matrices $A_{00,00}$, $A_{01,01}$, $A_{10,10}$ and $A_{11,11}$ are all equal to $\left(\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{smallmatrix}\right)$. Since this matrix cannot be written as the tensor of two 2×2 matrices, we conclude that the denotation A of $(\mathbf{teleport}\, \mathtt{skip})$ is indeed entangled.

We can compute the other matrices $A_{xy,zt}$ using the same argument: in general, $A_{xy,zt}$ is a composition of f and g, except that instead of giving (x, y) to g, we feed it with (z, t). We therefore get a function $\mathbf{qubit} \to \mathbf{qubit}$ constructed out of the U_{--} that might (if $xy = zt$) or might not be the identity. In general, the matrices $A_{xy,zt}$ is the denotation of the unitary $U_{zt}U_{xy}^*$. The denotation A is given in full details in Table 6.

6.3 Adequacy

In the following, we prove the adequacy of $\overline{\mathbf{CPMs}}^{\oplus}$ (Theorem 39). This amounts to achieving the converse inequality of Corollary 29. The proof uses a syntactic approach, following [6]. We introduce a bounded $\mathtt{let\text{-}rec}^n$, which can be unfolded at most n times. On the one hand, the language allowing only bounded `let-rec` is strongly normalizing (Lemma 34), hence the adequacy for it can be easily achieved by induction on the longest reduction sequence of a term (Corollary 35). On the other hand, the unbounded `let-rec` can be expressed as the supremum of its bounded approximants, both semantically (Lemma 37) and syntactically (Lemma 38). We then conclude the adequacy for the whole quantum λ-calculus by continuity.

Definition 32. Let us extend the grammar of terms (Table 1) by adding: (i) a new term Ω^A; (ii) a family of new term constructs $\mathtt{letrec}^n\, f^{A\multimap B}\, x = M\, \mathtt{in}\, N$ indexed by natural numbers $n \geqslant 0$.

The typing rules for these new constructs are

$$\frac{}{!\Delta \vdash \Omega^A : A}$$

$$A \quad = \quad \left(\begin{array}{llll}
A_{00,00} = \begin{pmatrix} 1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1 \end{pmatrix}, & A_{00,01} = \begin{pmatrix} 0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0 \end{pmatrix}, & A_{00,10} = \begin{pmatrix} 1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1 \end{pmatrix}, & A_{00,11} = \begin{pmatrix} 0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0 \end{pmatrix}, \\
A_{01,00} = \begin{pmatrix} 0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0 \end{pmatrix}, & A_{01,01} = \begin{pmatrix} 1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1 \end{pmatrix}, & A_{01,10} = \begin{pmatrix} 0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0 \end{pmatrix}, & A_{01,11} = \begin{pmatrix} 1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1 \end{pmatrix}, \\
A_{10,00} = \begin{pmatrix} 1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1 \end{pmatrix}, & A_{10,01} = \begin{pmatrix} 0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0 \end{pmatrix}, & A_{10,10} = \begin{pmatrix} 1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1 \end{pmatrix}, & A_{10,11} = \begin{pmatrix} 0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0 \end{pmatrix}, \\
A_{11,00} = \begin{pmatrix} 0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0 \end{pmatrix}, & A_{11,01} = \begin{pmatrix} 1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1 \end{pmatrix}, & A_{11,10} = \begin{pmatrix} 0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0 \end{pmatrix}, & A_{11,11} = \begin{pmatrix} 1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1 \end{pmatrix}
\end{array} \right).$$

Table 6: The denotation of the teleportation algorithm.

$$\frac{!\Delta, f : !(A \multimap B), x : A \vdash M : B \qquad !\Delta, \Gamma, f : !(A \multimap B) \vdash N : C}{!\Delta, \Gamma \vdash \texttt{letrec}^n\ f^{A \multimap B}\ x = M\ \texttt{in}\ N : C}$$

Their denotations are given, respectively, by the map $\mathbf{0}$ and the family of maps

$$!\Delta \otimes \Gamma \xrightarrow{c} !\Delta \otimes \Gamma \otimes !\Delta \xrightarrow{\mathrm{id} \otimes (\mathtt{dig};\mathtt{m};!(\Lambda\phi))^n} !\Delta \otimes \Gamma \otimes !(A \multimap B) \xrightarrow{\psi} C,$$

where $\phi \in \overline{\mathbf{CPMs}}^{\oplus}(!\Delta \otimes !(A \multimap B) \otimes A, B)$ and $\psi \in \overline{\mathbf{CPMs}}^{\oplus}(!\Delta \otimes \Gamma \otimes !(A \multimap B), C)$ are the denotations of the premises and $(\mathtt{dig};\mathtt{m};!(\Lambda\phi))^n \in \overline{\mathbf{CPMs}}^{\oplus}(!\Delta, !(A \multimap B))$ is defined as in Equations (10), (11).

The reduction rules are updated as follows.

$$[q, \ell, \texttt{letrec}^0\ f^{A \multimap B}\ x = M\ \texttt{in}\ N] \xrightarrow{1} [q, \ell, N\{(\lambda x^A.\Omega^B)/f\}]$$
$$[q, \ell, \texttt{letrec}^{n+1}\ f^{A \multimap B}\ x = M\ \texttt{in}\ N]$$
$$\xrightarrow{1} [q, \ell, N\{(\lambda x^A.\texttt{letrec}^n\ f^{A \multimap B}\ x = M\ \texttt{in}\ M)/f\}].$$

The additions to the language do not modify the properties of the language: subject reduction (Proposition 11) and totality (Lemma 13) hold as they are stated, while type safety (Proposition 12) and soundness (Proposition 28) are satisfied, with the proviso of considering the set of normal forms to consists of the set of values *and* the set of terms containing Ω in evaluating position.

Definition 33. A term is called *finitary* when it does not contain any occurrence of the un-indexed `let-rec` construct. It can however contain Ω and any of the indexed `let-rec`^{n}. We call a closure *finitary* when its term is finitary.

Lemma 34 (Strong normalization)**.** *If* $[q_1, \ell_1, M_1]$ *is finitary and typable, then every reduction sequence*

$$[q_1, \ell_1, M_1] \xrightarrow{p_1} [q_2, \ell_2, M_2] \xrightarrow{p_2} [q_3, \ell_3, M_3] \xrightarrow{p_3} \cdots$$

is finite.

Proof (Sketch). By reducing the quantum λ-calculus to a simply typed non-deterministic language without quantum states, for which a standard proof technique can be used. The terms of this language are the terms of the extended quantum λ-calculus, minus the `let-rec` construct. The operational semantics is obtained from Table 3 and the rules for `let-rec`^{n} by replacing closures with the respective terms and the rules of Table 3b by dummy reduction rules: like $U(\bullet \otimes \cdots \otimes \bullet) \to \bullet \otimes \cdots \otimes \bullet$, or $\texttt{new ff} \to \bullet$. The symbol $\bullet$ denotes a distinct term variable, which, by convention, it is never bound by an abstraction. Clearly, the strong normalization of this language implies that of the typed quantum λ-calculus. □

Corollary 35 (Finitary adequacy)**.** *Let* M *be a closed finitary term of unit type. Then* $[\![M]\!]_*^{\vdash 1} = \mathrm{Halt}_{[|\,\rangle,|\,\rangle,M]}$.

Proof (Sketch). We prove that, for any total finitary quantum closure of unit type $[q, \ell, M]$ we have $[\![M]\!]^{\ell \vdash 1}(qq^*) = \mathrm{Halt}_{[q,\ell,M]}$. In fact, by Lemma 34, there exists $m \in \mathbb{N}$ such that $\mathrm{Halt}_{[q,\ell,M]} = \sum_{[q',\ell',V]} \mathrm{Red}^m_{[q,\ell,M],[q',\ell',V]}$. The proof then follows by induction on m. □

Definition 36. Let $\lhd$ be a relation between finitary terms and general terms defined as the smallest congruence relation on terms satisfying, for every $M \lhd M'$ and $N \lhd N'$:

$$N\{(\lambda x^A.\Omega^B)/f\} \lhd (\texttt{letrec}\ f\ x = M'\ \texttt{in}\ N'),$$
$$(\texttt{letrec}^n\ f\ x = M\ \texttt{in}\ N) \lhd (\texttt{letrec}\ f\ x = M'\ \texttt{in}\ N').$$

Lemma 37. *If* $\Gamma \vdash M : A$*, then* $[\![M]\!]^{\Gamma \vdash A} = \bigvee_{\substack{M' \lhd M \\ M' \textit{ finitary}}} [\![M']\!]^{\Gamma \vdash A}$.

Proof (Sketch). By induction on the derivation of $\Gamma \vdash M : A$. □

Lemma 38. *If* $M \lhd M'$*, then* $\mathrm{Halt}_{[q,\ell,M]} \leqslant \mathrm{Halt}_{[q,\ell,M']}$.

Proof (Sketch). By induction on n, one proves the inequality: $\sum_{[q',\ell',N]} \mathrm{Red}^n_{[q,\ell,M],[q',\ell',N]} \leqslant \sum_{[q',\ell',N']} \mathrm{Red}^n_{[q,\ell,M'],[q',\ell',N']}$, from which trivially follows the statement. □

Theorem 39. *Let* M *be a program, i.e., a closed term of unit type. Then* $[\![M]\!]_*^{\vdash 1} = \mathrm{Halt}_{[|\,\rangle,|\,\rangle,M]}$.

Proof. By Corollary 29 we have $[\![M]\!]_*^{\vdash 1} \geqslant \mathrm{Halt}_{[|\,\rangle,|\,\rangle,M]}$. As for the converse: by Lemma 37, $[\![M]\!]_*^{\vdash 1} = \bigvee_{M' \lhd M} [\![M']\!]_*^{\vdash 1}$, which is equal to $\bigvee_{M' \lhd M} \mathrm{Halt}_{[|\,\rangle,|\,\rangle,M']}$ by Corollary 35, which is less or equal to $\mathrm{Halt}_{[|\,\rangle,|\,\rangle,M]}$ by Lemma 38. □

7. Structure of the sets of representable elements

We conclude this paper by an analysis of some of the properties of the denotation of terms.

Recall that a morphism in $\overline{\mathbf{CPMs}}^{\oplus}$ is a indexed family of either a completely positive map, or the element ∞. We show that (1) all types have a non-zero inhabitant; (2) provided that the term constant U ranges over arbitrary unitary matrices, the representable elements of a given homset form a convex set including $\mathbf{0}$; and (3) ∞ is not part of any representable element.

We first need two auxiliary definitions.

Definition 40. We define two type-indexed families of terms $\overline{\omega}_A$ and ω_A by mutual induction in Table 7. The term $\mathbf{c}$ represents the fair coin toss $\texttt{meas}\,(H\,(\texttt{new}\,\texttt{ff}))$ (recall Example 1) and the notation $\mu f x.M$ stands for $\texttt{letrec}\ f\ x = M\ \texttt{in}\ f$.

Lemma 41. *For all types* A*, we have* $\vdash \omega_A : 1 \multimap A$ *and* $\vdash \overline{\omega}_A : A \multimap 1$*. Moreover, the morphisms* $[\![\omega_A]\!]^{\vdash 1 \multimap A}$ *and* $[\![\overline{\omega}_A]\!]^{\vdash A \multimap 1}$*, seen as indexed families, do not contain the zero-CPM.*

Proof. The fact that their type is as specified in the lemma is a straightforward proof by structural induction on the term.

