Idempotents in dagger categories (extended abstract)

Peter Selinger[1]

Department of Mathematics and Statistics
Dalhousie University, Halifax, Nova Scotia, Canada

Abstract

Dagger compact closed categories were studied by Abramsky and Coecke (under the name "strongly compact closed categories") as an abstract presentation of the category of Hilbert spaces and linear maps, and as a framework in which to carry out the interpretation of quantum protocols. I subsequently showed that dagger compact closed categories can also describe *mixed* quantum computation, where the morphisms are completely positive maps. I introduced the CPM construction as a way to pass from the pure to the mixed setting. One technical detail of the $\mathbf{CPM}(\mathbf{C})$ construction is that it does not preserve biproducts. Therefore, to obtain an interpretation of classical types such as $\mathbf{bit} = I \oplus I$, one must work in the free biproduct completion $\mathbf{CPM}(\mathbf{C})^{\oplus}$. In this paper, we show that there is another view of classical types, namely as splittings of self-adjoint idempotents on quantum types. We show that all the objects of $\mathbf{CPM}(\mathbf{C})^{\oplus}$ arise as such splittings.

Keywords: Quantum computing, dagger categories, CPM construction, idempotents.

1 Introduction

Dagger compact closed categories are an abstract presentation of the category of Hilbert spaces and linear maps. They were recently introduced by Abramsky and Coecke under the name "strongly compact closed categories", for the purpose of studying quantum protocols [1]. Abramsky and Coecke showed that, even without assuming a complex vector space structure, many important properties of quantum mechanics can be formalized in this setting, including the notions of scalars, vectors, inner products, unitary and self-adjoint operators, projections, and the Born rule.

In [6], I showed that dagger compact closed categories can also describe *mixed* quantum computation, where the morphisms are completely positive maps. Completely positive maps are the common generalization of unitary transformations and measurements, and thus they capture both reversible and irreversible computation. They can also be understood as a combination of quantum amplitudes and classical

[1] Email: selinger@mathstat.dal.ca. Research supported by NSERC.

This is a preliminary version. The final version will be published in Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

probabilities. I introduced the CPM construction as a way to pass from any dagger compact closed category $\mathbf{C}$ describing pure quantum computation to a dagger compact closed category $\mathbf{CPM}(\mathbf{C})$ of mixed computations.

One of the interesting properties of the $\mathbf{CPM}(\mathbf{C})$ construction is that it does not preserve biproducts. Its objects correspond to the "simple" signatures of [5], i.e., to purely quantum data types. To be able to interpret classical types such as $\mathbf{bit} = I \oplus I$, or combined quantum/classical types such as $\mathbf{bit} \otimes \mathbf{qbit} \cong \mathbf{qbit} \oplus \mathbf{qbit}$, biproducts are needed. The solution proposed in [6], and the one also implicitly followed in [5], was to work in the free biproduct completion $\mathbf{CPM}(\mathbf{C})^{\oplus}$ of the category of completely positive maps.

Inspired by recent work of Coecke and Pavlovic [3], we show that there is another method of distilling classical types from their quantum counterparts. Unlike the free biproduct completion, which adds the classical types externally, the present construction is internal; the classical types are obtained by splitting certain self-adjoint idempotents on quantum types. Computationally, this means that classical data can be described as quantum data with additional properties (for example, the property of being a standard basis vector). Since idempotents are a special case of categorical limit, it also makes sense to speak of the "classical limit" of quantum mechanics in this setting.

The paper is organized as follows. In Section 2, we review the definitions of various classes of dagger categories that appeared in [6]. In Section 3, we discuss basic properties of idempotents and self-adjoint idempotents and their splittings. Section 4 recalls the CPM construction, and introduces the view of classical types as self-adjoint idempotents on quantum types. Finally, Section 5 delves into various technical properties of idempotents in dagger categories. We conclude with the, perhaps unexpected, observation that the category $\mathbf{CPM}(\mathbf{FdHilb})$ of Hilbert spaces and completely positive maps does not satisfy the square root axiom of positive operators.

2 Dagger structures

2.1 Dagger categories

Recall the definition of a dagger category.

Definition 2.1 (dagger category) A *dagger structure* on a category $\mathbf{C}$ is an involutive, identity-on-objects, contravariant functor $\dagger : \mathbf{C} \to \mathbf{C}$. A category that is equipped with a dagger structure is called a *dagger category*.

Concretely, this means that to every morphism $f : A \to B$ one associates a morphism $f^{\dagger} : B \to A$, called the *adjoint* of f, such that for all $f : A \to B$ and $g : B \to C$, one has $\mathrm{id}_A^{\dagger} = \mathrm{id}_A$, $(g \circ f)^{\dagger} = f^{\dagger} \circ g^{\dagger}$, and $f^{\dagger\dagger} = f$.

The prime example of a dagger category is the category $\mathbf{FdHilb}$ of finite-dimensional Hilbert spaces and linear maps, where the adjoint of $f : A \to B$ is given in the usual linear algebra way as the unique map $f^{\dagger}$ satisfying $\langle fx|y\rangle = \langle x|f^{\dagger}y\rangle$ for all $x \in A$, $y \in B$.

Remark 2.2 In the mathematical literature, it is common to write f^*, and not

$f^\dagger$, for the adjoint of a linear operator. However, the notation f^* is already used in compact closed categories for the transpose $f^* : B^* \to A^*$, which is distinct from the adjoint $f^\dagger : B \to A$. This is in keeping with the convention, common in category, of using the same notation for the object part and the morphism part of a functor. We therefore follow physics notation in denoting the adjoint by $f^\dagger$. The same convention is used by Abramsky and Coecke [1].

The literature on C^*-algebras contains a notion of **-categories*, which are similar to dagger categories (see e.g. [4]). However, most authors assume *-categories to have additional properties, such as enrichment in complex vector spaces, existence of square roots, etc., which we do not assume here.

2.2 Dagger compact closed categories

Definition 2.3 (dagger compact closed category) A *dagger compact closed category* is a compact closed category with a dagger structure, such that the functor $\dagger : \mathbf{C}^{op} \to \mathbf{C}$ is a functor of compact closed categories.

