



THE UNIVERSITY *of* EDINBURGH

Edinburgh Research Explorer

Mixed quantum states in higher categories

Citation for published version:

Heunen, C, Vicary, J & Wester, L 2014, Mixed quantum states in higher categories. in *Proceedings QPL 2014*. EPTCS, vol. 172, pp. 304-315. <https://doi.org/10.4204/EPTCS.172.22>

Digital Object Identifier (DOI):

[10.4204/EPTCS.172.22](https://doi.org/10.4204/EPTCS.172.22)

Link:

[Link to publication record in Edinburgh Research Explorer](#)

Published In:

Proceedings QPL 2014

General rights

Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.



Mixed quantum states in higher categories

Chris Heunen

Department of Computer Science,
University of Oxford
chris.heunen@cs.ox.ac.uk *

Jamie Vicary

Centre for Quantum Technologies,
National University of Singapore
Department of Computer Science,
University of Oxford
jamie.vicary@cs.ox.ac.uk

Linde Wester

Department of Computer Science,
University of Oxford
lindewester@gmail.com

There are two ways to describe the interaction between classical and quantum information categorically: one based on completely positive maps between Frobenius algebras, the other using symmetric monoidal 2-categories. This paper makes a first step towards combining the two. The integrated approach allows a unified description of quantum teleportation and classical encryption in a single 2-category, as well as a universal security proof applicable simultaneously to both scenarios.

1 Introduction

In the categorical approach to quantum information [1], there are two main approaches to modelling the interaction between classical and quantum data, which can be summarized as follows:

- Commutative Frobenius algebras model classical data, noncommutative Frobenius algebras model quantum data, completely positive maps model computational processes. The resulting compact category $\text{CP}^*[\mathbf{FHilb}]$, reviewed in Section 1.1, incorporates both pure and mixed states in a single setting, while admitting a graphical calculus [8–11, 13, 14, 16, 21].
- Objects model classical data, 1-morphisms model quantum data, 2-morphisms model computational processes. The resulting symmetric monoidal 2-category, reviewed in Section 1.2, provides universal syntactic models that can encode entire procedures as single equations [4, 19, 22].

This article makes a first step towards combining both approaches while retaining the advantages of each. Section 2 introduces a procedure that turns a suitable symmetric monoidal category \mathbf{C} into a symmetric monoidal 2-category $2[\mathbf{C}]$. It is based on the well-known structure of bimodules and homomorphisms, but with a new definition of bimodule composition in terms of splitting of an idempotent.

Section 3 investigates basic properties of $2[\text{CP}^*[\mathbf{FHilb}]]$. We show that on a large domain, which is sufficient for the intended application to quantum information, the 2-category is well-defined. We also prove the surprising result that every finite groupoid gives rise to an object in $2[\text{CP}^*[\mathbf{FHilb}]]$ in a canonical way, suggesting that the 2-category has a rich structure waiting to be explored.

Finally, Section 4 demonstrates the advantages of our combined approach. We obtain:

- An elegant abstract definition of measurement, that in $2[\text{CP}^*[\mathbf{FHilb}]]$ comes down to the usual mixed-state notion of positive operator-valued measurement.
- A single equation whose solutions in $2[\text{CP}^*[\mathbf{FHilb}]]$ simultaneously include implementations of quantum teleportation and of classical encrypted communication.
- A single proof of security that applies simultaneously to both procedures.

*Supported by the Engineering and Physical Sciences Research Council Fellowship EP/L002388/1.
We thank Aleks Kissinger for useful discussions.

There are several interesting directions for future work:

- How can objects of $2[\text{CP}^*[\mathbf{FHilb}]]$ be classified?
- Is there a direct construction $\mathbf{C} \mapsto \text{Mix}[\mathbf{C}]$ of 2-categories such that $2[\text{CP}^*[\mathbf{C}]] \cong \text{Mix}[2[\mathbf{C}]]$?
- What are nonstandard models such as $2[\text{CP}^*[\mathbf{Rel}]]$ like?
- Are there nonstandard solutions of the teleportation equation in $2[\text{CP}^*[\mathbf{FHilb}]]$, which are neither pure-state quantum teleportation or encrypted communication, but some hybrid process?

1.1 The CP*-construction

Categorical quantum mechanics deals with dagger monoidal categories [1], which admit a graphical calculus; see [18]. Within this well-documented setting, let us very briefly recall the CP* construction from the perspective of [14, Lemma 1.2]; for more details we refer to [10, 14, 16]. This construction turns a dagger compact category \mathbf{C} into a new category $\text{CP}^*[\mathbf{C}]$. An object in $\text{CP}^*[\mathbf{C}]$ is a *special dagger Frobenius algebra* in \mathbf{C} : an object A with morphisms $\circlearrowleft: A \otimes A \rightarrow A$ and $\circlearrowright: I \rightarrow A$ satisfying the *specialness* condition $\circlearrowleft \circ \circlearrowright = \text{id}$, as well as the *dagger Frobenius algebra* laws:

$$\text{Specialness: } \text{dot} \circ \text{loop} = \text{dot} \circ \text{loop} \quad \text{Frobenius: } \text{dot} \circ \text{loop} = \text{line} \circ \text{dot} \quad \text{Frobenius: } \text{dot} \circ \text{loop} = \text{dot} \circ \text{loop} \quad (1)$$

Commutative such objects are also called *classical structures*. A morphism $(A, \circlearrowleft, \circlearrowright) \rightarrow (B, \circlearrowleft, \circlearrowright)$ in $\text{CP}^*[\mathbf{C}]$ is a morphism $f: A \rightarrow B$ in \mathbf{C} satisfying the *complete positivity* condition

$$\text{loop} \circ f = g \circ g^\dagger \quad (2)$$

for some morphism $g: A \otimes B^* \rightarrow X$ in \mathbf{C} . This gives a well-defined dagger compact category $\text{CP}^*[\mathbf{C}]$ with the following basic interpretation:

Category theory	Geometry	Interpretation
Commutative objects	Lines with commutative dots	Classical information
Noncommutative objects	Lines with noncommutative dots	Quantum information
Morphisms	Vertices	Physical operations

The CP*-construction is of fundamental importance because it turns a category of pure states and processes into a category of mixed states: applying the CP*-construction to the category \mathbf{FHilb} of finite-dimensional Hilbert spaces and linear maps results in the category $\text{CP}^*[\mathbf{FHilb}]$ of finite-dimensional C*-algebras and completely positive maps.