The proof that for all A, the denotations of ω_A and $\overline{\omega}_A$ do not contain the zero-CPM is done by induction on A: For the types

$\omega_{\mathbf{qubit}}$	$= \lambda\mathtt{skip}.\mathtt{new}\,\mathtt{ff}$	$\overline{\omega}_{\mathbf{qubit}}$	$= \lambda x^{\mathbf{qubit}}.\mathtt{if}\ \mathtt{meas}\,x\ \mathtt{then}\ \mathtt{skip}\ \mathtt{else}\ \mathtt{skip}$
$\omega_{A\multimap B}$	$= \lambda\mathtt{skip}.\lambda x^{A}.(\overline{\omega}_A\, x);(\omega_B\,\mathtt{skip})$	$\overline{\omega}_{A\multimap B}$	$= \lambda f^{A\multimap B}.\overline{\omega}_B\,(f\,(\omega_A\,\mathtt{skip}))$
$\omega_{!(A\multimap B)}$	$= \lambda\mathtt{skip}.\lambda x^{A}.(\omega_{A\multimap B}\,\mathtt{skip})\,x$	$\overline{\omega}_{!(A\multimap B)}$	$= \mu g f^{!(A\multimap B)}.\mathtt{if}\ \mathbf{c}\ \mathtt{then}\ \mathtt{skip}\ \mathtt{else}\ (\overline{\omega}_{A\multimap B}\, f);(g\,f)$
ω_1	$= \lambda\mathtt{skip}.\mathtt{skip}$	$\overline{\omega}_1$	$= \lambda\mathtt{skip}.\mathtt{skip}$
$\omega_{A\otimes B}$	$= \lambda\mathtt{skip}.(\omega_A\,\mathtt{skip})\otimes(\omega_B\,\mathtt{skip})$	$\overline{\omega}_{A\otimes B}$	$= \lambda x^{A\otimes B}.\mathtt{let}\ z_1\otimes z_2\ =\ x\ \mathtt{in}\ (\overline{\omega}_A\, z_1);(\overline{\omega}_B\, z_2)$
$\omega_{A\oplus B}$	$= \lambda\mathtt{skip}.\mathtt{if}\ \mathbf{c}\ \mathtt{then}\ (\omega_A\,\mathtt{skip})\ \mathtt{else}\ (\omega_B\,\mathtt{skip})$	$\overline{\omega}_{A\oplus B}$	$= \lambda x^{A\oplus B}.\mathtt{match}\ x\ \mathtt{with}\ (z_1^A : \overline{\omega}_A\, z_1 \mid z_2^B : \overline{\omega}_B\, z_2)$
ω_{A^ℓ}	$= \mu f\,\mathtt{skip}.\mathtt{if}\ \mathbf{c}\ \mathtt{then}\ (\mathtt{skip})\ \mathtt{else}\ (\omega_A\,\mathtt{skip}) :: (f\,\mathtt{skip})$	$\overline{\omega}_{A^\ell}$	$= \mu f x^{A^\ell}.\mathtt{match}\ \mathtt{split}\ x\ \mathtt{with}$
			$(\ z_1^1\ :\ z_1 \ \Big\vert\ z_2^{A\otimes A^\ell}\ :\ \mathtt{let}\ y_1\otimes y_2 = z_2\ \mathtt{in}\ (\overline{\omega}_A\, y_1);(f\, y_2))$

Table 7: Two mutually recursive families of terms

$\mathbf{qubit}$ and 1, the result is immediate. For the types $A \oplus B$ and $A \otimes B$, invoking the induction hypothesis is enough. The interesting types are A^ℓ and $!(A \multimap B)$. The cases $\omega_{!(A\multimap B)}$ and $\overline{\omega}_{A^\ell}$ are straightforward. For the cases ω_{A^ℓ} and $\overline{\omega}_{!(A\multimap B)}$, one is careful to touch all possible instances: in the former, the term probabilistically generates lists of all possible lengths whereas in the latter the term is probabilistically consuming all possible repetitions of a non-zero input. □

Corollary 42. *All types are inhabited by at least one closed value of non-null denotation.*

Proof. Immediate with Lemma 41: for a given type A, choose the term $(\omega_A\,\mathtt{skip})$. □

Proposition 43. *Given a type A and a context Γ, the denotations $[\![M]\!]^{\Gamma\vdash A}$ of valid typing judgements $\Gamma \vdash M : A$ form a convex set including* $\mathbf{0}$.

Proof. Suppose that Γ is $x_1 : A_1, \ldots, x_n : A_n$. A term M mapping to $\mathbf{0}$ is $(\overline{\omega}_{A_1} x_1; \ldots; \overline{\omega}_{A_n} x_n; \mathbf{\Omega})$ where the term $\mathbf{\Omega}$ is a shortcut for $\mathtt{letrec}\ f\,x = f\,x\ \mathtt{in}\ f\,\mathtt{skip}$, of denotation $\mathbf{0}$.

Now, suppose that $f = [\![M_1]\!]^{\Gamma\vdash A}$ and $g = [\![M_2]\!]^{\Gamma\vdash A}$, and choose two non-negative real numbers ρ_1, ρ_2 such that $\rho_1 + \rho_2 = 1$. There exists an angle ϕ such that $(\cos\phi)^2 = \rho_1$ and that $(\sin\phi)^2 = \rho_2$. As the term constant U ranges over arbitrary unitaries, the unitary matrix $V_\phi = \left(\begin{smallmatrix}\cos\phi & -\sin\phi \\ \sin\phi & \cos\phi\end{smallmatrix}\right)$ is representable in the quantum lambda-calculus. The term $\mathbf{c}' = \mathtt{meas}\,(V_\phi\,(\mathtt{new}\,\mathtt{ff}))$ has denotation (ρ_1, ρ_2). We then conclude that the term $\mathtt{if}\ \mathbf{c}'\ \mathtt{then}\ M_1\ \mathtt{else}\ M_2$ has the denotation $\rho_1 f + \rho_2 g$. □

Proposition 44. *If $\Gamma \vdash M : A$ is valid, then ∞ is not part of the denotation $[\![M]\!]^{\Gamma\vdash A}$ of M.*

Proof. Suppose that ∞ were to be found in the interpretation of $x_1 : A_1, \ldots, x_n : A_n \vdash M : A$. Then the closed term

$$(\lambda x_1 \ldots x_n.\overline{\omega}_A\, M)(\omega_{A_1}\mathtt{skip})\ldots(\omega_{A_n}\mathtt{skip})$$

of type 1 has for denotation ∞, contradicting Theorem 39. □

This last proposition indicates that the element ∞ is really an artifact only needed for the categorical construction. The representable elements in the model are only built out of families of completely positive maps.

References

[1] V. Danos and T. Ehrhard. Probabilistic coherence spaces as a model of higher-order probabilistic computation. *Inform. Comput.*, 2011.

[2] T. Ehrhard. Finiteness spaces. *MSCS*, 15(4):615–646, 2005.

[3] J.-Y. Girard. Linear logic. *Th. Comp. Sc.*, 50:1–102, 1987.

[4] J.-Y. Girard. Normal functors, power series and lambda-calculus. *Ann. Pure Appl. Logic*, 37(2):129–177, 1988.

[5] J.-Y. Girard. Coherent banach spaces: a continuous denotational semantics. *Theoretical Computer Science*, 227:297, 1999.

[6] I. Hasuo and N. Hoshino. Semantics of higher-order quantum computation via geometry of interaction. In *Proceedings of LICS*, pages 237–246, 2011.

[7] Y. Lafont. *Logiques, catégories et machines*. PhD thesis, Université Paris 7, 1988.

[8] U. D. Lago, A. Masini, and M. Zorzi. Confluence results for a quantum lambda calculus with measurements. *Electr. Notes Theor. Comput. Sci.*, 270(2):251–261, 2011.

[9] J. Laird, G. Manzonetto, and G. McCusker. Constructing differential categories and deconstructing categories of games. *Information and Computation*, 222:247–264, 2013.

[10] J. Laird, G. McCusker, G. Manzonetto, and M. Pagani. Weighted relational models of typed lambda-calculi. In *LICS'13*, 2013.

[11] S. Mac Lane. *Categories for the Working Mathematician*. Springer, 2nd edition, Sept. 1998.

[12] O. Malherbe. *Categorical models of computation: partially traced categories and presheaf models of quantum computation*. PhD thesis, University of Ottawa, 2010.

[13] P.-A. Melliès. Categorical semantics of linear logic. *Panoramas et Synthèses*, 12, 2009.

[14] P.-A. Melliès, N. Tabareau, and C. Tasson. An explicit formula for the free exponential modality of linear logic. In *ICALP'09 (2)*, pages 247–260, 2009.

[15] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.

[16] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.

[17] P. Selinger. Towards a semantics for higher-order quantum computation. In *QPL'04*, TUCS General Publication No 33, pages 127–143, 2004.

[18] P. Selinger and B. Valiron. A lambda calculus for quantum computation with classical control. *Mathematical Structures in Computer Science*, 16(3):527–552, 2006.

[19] P. Selinger and B. Valiron. On a fully abstract model for a quantum linear functional language. In *QPL'06*, 2008.

[20] P. Selinger and B. Valiron. Quantum lambda calculus. In S. Gay and I. Mackie, editors, *Semantic Techniques in Quantum Computation*, chapter 9, pages 135–172. Cambridge University Press, 2009.

[21] B. Valiron. *Semantics for a higher-order functional programming language for quantum computation*. PhD thesis, University of Ottawa, 2008.

A. Appendix

In the following, $\circ$ denotes the functional composition, i.e., $\phi \circ \psi = \psi \,;\, \phi$.

A.1 Infinite biproduct completion

It is known that, under certain hypothesis, the infinite biproduct completion $\mathbf{C}^{\oplus}$ of a continuous commutative-monoid-enriched symmetrical monoidal category $\mathbf{C}$ gives a model of linear logic. In particular, $\mathbf{C}^{\oplus}$ denotes the exponential modality via the infinite biproduct of the equalizers of the symmetries of the n-fold monoidal product of $\mathbf{C}$ (if it exists). This construction has been mentioned in [14] and one can find specific instances in [9] (where the sum of the continuous commutative monoid structure of the $\mathbf{C}$ homsets is assumed to be idempotent) and in [10] (where the construction is applied to a continuous semiring $\mathcal{R}$ seen as a continuous commutative-monoid-enriched symmetrical monoidal category with a single object). In this section, we recall the construction of $\mathbf{C}^{\oplus}$, and in Section 5, we apply it to the category of completely positive maps with symmetries.

Definition 45. A *continuous semiring* $\mathcal{R}$ is defined to be a semiring $(|\mathcal{R}|, 0, 1, +, \cdot)$ equipped with an order relation $\prec$ such that 0 is the minimum, any directed set $D \subseteq |\mathcal{R}|$ has a directed sup $\bigvee$, and $+$ and $\cdot$ are continuous, i.e., $\bigvee(r + D) = r + \bigvee D$ and $\bigvee(r \cdot D) = r \cdot \bigvee D$.

From now on $\mathcal{R}$ will denote a continuous commutative semiring.