Concretely, the requirement that $\dagger$ is a functor of compact closed categories means that the structural natural isomorphisms $\alpha_{A,B,C} : A\otimes(B\otimes C) \to (A\otimes B)\otimes C$, $\lambda_A : I \otimes A \to A$, and $\sigma_{A,B} : B \otimes A \to A \otimes B$ are unitary, and that $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ and $\epsilon_A^\dagger = \sigma_{A^*,A} \circ \eta_A : I \to A \otimes A^*$.

The category **FdHilb** of finite dimensional Hilbert spaces is dagger compact closed.

Remark 2.4 The importance of dagger compact closed categories for the purpose of studying quantum protocols was discovered by Abramsky and Coecke, who used the term "strongly compact closed categories" [1]. The concept of a strict dagger compact closed category itself is older; it appears in the work of Baez and Dolan [2], where it is the special case for $n = 1$ and $k = 3$ of a "k-tuply monoidal n-categories with duals".

2.3 †-Biproducts

Recall that a category has biproducts if there is a zero object $\mathbf{0}$, and if for any A_1, A_2, there is an object $A_1 \oplus A_2$, with projections $p_i : A_1 \oplus A_2 \to A_i$ and injections $q_i : A_i \to A_1 \oplus A_2$, for $i = 1, 2$, such that the pair p_1, p_2 forms a product cone, the pair q_1, q_2 forms a coproduct cone, and $p_i \circ q_j = \delta_{ij}$. Here, $\delta_{ii} = \mathrm{id}_{A_i}$, and $\delta_{ij} = 0$ for $i \neq j$ (where $0 : A_j \to A_i$ is the unique morphism that factors through $\mathbf{0}$).

Definition 2.5 (†-biproduct, biproduct dagger category) Let $\mathbf{C}$ be a category with biproducts and a dagger structure. We say that the biproducts are *†-biproducts* if $p_i^\dagger = q_i : A_i \to A_1 \oplus A_2$, for all objects A_1, A_2 and $i = 1, 2$. A dagger category with †-biproducts is also called a *biproduct dagger category*. A dagger compact closed category with †-biproducts is also called a *biproduct dagger compact closed category*.

Remark 2.6 In any dagger category, products are automatically coproducts by duality. Indeed, if $A_1 \oplus A_2$ is a product with projections $p_i : A_1 \oplus A_2 \to A_i$, then $A_1 \oplus A_2$ is a coproduct with injections defined as $q_i := p_i^\dagger$. However, this is not

quite sufficient to imply that $\mathbf{C}$ has biproducts; the condition $p_i \circ q_j = \delta_{ij}$ is not redundant.

3 Idempotents in dagger categories

3.1 Idempotents

We briefly recall some standard properties of idempotents and their splittings.

Definition 3.1 (idempotent, splitting) A morphism $e : A \to A$ in a category is *idempotent* if $e \circ e = e$. We say that e *splits* if there exists an object B and morphisms $f : A \to B$, $g : B \to A$, such that $e = g \circ f$ and $\mathrm{id}_B = f \circ g$.

Lemma 3.2 *If an idempotent $e : A \to A$ splits, then the splitting is uniquely determined up to isomorphism. More precisely, if $f : A \to B$, $g : B \to A$ and $f' : A \to B'$, $g' : B' \to A$ are two splittings of e, then there exists a unique isomorphism $\varphi : B \to B'$ such that:*

$$\begin{tikzcd} & B \arrow[dr, "g"] \arrow[dd, "\varphi"] & \\ A \arrow[ur, "f"] \arrow[dr, "f'"'] & & A \\ & B' \arrow[ur, "g'"'] & \end{tikzcd}$$

It is well-known that splittings of idempotents can be added freely to a category:

Definition 3.3 (Karoubi envelope) Let $\mathbf{C}$ be a category and $\mathcal{I}$ a class of idempotents, containing all the identity morphism of $\mathbf{C}$. The category $\mathbf{Split}_{\mathcal{I}}(\mathbf{C})$ has objects (A, e), where $A \in |\mathbf{C}|$, $e : A \to A$, and $e \in \mathcal{I}$. A morphism $f : (A, e) \to (B, d)$ is $f : A \to B$ where $f = d \circ f \circ e$. Note that the identity morphism at (A, e) is given by e. If $\mathcal{I}$ is the class of *all* idempotents of $\mathbf{C}$, then $\mathbf{Split}_{\mathcal{I}}(\mathbf{C})$ is called the *Karoubi envelope* of $\mathbf{C}$, and is also written $\mathbf{Split}(\mathbf{C})$.

There is an obvious full embedding $\mathbf{C} \hookrightarrow \mathbf{Split}_{\mathcal{I}}(\mathbf{C})$, defined by $A \mapsto (A, \mathrm{id}_A)$. It is well-known that $\mathbf{Split}_{\mathcal{I}}(\mathbf{C})$ is the category obtained from $\mathbf{C}$ by freely splitting the idempotents in $\mathcal{I}$.

Remark 3.4 The splitting of an idempotent is a special case of a categorical limit and colimit. More precisely, if $e : A \to A$ is an idempotent, then $f : A \to B$, $g : B \to A$ is a splitting of e if and only if f is a colimit and g is a limit of the diagram

$$\begin{tikzcd} A \arrow[loop right, "e"] \end{tikzcd}$$

Remark 3.5 (Idempotents as data types) It is well-known in computer science that idempotents represent *properties* of data, and their splittings correspond to implementations of new data types as subsets of existing ones. We briefly recall this in an example. In a programming language with a built-in type of (positive or negative) integers $\mathbb{Z}$, one would typically implement the type of (non-negative) natural numbers as a subset of the integers. Programs on natural numbers are really programs on integers, but follow a special convention (namely, their possible inputs and outputs are restricted to the natural numbers). Note that the cooperation of the program is required to ensure that it follows the convention. One way to force the convention on an un-cooperating program is to pre- and post-compose it with a special "type checker" function $e : \mathbb{Z} \to \mathbb{Z}$ that "coerces" illegal values to legal ones. One such possible function is $e(n) = n$ if $n \geqslant 0$, and $e(n) = 0$ if $n < 0$. Note that e is idempotent. Now some given function $f : \mathbb{Z} \to \mathbb{Z}$ can be regarded as acting on natural numbers precisely if $e \circ f \circ e = f$. In other words, the data type of natural numbers arises as the splitting of the idempotent e, and moreover, the idempotent itself gives an operational meaning to the data type.