1.2 Higher quantum theory

Higher quantum theory [22, 23] separates classical and quantum information by replacing monoidal categories by monoidal weak 2-categories. These also have a graphical notation [15]:

Category theory	Geometry	Interpretation
Objects	Surfaces	Classical information
1-Morphisms	Lines	Quantum systems
2-Morphisms	Vertices	Physical operations

Graphically, composition of 1-morphisms is indicated by horizontal juxtaposition, and composition of 2-morphisms by vertical juxtaposition. The tensor product is given by ‘overlying’ regions one above the other, perpendicular to the plane of the page.

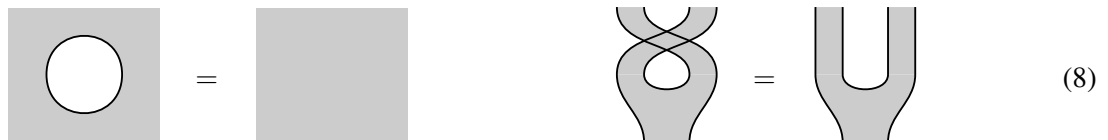
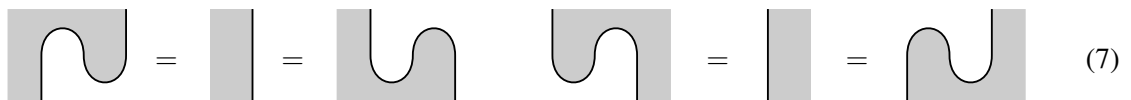
Just like in the 1-categorical case, the diagrams are interpreted as describing sequences of events taking place over time, with time running from bottom to top. A dagger provides a formal time-reversal of 2-morphisms, represented graphically by reflecting a diagram about a horizontal axis.

Definition 1. A *dagger 2-category* is a 2-category equipped with an involutive operation \dagger on 2-morphisms, such that $\mu^\dagger: G \Rightarrow F$ for all $\mu: F \Rightarrow G$, in a way that is functorial and compatible with the rest of the monoidal 2-category structure.

The core theory uses the graphical components summarized below, motivated in detail in [22].



Definition 2. An object in a symmetric monoidal 2-category has a *topological boundary* when it is equipped with data (4)-(6) satisfying the following axioms, which amount to saying that the boundary of a classical system is topological and that holes can be eliminated:



Whenever we make use of the above graphical notation, it is understood that we are depicting an object with topological boundary in a symmetric monoidal dagger 2-category.

2 The $2[-]$ construction

This section introduces a construction that turns a monoidal category \mathbf{C} into a 2-category $2[\mathbf{C}]$, in such a way that $2[\mathbf{CP}^*[\mathbf{C}]]$ has the appropriate structure to express the teleportation equation solely in terms of

objects and morphisms. The idea is to adapt the well-known algebraic construction of rings, bimodules, and bimodule homomorphisms [12]. In Section 2.1 we will see how our construction is defined, and in Section 2.2 we will see that objects in $2[\mathbf{C}]$ have a topological boundary in the sense of Definition 2.

2.1 Bimodules and composition

Definition 3. Let $(C, \lrcorner, \circlearrowleft)$ and $(D, \lrcorner, \circlearrowright)$ be dagger Frobenius algebras in a dagger monoidal category. A *dagger C-D-bimodule* is a morphism \mathbf{M} satisfying:

$$\begin{array}{c}
 \begin{array}{c} M \\ \boxed{\mathbf{M}} \\ \begin{array}{c} \lrcorner \\ \circlearrowleft \end{array} \\ \boxed{\mathbf{M}} \\ \begin{array}{c} \lrcorner \\ \circlearrowright \end{array} \\ C \quad C \quad M \quad D \quad D \end{array} \\
 = \\
 \begin{array}{c} M \\ \boxed{\mathbf{M}} \\ \begin{array}{c} \lrcorner \\ \circlearrowleft \end{array} \\ \begin{array}{c} \circlearrowleft \\ \circlearrowright \end{array} \\ C \quad C \quad M \quad D \quad D \end{array}
 \end{array}
 \quad
 \begin{array}{c}
 \begin{array}{c} M \\ \boxed{\mathbf{M}} \\ \begin{array}{c} \lrcorner \\ \circlearrowleft \end{array} \\ M \end{array} \\
 = \\
 \begin{array}{c} M \\ \boxed{\mathbf{M}^\dagger} \\ \begin{array}{c} \lrcorner \\ \circlearrowright \end{array} \\ M \end{array} \\
 = \\
 \begin{array}{c} C \quad M \quad D \\ \begin{array}{c} \lrcorner \\ \circlearrowleft \end{array} \\ \boxed{\mathbf{M}} \\ \begin{array}{c} \lrcorner \\ \circlearrowright \end{array} \\ C \quad M \quad D \end{array}
 \end{array}
 \quad (9)$$

We also call the object M the bimodule, and the map \mathbf{M} its *action*, and write $\mathbf{M}_\bullet = \mathbf{M}(\lrcorner \mid \bullet)$ and $\circlearrowleft \mathbf{M} = \mathbf{M}(\bullet \mid \lrcorner)$. A *homomorphism* of dagger C - D -bimodules is a morphism $f: M \rightarrow M'$ that respects that actions by satisfying $f\mathbf{M} = \mathbf{M}'(\text{id}_C \otimes f \otimes \text{id}_D)$.

If M is a C - D -bimodule, and N is a D - E -bimodule, the standard algebraic construction of *tensor product* gives a C - E -bimodule $M \otimes_D N$; see [12, Section 4.5]. It is constructed by forcing the right D -action on M and the left D -action on N to cooperate. More precisely, it is the coequalizer of the two morphisms $M \otimes D \otimes N \rightarrow M \otimes N$ induced by the two D -actions.

One way to guarantee the existence of such a coequalizer is to require that some morphisms have a sensible notion of *image*, as in the following definition and lemma. Recall that an endomorphism $p: A \rightarrow A$ is a *dagger idempotent* when $p^2 = p = p^\dagger$. A dagger idempotent p *splits* when $p = ii^\dagger$ and $i^\dagger i = \text{id}$ for some morphism i , called the *image* of p . Split idempotents are a special case of dagger coequalizers [17]: a dagger idempotent $p: A \rightarrow A$ splits if and only if p and id_A have a dagger coequalizer i^\dagger .