Definition 46. A symmetric monoidal category $\mathbf{C}$ is a *linear $\mathcal{R}$-category* when every homset is endowed with the structure of a module over the semiring $\mathcal{R}$, the composition is bilinear and the tensor preserves the module structure over $\mathcal{R}$ on homsets, that is $(f + f') \,;\, g = f \,;\, g + f' \,;\, g$, $f \,;\, (g + g') = f \,;\, g + f \,;\, g'$, $g \,; \mathbf{0} = \mathbf{0} = \mathbf{0} \,; g$, $(g+f) \otimes h = (g \otimes h) + (f \otimes h)$, and $g \otimes \mathbf{0} = \mathbf{0}$.

We moreover say that $\mathbf{C}$ is *continuous* when every homset is endowed with the structure of a complete partial order and composition, addition and scalar multiplication are continuous.

Remark 47. We cannot use Selinger's abstract cones [17], because the cancellation law fails in **CPMs** with ∞.

Lemma 48. *If $\mathbf{C}$ is a linear continuous $\mathcal{R}$-category, then we can define the indexed sum over a homset $\mathbf{C}(A, B)$ as*

$$\sum_{f \in S} f := \bigvee_{F \subseteq_{\mathrm{fin}} S} \Big(\sum_{f \in F} f \Big).$$

Proof. Just notice that $\{\sum_{f \in F} f \mid F \subseteq_{\mathrm{fin}} S\}$ is directed. □

From now on, we assume that $\mathbf{C}$ is a symmetric monoidal linear continuous $\mathcal{R}$-category $\mathbf{C}$.

Reminder of Definition 15 ($\mathbf{C}^{\oplus}$). An *object* of $\mathbf{C}^{\oplus}$ is a pair $\mathfrak{A} = (|\mathfrak{A}|, (\mathfrak{A}_a)_{a \in |\mathfrak{A}|})$ of a (possibly infinite) set of indexes $|\mathfrak{A}|$, called the *web* of $\mathfrak{A}$, and a $|\mathfrak{A}|$-family of objects in $\mathbf{C}$. The *homset* $\mathbf{C}^{\oplus}(\mathfrak{A}, \mathfrak{B})$ is the set of the $|\mathfrak{A}| \times |\mathfrak{B}|$ matrices of morphisms $\phi = (\phi_{a,b})_{(a,b) \in |\mathfrak{A}| \times |\mathfrak{B}|}$ in $\mathbf{C}$.

Given $\phi \in \mathbf{C}^{\oplus}(\mathfrak{A}, \mathfrak{B})$ and $\psi \in \mathbf{C}^{\oplus}(\mathfrak{B}, \mathfrak{C})$, the *composition* $\phi \,;\, \psi$ is the matrix product:

$$(\phi \,;\, \psi)_{a,c} = \sum_{b \in |\mathfrak{B}|} \phi_{a,b} \,;\, \psi_{b,c} \tag{13}$$

where the sum is defined by Lemma 48. The identity is the diagonal matrix $\mathrm{id}_{a,a'} := \mathrm{id}_{\mathfrak{A}_a}$ if $a = a'$, and $\mathrm{id}_{a,a'} := \mathbf{0}$ if $a \neq a'$.

A.1.1 Linear structure

We recall how the structure defining a compact closed category is inherited by $\mathbf{C}^{\oplus}$ from $\mathbf{C}$. That means that $\mathbf{C}^{\oplus}$ is symmetric monoidal and that it is a closed (resp. $\star$-autonomous, compact closed) whenever $\mathbf{C}$ is closed (resp. $\star$-autonomous, compact closed). In addition, $\mathbf{C}^{\oplus}$ has biproducts even if $\mathbf{C}$ does not.

Biproduct The category $\mathbf{C}^{\oplus}$ is the free biproduct completion of $\mathbf{C}$. The biproduct $\bigoplus_{i \in I} \mathfrak{A}_i$ of a family $(\mathfrak{A}_i)_{i \in I}$ of objects in $\mathbf{C}^{\oplus}$ is defined by

$$|\bigoplus_{i \in I} \mathfrak{A}_i| := \bigcup_{i \in I} \{i\} \times |\mathfrak{A}_i|, \qquad \big(\bigoplus_{i \in I} \mathfrak{A}_i\big)_{(j,a)} := (\mathfrak{A}_j)_a, \tag{14}$$

$$(\pi^j)_{(i,a),a'} := \delta_{i,j} \delta_{a,a'} \, \mathrm{id}_{\mathfrak{A}_a}, \quad (\iota^j)_{a,(i,a')} := \delta_{i,j} \delta_{a,a'} \, \mathrm{id}_{\mathfrak{A}_a} . \tag{15}$$

The tupling $\langle \phi_i \rangle_{i \in I}$ (resp. (co)-tupling $[\phi_i]_{i \in I}$) of a family of morphisms $\phi_i \in \mathbf{C}^{\oplus}(\mathfrak{A}, \mathfrak{B}_i)$ (resp. $\psi_i \in \mathbf{C}^{\oplus}(\mathfrak{A}_i, \mathfrak{B})$) is defined by:

$$(\langle \phi_i \rangle_{i \in I})_{a,(i,b)} := (\phi_i)_{a,b} \qquad ([\psi_i]_{i \in I})_{(i,a),b} := (\psi_i)_{a,b} \tag{16}$$

Proposition 49. *The object $\bigoplus_{i \in I} \mathfrak{A}_i$ together with the projections $(\pi^i)_{i \in I}$ and injections $(\pi^i)_{i \in I}$ is a biproduct of $\mathbf{C}^{\oplus}$.*

Proposition 50. *The category $\mathbf{C}^{\oplus}$ is the free biproduct completion of $\mathbf{C}$, i.e., for every category $\mathbf{D}$ endowed with a biproduct of families, and every functor $F : \mathbf{C} \to \mathbf{D}$, there exists a unique functor $F^{\dagger} : \mathbf{C}^{\oplus} \to \mathbf{D}$ commuting with biproducts.*

Proof. For any object $\mathfrak{A}$ of $\mathbf{C}^{\oplus}$, define $F^{\dagger}(\mathfrak{A}) = \bigoplus_{a \in |\mathfrak{A}|} F(\mathfrak{A}_a)$, and for every morphism $\phi \in \mathbf{C}^{\oplus}(\mathfrak{A}, \mathfrak{B})$, define $F^{\dagger}(\mathfrak{A}) = \langle [F(\phi_{a,b})]_{a \in |\mathfrak{A}|} \rangle_{b \in |\mathfrak{B}|}$. □

Monoidal product The bifunctor $\otimes : \mathbf{C}^{\oplus} \times \mathbf{C}^{\oplus} \to \mathbf{C}^{\oplus}$ is defined on objects $\mathfrak{A}, \mathfrak{B}$ by

$$|\mathfrak{A} \otimes \mathfrak{B}| := |\mathfrak{A}| \times |\mathfrak{B}|, \qquad (\mathfrak{A} \otimes \mathfrak{B})_{(a,b)} := \mathfrak{A}_a \otimes \mathfrak{B}_b, \tag{17}$$

where the $\otimes$ in the right-hand side of the second equation is that of the category $\mathbf{C}$. The action of $\otimes$ on morphisms is defined componentwise; given $\phi \in \mathbf{C}^{\oplus}(\mathfrak{A}, \mathfrak{B})$ and $\psi \in \mathbf{C}^{\oplus}(\mathfrak{C}, \mathfrak{D})$, we set for $(a, c) \in |\mathfrak{A} \otimes \mathfrak{C}|$, $(b, d) \in |\mathfrak{B} \otimes \mathfrak{D}|$,

$$(\phi \otimes \psi)_{(a,c),(b,d)} := \phi_{a,b} \otimes \psi_{c,d}. \tag{18}$$

The tensor unit is given by the space $\mathbf{1}$:

$$|\mathbb{1}| := \{*\}, \qquad \mathbb{1}_* := \mathbf{1}, \tag{19}$$

where $\mathbf{1}$ is the tensor unit of $\mathbf{C}$.

Proposition 51. *The operation $\otimes$ is a bifunctor endowing a symmetric monoidal structure on $\mathbf{C}^{\oplus}$ whose unit object is the space $\mathbb{1}$. Moreover, $\mathbf{C}^{\oplus}$ is a linear continuous $\mathcal{R}$-category with addition and scalar multiplication defined componentwise.*

Proof. The natural transformations $\alpha, \lambda, \rho, \sigma$, proving the associativity, the neutrality of $\mathbb{1}$, and the symmetry of $\otimes$, are defined componentwise from the corresponding isomorphisms in the category $\mathbf{C}$. So, for example, the associator isomorphism is given by $\alpha^{\mathfrak{A},\mathfrak{B},\mathfrak{C}}_{((a,b),c),(a',(b',c'))} = \delta_{a,a'} \delta_{b,b'} \delta_{c,c'} \alpha^{\mathfrak{A}_a,\mathfrak{B}_b,\mathfrak{C}_c}$, where $\alpha^{\mathfrak{A}_a,\mathfrak{B}_b,\mathfrak{C}_c}$ is the associativity isomorphism in $\mathbf{C}$, and $\delta_{a,a'}$ is the Kronecker delta. The commutativity of the pentagonal diagram follows immediately from its commutativity in $\mathbf{C}$.

Similarly, for the unit isomorphisms and the braiding σ.

The axioms of the continuous $\mathcal{R}$-module structure trivially follow from those of $\mathbf{C}$, except for the continuity of the composition, where one uses the commutativity of $\bigvee$:

$$\begin{aligned}((\bigvee_i \phi_i) \,;\, \psi)_{a,c} &= \sum_b \bigvee_i ((\phi_i)_{a,b} \,;\, \psi_{b,c}) \\ &= \bigvee_i \sum_b ((\phi_i)_{a,b} \,;\, \psi_{b,c}) \\ &= \bigvee_i (\phi_i \,;\, \psi)_{a,c}\end{aligned}$$

□

Notice that the associativity and unit isomorphisms allow us to define the n-fold tensor product $\mathfrak{A}^{\otimes n}$ of an object $\mathfrak{A}$ by $|\mathfrak{A}^{\otimes n}| := \{(a_1, \dots, a_n) \mid \forall i \leqslant n, a_i \in |\mathfrak{A}|\}$ and $\mathfrak{A}^{\otimes n}_{(a_1,\dots,a_n)} := \mathfrak{A}_{a_1} \otimes \cdots \otimes \mathfrak{A}_{a_n}$. Notice also that the group of permutations S_n on $\{1, \dots, n\}$ gives the $n!$ symmetries of $\mathfrak{A}^{\otimes n}$, namely $\sigma \in S_n$ can be seen as the symmetry defined as:

$$\sigma_{(a_1,\dots,a_n),(a'_1,\dots,a'_n)} := \left(\bigoplus_{i=1}^{n} \delta_{a_{\sigma(i)},a'_i}\right) \sigma^{\mathfrak{A}_{a_1} \otimes\cdots\otimes \mathfrak{A}_{a_n}, \mathfrak{A}_{a_{\sigma(1)}} \otimes\cdots\otimes \mathfrak{A}_{a_{\sigma(n)}}}$$

As usual on vector space based categories, the tensor product distributes over products. In fact, note that the web $|(\bigoplus_{i\in I} \mathfrak{A}_i) \otimes \mathfrak{B}|$ is in bijection with the web $|\bigoplus_{i\in I}(\mathfrak{A}_i \otimes \mathfrak{B})|$ via the mapping $((i, a), b) \mapsto (i, (a, b))$. Moreover, the objects of **C** associated with $((i, a), b)$ and $(i, (a, b))$ are the same. This induces an isomorphism $\mathtt{distr}$ in the homset $\mathbf{C}^{\oplus}((\bigoplus_{i\in I} \mathfrak{A}_i) \otimes \mathfrak{B}, \bigoplus_{i\in I}(\mathfrak{A}_i \otimes \mathfrak{B}))$, defined by

$$\mathtt{distr}_{((i,a),b),((i',(a',b'))} := \delta_{i,i'} \delta_{a,a'} \delta_{b,b'} \, \mathrm{id}_{\mathfrak{A}_{i\,a} \otimes \mathfrak{B}_b} \,. \tag{20}$$