3.2 †-Idempotents

Definition 3.6 (†-idempotent, †-splitting) In a dagger category, a †-idempotent is a self-adjoint idempotent, i.e., a morphism satisfying $e \circ e = e$ and $e = e^\dagger$. We say that e *†-splits* if there exists an object B and morphisms $f : A \to B$, $g : B \to A$, such that $e = g \circ f$, $\mathrm{id}_B = f \circ g$, and $g = f^\dagger$.

Lemma 3.7 *Every †-idempotent is positive, because $e = e \circ e = e^\dagger \circ e$. Also, if e is any idempotent, and e †-splits, then $e = f^\dagger \circ f = e^\dagger$, so e is †-idempotent.*

Example 3.8 In the dagger category **FdHilb**, the †-idempotents are precisely the *orthogonal projections* onto some subspace.

Remark 3.9 By Lemma 3.2, splittings of idempotents are unique up to isomorphism. However, not every splitting of a †-idempotent is a †-splitting. For example, let $e : \mathbb{C}^2 \to \mathbb{C}^2$ be the projection given by $e(x, y) = (x, 0)$. Then e †-splits as $f(x, y) = x$, $g(x) = (x, 0)$. But e also has other, non-dagger splittings, for example, $f'(x, y) = 2x$, $g'(x) = (x/2, 0)$. Also note that in this example, the unique map φ from Lemma 3.2 is $\varphi(x) = 2x$, which is an isomorphism, but not unitary.

Lemma 3.10 *†-Splittings are uniquely determined up to unitary isomorphism. More precisely, let $e = f^\dagger \circ f = g^\dagger \circ g : A \to A$, where $f \circ f^\dagger = \mathrm{id}_B$ and $g \circ g^\dagger = \mathrm{id}'_B$, and let $\varphi : B \to B'$ be the unique isomorphism making the following diagram commute:*

$$\begin{tikzcd}
 & B \arrow[dr, "f^\dagger"] \arrow[dd, "\varphi"] & \\
A \arrow[ur, "f"] \arrow[dr, "g"'] & & A \\
 & B' \arrow[ur, "g^\dagger"'] &
\end{tikzcd}$$

Then φ is unitary.

Proof. We have $\varphi = \varphi \circ f \circ f^\dagger = g \circ f^\dagger$, and similarly $\varphi^{-1} = \varphi^{-1} \circ g \circ g^\dagger = f \circ g^\dagger$. Hence $\varphi^{-1} = \varphi^\dagger$ as desired. □

Remark 3.11 In general, the Karoubi envelope of a dagger category **C** is not a dagger category. Consider for example the category **C** whose objects are finite sets, and whose morphisms $f : A \to B$ are pairs of functions $f_1 : A \to B$ and $f_2 : B \to A$. This has an obvious dagger structure via $(f_1, f_2)^\dagger = (f_2, f_1)$. Let $A = \{0, 1\}$ be a two-element set, and consider $e : A \to A$ given by $e(x) = 0$. Then $X = (A, (e, \mathrm{id}_A))$ and $Y = (A, (\mathrm{id}_A, e))$ are objects of $\mathbf{Split}(\mathbf{C})$. It is easy to check that the cardinalities of $\hom(X, Y)$ and $\hom(Y, X)$ are 4 and 1, respectively, proving that $\mathbf{Split}(\mathbf{C})$ can have no dagger structure.

However, everything goes well if we restrict ourselves to †-idempotents.

Proposition 3.12 *Let **C** be a dagger category, and let $\mathcal{I}$ be a class of †-idempotents, containing all the identity morphism of **C**. Then $\mathbf{Split}_{\mathcal{I}}(\mathbf{C})$ possesses a natural dagger structure.*

Proof. Given a morphism $g : (A, e) \to (B, d)$ of $\mathbf{Split}_{\mathcal{I}}(\mathbf{C})$, define its adjoint as $g^\dagger : B \to A$. Note that this is a well-defined morphism $g^\dagger : (B, d) \to (A, e)$, because $e \circ g^\dagger \circ d = e^\dagger \circ g^\dagger \circ d^\dagger = (d \circ g \circ e)^\dagger = g^\dagger$. Further, this assignment is involutive and functorial. □

Note that the embedding $\mathbf{C} \hookrightarrow \mathbf{Split}_{\mathcal{I}}(\mathbf{C})$ preserves the dagger structure. Moreover, every $e \in \mathcal{I}$ †-splits in $\mathbf{Split}_{\mathcal{I}}(\mathbf{C})$, and $\mathbf{Split}_{\mathcal{I}}(\mathbf{C})$ is the free category with this property.

Definition 3.13 (†-Karoubi envelope) If $\mathcal{I}$ is the class of all †-idempotents of a dagger category **C**, then $\mathbf{Split}_{\mathcal{I}}(\mathbf{C})$ is called the *†-Karoubi envelope* of **C**, and is also written $\mathbf{Split}^\dagger(\mathbf{C})$.

3.3 Operations on †-idempotents

Lemma 3.14 *(a) If $e : A \to A$ and $d : B \to B$ are †-idempotents in a dagger compact closed category, then so are $e \otimes d : A \otimes B \to A \otimes B$ and $e^* : A^* \to A^*$.*

(b) If $e : A \to A$ and $d : B \to B$ are †-idempotents in a biproduct dagger category, then so is $e \oplus d : A \oplus B \to A \oplus B$.

Proof. Obvious. □

The following lemma makes sense in a commutative-monoid enriched category. Recall that a category is *enriched in commutative monoids* if each hom-set is equipped with a commutative, associative addition operation with unit, such that composition is bilinear. In the case of a dagger category, we also require the enrichment to satisfy $(f + g)^\dagger = f^\dagger + g^\dagger$ (and therefore, $0^\dagger = 0$).

