Replace this file with prentcsmacro.sty for your meeting,
or with entcsmacro.sty for your meeting. Both can be
found at the ENTCS Macro Home Page.

Bases in diagramatic quantum protocols

Bob Coecke[1,2] Simon Perdrix[3,4]

Oxford University Computing Laboratory
Wolfson Building, Parks Road, OX1 3QD Oxford, UK

Éric Oliver Paquette[5,6]

Département d'Informatique et de Recherche Opérationelle
LITQ, Université de Montréal, Montréal, Canada

Abstract

This paper contains two new results:

(i) We amend the notion of abstract base in a dagger symmetric monoidal category, as well as its corresponding graphical representation, in order to accommodate non-self-dual dagger compact structures; this is crucial for obtaining a planar diagrammatical representation of the induced dagger compact structure as well as for representing several incompatible bases within one diagrammatic calculus.

(ii) We (crucially) rely on these base structures in a purely diagrammatic derivation of the quantum state transfer protocol; this derivation provides interesting insights in the distinct structural resources required for state-transfer and teleportation as models of quantum computing.

Keywords: categorical semantics, quantum protocols, diagrammatic calculus, abstract bases.

1 Introduction

Categorical axiomatisation of quantum mechanics enables rigourous and abstract design of quantum protocols. This research program was initiated by Abramsky and Coecke with their categorical analysis of the quantum teleportation protocol [1]. They showed that dagger compact categories capture essential structures of

[1] B. C. is supported by EPSRC Advanced Research Fellowship EP/D072786/1 entitled *The Structure of Quantum Information and its Ramifications for IT*.

[2] Email: bob.coecke@comlab.ox.ac.uk

[3] S. P. is employed on the EC-IST-FP6 STREP 033763 entitled *Foundational Structures in Quantum Information and Computation* – acronym QICS.

[4] Email: simon.perdrix@comlab.ox.ac.uk

[5] É. O. P. thanks Oxford University Computing Laboratory, Bob Coecke and Mehrnoosh Sadrzadeh for their hospitality during his visit in which part of this work was realised. This visit was supported by EPSRC Advanced Research Fellowship EP/D072786/1. He also thanks Gilles Brassard's chaire de recherche du Canada en informatique quantique for financing and Michel Boyer for discussions and feedback on some problems that are discussed in the present paper.

[6] Email: couserid@codept.coinst.coedu

the quantum mechanical formalism including *unitarity, (self-)adjointness, trace, Bell-states, and Dirac calculus*. These enable design of the quantum teleportation and related protocols. The use of compact structures was inspired by Kelly and Laplaza's much earlier work on coherence [14]. A particularly appealing feature of dagger compact categories is that they come with an intuitive diagrammatic calculus, made precise by Selinger in [20], extending the one due to Joyal and Street [11]. Another notable contribution to this program, also in [20], is Selinger's construction of *mixed states* and *completely positive maps*.

Protocols such as quantum teleportation involve both measurement as well as operations that depend on measurement outcomes. The dagger compact structure does not capture classical data and hence, classical data can only be represented syntactically, e.g. by 'indices' which relate control operations to measurement outcomes. If one wants to represent classical data as explicit categorical structure one needs to go beyond dagger compactness. In [1] Abramsky and Coecke used biproducts for this purpose, which, at the same time, could be used to express *superpositions*. However, as argued in [4], the biproduct requirement prevents the passage from the vectorial to the projective realm, a step which is essential to eliminate redundant global phase data. This in particular meant that the approach did not capture an essential component of quantum measurements, namely *decoherence*, which structurally separates the initial superposed states from the resulting *probabilistic mixtures*. This problem was overcome both in [4] and [20] by passing from vectors to density operators.