Definition 4. A dagger monoidal category *has dagger Frobenius images* when for all classical structures $(C, \lrcorner, \circlearrowleft)$, $(D, \lrcorner, \circlearrowright)$, (E, \lrcorner, \bullet) , for all C - D -bimodules \mathbf{M} and all D - E -bimodules \mathbf{N} , the following dagger idempotent splits:

$$\begin{array}{c}
 \begin{array}{c} M \\ \boxed{\mathbf{M}} \\ \begin{array}{c} \lrcorner \\ \circlearrowleft \end{array} \\ M \end{array} \\
 \begin{array}{c} \circlearrowleft \\ \circlearrowright \end{array} \\
 \begin{array}{c} N \\ \boxed{\mathbf{N}} \\ \begin{array}{c} \lrcorner \\ \bullet \end{array} \\ N \end{array} \\
 \begin{array}{c} \circlearrowleft \\ \circlearrowright \end{array} \\
 M \otimes N
 \end{array}
 \quad (10)$$

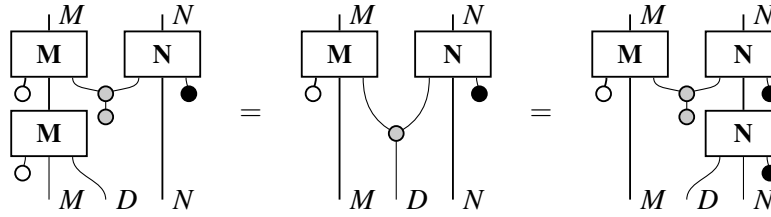
Notice that this morphism is indeed dagger idempotent by (9).

We denote the image of (10) by $i: M \circ N \rightarrow M \otimes N$. It is a dagger C - E -bimodule:

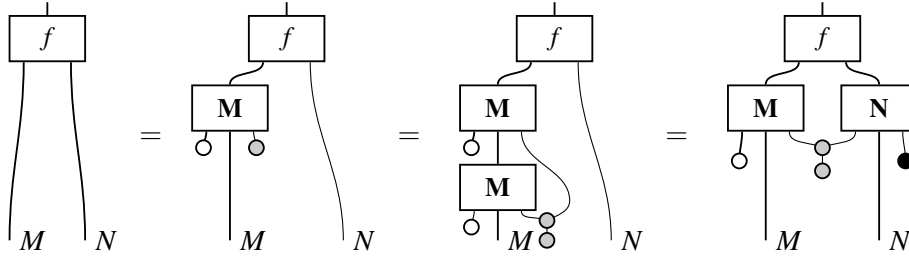
$$\begin{array}{c}
 \begin{array}{c} M \circ N \\ \boxed{\mathbf{M \circ N}} \\ \begin{array}{c} \lrcorner \\ \bullet \end{array} \\ C \quad M \circ N \quad E \end{array} \\
 := \\
 \begin{array}{c} M \circ N \\ \boxed{i^\dagger} \\ \begin{array}{c} \lrcorner \\ \bullet \end{array} \\ \begin{array}{c} \boxed{\mathbf{M}} \quad \boxed{\mathbf{N}} \\ \begin{array}{c} \circlearrowleft \\ \circlearrowright \end{array} \\ \boxed{i} \\ \begin{array}{c} \lrcorner \\ \bullet \end{array} \\ C \quad M \circ N \quad E \end{array}
 \end{array}
 \quad (11)$$

Lemma 5. *If (10) splits with image i , then i^\dagger is a coequalizer of $\circ\mathbf{M} \otimes \text{id}_N$ and $\text{id}_M \otimes \mathbf{N}_\bullet$.*

Proof. Observe that $i^\dagger(\circ\mathbf{M} \otimes \text{id}_N) = i^\dagger(\text{id}_M \otimes \mathbf{N}_\bullet)$ because $(\mathbf{M} \circ \mathbf{N})(\circ\mathbf{M} \otimes \text{id}_N) = (\text{id}_M \otimes \mathbf{N}_\bullet)(\circ\mathbf{M} \otimes \text{id}_N)$:



Suppose that $f(\circ\mathbf{M} \otimes \text{id}_N) = f(\text{id}_M \otimes \mathbf{N}_\bullet)$. Then f factors through i^\dagger as $f = fi^\dagger$:



This mediating map is unique: if $f = mi^\dagger$, then $m = mi^\dagger i = fi$. □

We can use this technique to re-prove many standard results about bimodules in a graphical way, such as the following simple result, that will be useful later.

Lemma 6. *For any dagger Frobenius algebra $(A, \circlearrowleft, \circlearrowright)$, the identity A - A -bimodule is \circlearrowleft .* □

With this preparation we can now define our main construction.

Proposition 7. *If \mathbf{C} is a dagger monoidal category that has dagger Frobenius images, then the following data define a symmetric monoidal (weak) 2-category $2[\mathbf{C}]$:*

- objects are classical structures in \mathbf{C} ;
- 1-morphisms are dagger bimodules; the identity 1-morphism on $(C, \circlearrowleft, \circlearrowright)$ is \circlearrowleft ;
- 2-morphisms are dagger bimodule homomorphisms;
- horizontal composition of 1-morphisms is given by (11);
- horizontal composition of 2-morphisms follows from the universal property of Lemma 5;
- monoidal structure is inherited from \mathbf{C} .

More precisely, the horizontal composition of 2-morphisms $f: \mathbf{M} \rightarrow \mathbf{M}'$ and $g: \mathbf{N} \rightarrow \mathbf{N}'$ is the unique arrow making the following diagram commute:

$$\begin{array}{ccccc}
 M \otimes D \otimes N & \xrightarrow[\text{id}_M \otimes \mathbf{N}_\bullet]{\circ\mathbf{M} \otimes \text{id}_N} & M \otimes N & \xrightarrow{i^\dagger} & M \circ N \\
 (f \otimes \text{id}_D \otimes g) \downarrow & & \downarrow f \otimes g & & \downarrow f \circ g \\
 M' \otimes D \otimes N' & \xrightarrow[\text{id}_{M'} \otimes \mathbf{N}'_\bullet]{\circ\mathbf{M}' \otimes \text{id}_{N'}} & M' \otimes N' & \xrightarrow{i'^\dagger} & M' \circ N'
 \end{array}$$

Proof. For verification that these data indeed satisfy all the conditions required of a weak 2-category, see [24]. Verifying monoidality is a huge exercise that nevertheless seems straightforward enough. \square

We end this subsection by listing some properties of the $2[-]$ -construction; for proofs we refer to [24].