Lemma 3.15 *Suppose **C** is a dagger category enriched in commutative monoids. Then $0 : A \to A$ is †-idempotent. Also, if $e, d : A \to A$ are †-idempotents such that $e \circ d = 0$, then $e + d : A \to A$ is †-idempotent.*

Proof. First, note that $d \circ e = d^\dagger \circ e^\dagger = (e \circ d)^\dagger = 0^\dagger = 0$. Then $(e + d) \circ (e + d) = e \circ e + e \circ d + d \circ e + d \circ d = e + 0 + 0 + d = e + d$. Also, $e + d$ is self-adjoint. □

3.4 Structures preserved by the †-Karoubi envelope

The splitting of idempotents preserves all the structure that we are interested in, as the following proposition shows.

Proposition 3.16 *Let **C** be a dagger category, and consider its †-Karoubi envelope $\mathbf{Split}^\dagger(\mathbf{C})$.*

*(a) If **C** is enriched in commutative monoids (as a dagger category), then so is $\mathbf{Split}^\dagger(\mathbf{C})$.*

(b) If **C** *is dagger compact closed, then so is* $\mathbf{Split}^\dagger(\mathbf{C})$.

(c) If **C** *has* †*-biproducts, then so does* $\mathbf{Split}^\dagger(\mathbf{C})$.

Proof. (a) Consider objects $\boldsymbol{A} = (A, a)$, $\boldsymbol{B} = (B, b)$ of $\mathbf{Split}^\dagger(\mathbf{C})$, and morphisms $f, g : \boldsymbol{A} \to \boldsymbol{B}$. Then $b \circ (f+g) \circ a = (b \circ f \circ a) + (b \circ g \circ a) = f + g$, hence $f + g : \boldsymbol{A} \to \boldsymbol{B}$ is well-defined. Also, clearly $b \circ 0 \circ a = 0$, so $0 : \boldsymbol{A} \to \boldsymbol{B}$.

(b) Let $\boldsymbol{A} = (A, a)$, $\boldsymbol{B} = (B, b)$, and $\boldsymbol{C} = (C, c)$. Define $\boldsymbol{A} \otimes \boldsymbol{B} = (A \otimes B, a \otimes b)$, $\boldsymbol{A}^* = (A^*, a^*)$, and $\boldsymbol{I} = (I, \mathrm{id})$. These are well-defined objects by Lemma 3.14(a). For $f : \boldsymbol{A} \to \boldsymbol{A}'$ and $g : \boldsymbol{B} \to \boldsymbol{B}'$, we have $f \otimes g : \boldsymbol{A} \otimes \boldsymbol{B} \to \boldsymbol{A}' \otimes \boldsymbol{B}'$. The structural maps are given by:

$$\begin{aligned}
\alpha_{\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}} &= \alpha_{A,B,C} \circ ((a \otimes b) \otimes c) &&: (\boldsymbol{A} \otimes \boldsymbol{B}) \otimes \boldsymbol{C} \to \boldsymbol{A} \otimes (\boldsymbol{B} \otimes \boldsymbol{C}) \\
\lambda_{\boldsymbol{A}} &= \lambda_A \circ (\mathrm{id} \otimes a) &&: \boldsymbol{I} \otimes \boldsymbol{A} \to \boldsymbol{A} \\
\sigma_{\boldsymbol{A},\boldsymbol{B}} &= \sigma_{A,B} \circ (a \otimes b) &&: \boldsymbol{A} \otimes \boldsymbol{B} \to \boldsymbol{B} \otimes \boldsymbol{A} \\
\eta_{\boldsymbol{A}} &= (a^* \otimes a) \circ \eta_A &&: \boldsymbol{I} \to \boldsymbol{A}^* \otimes \boldsymbol{A} \\
\epsilon_{\boldsymbol{A}} &= \epsilon_A \circ (a \otimes a^*) &&: \boldsymbol{A} \otimes \boldsymbol{A}^* \to \boldsymbol{I}
\end{aligned}$$

It is then routine to check that these are indeed well-defined, natural, satisfy the coherence conditions, and respect the dagger structure.

(c) For $\boldsymbol{A}_1 = (A_1, a_1)$ and $\boldsymbol{A}_2 = (A_2, a_2)$, define $\boldsymbol{A}_1 \oplus \boldsymbol{A}_2 = (A_1 \oplus A_2, a_1 \oplus a_2)$. This is a well-defined object by Lemma 3.14(b). The structural maps are given by:

$$\begin{aligned}
\boldsymbol{p}_i &= a_i \circ p_i : \boldsymbol{A}_1 \oplus \boldsymbol{A}_2 \to \boldsymbol{A}_i \\
\boldsymbol{q}_i &= q_i \circ a_i : \boldsymbol{A}_i \to \boldsymbol{A}_1 \oplus \boldsymbol{A}_2
\end{aligned}$$

The required properties are checked routinely. □

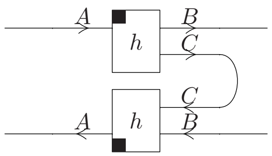
4 Idempotents and the CPM-construction

4.1 Complete positivity

Let **C** be a dagger compact closed category. Recall from [6] that a morphism $f : A^* \otimes A \to B^* \otimes B$ is called *completely positive* if there exists an object C and a morphism $h : A \to C \otimes B$ such that

$$f = A^* \otimes A \xrightarrow{h_* \otimes h} B^* \otimes C^* \otimes C \otimes B \xrightarrow{B^* \otimes \epsilon_{C^*} \otimes B} B^* \otimes I \otimes B \xrightarrow{\cong} B^* \otimes B.$$

In the graphical language of [6], a positive map can be visualized as follows:

$f \quad =$ 

Selinger

Definition 4.1 (CPM construction) Let **C** be a dagger compact closed category. Its *category of completely positive maps*, written **CPM(C)**, is defined as follows: it has the same objects as **C**, and a morphism $f : A \to B$ in **CPM(C)** is a completely positive morphism $f : A^* \otimes A \to B^* \otimes B$ in **C**.