But, non of these *additive* structures enabled elegant diagrammatic representation. The more abstract *classical objects* introduced by Coecke and Pavlovic in [8], and inspired on Carboni and Walter's Frobenius structures [3], are expressed entirely in terms of the *multiplicative* tensor structure. In [6] it was shown by two of the present authors that these classical objects did allow elegant diagrammatic representation: computation proceeds by the purely diagrammatic so-called *spider theorem*.[7] Classical objects moreover admit an operational interpretation in terms of copying and erasing [8]. More precisely, they exploit the fact that while classical data can be arbitrarily copies and erased, quantum data can't. Formally, classical objects 'refine' the dagger compact structures of [1] in the sense that if an object comes with a classical object structure than it also admits a compact structure [7]. Recently, Coecke, Pavlovic and Vicary showed that for finite dimensional Hilbert spaces these classical objects, or more precisely, *special co-commutative dagger Frobenius comonoids*, are in one-to-one correspondence with orthonormal bases [9]. Also recently, Coecke and Duncan showed that they enable to axiomatize the key quantum mechanical notion of *complementary observables* [5].

However, all wasn't shiny and bright. These classical objects forced objects to be self-dual relative to the compact structure, that is, $A^* = A$, while Selinger's graphical calculus crucially relied on $A^* \neq A$. Also, when considering several classical objects at once, the induced compact structures do not necessarily coincide, which has severe consequences for the diagrammatic calculus. For example, while in [5] the authors were able to axiomatize the complementary X- and Z-observables, by

[7] Variants of this theorem also known in other contexts such as topological quantum field theories [15], abstract category theory [16] and representation theory [17].

no means they could adjoin the Y-observable on the same footing, exactly because it induces a different compact structure than the X- and Z-observables do.

In this paper, firstly, we introduce an elaboration on the classical objects of [8], to which we refer as *base structures*, which bypasses these problems. While classical objects 'factorize' compact structures in terms of a comonoid multiplication and its unit, we introduce a third component, namely, a unitary comonoid homomorphism. This homomorphism is an *explicit witness for the passage from a space to its dual*. A different but equivalent perspective is that in dagger symmetric monoidal categories, classical objects do not refine but are complementary to compact structures. Together they then induce our base structures. These bases structures allow for the 'non-trivial duals', required, for example, to accommodate Selinger's diagrammatic representation of mixed states and completely positive maps. Whenever dealing with several observables, for example the X-, the Z- as well as the Y-observable, we can model them relative to a unique compact structure.

Next, we show that these base structures enable a diagrammatic description, among other protocols, of Perdrix' state transfer protocol [18]. State transfer is key to the unification of measurement-only and one-way models of quantum computation [10]. Moreover, state transfer, as a substitute for teleportation, is a key feature for optimizing the resources of measurement-only quantum computation [19]. More generally, measurement-based quantum computational models have recently become very prominent within the landscape of quantum computing due to the their great promise for actual implementation [13]. The diagrammatic analysis of both teleportation and state transfer reveals important structural differences between these two measurement-only quantum computational models.

In this paper we chose to present classical data by indices. We do this to stress that, for state transfer, contra teleportation, base structures are already required even when representing classical data as indices. Since classical objects were specifically crafted to represent classical information flow as categorical structure, and since base structures extend classical objects, we could have easily provided a fully comprehensive purely categorical description of classical data. But then the main point we wanted to stress here wouldn't have come out as clear.

2 Categorical semantics and graphical language

2.1 Dagger symmetric monoidal category

A *symmetric monoidal category* consists of a category $\mathcal{C}$, a bifunctor $-\otimes- : \mathcal{C}\times\mathcal{C} \to \mathcal{C}$, a unit object I and natural isomorphisms $\lambda_A : A \simeq A\otimes I$, $\alpha_{A,B,C} : A\otimes(B\otimes C) \simeq (A\otimes B)\otimes C$ and $\sigma_{A,B} : A\otimes B \simeq B\otimes A$ satisfying the usual coherence conditions.