- If \mathbf{C} has a dagger, so does $2[\mathbf{C}]$.
- If \mathbf{C} is compact, so is $2[\mathbf{C}]$: 1-morphisms have duals that are both left and right adjoint.
- If \mathbf{C} has dagger biproducts, so do all hom-categories of $2[\mathbf{C}]$.
- The scalars of $2[\mathbf{C}]$ correspond to \mathbf{C} : there is an isomorphism $2[\mathbf{C}](I, I) \cong \mathbf{C}$ of categories.

2.2 Topological boundaries

We now show that objects of $2[\mathbf{C}]$ have topological boundaries in the sense of Definition 2.

Definition 8. The *boundaries* of a special dagger Frobenius algebra $(A, \circlearrowleft, \circlearrowright)$ in \mathbf{C} are canonical bimodules $(A, \circlearrowleft, \circlearrowright) \xrightarrow{\mathbf{L}} (I, \lambda_I, \text{id}_I)$ and $(I, \lambda_I, \text{id}_I) \xrightarrow{\mathbf{R}} (A, \circlearrowleft, \circlearrowright)$ induced by the multiplication map \circlearrowleft :

$$\boxed{\mathbf{L}} := \text{diagram} \quad \boxed{\mathbf{R}} := \text{diagram} \quad (12)$$

The diagram shows two boxes labeled L and R. Box L is defined as a diagram with a vertical line on the left, a circle with a dot on top, and a vertical line on the right. A dashed line indicates the monoidal unit object. Box R is defined as a diagram with a vertical line on the right, a circle with a dot on top, and a vertical line on the left. A dashed line indicates the monoidal unit object.

The dashed lines indicate the monoidal unit object; we will typically omit these from now on. These boundaries are depicted as lines that bound solid regions, as shown in the diagrams (4).

Lemma 9. For a special dagger Frobenius algebra $(A, \circlearrowleft, \circlearrowright)$, the composite bimodule

$$(I, \lambda_I, \text{id}_I) \xrightarrow{\mathbf{R}} (A, \circlearrowleft, \circlearrowright) \xrightarrow{\mathbf{L}} (I, \lambda_I, \text{id}_I)$$

is isomorphic to the object A .

Proof. By Lemma 5, we must find the dagger splitting of the left-hand diagram below:

$$\text{diagram} = \text{diagram} \quad (13)$$

The diagram shows two diagrams separated by an equals sign. The left diagram has a vertical line on the left, a circle with a dot on top, and a vertical line on the right. The right diagram has a vertical line on the right, a circle with a dot on top, and a vertical line on the left.

By the dagger Frobenius axioms it equals the right-hand diagram. But the dagger specialness axiom makes this a dagger splitting via the object A , so the object A gives the composite of the bimodules. \square

Lemma 10. The boundaries of a special dagger Frobenius monoid $(A, \circlearrowleft, \circlearrowright)$ in \mathbf{C} can be equipped with data (5) and (6) satisfying equations (7) and (8) as follows:

$$\begin{array}{cccc} \begin{array}{c} \mathbf{L} \quad \mathbf{R} \\ \text{diagram} \\ \text{id}_A \end{array} & \begin{array}{c} \text{id}_A \\ \text{diagram} \\ \mathbf{L} \quad \mathbf{R} \end{array} & \begin{array}{c} \mathbf{L} \quad \mathbf{R} \\ \text{diagram} \\ \text{id}_I \end{array} & \begin{array}{c} \text{id}_I \\ \text{diagram} \\ \mathbf{L} \quad \mathbf{R} \end{array} \\ \circlearrowleft : A \rightarrow A \otimes A & \circlearrowright : A \otimes A \rightarrow A & \circ : I \rightarrow A & \circ : A \rightarrow I \end{array} \quad (14)$$

The diagram shows four diagrams arranged in a row. Each diagram has a circle with a dot on top. The first diagram has a vertical line on the left and a vertical line on the right. The second diagram has a vertical line on the left and a vertical line on the right. The third diagram has a vertical line on the left and a vertical line on the right. The fourth diagram has a vertical line on the left and a vertical line on the right.

Note that we are relying on Lemmas 6 and 9 for these definitions to make sense.

Proof. Equations (7) follow immediately from the (co)unit equation for a dagger Frobenius algebra. Equations (8) follow immediately from specialness and commutativity. \square

3 The case of Hilbert spaces

This section discusses $2[\mathbf{CP}^*[\mathbf{FHilb}]]$. We show that a substantial portion is well-defined, which we characterize in concrete terms: it consists of natural numbers, matrices of finite-dimensional C^* -algebras, and matrices of completely positive maps. Thus this is completely analogous to the case of $2[\mathbf{FHilb}]$, which is equivalent to the 2-category of 2-Hilbert spaces that consists of natural numbers, matrices of Hilbert spaces, and matrices of linear maps [3, 24]. The difficulty of establishing that $2[\mathbf{CP}^*[\mathbf{FHilb}]]$ is well-defined in general arises because $\mathbf{CP}^*[\mathbf{FHilb}]$ does not have good completeness properties.

Lemma 11. *Not all coequalizers in the category $\mathbf{CP}^*[\mathbf{FHilb}]$ are split epimorphisms.*

Proof. Due to the dagger we may equivalently show that not all equalizers split. Suppose the completely positive maps $f = (1\ 1\ 0\ 0)$ and $g = (0\ 0\ 1\ 1) : \mathbb{C}^4 \rightarrow \mathbb{C}$ had an equalizer $e : A \rightarrow \mathbb{C}^4$ in $\mathbf{CP}^*[\mathbf{FHilb}]$. Then $fe = ge$, so e factors through the equalizer of f and g in \mathbf{FHilb} :

$$\begin{array}{ccccc}
 \mathbb{C}^3 & \xrightarrow{\begin{pmatrix} -1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}} & \mathbb{C}^4 & \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} & \mathbb{C} \\
 \uparrow m & \nearrow e & & & \\
 A & & & &
 \end{array}$$

We show below that the function e is injective¹. Then the linear map m is injective, and so $\dim(A) \leq 3$. It follows that A must be a commutative C^* -algebra (as 2-by-2 matrices already have dimension 4).