Hom-closure If **C** is closed, then $\mathbf{C}^{\oplus}$ is also closed. The object of linear morphisms is defined as

$$|\mathfrak{A} \multimap \mathfrak{B}| := |\mathfrak{A}| \times |\mathfrak{B}|, \quad (\mathfrak{A} \multimap \mathfrak{B})_{(a,b)} := \mathfrak{A}_a \multimap \mathfrak{B}_b, \tag{21}$$

where the $\multimap$ in the right-hand side of the second equation is the object of the homset $\mathbf{C}(\mathfrak{A}_a, \mathfrak{B}_b)$. For every pair of objects $\mathfrak{A}$, $\mathfrak{B}$, the evaluation morphism $\mathrm{Eval}^{\mathfrak{A},\mathfrak{B}} : \mathbf{C}^{\oplus}((\mathfrak{A} \multimap \mathfrak{B}) \otimes \mathfrak{A}, \mathfrak{B})$ is defined componentwise:

$$\mathrm{Eval}^{\mathfrak{A},\mathfrak{B}}_{((a,b),a'),b'} := \delta_{a,a'} \delta_{b,b'} \, \mathrm{eval}^{\mathfrak{A}_a,\mathfrak{B}_b}, \tag{22}$$

where $\mathrm{eval}^{\mathfrak{A}_a,\mathfrak{B}_b}$ is the evaluation morphism in $\mathbf{C}((\mathfrak{A}_a \multimap \mathfrak{B}_b) \otimes \mathfrak{A}_a, \mathfrak{B}_b)$.

Proposition 52. *If* **C** *has a left-closed structure, then the family of objects* $\mathfrak{A} \multimap \mathfrak{B}$ *and morphisms* $\mathrm{Eval}^{\mathfrak{A},\mathfrak{B}}$*, for every* $\mathfrak{A}$*,* $\mathfrak{B}$*, endows* $\mathbf{C}^{\oplus}$ *with a left closed structure.*

Proof. We must prove the universal property defining a left closed structure, i.e., for every morphism $\phi \in \mathbf{C}^{\oplus}(\mathfrak{A} \otimes \mathfrak{C}, \mathfrak{B})$, there is a unique morphism $\Lambda(\phi) \in \mathbf{C}^{\oplus}(\mathfrak{C}, \mathfrak{A} \multimap \mathfrak{B})$ such that:

$$\begin{tikzcd} \mathfrak{C} \otimes \mathfrak{A} \arrow[d, dotted, "\Lambda(\phi)\otimes\mathfrak{A}"'] \arrow[dr, "\phi"] & \\ (\mathfrak{A} \multimap \mathfrak{B}) \otimes \mathfrak{A} \arrow[r, "\mathrm{Eval}^{\mathfrak{A},\mathfrak{B}}"] & \mathfrak{B}. \end{tikzcd} \tag{23}$$

The definition of $\Lambda(\phi)$ is componentwise, using the same universal property for each **C** component of Eval, i.e., $\Lambda(\phi)_{c,(a,b)} := \Lambda(\phi_{(c,a),b})$, where $\Lambda(\phi_{(c,a),b})$ is the unique morphism such that $(\Lambda(\phi_{c,(a,b)}) \otimes \mathfrak{A}_a) \,;\, \mathrm{eval}^{\mathfrak{A}_a,\mathfrak{B}_b} = \phi_{(c,a),b}$. The commutativity of the diagram follows immediately from the definitions and this latter equality. The uniqueness of $\Lambda(\phi)$ follows from the fact that for any morphism $\psi \in \mathbf{C}^{\oplus}(\mathfrak{C}, \mathfrak{A} \multimap \mathfrak{B})$, diagram (23) must satisfy the equation $(\psi_{c,(a,b)} \otimes \mathfrak{A}_a) \,;\, \mathrm{eval}^{\mathfrak{A}_a,\mathfrak{B}_b} = \phi_{(c,a),b}$ and hence $\psi_{c,(a,b)} = \Lambda(\phi_{c,(a,b)})$. □

As usual the universal property defined by diagram 23 induces an isomorphism from $\mathbf{C}^{\oplus}(\mathfrak{C} \otimes \mathfrak{A}, \mathfrak{B})$ to $\mathbf{C}^{\oplus}(\mathfrak{C}, \mathfrak{A} \multimap \mathfrak{B})$, which we denote by $\Lambda(-)$ and its inverse by $\mathrm{App}(-)$.

Dualizing object: The dualizing object $\bot$ (if it exists) in **C** can be seen as an object of **C** defined by:

$$|\bot| := \{*\}, \qquad\qquad \bot_* := \bot, \tag{24}$$

Proposition 53. *If* **C** *is* $\star$*-autonomous, then so it is* $\mathbf{C}^{\oplus}$ *with the dualizing object* $\bot$*. Moreover, if* **C** *is compact closed, than so is* $\mathbf{C}^{\oplus}$*.*

Proof. The isomorphism $\partial^{\mathfrak{A}} \in \mathbf{C}^{\oplus}(\mathfrak{A}, (\mathfrak{A} \multimap \imath) \multimap \imath))$ is defined as $\partial^{\mathfrak{A}}_{a,((a',*),*)} = \delta_{a,a'} \partial^{\mathfrak{A}_a}$, where as usual $\partial^{\mathfrak{A}_a}$ is the corresponding isomorphism in **C**. □

A.1.2 Exponential structure

We define the free exponential comonoid showing that $\mathbf{C}^{\oplus}$ is a Lafont category [13]. Such a comonoid is the infinite biproduct of the equalizers of the symmetries of the n-fold tensors, following the formula described in [14].

The next subsection shows how $\mathbf{C}^{\oplus}$ inherits such equalizers (here called *symmetric tensor powers*) from **C**, and the subsection after that gives the free exponential comonoid of $\mathbf{C}^{\oplus}$.

Symmetric Tensor Powers

Definition 54. The *symmetric n-th power* (A^n, eq^{A^n}) of an object A of a symmetric monoidal category **C** is the equalizer of the $n!$ symmetries of the n-ary tensor $A^{\otimes n}$. That is, A^n is an object of **C**, eq^{A^n} is a morphism in $\mathbf{C}(A^n, A^{\otimes n})$ equalizing the symmetries of $A^{\otimes n}$ (i.e., for every permutation $\sigma \in S_n$, $eq^{A^n};\sigma = eq^{A^n}$) enjoying the following universal property: for every object D and morphism $f \in \mathbf{C}(D, A^{\otimes n})$ equalizing the symmetries of $A^{\otimes n}$, there exists a unique morphism $f^\dagger$ such that

$$\begin{tikzcd} A^n \arrow[r, "eq^{A^n}"] & A^{\otimes n} \arrow[r, shift left, "\sigma_1"] \arrow[r, shift right, "\sigma_{n!}"'] & A^{\otimes n}. \\ D \arrow[u, dotted, "\text{unique } f^\dagger"] \arrow[ur, "f"] & & \end{tikzcd}$$

For $\mathbf{C}^{\oplus}$ to inherit the powers of **C**, we need the additional hypothesis that such equalizers preserve the tensor product.

Definition 55. An equalizer (E, eq) *preserves tensor products* whenever for every object B the pair $(E \otimes B, eq \otimes \mathrm{id}_B)$ is the equalizer of the diagram obtained from the diagram equalized by (E, eq) by replacing each object A with $A \otimes B$ and each arrow f by $f \otimes \mathrm{id}_B$.

Lemma 56. *If* (A^n, eq^{A^n}) *and* (B^m, eq^{B^m}) *preserve tensor products, then* $(A^n \otimes B^m, eq^{A^n} \otimes eq^{B^m})$ *is the equalizer of the endomorphisms of* $A^{\otimes n} \otimes B^{\otimes m}$ *of the shape* $\sigma \otimes \rho$*, for* $\sigma \in S_n$*,* $\rho \in S_m$*. Moreover, such an equalizer preserves tensor products.*

Proof. Clearly, $eq^{A^n} \otimes eq^{B^m}$ equalizes the group of the $n! \times m!$ symmetries of $A^{\otimes n} \otimes B^{\otimes m}$ which keep A's copies separate from B's copies. As for the universal property, one notices that $eq^{A^n} \otimes eq^{B^m} = eq^{A^n} \otimes \mathrm{id}_{B^m} \,;\, \mathrm{id}_{A^{\otimes n}} \otimes eq^{B^m}$. Then, take a morphism $f \in \mathbf{C}(D, A^{\otimes n} \otimes B^{\otimes m})$ equalizing the permutations in $S_n \times S_m$. We get a unique $f^\dagger \in \mathbf{C}(D, A^{\otimes n} \otimes B^m)$ by applying the universal property to the equalizer $\mathrm{id}_{A^{\otimes n}} \otimes eq^{B^m}$ and from that we get a unique $f^{\dagger^\dagger} \in \mathbf{C}(D, A^n \otimes B^m)$ applying the universal property to the equalizer $eq^{A^n} \otimes \mathrm{id}_{B^m}$. □

Lemma 57. *If* $\mathbf{C}$ *has symmetric* n*-th powers for every* $n \in \mathbb{N}$ *preserving tensor products, then* $\mathbf{C}^\oplus$ *also has symmetric* n*-th powers for every* $n \in \mathbb{N}$ *and they also preserve tensor products. In particular, the object* $\mathfrak{A}^n$ *can be defined by choosing an arbitrary order on the elements of* $|\mathfrak{A}|$ *and then setting*

$$|\mathfrak{A}^n| := \mathcal{M}_n(|\mathfrak{A}|), \quad \mathfrak{A}^n_p := \bigotimes_{a\in|p|} \mathfrak{A}_a^{p(a)},$$

where the support $|u|$ *of a set of multisets* u *is* $|u| := \bigcup_{p\in u} |p|$*, and the object* $\mathfrak{A}_a^{p(a)}$ *is the* $p(a)$*-th power in* $\mathbf{C}$ *of the* $\mathfrak{A}_a$*. Finally, the object* $\bigotimes_{a\in|p|} \mathfrak{A}_a^{p(a)}$ *denotes the tensor of the spaces* $\mathfrak{A}_a^{p(a)}$ *along the order we have fixed on* $|\mathfrak{A}|$*. Different orders give isomorphic objects, all presenting the symmetric* n*-power, so we leave the order implicit. The morphism* $(eq^{\mathfrak{A}^n})_{p,(a_1,\dots,a_n)}$ *is* $\mathbf{0}$ *if* $p \neq [a_1, \dots, a_n]$*; otherwise it is equal to the following composition of morphisms*

$$\begin{tikzcd}
& \bigotimes_{a\in|p|} \mathfrak{A}_a^{\otimes p(a)} \arrow[dr, "\alpha\,;\mathtt{ren}_{(a_1\dots a_n)}"] & \\
\bigotimes_{a\in|p|} \mathfrak{A}_a^{p(a)} \arrow[ur, "\bigotimes_{a\in|p|} eq^{A_a^{p(a)}}"] & & \bigotimes_{i=1}^n \mathfrak{A}_{a_i},
\end{tikzcd}$$

where $\alpha\ ;\ \mathtt{ren}_{(a_1,\dots,a_n)}$ *is the composition of the associator and any symmetry mapping the object* $\bigotimes_{a\in|p|} \mathfrak{A}_a^{\otimes p(a)}$ *to the object* $\bigotimes_{i=1}^n \mathfrak{A}_{a_i}$*.*