Theorem 4.2 ([6]) *If* **C** *is dagger compact closed, then so is* **CPM(C)**. □

The category **CPM(FdHilb)** appears in the interpretation of quantum programming languages as the category of “simple” signatures and completely positive maps, cf. [5, Sec. 6.1 and Rem. 6.9]. Concretely, this means that its objects represent purely quantum types such as **qbit** and **qbit** ⊗ **qbit**. However, in the semantics of quantum programming language, one also requires types with *classical* attributes. These appear as direct sums $A_1 \oplus \ldots \oplus A_n$ of quantum types. The interpretation of programming languages, as described in [5], thus takes place not in **CPM(FdHilb)**, but in its *free biproduct completion* $\mathbf{CPM}(\mathbf{FdHilb})^\oplus$.

Definition 4.3 (CPM construction with biproducts) Let **C** be a biproduct dagger compact closed category. Then $\mathbf{CPM}(\mathbf{C})^\oplus$ is defined as the biproduct completion of **CPM(C)**. Concretely, the objects of $\mathbf{CPM}(\mathbf{C})^\oplus$ are finite sequences $(A_1, \ldots, A_n)$ of objects of **C**, and a morphism $f : (A_i)_i \to (B_j)_j$ is a matrix $(f_{ij})_{ij}$, where each $f_{ij} : A_i \to B_j$ is a morphism of **CPM(C)**. Composition is defined in the usual way by matrix multiplication.

Note the difference between the object (A, B), which is the biproduct of A and B in $\mathbf{CPM}(\mathbf{C})^\oplus$, and the object $A \oplus B$, which is the biproduct of A and B in **C**. These objects are not isomorphic. The operation $A \oplus B$ is not a biproduct in **CPM(C)**; in fact, it is not even functorial there.

4.2 Classical types as idempotents

In the previous section, classical types were added to **CPM(C)** by taking its biproduct completion. We now show that there is an alternative method for completing **CPM(C)** with classical types, namely by splitting idempotents. In light of Remark 3.5, this gives an operational interpretation and an implementation of the type of classical bits in terms of quantum bits.

Example 4.4 In the category $\mathbf{CPM}(\mathbf{FdHilb})^\oplus$, the type **qbit** of quantum bits corresponds to the object $\mathbb{C}^2$, and the type **bit** of classical bits corresponds to the object $I \oplus I = (\mathbb{C}, \mathbb{C})$. The are related by completely positive maps **new** : **bit** → **qbit** (for creating a new quantum bit) and **measure** : **qbit** → **bit** (for measuring a quantum bit). In the notation of [5], these maps are defined as:

$$\mathbf{new}(a, d) = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \qquad \mathbf{measure}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a, d)$$

These two maps are each other's adjoints: $\mathbf{new}^\dagger = \mathbf{measure}$. They are also onesided inverses, and therefore form a splitting of a †-idempotent as follows:

$$\begin{tikzcd} \mathbf{bit} \arrow[d, "\mathbf{new}"'] \arrow[dr, "\mathrm{id}"] & \\ \mathbf{qbit} \arrow[r, "\mathbf{measure}"'] & \mathbf{bit} \end{tikzcd} \qquad \begin{tikzcd} \mathbf{qbit} \arrow[r, "\mathbf{measure}"] \arrow[dr, "e"'] & \mathbf{bit} \arrow[d, "\mathbf{new}"] \\ & \mathbf{qbit} \end{tikzcd}$$

Therefore, the type **bit** arises by splitting the †-idempotent $e = \mathbf{new} \circ \mathbf{measure}$ on the type **qbit**.

The following theorem shows that Example 4.4 generalizes from the type **bit** to arbitrary types.

Theorem 4.5 *Let* $\mathbf{C}$ *be a biproduct dagger category, and consider its category of completely positive maps* $\mathbf{CPM}(\mathbf{C})$*. Then the †-Karoubi envelope* $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$ *has finite †-biproducts.*

Proof. The zero object $\mathbf{0}$ of $\mathbf{C}$ also acts as a zero object in $\mathbf{CPM}(\mathbf{C})$, and hence $(\mathbf{0}, \mathrm{id})$ is a zero object in $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$. Therefore, we only have to show that $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$ has binary biproducts. Consider two objects (A_1, e_1) and (A_2, e_2) of $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$. Therefore $e_i : A_i^* \otimes A_i \to A_i^* \otimes A_i$ is completely positive and †-idempotent in $\mathbf{C}$, for $i = 1, 2$. Let $D = A_1 \oplus A_2$ in $\mathbf{C}$, and define $d_i : D^* \otimes D \to D^* \otimes D$ by:

$$d_i = D^* \otimes D \xrightarrow{p_{i*} \otimes p_i} A_i^* \otimes A_i \xrightarrow{e_i} A_i^* \otimes A_i \xrightarrow{q_{i*} \otimes q_i} D^* \otimes D.$$

Here, $p_i : A_1 \oplus A_2 \to A_i$ and $q_i : A_i \to A_1 \oplus A_2$ are the projections and co-projections from the biproduct structure of $\mathbf{C}$. Finally, let $d = d_1 + d_2$. We claim that (D, d) is the biproduct of (A_1, e_1) and (A_2, e_2) in $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$.

First, it is immediate from the definitions that d_i is completely positive and †-idempotent; moreover, $d_1 \circ d_2 = 0$. Therefore, $d = d_1 + d_2$ is †-idempotent by Lemma 3.15, and completely positive by [6, Lemma 5.2]. Therefore, (D, d) is a well-defined object of $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$.