Suppose $e(a) = 0$ with $a = x + iy$ for self-adjoint $x, y \in A$. Then $e(x) = e(y) = 0$ because positive maps preserve adjoints [20, page 2]. Say $x = x_+ - x_-$ for positive $x_+, x_- \in A$; then $e(x_+) = e(x_-)$. But the completely positive maps $h_{\pm} : \mathbb{C} \rightarrow A$ defined by $h_{\pm}(1) = x_{\pm}$ satisfy $eh_+ = eh_-$. So $h_+ = h_-$ since e is monic, whence $x = 0$. Similarly $y = 0$. So $\ker(e) = \{0\}$, and e is injective.

On the other hand, there are at least four completely positive maps $\mathbb{C} \rightarrow \mathbb{C}^4$, given by $x_1 = (1, 0, 1, 0)$, $x_2 = (1, 1, 0, 0)$, $x_3 = (0, 1, 0, 1)$, $x_4 = (0, 0, 1, 1)$, which satisfy $fx_i = gx_i$. No x_i is a linear combination of the others with nonnegative coefficients. If d is a retraction of e , therefore none of $dx_i \in A$ is a linear combination of the others with nonnegative coefficients, as $edx_i = x_i$. Moreover $dx_i \geq 0$ by completely positivity of d . But this contradicts $\dim(A) \leq 3$ as A is commutative. \square

It follows immediately that $\mathbf{CP}^*[\mathbf{FHilb}]$ does not have dagger coequalizers. The point is that there are nevertheless enough coequalizers for our purposes, as we show below.

3.1 Analysis

A subcollection of the objects in $\mathbf{CP}^*[\mathbf{FHilb}]$ are classical structures $C = (A, \circlearrowleft, \circlearrowright)$ in \mathbf{FHilb} . Since the morphisms \circlearrowleft and \circlearrowright are completely positive with respect to this algebra structure, this also gives rise to an algebra $C' = (C, \circlearrowleft, \circlearrowright)$ in $\mathbf{CP}^*[\mathbf{FHilb}]$. We call this a *classical structure over itself*. Note that, up to isomorphism $C \cong \mathbb{C}^n$, such structures are just natural numbers. In this section, except for the last theorem, we restrict consideration to objects of $2[\mathbf{CP}^*[\mathbf{FHilb}]]$ which are classical structures over themselves.

Lemma 12. *There is a one-to-one correspondence between dagger bimodules on classical structures over themselves in $\mathbf{CP}^*[\mathbf{FHilb}]$, and matrices of finite-dimensional C^* -algebras.*

¹We thank Narutaka Ozawa for this observation.

Proof. Let $\mathbf{M}: \mathbb{C}^m \otimes M \otimes \mathbb{C}^n \rightarrow M$ be a dagger \mathbb{C}^m - \mathbb{C}^n -bimodule in $\text{CP}^*[\mathbf{FHilb}]$, between classical structures over themselves. Then M is a finite-dimensional \mathbb{C}^* -algebra, and \mathbf{M} is a completely positive map. By 16, the units of \mathbb{C}^m and \mathbb{C}^n are given by the sum over the standard basis vectors $|i\rangle$ and $|j\rangle$ of \mathbb{C}^m and \mathbb{C}^n , respectively. Set $p_{ij} = (|i\rangle\langle i|) \otimes \text{id}_M \otimes (|j\rangle\langle j|)$; this is a completely positive dagger idempotent. Hence its image $M_{ij} = p_{ij}(M)$ is a finite-dimensional \mathbb{C}^* -algebra by a classic theorem of Choi and Effros [6]; see [14, Proposition 2.4]. Thus the bimodule \mathbf{M} gives rise to a matrix (M_{ij}) of finite-dimensional \mathbb{C}^* -algebras.

Conversely, let (M_{ij}) be an m -by- n matrix of finite-dimensional \mathbb{C}^* -algebras. Set $M = \bigoplus_{i,j} M_{ij}$, and define $\mathbf{M}: \mathbb{C}^m \otimes M \otimes \mathbb{C}^n \rightarrow M$ by mapping $|i\rangle \otimes a \otimes |j\rangle$ to $1_{ij} \cdot a$, where 1_{ij} is the unit of M_{ij} . In other words, $\mathbf{M}(|i\rangle \otimes a \otimes |j\rangle)$ is the projection of $a \in A$ onto the summand M_{ij} . This is a $*$ -homomorphism, and hence a completely positive map [10, Lemma 3.8]. To verify that it is a bimodule, we need to check equation (9). The first two equalities are easily verified, the third equality uses that $\mathbf{M}^\dagger: M \rightarrow \mathbb{C}^m \otimes M \otimes \mathbb{C}^n$ maps $b \in M$ to $\sum_{i,j} |i\rangle \otimes (1_{ij}b) \otimes |j\rangle$. Hence these two constructions, which are inverse to each other, are well-defined. \square

It follows that an important part of $2[\text{CP}^*[\mathbf{FHilb}]]$ is well-defined, which will be sufficient for our applications in Section 4 to quantum information and encryption.

Proposition 13. *Let (C, ρ, ϕ) , (D, ρ, ϕ) , (E, ρ, \bullet) be classical structures over themselves in $\text{CP}^*[\mathbf{FHilb}]$, and let \mathbf{M} and \mathbf{N} be a C - D -bimodule and a D - E -bimodule. The idempotent (10) splits.*

Proof. Write $|i\rangle, |j\rangle, |k\rangle$ for the standard bases of $\mathbb{C}^l, \mathbb{C}^m, \mathbb{C}^n$. Let \mathbf{M} be a dagger \mathbb{C}^l - \mathbb{C}^m -bimodule, and let \mathbf{N} be a dagger \mathbb{C}^m - \mathbb{C}^n -bimodule in $\text{CP}^*[\mathbf{FHilb}]$. Then (10) maps $m \otimes n$ to $\sum_{i,j,k} \mathbf{M}(|i\rangle \otimes m \otimes |j\rangle) \otimes \mathbf{N}(|j\rangle \otimes n \otimes |k\rangle)$. This morphism is a sum of orthogonal projections, and hence a projection itself. As in the proof of Lemma 12, this means that it has a well-defined dagger image in $\text{CP}^*[\mathbf{FHilb}]$. The proof is finished by noticing that any classical structure in \mathbf{FHilb} is isomorphic to the commutative \mathbb{C}^* -algebra \mathbb{C}^n for some n . \square