Proof. Let us prove that the morphism $eq^{\mathfrak{A}^n}$ is well-defined, i.e., that the composition $\bigotimes_{a\in|p|} eq^{A_a^{p(a)}} ; \alpha\ ;\ \mathtt{ren}_{\vec{a}_i}$ is independent of the chosen symmetry $\mathtt{ren}_{\vec{a}_i}$, for any sequence $\vec{a}_i = (a_1, \dots, a_n) \in |\mathfrak{A}^{\otimes n}|$. In fact, for any $\sigma \in S_n$ such that $\alpha\ ;\ \sigma$ maps $\bigotimes_{a\in|p|} \mathfrak{A}_a^{\otimes p(a)}$ to $\bigotimes_{i=1}^n \mathfrak{A}_{a_i}$, there is a family $\{\sigma_a\}_{a\in|p|}$ of permutations $\sigma_a \in S_{p(a)}$ such that $\alpha\ ;\ \sigma = \bigotimes_{a\in|p|} \sigma_a\ ;\ \alpha\ ;\ \mathtt{ren}_{\vec{a}_i}$. Indeed, for $i, j \leqslant p(a)$, define $\sigma_a(i) = j$ whenever the i-th occurrence of a in $(a_1, \dots, a_n)$ becomes the j-th occurrence of a in the sequence $(a_{\sigma^{-1}(1)}, \dots, a_{\sigma^{-1}(n)})$. Then,

$$\bigotimes_{a\in|p|} eq^{A_a^{p(a)}} ;\alpha\ ;\ \sigma = \bigotimes_{a\in|p|} (eq^{A_a^{p(a)}} ;\sigma_a)\ ;\ \alpha\ ;\ \mathtt{ren}_{\vec{a}_i}$$

and the latter is equal to $\bigotimes_{a\in|p|} eq^{A_a^{p(a)}} ; \alpha\ ;\ \mathtt{ren}_{\vec{a}_i}$, since we have $eq^{A_a^{p(a)}} ; \sigma_a = eq^{A_a^{p(a)}}$ for every a.

Let us now prove that $(\mathfrak{A}^n, eq^{\mathfrak{A}^n})$ is the equalizer of the $n!$ symmetries of $\mathfrak{A}^{\otimes n}$. We first prove that $eq^{\mathfrak{A}^n} ; \sigma = eq^{\mathfrak{A}^n}$, for any symmetry $\sigma \in S_n$. The proof is componentwise: in case $\vec{a}_i = (a_1, \dots a_n)$ is not an enumeration of a multiset p (i.e., $p \neq [a_1, \dots, a_n]$), then both $(eq^{\mathfrak{A}^n} ;\sigma)_{p,\vec{a}_i}$ and $eq^{\mathfrak{A}^n}{}_{p,\vec{a}_i}$ are equal to $\mathbf{0}$. Otherwise, we have $(eq^{\mathfrak{A}^n} ;\sigma)_{p,\vec{a}_i} = (\bigotimes_{a\in|p|} eq^{\mathfrak{A}_a^{p(a)}})\ ;\ \alpha\ ;\ \sigma_{\vec{a}_{\sigma^{-1}(i)},\vec{a}_i}$, but the latter is equal to $(eq^{\mathfrak{A}^n} ;\sigma)_{p,\vec{a}_i}$ since we proved that such a morphism is invariant under the symmetries with $\bigotimes_{i=1}^n \mathfrak{A}_{a_i}$ as codomain.

Now, let us take a morphism $\phi \in \mathbf{C}^\oplus(\mathfrak{B}, \mathfrak{A}^{\otimes n})$ equalizing the group of the $n!$ symmetries of $\mathfrak{A}^{\otimes n}$ and let us prove that ϕ has a unique decomposition into $\phi^\dagger\ ;\ eq^{\mathfrak{A}^n}$. The definition of $\phi^\dagger$ is given componentwise and depends on the order $\preccurlyeq$ on $|\mathfrak{A}|$ assumed for giving a particular presentation of the object $\mathfrak{A}^n$. Let $b \in |\mathfrak{B}|$, $p \in |\mathfrak{A}^n|$, and let $p^{\preccurlyeq} = (a_1, \dots, a_n)$ be the unique sequence which is an enumeration of p increasing with respect to $\preccurlyeq$ (i.e., $a_i \preccurlyeq a_{i+1}$ for every i). Notice that $\phi_{b,p^{\preccurlyeq}} ;\alpha \in \mathbf{C}(\mathfrak{B}_b, \bigotimes_{a\in|p|} \mathfrak{A}_a^{\otimes p(a)})$. Notice that $\phi_{b,p^{\preccurlyeq}}\ ;\ \alpha$ equalizes the symmetries of the form $\bigotimes_{a\in|p|} \rho_a$, with $\rho_a \in S_{p(a)}$. In fact, there exists a permutation $\rho \in S_n$ such that $\phi_{b,p^{\preccurlyeq}}\ ;\ \alpha\ ;\ \bigotimes_{a\in|p|} \rho_a = \phi_{b,p^{\preccurlyeq}}\ ;\ \rho\ ;\ \alpha$ and this last morphism is equal to $\phi_{b,\vec{a}_i}\ ;\ \alpha$ since by hypothesis ϕ equalizes all permutations in S_n. Since $(\bigotimes_{a\in|p|} \mathfrak{A}_a^{p(a)}, \bigotimes_{a\in|p|} eq^{\mathfrak{A}_a^{p(a)}})$ is the equalizer of the permutations of the form $\bigotimes_{a\in|p|} \rho_a$ (Lemma 56), we have that there exists a unique morphism $(\phi_{b,p^{\preccurlyeq}}\ ;\ \alpha)^\dagger \in \mathbf{C}(\mathfrak{B}_b, \bigotimes_{a\in|p|} \mathfrak{A}_a^{p(a)})$ such that $(\phi_{b,p^{\preccurlyeq}}\ ;\ \alpha)^\dagger\ ;\ \bigotimes_{a\in|p|} eq^{\mathfrak{A}_a^{p(a)}} = \phi_{b,p^{\preccurlyeq}}\ ;\ \alpha$.

Define $\phi^\dagger_{b,p} := (\phi_{b,p^{\preccurlyeq}}\ ;\ \alpha)^\dagger$. We have, for any $b \in |B|$ and $\vec{a}_i = (a_1, \dots, a_n) \in |\mathfrak{A}^{\otimes n}|$, writing $p = [a_1, \dots, a_n]$,

$$\begin{aligned}
(\phi^\dagger\ ;\ eq^{\mathfrak{A}^n})_{b,\vec{a}_i} &= \phi^\dagger_{b,p}\ ;\ \bigotimes_{a\in|p|} eq^{\mathfrak{A}_a^{p(a)}} ;\alpha\ ;\ \mathtt{ren}_{\vec{a}_i} \\
&= \phi_{b,\vec{a}_{\sigma(i)}}\ ;\ \alpha'\ ;\ \alpha\ ;\ \mathtt{ren}_{\vec{a}_i} \\
&= \phi_{b,\vec{a}_{\sigma(i)}}\ ;\ \mathtt{ren}_{\vec{a}_i} \\
&= \phi_{b,\vec{a}_i}
\end{aligned}$$

where σ is the permutation in S_n transforming $\vec{a}_i$ into $p^{\preccurlyeq}$ and α' the associator such that $\phi_{b,p^{\preccurlyeq}}\ ;\ \alpha' \in \mathbf{C}(\mathfrak{B}_b, \bigotimes_{a\in|p|} \mathfrak{A}_a^{\otimes p(a)})$. The passage from the second to the third line is the remark that α' is the inverse of α. The last line is achieved by the hypothesis that ϕ equalizes all permutations on S_n.

The uniqueness of $\phi^\dagger$ is inferred from that of $\phi^\dagger_{b,p}$.

The fact that $(\mathfrak{A}^n, eq^{\mathfrak{A}^n})$ preserves tensor products can be easily achieved by checking that the whole proof continues to hold if we add the needed tensors. □

Free Exponential Comonoid

Lemma 58. *If* $\mathbf{C}$ *has the symmetric* n*-th power of every object and if such a power preserves tensor products, then in* $\mathbf{C}^\oplus$ *the object* $!\mathfrak{A} := \bigoplus_n \mathfrak{A}^n$ *is the free commutative comonoid generated by* $\mathfrak{A}$*, the co-multiplication, here called* contraction $\mathtt{c}^{\mathfrak{A}} \in \mathbf{C}^\oplus(!\mathfrak{A}, !\mathfrak{A} \otimes !\mathfrak{A})$*, the counit, here called* weakening $\mathtt{w}^{\mathfrak{A}} \in \mathbf{C}^\oplus(!\mathfrak{A}, \mathbf{1})$*, and the* dereliction $\mathtt{d}^{\mathfrak{A}} \in \mathbf{C}^\oplus(!\mathfrak{A}, \mathfrak{A})$ *are given by*

$$\mathtt{w}^{\mathfrak{A}} := \pi^0, \qquad \mathtt{d}^{\mathfrak{A}} := \pi^1,$$
$$\mathtt{c}^{\mathfrak{A}} := \langle\langle \pi^{n+m}\ ;\ \overline{\mathtt{c}}^{n,m} \rangle_m\ ;\ \mathtt{distr}^{-1}\ ;\ \sigma \rangle_n\ ;\ \mathtt{distr}^{-1},$$

where $\overline{\mathtt{c}}^{n,m}$ *is the unique morphism commuting the diagram*

$$\begin{tikzcd}
\mathfrak{A}^{\otimes(n+m)} \arrow[r, "\alpha"] & \mathfrak{A}^{\otimes n} \otimes \mathfrak{A}^{\otimes m} \\
\mathfrak{A}^{n+m} \arrow[u, "eq^{\mathfrak{A}^{n+m}}"] \arrow[r, "\overline{\mathtt{c}}_{\mathfrak{A},n,m}"] & \mathfrak{A}^n \otimes \mathfrak{A}^m \arrow[u, "eq^{\mathfrak{A}^n} \otimes eq^{\mathfrak{A}^m}"']
\end{tikzcd} \tag{25}$$

which exists by applying the universal property to the equalizer $eq^{\mathfrak{A}^n} \otimes eq^{\mathfrak{A}^m}$ *(see Lemma 56).*

Proof. The morphisms $\mathtt{w}$ and $\mathtt{c}$ give a structure of comonoid to $!\mathfrak{A}$. In fact by using the uniqueness of the morphism $\overline{\mathtt{c}}_{n,m}$ in diagram (25) one can check the three equations

$$\mathtt{c}\ ;\ (\mathtt{c} \otimes !\mathfrak{A})\ ;\ \alpha = \mathtt{c}\ ;\ (!\mathfrak{A} \otimes \mathtt{c}),$$
$$\mathtt{c}\ ;\ \mathfrak{A} \otimes \mathtt{w}\ ;\ \rho = \mathfrak{A}, \qquad \mathtt{c}\ ;\ \mathtt{w} \otimes \mathfrak{A}\ ;\ \lambda = \mathfrak{A}.$$

For example, by an easy computation one can reduce the first equation to checking that, for every $n, m, r \in \mathbb{N}$, we have the equation : $\overline{\mathtt{c}}_{n+m,r}\ ;\ \overline{\mathtt{c}}_{n,m} \otimes \mathrm{id}_{\mathfrak{A}^r} ;\alpha = \overline{\mathtt{c}}_{n,m+r}\ ;\ \mathrm{id}_{\mathfrak{A}^n} \otimes \overline{\mathtt{c}}_{m,r}$. Then, by using diagram (25), such an equation is reduced to proving the equality of a composition of the associator morphisms mapping the space $\mathfrak{A}^{\otimes(n+m+r)}$ into $\mathfrak{A}^{\otimes n} \otimes (\mathfrak{A}^{\otimes m} \otimes \mathfrak{A}^{\otimes r})$. Such a composition is always unique by the Monoidal Coherence Theorem [11].