To prove that it is the desired †-biproduct, we define the following morphisms in $\mathbf{CPM}(\mathbf{C})$, for $i = 1, 2$:

$$\begin{aligned} P_i &= D^* \otimes D \xrightarrow{p_{i*} \otimes p_i} A_i^* \otimes A_i \xrightarrow{e_i} A_i^* \otimes A_i, \\ Q_i &= A_i^* \otimes A_i \xrightarrow{e_i} A_i^* \otimes A_i \xrightarrow{q_{i*} \otimes q_i} D^* \otimes D. \end{aligned}$$

Then $e_i \circ P_i \circ d = P_i$ and $d \circ Q_i \circ e_i = Q_i$, hence $P_i : (D, d) \to (A_i, e_i)$ and $Q_i : (A_i, e_i) \to (D, d)$ are well-defined morphisms of $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$. Since $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$ already possesses a commutative-monoid enrichment by Proposition 3.16(a), to show that these maps define a †-biproduct structure, it suffices to show that $P_i = Q_i^\dagger$, $P_i \circ Q_i = \mathrm{id}_{(A_i, e_i)} = e_i$, $P_i \circ Q_j = 0$ for $i \neq j$, and $(Q_1 \circ P_1) + (Q_2 \circ P_2) = \mathrm{id}_{(D,d)} = d$. All of these properties follow directly from the definitions. □

Corollary 4.6 *If* $\mathbf{C}$ *be a biproduct dagger compact closed category, then so is* $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$.

Proof. From Proposition 3.16(b), Theorem 4.2, and Theorem 4.5. □

Corollary 4.7 *There is a canonical full embedding*

$$\mathbf{CPM}(\mathbf{C})^\oplus \hookrightarrow \mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C})).$$

Proof. By the fact that $\mathbf{CPM}(\mathbf{C})$ is fully embedded in $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{C}))$, together with the universal property of $\mathbf{CPM}(\mathbf{C})^\oplus$. □

Remark 4.8 The last corollary means that every classical data type, and indeed every combined classical/quantum type, can be obtained by splitting an idempotent on a purely quantum type. In light of the fact that the splitting of an idempotent is a special case of a categorical limit (cf. Remark 3.4), this lends a new meaning to the phrase "classical objects arise as limits of quantum objects".

Remark 4.9 In the case where $\mathbf{C} = \mathbf{FdHilb}$, it is an open problem whether the embedding of Corollary 4.7 is an equivalence of categories. Equivalently, it is not known whether the results of splitting †-idempotents in $\mathbf{CPM}(\mathbf{FdHilb})$ are *precisely* the classical and quantum types, or whether there are additional objects in $\mathbf{Split}^\dagger(\mathbf{CPM}(\mathbf{FdHilb}))$ that are neither classical nor quantum. The latter possibility seems highly unlikely for physical reasons, as there is no evidence in nature of a "third possibility" between classical and quantum phenomena. However, we do not currently have a proof of this.

5 More properties of †-idempotents

In this section, we explore some further technical properties of †-idempotents. For example, we address questions such as: is a †-idempotent uniquely determined by its image? If a †-idempotent splits, then does it †-split? The reader who is not very interested in technical details is advised to skip this section.

5.1 Isometries as †-subobjects

Definition 5.1 (isometry) A morphism $f : A \to B$ in a dagger category is an *isometry* if $f^\dagger \circ f = \mathrm{id}_A$.

Note that an isometry $f : A \to B$ is necessarily monic; we can think of it as a special kind of subobject of B, namely, one that arises from splitting a †-idempotent $f \circ f^\dagger$ on B. We also call f (and sometimes by abuse of terminology, A) a *†-subobject* of B.

Example 5.2 In the category $\mathbf{FdHilb}$, the isometries are precisely the linear functions $f : A \to B$ that are one-to-one and preserve the inner product.

Lemma 5.3 *A morphism* $f : A \to B$ *is unitary if and only if it is an isometry and an isomorphism.* □

Isometries share many of the common properties of monomorphisms, for example the following:

Lemma 5.4 *Suppose f is an isometry and $f \circ g = h$. Then h is an isometry if and only if g is an isometry.*

Proof. Suppose h is an isometry. Then $g^\dagger \circ g = g^\dagger \circ f^\dagger \circ f \circ g = h^\dagger \circ h = \mathrm{id}$, so g is an isometry. Conversely, suppose g is an isometry. Then $h^\dagger \circ h = g^\dagger \circ f^\dagger \circ f \circ g = g^\dagger \circ g = \mathrm{id}$, so h is an isometry. $\square$

We may ask whether every subobject is isomorphic to a †-subobject. For example, this is true in **FdHilb**, because every monic in this category has a subspace as its image, and is isomorphic, as a subobject, to the subspace inclusion. However, this property is false in a general dagger category, as the following counterexample shows.

Example 5.5 Let **Z** be the dagger compact closed category consisting of a single object $\bullet$, and where the morphisms are the integers $n \in \mathbb{Z}$. Composition and tensor product of morphisms are defined by multiplication $n \circ m = n \otimes m = nm$, and $n^\dagger = n$. Note that all non-zero morphisms are monic, but the only isometries are ± 1, which are also the only isomorphisms. So, for example, $2 : \bullet \to \bullet$ is a subobject not isomorphic to a †-subobject.

Similar, but less degenerate examples are the dagger compact closed categories of free modules over the ring $\mathbb{Z}$ (or over the Gaussian integers $\mathbb{Z} + i\mathbb{Z}$, or over the rig $\mathbb{N}$).

The following proposition characterizes exactly when a given subobject is isomorphic to a †-subobject.

Proposition 5.6 *Let $f : A \to B$ be monic. The following are equivalent:*

(1) f, as a subobject, is isomorphic to a †-subobject, i.e., there exists an isomorphism $\varphi : A \to A'$ and an isometry $g : A' \to B$ such that $f = g \circ \varphi$.

(2) There exists an object A' and an isomorphism $\varphi : A \to A'$ such that $f^\dagger \circ f = \varphi^\dagger \circ \varphi$.

Proof. First, assume (1). Since g is an isometry, we have $g^\dagger \circ g = \mathrm{id}_{A'}$, hence $f^\dagger \circ f = \varphi^\dagger \circ g^\dagger \circ g \circ \varphi = \varphi^\dagger \circ \varphi$, therefore (2) holds. Conversely, assume (2) and let $g = f \circ \varphi^{-1}$. Then $g^\dagger \circ g = \varphi^{-1\dagger} \circ f^\dagger \circ f \circ \varphi^{-1} = \varphi^{-1\dagger} \circ \varphi^\dagger \circ \varphi \circ \varphi^{-1} = \mathrm{id}_{A'}$, therefore g is an isometry and (1) holds. $\square$

5.2 The image of a †-idempotent

Every †-idempotent $e : B \to B$ induces a canonical subobject of (B, id) in $\mathbf{Split}^\dagger(\mathbf{C})$, namely $e : (B, e) \to (B, \mathrm{id})$. We call this subobject the *image* of e. An object [unitarily] isomorphic to the image already exists in **C** if and only if e [†-]splits in **C**.