Lemma 14. *There is a one-to-one correspondence between homomorphisms of dagger bimodules between classical structures over themselves in $\text{CP}^*[\mathbf{FHilb}]$, and matrices of completely positive maps between finite-dimensional \mathbb{C}^* -algebras.*

Proof. Let $f: \mathbf{M} \rightarrow \mathbf{N}$ be a homomorphism of dagger \mathbb{C}^m - \mathbb{C}^n -bimodules in $\text{CP}^*[\mathbf{FHilb}]$. Write $|i\rangle$ and $|j\rangle$ for the standard bases of \mathbb{C}^m and \mathbb{C}^n . According to the proof of Lemma 12, let $p_{ij}: M \rightarrow M_{ij}$ and $q_{ij}: N \rightarrow N_{ij}$ be the completely positive maps implementing the biproduct decompositions $M = \bigoplus_{i,j} M_{ij}$ and $N = \bigoplus_{i,j} N_{ij}$. Then $f_{ij} = q_{ij} f p_{ij}^\dagger: M_{ij} \rightarrow N_{ij}$ is an m -by- n matrix of completely positive maps. Conversely, let (f_{ij}) be an m -by- n matrix of completely positive maps $f_{ij}: M_{ij} \rightarrow N_{ij}$. According to Lemma 12 we have to find a map $f: M \rightarrow N$ for $M = \bigoplus_{i,j} M_{ij}$ and $N = \bigoplus_{i,j} N_{ij}$. Just take $f = \bigoplus_{i,j} f_{ij}$; this is well-defined because $\text{CP}^*[\mathbf{C}]$ inherits biproducts from \mathbf{C} [14, Theorem 3.2]. We have to verify that this is a well-defined homomorphism of dagger bimodules:

$$\begin{aligned} f\mathbf{M}(|i_0\rangle \otimes a \otimes |j_0\rangle) &= f(1_{i_0 j_0} a) = \bigoplus_{i,j} f_{ij}(1_{i_0 j_0} a) = f_{i_0 j_0}(1_{i_0 j_0} a) \\ &= 1_{i_0 j_0} \bigoplus_{i,j} f_{ij}(1_{ij} a) \\ &= 1_{i_0 j_0} f(a) = \mathbf{N}(|i_0\rangle \otimes f(a) \otimes |j_0\rangle) \end{aligned}$$

These two constructions are clearly inverse to each other. \square

We can now characterize a well-defined part of $2[\text{CP}^*[\mathbf{FHilb}]]$.

Theorem 15. *The following full sub-2-category is well-defined within $2[\mathbf{CP}^*[\mathbf{FHilb}]]$:*

- *objects are natural numbers m ;*
- *1-morphisms $m \rightarrow n$ are m -by- n matrices (M_{ij}) of finite-dimensional C^* -algebras;*
- *2-morphisms $(M_{ij}) \rightarrow (N_{ij})$ are m -by- n matrices (f_{ij}) of completely positive maps;*
- *horizontal composition of 1-morphisms is given by $(\bigoplus_j M_{ij} \otimes N_{jk})$;*
- *horizontal composition of 2-morphisms is given by $(\bigoplus_j f_{ij} \otimes g_{jk})$;*
- *vertical composition of 2-morphisms is given by $(g_{ij}f_{ij})$.*

Proof. It suffices to show that the correspondences of Lemmas 12 and 14 turn the compositions of Proposition 7 into the ones of the statement. Let \mathbf{M} and \mathbf{M}' be \mathbb{C}^l - \mathbb{C}^m -bimodules, and let \mathbf{N} and \mathbf{N}' be \mathbb{C}^m - \mathbb{C}^n -bimodules. These correspond to matrices of C^* -algebras, where M_{ij} is the image of $|i\rangle\langle i| \otimes \text{id}_M \otimes |j\rangle\langle j|$. Let $f: \mathbf{M} \rightarrow \mathbf{M}'$ and $g: \mathbf{N} \rightarrow \mathbf{N}'$ be bimodule homomorphisms. These correspond to matrices of completely positive maps $f_{ij}: M_{ij} \rightarrow M'_{ij}$ and $g_{ij}: N_{ij} \rightarrow N'_{ij}$. Now, by definition $M \circ N$ is the image of the map $\sum_{i,j,k} \mathbf{M}(|i\rangle \otimes [-] \otimes |j\rangle) \otimes \mathbf{N}(|j\rangle \otimes [-] \otimes |k\rangle)$. But this is just $\bigoplus_{i,j,k} M_{ij} \otimes N_{jk}$. Similarly, horizontal composition of f and g corresponds to $(\bigoplus_j f_{ij} \otimes g_{jk})$. \square

In future work we would of course like to show that $2[\mathbf{CP}^*[\mathbf{FHilb}]]$ is completely well-defined. The first task will be to characterize its objects up to isomorphism. We offer the following theorem, which generalizes [7, Corollary 3.10], as evidence that this is a nontrivial question. Recall that a state $x \in C$ of a classical structure $(C, \blacktriangleright, \blacktriangleleft)$ in \mathbf{FHilb} is *copyable* when $\blacktriangleright'(x) = x \otimes x$.

Theorem 16. *Consider a classical structure C in \mathbf{FHilb} as an object of $\mathbf{CP}^*[\mathbf{FHilb}]$. There is a one-to-one correspondence between dagger special Frobenius algebras on C in $\mathbf{CP}^*[\mathbf{FHilb}]$, and finite groupoids whose morphisms are the copyable states of C .*

Proof. Let $(\mathbb{C}^n, \blacktriangleright, \blacktriangleleft)$ be a dagger special Frobenius algebra on \mathbb{C}^n in $\mathbf{CP}^*[\mathbf{FHilb}]$. That is, it is a dagger special Frobenius algebra in \mathbf{FHilb} —i.e. a finite-dimensional C^* -algebra [21]—satisfying the extra condition that \blacktriangleright and \blacktriangleleft are completely positive maps. Since they are maps between commutative C^* -algebras, saying that \blacktriangleright and \blacktriangleleft are completely positive is the same as saying that they are linear maps that preserve positive elements [20, Theorem 1.2.4]. Write \blacktriangleright and \blacktriangleleft as a matrix using the standard basis $|i\rangle$ of \mathbb{C}^n . Then all matrix entries $\langle i | \blacktriangleright | jk \rangle$ and $\langle i | \blacktriangleleft | 1 \rangle$ are nonnegative real numbers, and conversely, if all the matrix entries are nonnegative, then the linear maps \blacktriangleright and \blacktriangleleft certainly preserve positive elements. Thus $(\mathbb{C}^n, \blacktriangleright, \blacktriangleleft)$ is a dagger special Frobenius algebra in $\mathbf{CP}^*[\mathbf{FHilb}]$ if and only if it is a C^* -algebra whose multiplication and unit have nonnegative matrix entries on the standard basis $|i\rangle$ of \mathbb{C}^n .