The comonoid is moreover commutative. In fact, the equation $\mathtt{c} = \mathtt{c} \,;\, \sigma$ is equivalent to proving, for every pair of numbers m, n, that $\overline{\mathtt{c}}_{n,m} = \overline{\mathtt{c}}_{m,n} \,;\, \sigma$. The claim follows similarly to the previous cases. In fact from the naturality of σ one gets $\sigma \,;\, eq^{\mathfrak{A}^m} \otimes eq^{\mathfrak{A}^n} = eq^{\mathfrak{A}^n} \otimes eq^{\mathfrak{A}^m} ;\sigma$.

Finally, let us prove that the comonoid is free. Let $\mathfrak{B}$, $\mu \in \mathbf{C}^{\oplus}(\mathfrak{B}, \mathfrak{B} \otimes \mathfrak{B})$, $\nu \in \mathbf{C}^{\oplus}(\mathfrak{B}, \mathbf{1})$ be a commutative comonoid and $\epsilon \in \mathbf{C}^{\oplus}(\mathfrak{B}, \mathfrak{A})$. We prove that there exists a unique comonoid morphism $\epsilon^{\dagger}$ such that

$$\begin{tikzcd}
!\mathfrak{A} \arrow[r, "\mathtt{d}"] & \mathfrak{A}. \\
\mathfrak{B} \arrow[u, "\epsilon^{\dagger}"] \arrow[ur, "\epsilon"'] &
\end{tikzcd} \tag{26}$$

We define the n-ary diagonal $\mu^n \in \mathbf{C}^{\oplus}(\mathfrak{B}, \mathfrak{B}^{\otimes n})$ as follows:

$$\mu^0 := \nu, \qquad \mu^{n+1} := \mu \,;\, \mu^n \otimes \mathrm{id}\,.$$

By induction on n one can prove that

$$\mu^{n+m} = \mu \,;\, \mu^n \otimes \mu^m \,;\, \alpha\lambda. \tag{27}$$

Then, we define ϵ^n as the unique morphism making this diagram commute:

$$\begin{tikzcd}
\mathfrak{A}^n \arrow[rr, "eq^{\mathfrak{A}^n}"] & & \mathfrak{A}^{\otimes n}. \\
& \mathfrak{B}^{\otimes n} \arrow[ur, "\epsilon^{\otimes n}"'] & \\
\mathfrak{B} \arrow[uu, dotted, "\text{unique } \epsilon^n"] \arrow[ur, "\mu^n"'] & &
\end{tikzcd} \tag{28}$$

Such a morphism is well-defined since by the commutativity of μ the morphism $\mu^n \,;\, \epsilon^{\otimes n}$ equalizes the $\mathfrak{A}^{\otimes n}$ symmetries and by Lemma 57, $(\mathfrak{A}^n, eq^{\mathfrak{A}^n})$ is the equalizer of such symmetries. We then set $\epsilon^{\dagger} := \langle \epsilon^n \rangle_n$.

The morphism $\epsilon^{\dagger}$ makes the diagram (26) commute, namely $\epsilon^{\dagger} \,;\, \mathtt{d} = \epsilon^1 = \epsilon$. We also have $\epsilon^{\dagger} \,;\, \mathtt{w} = \epsilon^0 = \nu$. The last equation we need to check is $\epsilon^{\dagger} \,;\, \mathtt{c} = \mu \,;\, \epsilon^{\dagger} \otimes \epsilon^{\dagger}$. First, notice that proving such an equation is equivalent to proving the commutativity of the following, for every $n, m \in \mathbb{N}$:

$$\begin{tikzcd}
& & \mathfrak{A}^{\otimes n} \otimes \mathfrak{A}^{\otimes m} & & \\
\mathfrak{A}^n \otimes \mathfrak{A}^m \arrow[urr, "eq^{\mathfrak{A}^n} \otimes eq^{\mathfrak{A}^m}"] & & & & \mathfrak{A}^n \otimes \mathfrak{A}^m. \arrow[ull, "eq^{\mathfrak{A}^n} \otimes eq^{\mathfrak{A}^m}"'] \\
& \mathfrak{A}^{n+m} \arrow[ul, "\overline{\mathtt{c}}_{n,m}"] & & B \otimes B \arrow[ur, "\epsilon^n \otimes \epsilon^m"'] & \\
& & B \arrow[ul, "\epsilon^{n+m}"] \arrow[ur, "\mu"'] & &
\end{tikzcd}$$

In fact, the right-hand side (as well as the left-hand side) of the diagram equalizes the group of $n! \times m!$ permutations of $\mathfrak{A}^{\otimes n} \otimes \mathfrak{A}^{\otimes m}$. So by the universal property of $eq^{\mathfrak{A}^n} \otimes eq^{\mathfrak{A}^m}$ (which are the equalizers of such permutations, since tensor equalizers preserve tensors by Lemma 57), we have that there is a unique morphism that composed with $eq^{\mathfrak{A}^n} \otimes eq^{\mathfrak{A}^m}$ gives that side of the diagram. The commutativity of the diagram then implies $\epsilon^{n+m} \,;\, \overline{\mathtt{c}}_{n,m} = \mu \,;\, \epsilon^n \otimes \epsilon^m$. From this then follows that for every $b \in |\mathfrak{B}|$, $p, q \in |!\mathfrak{A}|$ such that the cardinality of p (resp. of q) is n (resp. m), we have $(\epsilon^{\dagger} \,;\, \mathtt{c})_{b,(p,q)} = (\mu \,;\, \epsilon^{\dagger} \otimes \epsilon^{\dagger})_{b,(p,q)}$. The claim follows since the diagram commutes for every $n, m \in \mathbb{N}$.

So let us prove such a diagram. We have:

$$\begin{aligned}
&\epsilon^{n+m} \,;\, \overline{\mathtt{c}}_{n,m} \,;\, (eq^{\mathfrak{A}^n}) \otimes (eq^{\mathfrak{A}^m}) \\
&= \epsilon^{n+m} \,;\, eq^{\mathfrak{A}^{n+m}} ;\alpha && \text{by (25)} \\
&= \mu^{n+m} \,;\, \epsilon^{\otimes(n+m)} \,;\, \alpha && \text{by (28)} \\
&= \mu \,;\, \mu^n \otimes \mu^m \,;\, \alpha \,;\, \epsilon^{\otimes(n+m)} \,;\, \alpha && \text{by (27)} \\
&= \mu \,;\, (\mu^n \,;\, \epsilon^{\otimes n}) \otimes (\mu^m \,;\, \epsilon^{\otimes m}) && \\
&= \mu \,;\, \epsilon^n \otimes \epsilon^m \,;\, eq^{\mathfrak{A}^n} \otimes eq^{\mathfrak{A}^m} && \text{by (25)}
\end{aligned}$$

The uniqueness easily follows using the uniqueness of diagram 28. □

A $\star$-autonomous category such that each object has a free comonoid is usually called a *Lafont category*, which is known to be a model of linear logic [13]. In particular, the linear exponential comonad is given by the functorial promotion mapping an object $\mathfrak{A}$ to $!\mathfrak{A}$ and a morphism $\phi \in \mathbf{C}^{\oplus}(\mathfrak{A}, \mathfrak{B})$ to the unique comonoid morphism $!\phi \in \mathbf{C}^{\oplus}(!\mathfrak{A}, !\mathfrak{B})$ satisfying the equation $\mathtt{d} \,;\, \phi = !\phi \,;\, \mathtt{d}$, which has exactly one solution by the freeness of the exponential comonoid on $\mathfrak{B}$. Weakening gives the counit and the co-multiplication (also called *digging*) is the unique comonoid morphism $\mathtt{dig} \in \mathbf{C}^{\oplus}(!\mathfrak{A}, !!\mathfrak{A})$ such that $\mathtt{dig} \,;\, \mathtt{d} = \mathrm{id}$. Finally, the last morphism which is essential to interpret our calculus is $\mathtt{m} \in \mathbf{C}^{\oplus}(!\mathfrak{A} \otimes !\mathfrak{B}, !(\mathfrak{A} \otimes \mathfrak{B}))$ which is the unique comonoid morphism such that $\mathtt{m} \,;\, \mathtt{d} = \mathtt{d} \otimes \mathtt{d}$.

A.2 Proof of the compact closure of $\overline{\mathbf{CPMs}}$.

The tensor $\otimes$ is defined on objects by

$$(n, G) \otimes (m, H) := (nm, G \otimes H),$$

where we use the isomorphism $\mathbb{C}^{nm,nm} = \mathbb{C}^{n \times m, n \times m}$ obtained by the lexicographic order on the pairs $(i, j) \in n \times m$, and $G \otimes H$ is intended to be the subgroup of S_{nm} of the permutations of the form $g \otimes h$, with $g \in G, h \in H$ acting as $(i, j) \mapsto (g(i), h(j))$. Notice that whenever f is in $\overline{\mathbf{CPMs}}((n, G), (n', G'))$ and $h \in \overline{\mathbf{CPMs}}((m, H), (m', H'))$, then the usual tensor product $f \otimes h$ (with in addition the equalities $\infty \otimes h = f \otimes \infty = \infty$) enjoys the condition $G{\otimes}G';f{\otimes}h;H{\otimes}H' = (G;f;G'){\otimes}(H;g;H') = f{\otimes}h$.

The tensor unit is $I = (1, \{\mathrm{id}\})$. Symmetries, unit, and associativity maps are obtained from those of **CPM** by pre-composing and post-composing with the actions of the groups of the objects. For example, the two symmetries of $(n, G) \otimes (m, H)$ are $G \otimes H$ (which is the identity in this category) and $G \otimes H \,;\, \sigma \,;\, H \otimes G$, where σ is the symmetry in **CPM** of $n \otimes m$. The idempotence of G and H ensures that the two morphisms are in $\overline{\mathbf{CPMs}}$ and one can check that they give a symmetric monoidal structure to **CPMs**.