Definition 5.7 (ordering of idempotents) Given two idempotents $e, d : B \to B$, we write $e \leqslant d$ if the image of e is contained in the image of d as subobjects of (B, id). This is the case if and only if $d \circ e = e$.

Proposition 5.8 *†-Idempotents are uniquely determined by their image. Concretely, if $e, d : B \to B$ are †-idempotents such that $d \leqslant e$ and $e \leqslant d$, then $d = e$. The corresponding property of (non-†) idempotents is not true.*

Proof. Under the given hypotheses, $d = d^\dagger = (e \circ d)^\dagger = d^\dagger \circ e^\dagger = d \circ e = e$. The corresponding property for (non-†) idempotents already fails in the category of sets; for example, there are two different idempotents $e, d : \{1,2,3\} \to \{1,2,3\}$ with image $\{1,2\}$. $\square$

Corollary 5.9 *The †=idempotents on a given object are partially ordered by $\leqslant$.* $\square$

The partial order $\leqslant$ is an abstract analogue to the usual Birkhoff-von Neumann lattice of projections on a Hilbert space. However, it need not in general be a lattice.

One may ask for the converse of Proposition 5.8: does every monomorphism $f : A \to B$ arise as the image of some †-idempotent. This is true, for example, in **FdHilb**, but fails in the categories from Example 5.5. The following proposition characterizes precisely which monics are the images of †-idempotents.

Proposition 5.10 *Let $f : A \to B$ be a monic. The following are equivalent:*

(1) There exists some †-idempotent $e : B \to B$ (necessarily unique by Proposition 5.8) such that (A, id) and (B, e) are isomorphic as subobjects of (B, id) in $\mathbf{Split}^\dagger(\mathbf{C})$.

(2) $f^\dagger \circ f$ is invertible.

Proof. First, assume (1) holds. Let $\varphi : (A, \mathrm{id}) \to (B, e)$ be the isomorphism, with inverse $\psi : (B, e) \to (A, \mathrm{id})$. Then by assumption, $e \circ \varphi = f$. Also, since φ is a morphism of $\mathbf{Split}^\dagger(\mathbf{C})$, $e \circ \varphi = \varphi$, therefore $\varphi = f$. The fact that f and ψ are inverses in $\mathbf{Split}^\dagger(\mathbf{C})$ means that $\psi \circ f = \mathrm{id}_A$ and $f \circ \psi = e$ in **C**. Also, since e is self-adjoint, $\psi^\dagger \circ f^\dagger = e^\dagger = e$. Then $f^\dagger \circ f \circ \psi \circ \psi^\dagger = f^\dagger \circ e \circ \psi^\dagger = f^\dagger \circ \psi^\dagger \circ f^\dagger \circ \psi^\dagger = \mathrm{id}_A$. Also $\psi \circ \psi^\dagger \circ f^\dagger \circ f = \psi \circ e \circ f = \psi \circ f \circ \psi \circ f = \mathrm{id}_A$. Therefore, $f^\dagger \circ f$ is invertible with inverse $\psi \circ \psi^\dagger$, proving (2).

Conversely, assume (2), and let $k = (f^\dagger \circ f)^{-1}$. Define $g = k \circ f^\dagger$. Then $g \circ f = \mathrm{id}_A$, therefore $f \circ g : B \to B$ is idempotent. Further, $f \circ g$ is self-adjoint. Let $e = f \circ g$. Then the following diagram is well-defined and commutes in $\mathbf{Split}^\dagger(\mathbf{C})$, proving (2).

$$
\begin{tikzcd}
(B, e) \arrow[dr, "e"] \arrow[d, bend right, "g"'] & \\
(A, \mathrm{id}) \arrow[u, bend right, "f"'] \arrow[r, "f"'] & (B, \mathrm{id})
\end{tikzcd}
$$

$\square$

5.3 Splitting vs. †-splitting

Suppose that $e : B \to B$ is a †-idempotent, and also assume that e splits. Can one conclude that e †-splits? This is another example of a property that is true in **FdHilb**, but is false in general. For example, it fails in Hilbert spaces over the rational complex field, where all idempotents split, but for example the †-idempotent

$$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

does not †-split. It turns out that this question is closely related to the equivalent properties of Proposition 5.6. This is made precise in the following.

Proposition 5.11 *Let $e : B \to B$ is a †-idempotent, and suppose that e splits via $h : B \to A$, $f : A \to B$. Then e †-splits if and only if f satisfies the equivalent conditions of Proposition 5.6.*

Proof. First, suppose that e †-splits as $e = g \circ g^\dagger$, where $g^\dagger \circ g = \mathrm{id}_C$. Then g is an isometry. Also, by uniqueness of splittings (see Lemma 3.2), there exists an isomorphism $\varphi : A \to C$ such that $f = g \circ \varphi$. Therefore, f satisfies condition (1). Conversely, suppose that f satisfies (1), so that $f = g \circ \varphi$ for some isometry g and isomorphism φ. We claim that $g \circ g^\dagger = e$. Indeed, $g^\dagger \circ f = g^\dagger \circ g \circ \varphi = \varphi$. Therefore $h^\dagger \circ \varphi^\dagger \circ \varphi = h^\dagger \circ f^\dagger \circ g \circ g^\dagger \circ f = e^\dagger \circ g \circ g^\dagger \circ f = e \circ g \circ g^\dagger \circ g \circ \varphi = e \circ g \circ \varphi = e \circ f = f \circ h \circ f = f$. Therefore $g \circ g^\dagger = f \circ \varphi^{-1} \circ \varphi^{-1\dagger} \circ f^\dagger = h^\dagger \circ \varphi^\dagger \circ \varphi \circ \varphi^{-1} \circ \varphi^{-1\dagger} \circ f^\dagger = h^\dagger \circ \varphi^\dagger \circ \varphi^{-1\dagger} \circ f^\dagger = h^\dagger \circ f^\dagger = e^\dagger = e$. Therefore e †-splits. □

5.4 *The square root axiom*

Recall that a morphism $f : A \to A$ in a dagger category is called *positive* if there exists some object B and some $g : A \to B$ such that $f = g^\dagger \circ g$.