But then, by [2, Proposition 34], the matrix entries of \blacktriangleright must in fact be either 0 or 1 (see also [10, Section 5.2].) So we may equally think of the matrix of \blacktriangleright as a morphism in the category \mathbf{Rel} of sets and relations, where it still is a special dagger Frobenius algebra. Hence it encodes the multiplication of a groupoid whose arrows are the row indices $|i\rangle$ [13]. As units for a monoid are unique, also the matrix of \blacktriangleleft must take values in $\{0, 1\}$, and encode the identities of the groupoid. Finally, any classical structure C in \mathbf{FHilb} is isomorphic to \mathbb{C}^n for some n , with the standard basis of \mathbb{C}^n corresponding to the copyable states of C . Similarly, a $*$ -isomorphism between classical structures in \mathbf{Rel} corresponds to an isomorphism of groupoids [13, Theorem 19]. \square

We leave open the interesting question of whether isomorphism between these objects in $2[\mathbf{CP}^*[\mathbf{FHilb}]]$ (so-called *Morita equivalence*) corresponds to *equivalence* of groupoids.

4 Applications

We now consider applications to quantum information of the well-defined part of $2[\text{CP}^*[\mathbf{FHilb}]]$ constructed in Theorem 15. We give an abstract 2-categorical definition of *measurement*, and show it recovers the ordinary notion positive operator-valued measure. We then analyze the 2-categorical equation for quantum teleportation, and show that it has solutions in our 2-category given by both encrypted communication and quantum teleportation. We then give a proof of a security property, which applies simultaneously to both types of solution.

4.1 Measurement

Earlier work on the 2-categorical syntax for pure-state quantum theory [22] demonstrated that a projective quantum measurement corresponds to a *unitary* 2-morphism which converts a local system into an extended system. Since our measurements in general are mixed, unitarity is not appropriate; instead we impose a counit-preservation condition.

Definition 17. In $2[\text{CP}^*[\mathbf{FHilb}]]$, a *measurement* is a counit-preserving 2-morphism of type:

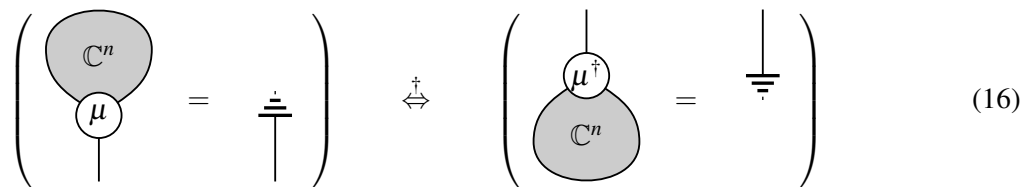

(15)

It is not ideal that we must modify the definition of a measurement in this way. The situation is analogous to the work in [19], where measurements were required to be kernel-free. That requirement can be replaced with the more elegant unitarity condition [4]. With further work we hope to show the same in the current setting, a task which is likely to require making use of a larger part of $2[\text{CP}^*[\mathbf{FHilb}]]$ than we have so-far shown to be well-defined. However, Definition 17 elegantly captures precisely the desired notion, as we now show.

Theorem 18. *Restricting to the part of $2[\text{CP}^*[\mathbf{FHilb}]]$ defined in Theorem 15, measurements on matrix algebras are exactly positive operator-valued measures.*

Proof. The 2-morphism μ is a trace-preserving completely positive map from a matrix algebra to a classical structure. Its adjoint μ^\dagger is therefore a completely positive map out of a classical structure. Such a map is completely defined by its action on the n copyable states of the classical structure, which must be sent to positive elements of $H \otimes H^*$. Thus μ^\dagger is defined by a family of n positive operators $P_i : H \rightarrow H$.

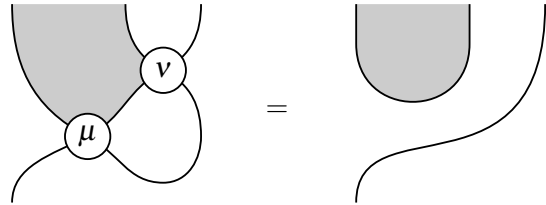
The counit-preservation condition is given by the left-hand condition below:


(16)

On the right-hand side we take the adjoint of this condition. We use the ‘earth’ symbol to represent the counit of a matrix algebra, which is just the trace map, following previous work [11]. The second equation says precisely that $\sum_i P_i = \text{id}_H$, which is exactly the condition for the family of positive operators P_i to define a positive operator-valued measurement. □

4.2 Unification of quantum teleportation and classical encrypted communication

Definition 19. In a symmetric monoidal 2-category containing an object with a topological boundary, *teleportation* is a solution to the following equation with μ a measurement and ν unitary:


(17)

Note that this definition relies on our earlier Definition 17 of a measurement.

Theorem 20. *When the nontrivial region is labelled by a discrete groupoid, solutions to the teleportation equation in $2[\text{CP}^*[\mathbf{FHilb}]]$ can be obtained as follows:*

1. *when the incoming system is a classical structure, by implementations of classical encrypted communication using a one-time pad;*
2. *when the incoming system is a matrix algebra, by implementations of quantum teleportation.*

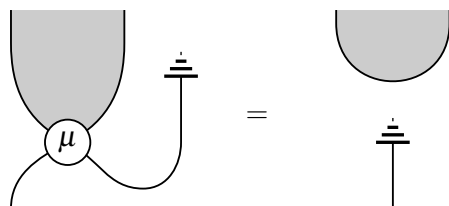
Proof. We can only give a sketch here. It is already established separately that both classical encrypted communication via a one-time pad [19] and quantum teleportation [22] can be characterized exactly as solutions to this equation, in $\mathbf{2Rel}$ and $\mathbf{2Hilb}$ respectively. Both families of solutions can be embedded into $2[\text{CP}^*[\mathbf{FHilb}]]$ in an appropriate fashion. \square

It is an interesting open question whether these are the only solutions, or whether solutions exist which somehow *mix* the encryption and teleportation aspects.