The compact closure is given by $(n, G)^* := (n, G)$; the unit $\eta_{(n,G)} \in \mathbf{CPMs}(I, (n, G)^* \otimes (n, G))$ (resp. co-unit $\epsilon_{(n,G)} \in \mathbf{CPMs}((n, G) \otimes (n, G)^*, I))$ is the composition (resp. precomposition) of the unit (resp. co-unit) of **CPM** with $G \otimes G$. In other words, writing $E_{i,j}$ for the matrix having 0 everywhere, except 1 at (i, j):

$$\eta_{(n,G)}(1) := \sum_{i,j} G(E_{i,j}) \otimes G(E_{i,j})$$

$$\epsilon_{(n,G)}(E_{i,j} \otimes E_{i',j'}) := \sum_{g,g' \in G} \frac{1}{\#G^2} \delta_{g(i),g'(i')} \delta_{g(j),g'(j')}$$

These maps are completely positive:

- The unit is completely positive because $\sum_{i,j} E_{i,j}$ is a positive matrix, and because $G \otimes G$ is completely positive: This makes $\eta(1)$ positive. Therefore, for any positive matrix A, $(\eta \otimes \mathrm{id})(A)$ is simply $(\eta(1)) \otimes A$ which is positive.
- Let f be the map sending $E_{i,j} \otimes E_{i',j'}$ to $\delta_{i,i'} \delta_{j,j'}$. This map is completely positive as its characteristic matrix $\sum_{i,j} E_{i,j} \otimes E_{i,j}$ is positive.

Since the counit can be written as $\frac{1}{\#G^2}\left(\sum_{g,g'}(g \otimes g')\right) \circ f$, it is completely positive.

We have to prove that

$$\rho^{-1}_{(n,G)} \mathbin{;} \mathrm{id}_{(n,G)} \otimes \eta_{(n,G)} \mathbin{;} \alpha \mathbin{;} \epsilon_{(n,G)} \otimes \mathrm{id}_{(n,G)} \mathbin{;} \lambda_{(n,G)} = G$$

and its dual starting with $\lambda^{-1}_{(n,G)^*}$. Let us denote the elements of the base of $\mathbb{C}^{n\times n}$ by $\{e_h\}_{h\in n\times n}$ and the action of $g \in G$ on e_h by $e_{g(h)}$. By an easy computation, we have that the left-hand side morphism applied to e_h is equal to:

$$\sum_{k\in n\times n}\sum_{g,g'\in G}\frac{1}{(\#G)^2}\delta_{g'(h),g(k)}G(e_k) \tag{29}$$

$$= \sum_{k\in n\times n}\sum_{g,g'\in G}\frac{1}{(\#G)^2}\delta_{g^{-1}g'(h),k}G(e_k) \tag{30}$$

$$= \sum_{k\in n\times n}\sum_{g\in G}\sum_{g'\in g^{-1}G}\frac{1}{(\#G)^2}\delta_{g'(h),k}G(e_k) \tag{31}$$

$$= \sum_{k\in n\times n}\sum_{g\in G}\sum_{g'\in G}\frac{1}{(\#G)^2}\delta_{g'(h),k}G(e_k) \tag{32}$$

$$= \sum_{k\in n\times n}\sum_{g'\in G}\frac{1}{\#G}\delta_{g'(h),k}G(e_k) \tag{33}$$

$$= \sum_{g'\in G}\frac{1}{\#G}G(e_{g'(k)}) \tag{34}$$

$$= G \mathbin{;} G(e_k) = G(e_k) \tag{35}$$

The same holds for the dual.

A.3 Complete proof of Adequacy

From now on, we consider the language extended with the Ω and the bounded `let-rec`^{n} constructor, as in Definition 32.

Lemma 59. *Together with the new constructs, the language still enjoys subject reduction (Proposition 11) and totality (Lemma 13).*

Proof. Subject reduction. The proof uses the substitution lemma (Lemma 10), still valid with the two additional constructs.

Totality. The two new rewrite rules add two cases to the induction: since they do not modify the quantum state, the proof carries through. □

Definition 60. A *Ω-term* is a term generated by the following grammar:

$$\begin{aligned} O \ ::= {} & \Omega \mid \Omega M \mid V\Omega \mid \Omega;N \mid \Omega\otimes N \mid V\otimes\Omega \mid \\ & \mathtt{let}\ x^A \otimes y^B \ = \ \Omega\ \mathtt{in}\ N \mid \mathtt{in}_\ell\ \Omega \mid \mathtt{in}_r\ \Omega \mid \\ & \mathtt{match}\ \Omega\ \mathtt{with}\ (x^A : N | y^B : N'). \end{aligned}$$

Lemma 61. *If $[q,\ell,M]$ is typable then either M is a value, or a Ω-term, or there is a closure $[q',\ell',M']$ such that $[q,\ell,M] \xrightarrow{p} [q',\ell',M']$. Moreover, if M is neither a value nor a Ω-term, the total probability of all possible single-step reductions from $[q,\ell,M]$ is* 1.

Proof. The proof by induction on the typing derivation of M carries through with the added constructs. □

Lemma 62 (Invariance of the interpretation)**.** *Let $\ell = |y_1,\dots,y_m\rangle$ and $\ell \vdash M : A$. If M is not a value, nor an Ω-term, then for all quantum states $q \in \mathbb{C}^{2^m}$,*

$$[\![M]\!]^{\ell\vdash A}(qq^*) = \sum_{[q,\ell,M]\xrightarrow{p}[q',\ell',N]} p\cdot[\![N]\!]^{\ell'\vdash A}(q'q'^*).$$

Proof. We only have to check for three additional cases to extend the proof.

- The case $M = \Omega$ is satisfied, as Ω does not reduce, and its denotation is $\mathbf{0}$.
- In the case `letrec`$^{n+1}$ $f\,x = M$ `in` N, the equation becomes

  $$\begin{aligned} & [\![\mathtt{letrec}^{n+1}\ f\,x = M\ \mathtt{in}\ N]\!]^{\ell\vdash A}(qq^*) = \\ & \qquad [\![N\{(\lambda x.\mathtt{letrec}^{n}\ f\,x = M\ \mathtt{in}\ M)/f\}]\!]^{\ell'\vdash A}(q'q'^*), \end{aligned}$$

  which is valid because of the definition of the operation $(\ )^n$ (Equations (10) and (11)). Indeed, if ϕ is the denotation of M,

  $$[\![!\Delta \vdash \lambda x.\mathtt{letrec}^{n}\ f\,x = M\ \mathtt{in}\ M]\!] =$$

  $$!\Delta \xrightarrow{\mathtt{c}} !\Delta\otimes!\Delta \xrightarrow{\mathrm{id}\otimes(\mathtt{dig};\mathtt{m};!(\Lambda\phi))^n} !\Delta\otimes!(A\multimap B) \xrightarrow{!(\Lambda\phi)} !(A\multimap B),$$

  whereas, provided that ψ is the denotation of N,

  $$[\![!\Delta,\Gamma \vdash \mathtt{letrec}^{n+1}\ f\,x = M\ \mathtt{in}\ N]\!] =$$

  $$\begin{tikzcd} !\Delta\otimes\Gamma \arrow[d, "\mathtt{c}"] & & !(A\multimap B) \\ !\Delta\otimes\Gamma\otimes!\Delta \arrow[rr, "\mathrm{id}\otimes(\mathtt{dig};\mathtt{m};!(\Lambda\phi))^{n+1}"] & & !\Delta\otimes\Gamma\otimes!(A\multimap B), \arrow[u, "\psi"] \end{tikzcd}$$

  which is precisely $[\![N\{(\lambda x.\mathtt{letrec}^{n}\ f\,x = M\ \mathtt{in}\ M)/f\}]\!]$, by noticing that

  $$(\mathtt{dig};\mathtt{m};!(\Lambda\phi))^{n+1} = [\![!\Delta \vdash \lambda x.\mathtt{letrec}^{n}\ f\,x = M\ \mathtt{in}\ M]\!].$$

- The last case is `letrec`^{0} $f\,x = M$ `in` N, using the fact that the denotation of Ω is $\mathbf{0}$. □

Reminder of Definition 33. A term is called *finitary* when it does not contain any occurrence of the un-indexed `let-rec` construct. It can however contain Ω and any of the indexed `let-rec`^{n}. We call a closure *finitary* when its term is finitary.

Lemma 63. *A finitary closure only reduces to finitary closures.*

Proof. The only rewrite rule creating a term with an un-indexed `let-rec` construct already has a term with an un-indexed `let-rec` construct as redex. □

Reminder of Lemma 34. *If $[q_1,\ell_1,M_1]$ is finitary, then every rewrite sequence*

$$[q_1,\ell_1,M_1] \xrightarrow{p_1} [q_2,\ell_2,M_2] \xrightarrow{p_2} [q_3,\ell_3,M_3] \xrightarrow{p_3} \cdots$$

is finite. Moreover, a normal form of such a sequence is a closure having as term either a value or an Ω-term.

Proof. The first claim of the lemma is proved by showing that the language is strongly normalizing. The second claim follows from Lemma 61.

Strong normalization of the language is proved by reducing it to a non-deterministic language without quantum states, for which a standard proof technique can be used.

Let us define the language *AUX* whose terms are the terms of the extended quantum lambda-calculus, minus the `let-rec` construct, and whose operational semantics is given in Table 8. The operational semantics is obtained from Table 3 and the rules for `let-rec`^{n} by replacing closures with the respective terms and the rules of Table 3b by dummy reduction rules:

$$U(\bullet\otimes\cdots\otimes\bullet) \to \bullet\otimes\cdots\otimes\bullet \qquad \mathtt{new}\ \mathtt{ff} \to \bullet \qquad \mathtt{new}\ \mathtt{tt} \to \bullet$$

$$\mathtt{meas}\ \bullet \to \mathtt{tt} \qquad \mathtt{meas}\ \bullet \to \mathtt{ff}$$

where $\bullet$ denotes a distinct term variable, which, by convention, it is never bound by an abstraction. Intuitively, $\bullet$ corresponds to the variables pointing to the quantum state.

The type system of the language *AUX* is a simple type system with function types, pairs, coproducts, lists, and a base type **qubit**:

$$A, B, C ::= \textbf{qubit} \mid A \to B \mid 1 \mid A \times B \mid A \oplus B \mid A^{\ell}.$$

The typing rules are found in Table 9. Note that we treat the distinctive term variable $\bullet$ as a term constant, with its own typing rule.

The language *AUX* satisfies subject reduction, and can be shown to be strongly normalizing using a standard technique (e.g. using reducibility candidates).