Definition 5.12 (square root axiom) We say that a dagger category satisfies the *square root axiom* if every positive $f : A \to A$ has some positive square root $r : A \to A$, with $f = r \circ r$. We say that the *unique square root axiom* is satisfied if r is unique.

The square root axioms does not hold in all dagger categories, but when it holds, it has some useful consequences, such as the following.

Proposition 5.13 *Under the square root axiom, the conditions of Propositions 5.6 and 5.10 are equivalent.*

Proof. Condition (2) of Proposition 5.6 trivially implies condition (2) of Proposition 5.10. The converse uses the square root axiom. Suppose that $f^\dagger \circ f$ is invertible. It is also positive, hence, by the square root axiom, there exists some positive $r : A \to A$ such that $f^\dagger \circ f = r \circ r = r^\dagger \circ r$. Since $r \circ r$ is invertible, so is r (this holds in any category). Therefore condition (2) of Proposition 5.6 is satisfied with $\varphi = r$. □

Proposition 5.14 *In a dagger category satisfying the square root axiom, any two isomorphic objects are unitarily isomorphic.*

Proof. Suppose $f : A \to B$ is an isomorphism. Then $f^\dagger \circ f : A \to A$ is positive, there exists some positive $r : A \to A$ such that $f^\dagger \circ f = r \circ r = r^\dagger \circ r$, and r is invertible. Let $g = f \circ r^{-1}$, then $g : A \to B$ is an isomorphism, and $g \circ g^\dagger =$

$f \circ r^{-1} \circ r^{-1\dagger} \circ f^\dagger = f \circ (r^\dagger \circ r)^{-1} \circ f^\dagger = f \circ (f^\dagger \circ f)^{-1} \circ f^\dagger = \mathrm{id}_B$. Therefore, g is unitary. □

5.5 **CPM(FdHilb)** *does not satisfy the square root axiom*

The unique square root axiom holds in **FdHilb**, and is the reason for many regularity properties of that category. It also has a physical interpretation: If the evolution of nature is broken into discrete time steps, then one can continually half the step size. Nature therefore evolves continuously.

It is perhaps surprising that the square root axiom actually fails in the category **CPM(FdHilb)** of completely positive maps. Here is a counterexample.

$$F\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+d & b \\ c & a+d \end{pmatrix}$$

is completely positive, therefore a morphism $F : \mathbb{C}^2 \to \mathbb{C}^2$ in **CPM(FdHilb)**. Under the forgetful functor **CPM(FdHilb)** $\to$ **FdHilb**, the unique positive square root of F is

$$H\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}(a+d) & b \\ c & \frac{1}{\sqrt{2}}(a+d) \end{pmatrix}.$$

However, the map H is not completely positive, and therefore it is not a morphism of **CPM(FdHilb)**. It follows that F has no positive square root in **CPM(FdHilb)**. On the other hand, F is positive, because $F = G^\dagger \circ G$, where

$$G\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{\sqrt{3}}\begin{pmatrix} a+d & c & b \\ b & a+d & c \\ c & b & a+d \end{pmatrix}$$

It follows that **CPM(FdHilb)** does not satisfy the square root axiom. This fact is perhaps not surprising physically; it seems to suggest that time steps cannot always be halved when evolution proceeds via completely positive maps, and therefore, that time is not as continuous as it is in the unitary case.

6 Conclusion

The category **CPM(FdHilb)** continues to be an interesting object of study. It plays a fundamental role in finite dimensional quantum mechanics, and the basis of denotational semantics of quantum programming languages and protocols. The interplay between classical and quantum entities is particularly interesting, both at the level of morphisms (mixed vs. pure, completely positive vs. unitary) and at the level of objects (tensor vs. biproduct, simple vs. composite).

In this paper, we have made some progress towards understanding the internals of this category, by showing that classical data types can be identified with certain self-adjoint idempotents on purely quantum types. To this end, we have studied the theory of self-adjoint idempotents and their splittings in the setting of dagger categories. It turns out that many of the properties familiar from projections in Hilbert spaces are true in this more general setting. However, there are important differences; for example, properties that rely on the square root axiom will be true in **FdHilb**, but not necessarily in **CPM**(**FdHilb**), where the square root axiom has been demonstrated to fail.

As mentioned in the introduction, this work was partly inspired by the work of Coecke and Pavlovic [3], who have given another method of deriving classical types from quantum ones. In both approaches, classical types are described as quantum types equipped with additional structure; in the present work, this additional structure is given by an idempotent, whereas in the work of Coecke and Pavlovic, it is given by copying and deleting operations. The precise technical relationship between these approaches remains to be explored.

References

[1] Abramsky, S. and B. Coecke, *A categorical semantics of quantum protocols*, in: *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, LICS 2004*, IEEE Computer Society Press, 2004, pp. 415–425.

[2] Baez, J. C. and J. Dolan, *Higher-dimensional algebra and topological quantum field theory*, Jour. Math. Phys. **36** (1995), pp. 6073–6105, available from arXiv:q-alg/9503002.

[3] Coecke, B. and D. Pavlovic, *Quantum measurements without sums*, in: G. Chen, L. H. Kauffman and S. J. Lomonaco, editors, *Mathematics of Quantum Computing and Technology*, Taylor and Francis, 2006 To appear.

[4] Ghez, P., R. Lima and J. E. Roberts, *W^*-categories*, Pacific Journal of Mathematics **120** (1985), pp. 79–109.

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

[6] Selinger, P., *Dagger compact closed categories and completely positive maps*, in: *Proceedings of the 3rd International Workshop on Quantum Programming Languages*, Electronic Notes in Theoretical Computer Science (to appear).