4.3 Security of teleportation

In both quantum teleportation and classical encrypted communication with a one-time pad, it is true that if you throw away the second half of the cryptographic resource—the entangled state or the secret key, respectively—all information about the message is lost. An abstract proof of this has already been given in the 2-categorical setup for the case of encrypted communication [19]. We now give a general proof that applies simultaneously to quantum teleportation and encrypted communication.

Theorem 21. *For any solution to the teleportation equation (17), destroying the second half of the shared resource is equivalent to destroying the original message:*


(18)

Proof. Adjoin a trace map to the final system on both sides of the teleportation equation (17). The map ν is a family of invertible completely positive maps by Lemma 14, and thus is necessarily trace-preserving [5, Theorem 3.3]; the left-hand side therefore simplifies, giving equation (18). \square

References

- [1] S. Abramsky & B. Coecke (2004): *Categorical Semantics of Quantum Protocols*. In: *Proceedings of the 19th ACM/IEEE Symposium on Logic in Computer Science*, IEEE, pp. 415–425, doi:10.1109/LICS.2004.1319636.
- [2] S. Abramsky & C. Heunen (2012): *H^* -Algebras and Nonunital Frobenius Algebras*. In: *Clifford Lectures, Proceedings of Symposia in Applied Mathematics 71*, American Mathematical Society, pp. 1–24.
- [3] J. C. Baez (1997): *Higher-Dimensional Algebra II: 2-Hilbert Spaces*. *Adv. Math.* 127, pp. 125–189, doi:10.1006/aima.1997.1617.
- [4] K. Bar & J. Vicary (2014): *Groupoid Semantics for Thermal Computing*. <http://arxiv.org/abs/1401.3280>.
- [5] D. Cariello (2012): *An Elementary Description of the Positive Maps with Positive Inverse*. In: *National Congress of Applied Mathematics and Computation 34*. <http://www.sbm.org.br/eventos/cnmac/xxxiv.cnmac/pdf/541.pdf>.
- [6] M.-D. Choi & E. G. Effros (1977): *Injectivity and Operator Spaces*. *J. Func. Anal.* 24, pp. 156–209, doi:10.1016/0022-1236(77)90052-0.
- [7] B. Coecke, R. Duncan, A. Kissinger & Q. Wang (2012): *Strong Complementarity and Non-Locality in Categorical Quantum Mechanics*. In: *Logic in Computer Science 27*, IEEE, pp. 245–254, doi:10.1109/LICS.2012.35.
- [8] B. Coecke & C. Heunen (2012): *Pictures of Quantum Processes in Arbitrary Dimension*. In: *Quantum Physics and Logic IX, Electronic Proceedings in Theoretical Computer Science 95*, pp. 27–35, doi:10.4204/EPTCS.95.4.
- [9] B. Coecke, C. Heunen & A. Kissinger (2013): *Compositional Quantum Logic*. In: *Computation, Logic, Games, and Quantum Foundations*, Springer, pp. 21–36, doi:10.1007/978-3-642-38164-5_3.
- [10] B. Coecke, C. Heunen & A. Kissinger (2014): *Categories of Quantum and Classical Channels*. *Q. Inf. Processing*, doi:10.1007/s11128-014-0837-4.
- [11] B. Coecke & S. Perdrix (2012): *Environment and Classical Channels in Categorical Quantum Mechanics*. *Logical Methods in Computer Science* 8(4), pp. 1–24, doi:10.2168/LMCS-8(4:14)2012.
- [12] M. Hazewinkel, N. Gubareni & V. V. Kirichenko (2004): *Algebras, Rings and Modules*. 1, Kluwer.
- [13] C. Heunen, I. Contreras & A. Cattaneo (2013): *Relative Frobenius Algebras are Groupoids*. *Journal of Pure and Applied Algebra* 217, pp. 114–124, doi:10.1016/j.jpaa.2012.04.002.
- [14] C. Heunen, A. Kissinger & P. Selinger (2013): *Completely Positive Projections and Biproducts*. In: *Quantum Physics and Logic X, Electronic Proceedings in Theoretical Computer Science*.
- [15] A. D. Lauda (2006): *Frobenius Algebras and Ambidextrous Adjunctions*. *Theory Appl. Categories* 16(4), pp. 84–122.
- [16] P. Selinger (2005): *Dagger Compact Categories and Completely Positive Maps*. In: *Quantum Physics and Logic III, Electronic Notes in Theoretical Computer Science 170*, pp. 139–163, doi:10.1016/j.entcs.2006.12.018.
- [17] P. Selinger (2006): *Idempotents in Dagger Categories*. *Electronic Notes in Theoretical Computer Science* 210, pp. 107–122, doi:10.1016/j.entcs.2008.04.021. *Proceedings of the 4th International Workshop on Quantum Programming Languages*.
- [18] P. Selinger (2011): *A survey of graphical languages for monoidal categories*. In: *New Structures for Physics, Lecture Notes in Physics 813*, Springer, pp. 289–355, doi:10.1007/978-3-642-12821-9_4.
- [19] M. Stay & J. Vicary (2013): *Bicategorical Semantics of Nondeterministic Computation*. In: *Mathematical Foundations of Programming Semantics 29, Elec. Notes Theor. Comp. Sci.* 298, pp. 367–382, doi:10.1016/j.entcs.2013.09.022.
- [20] E. Størmer (2013): *Positive Linear Maps of Operator Algebras*. Springer.
- [21] J. Vicary (2011): *Categorical Formulation of Quantum Algebras*. *Comm. Math. Phys.* 304(3), pp. 765–796, doi:10.1007/s00220-010-1138-0.
- [22] J. Vicary (2012): *Higher Semantics of Quantum Protocols*. In: *Proceedings of the 27th ACM/IEEE Symposium on Logic in Computer Science*, pp. 606–615, doi:10.1109/LICS.2012.70.
- [23] J. Vicary (2013): *Topological Structure of Quantum Algorithms*. In: *Proceedings of the 28th ACM/IEEE Symposium on Logic in Computer Science*, pp. 93–102, doi:10.1109/LICS.2013.14.
- [24] L. Wester (2013): *Categorical Models for Quantum Computing*. Master’s thesis, University of Oxford.