One can map a finitary program from the quantum lambda calculus to the language *AUX* as follows:

$$[q, \ell, M] \qquad \longmapsto \qquad \overline{M}$$

where $\overline{M}$ is M where all the variables of ℓ have been replaced with $\bullet$. It is straightforward to check that M is well-typed, then so is $\overline{M}$, and that if

$$[q, \ell, M] \xrightarrow{p} [q', \ell', M']$$

then

$$\overline{M} \to \overline{M'}.$$

This concludes the proof of the lemma: if there were an infinite reduction sequence in the quantum lambda-calculus starting with a finitary program, it would generate an infinite rewrite sequence in *AUX* , which is not possible. □

Corollary 64. *For any finitary closure $[q, \ell, M]$, there exists a number $m \in \mathbb{N}$ such that:*

$$\mathrm{Halt}_{[q,\ell,M]} = \sum_{[q',\ell',V]} \mathrm{Red}^{m}_{[q,\ell,M],[q',\ell',V]} \,.$$

Proof. By König's Lemma and Lemma 34, the reduction tree with root $[q, \ell, M]$ is finite. Let m be its height. We have that for every $m' > m$, and every $[q', \ell', V]$, $\mathrm{Red}^{m'}_{[q,\ell,M],[q',\ell',V]} = \mathrm{Red}^{m}_{[q,\ell,M],[q',\ell',V]}$. We conclude by the definition of Halt (Equation (5)). □

Reminder of Corollary 35. *Let M be a closed finitary term of unit type. Then $[\![M]\!]^{\vdash 1}_{*} = \mathrm{Halt}_{[|\,\rangle,|\,\rangle,M]}$.*

Proof. We prove that, for any total finitary quantum closure of unit type $[q, \ell, M]$:

$$[\![M]\!]^{\ell \vdash 1}(qq^{*}) = \mathrm{Halt}_{[q,\ell,M]} \,.$$

In fact, by Corollary 64, there exists $m \in \mathbb{N}$ such that $\mathrm{Halt}_{[q,\ell,M]} = \sum_{[q',\ell',V]} \mathrm{Red}^{m}_{[q,\ell,M],[q',\ell',V]}$. The proof is by induction on m. If $m = 0$, then either $M = \mathtt{skip}$ and $\mathrm{Halt}_{[q,\ell,M]} = 1$ or a M is an Ω-term and $\mathrm{Halt}_{[q,\ell,M]} = 0$. Notice that in both cases, being the closure total, we have that q and ℓ are empty. We conclude trivially by the definition of $[\![\mathtt{skip}]\!]$ and the fact that the semantics of an Ω-term is the zero matrix. The induction step follows by the induction hypothesis and Lemma 62. □

Reminder of Definition 36. Let $\lhd$ be a relation between finitary terms and general terms defined as the smallest congruence relation on terms satisfying, for every $M \lhd M'$ and $N \lhd N'$:

$$N\{(\lambda x^{A}.\Omega^{B})/f\} \lhd (\mathtt{letrec}\; f\, x = M' \;\mathtt{in}\; N')$$
$$(\mathtt{letrec}^{n}\; f\, x = M \;\mathtt{in}\; N) \lhd (\mathtt{letrec}\; f\, x = M' \;\mathtt{in}\; N')$$

Reminder of Lemma 37. *For every typing judgement $\Gamma \vdash M : A$, we have:*

$$[\![M]\!]^{\Gamma \vdash A} = \bigvee_{\substack{M' \lhd M \\ M' \text{ finitary}}} [\![M']\!]^{\Gamma \vdash A}.$$

Proof. By structural induction on the derivation of $\Gamma \vdash M : A$, one proves that: (i) $\Gamma \vdash M' : A$ is derivable for every $M' \lhd M$; (ii) $\{[\![M']\!]^{\Gamma \vdash A} \;;\; M' \lhd M\}$ is directed; (iii) the equation in the statement holds. All cases are trivial consequences of the induction hypothesis and the continuity of all the categorical constructs. In the $\mathtt{rec}$ rule case, one notices that by definition $\mathrm{Y}\,(\mathtt{dig};\mathtt{m};!(\Lambda\phi)) = \bigvee_{n=0}^{\infty}(\mathtt{dig};\mathtt{m};!(\Lambda\phi))^{n}$. □

Lemma 65. *Let $M \lhd M'$, and let $[q, \ell, M] \xrightarrow{p} [q', \ell', N]$. Then there exists a unique N' such that $N \lhd N'$ and $[q, \ell, M'] \xrightarrow{p} [q', \ell', N']$.*

Reminder of Lemma 38. *For every $M \lhd M'$, we have that $\mathrm{Halt}_{[q,\ell,M]} \leqslant \mathrm{Halt}_{[q,\ell,M']}$.*

Proof. We prove by induction on n the inequality:

$$\sum_{[q',\ell',N]} \mathrm{Red}^{n}_{[q,\ell,M],[q',\ell',N]} \leqslant \sum_{[q',\ell',N']} \mathrm{Red}^{n}_{[q,\ell,M'],[q',\ell',N']} \,.$$

from which trivially follows the statement.

The case $n = 0$ is trivial, as both sides are equal to 1. Suppose that the result is true for n, and consider the value

$$\begin{aligned}&\sum_{[q',\ell',N]} \mathrm{Red}^{n+1}_{[q,\ell,M],[q',\ell',N]} = \\ &\sum_{[q',\ell',N]} \sum_{[q'',\ell'',P]} \mathrm{Red}_{[q,\ell,M],[q'',\ell'',P]} \mathrm{Red}^{n}_{[q'',\ell'',P],[q',\ell',N]} = \\ &\sum_{[q'',\ell'',P]} \mathrm{Red}_{[q,\ell,M],[q'',\ell'',P]} \sum_{[q',\ell',N]} \mathrm{Red}^{n}_{[q'',\ell'',P],[q',\ell',N]} \,.\end{aligned} \tag{36}$$

From Lemma 65, we deduce that for every P there exists a unique P' such that $\mathrm{Red}_{[q,\ell,M],[q'',\ell'',P]} = \mathrm{Red}_{[q,\ell,M'],[q'',\ell'',P']}$ and such that $P \lhd P'$. Remark that, independently from the rewrites P of M, there might exist other terms P' such that we have $\mathrm{Red}_{[q,\ell,M'],[q'',\ell'',P']} \neq 0$. For example, if M were Ω, although there would be no such P there would still be one P'.

Now, from induction hypothesis, we infer that for all of the pairs (P, P'),

$$\begin{aligned}&\sum_{[q',\ell',N]} \mathrm{Red}^{n}_{[q'',\ell'',P],[q',\ell',N]} \leqslant \\ &\qquad \sum_{[q',\ell',N']} \mathrm{Red}^{n}_{[q'',\ell'',P'],[q',\ell',N']} \,.\end{aligned} \tag{37}$$

Using Equations (36) and (37) we deduce that

$$\begin{aligned}&\sum_{[q',\ell',N]} \mathrm{Red}^{n+1}_{[q,\ell,M],[q',\ell',N]} \leqslant \\ &\sum_{[q'',\ell'',P']} \mathrm{Red}_{[q,\ell,M],[q'',\ell'',P']} \sum_{[q',\ell',N']} \mathrm{Red}^{n}_{[q'',\ell'',P'],[q',\ell',N']} = \\ &\qquad \sum_{[q',\ell',N']} \mathrm{Red}^{n+1}_{[q,\ell,M'],[q',\ell',N']} \,.\end{aligned} \tag{38}$$

This finishes the proof of the lemma. □

$$
\begin{array}{cc}
(\lambda x^A.M)\,V \to M\{V/x\} & \mathtt{let}\;x^A \otimes y^B \;=\; V \otimes W \;\mathtt{in}\;N \to N\{V/x, W/y\} \\
\mathtt{skip};N \to N & \mathtt{match}\;(\mathtt{in}_\ell\;V)\;\mathtt{with}\;(x^A : M | y^B : N) \to M\{V/x\} \\
\mathtt{split}\,V \to V & \mathtt{match}\;(\mathtt{in}_r\;V)\;\mathtt{with}\;(x^A : M | y^B : N) \to N\{V/y\}
\end{array}
$$

$$\mathtt{letrec}^0\;f^{A\multimap B}\;x = M\;\mathtt{in}\;N \to N\{(\lambda x^A.\Omega^B)/f\}$$

$$\mathtt{letrec}^{n+1}\;f^{A\multimap B}\;x = M\;\mathtt{in}\;N \to N\{(\lambda x^A.\mathtt{letrec}^n\;f^{A\multimap B}\;x = M\;\mathtt{in}\;M)/f\}$$

(a) Classical control.

$$U(\bullet \otimes \cdots \otimes \bullet) \to \bullet \otimes \cdots \otimes \bullet \qquad \mathtt{new}\;\mathtt{ff} \to \bullet \qquad \mathtt{new}\;\mathtt{tt} \to \bullet \qquad \mathtt{meas}\;\bullet \to \mathtt{tt} \qquad \mathtt{meas}\;\bullet \to \mathtt{ff}$$

(b) What used to refer to quantum data.

$$MN \to M'N \qquad M \otimes N \to M' \otimes N \qquad \mathtt{in}_\ell\;M \to \mathtt{in}_\ell\;M' \qquad VM \to VM' \qquad V \otimes M \to V \otimes M' \qquad \mathtt{in}_r\;M \to \mathtt{in}_r\;M'$$

$$M;N \to M';N \qquad \mathtt{let}\;x^A \otimes y^B \;=\; M\;\mathtt{in}\;N \to \mathtt{let}\;x^A \otimes y^B \;=\; M'\;\mathtt{in}\;N$$

$$\mathtt{match}\;M\;\mathtt{with}\;(x^A : P | y^B : N) \to \mathtt{match}\;M'\;\mathtt{with}\;(x^A : P | y^B : N)$$

(c) Congruence rules, under the hypothesis that $M \to M'$.

Table 8: Rewrite system for the language *AUX* of Lemma 34.

$$\frac{}{\Delta, x : A \vdash x : A}\;ax \qquad \frac{}{\Delta \vdash \mathtt{skip} : 1}\;1_I \qquad \frac{}{\Delta \vdash \Omega : A}\;\Omega \qquad \frac{}{\vdash \bullet : \mathbf{qubit}}\;\bullet$$

$$\frac{\Delta, x : A \vdash M : B}{\Delta \vdash \lambda x^A.M : A \to B}\;\to_I \qquad \frac{\Delta \vdash M : A \to B \quad \Delta \vdash N : A}{\Delta \vdash MN : B}\;\to_E \qquad \frac{\Delta \vdash M : 1 \quad \Delta \vdash N : A}{\Delta \vdash M;N : A}\;1_E$$

$$\frac{\Delta \vdash M : A \quad \Delta \vdash N : B}{\Delta \vdash M \otimes N : A \times B}\;\times_I \qquad \frac{\Delta \vdash M : A \times B \quad \Delta, x : A, y : B \vdash N : C}{\Delta \vdash \mathtt{let}\;x^A \times y^B \;=\; M\;\mathtt{in}\;N : C}\;\times_E$$

$$\frac{\Delta \vdash M : A}{\Delta \vdash \mathtt{in}_\ell\;M : A \oplus B}\;\oplus_I^\ell \qquad \frac{\Delta \vdash M : B}{\Delta \vdash \mathtt{in}_r\;M : A \oplus B}\;\oplus_I^r \qquad \frac{\Delta \vdash P : A \oplus B \quad \begin{array}{c}\Delta, y : B \vdash N : C \\ \Delta, x : A \vdash M : C\end{array}}{\Delta \vdash \mathtt{match}\;P\;\mathtt{with}\;(x^A : M | y^B : N) : C}\;\oplus_E$$

$$\frac{\Delta \vdash M : 1 \oplus (A \times A^\ell)}{\Delta, \Gamma \vdash M : A^\ell}\;-_I^\ell \qquad \frac{}{\Delta \vdash \mathtt{split}^A : A^\ell \to 1 \oplus (A \times A^\ell)}\;\mathtt{split} \qquad \frac{\Delta, f : (A \multimap B), x : A \vdash M : B \quad \Delta, f : (A \multimap B) \vdash N : C}{\Delta \vdash \mathtt{letrec}^{n+1}\;f^{A\multimap B}\;x = M\;\mathtt{in}\;N : C}\;\mathtt{rec}$$

$$\frac{}{\Delta \vdash \mathtt{meas} : \mathbf{qubit} \to \mathbf{bit}}\;\mathtt{meas} \qquad \frac{}{\Delta \vdash \mathtt{new} : \mathbf{bit} \to \mathbf{qubit}}\;\mathtt{new} \qquad \frac{U \text{ of arity } n}{\Delta \vdash U : \mathbf{qubit}^{\times n} \to \mathbf{qubit}^{\times n}}\;U$$

Table 9: Typing rules for the language *AUX* .