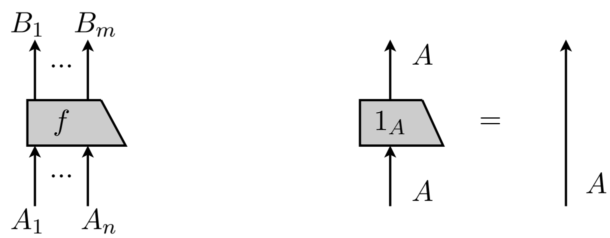
A $\dagger$-*symmetric monoidal category* ($\dagger$-SMC) [20] is a symmetric monoidal category together with an involutive, identity-on-objects, contravariant endofunctor $\dagger : \mathcal{C} \to \mathcal{C}$, which preserves the monoidal structure, i.e.

$$(g\circ f)^\dagger = f^\dagger \circ g^\dagger \qquad f^{\dagger\dagger} = f \qquad (f\otimes g)^\dagger = f^\dagger \otimes g^\dagger$$

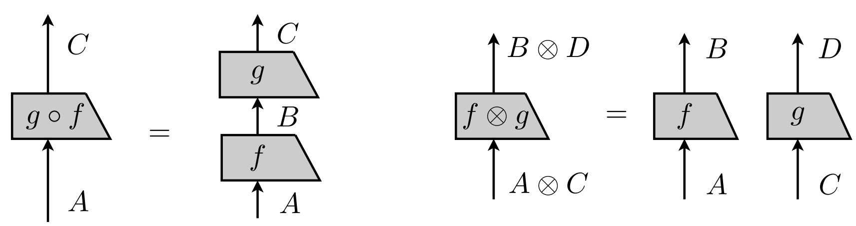
and also $\alpha^\dagger_{A,B,C} = \alpha^{-1}_{A,B,C}$, $\lambda^\dagger_A = \lambda^{-1}_A$ and $\sigma^\dagger_{A,B} = \sigma^{-1}_{A,B}$, that is, the natural isomorphisms of the structures are 'unitary'. Indeed, in a $\dagger$-SMC, a morphism $f : A \to B$ is *unitary* if it is an isomorphism such that $f^{-1} = f^{\dagger}$. In what follows, for convenience, we will take α, λ and ρ to be strict.

Example 2.1 The category **FdHilb**, of finite dim. Hilbert spaces, linear maps and tensor products, is a †-SMC, where $(-)^{\dagger}$ is the adjoint.

A rigourous graphical language for symmetric monoidal categories has been introduced by Joyal and Street [11] and extended to †-SMCs by Selinger [20]. Such a graphical calculus is handy not only to get a representation of the information flow but is also a powerful proof technique. Indeed, in a †-SMC (and richer structures which we introduce below), an equation holds if and only if there is an equality between their respective graphical representations [11,20]. Elementary components of this calculus are as follows: - The identity $1_I : I \to I$ is represented by the empty picture. - A morphism $f : A_1 \otimes ... \otimes A_n \to B_1 \otimes ... \otimes B_m$ and the identity $1_A : A \to A$ are depicted respectively as

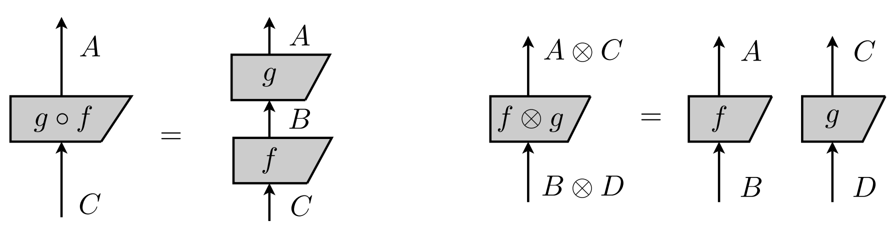


- The composite $g \circ f : A \to C$ for $f : A \to B$ and $g : B \to C$ and tensor $f \otimes g : A \otimes C \to B \otimes D$ for $f : A \to B$ and $g : C \to D$ are graphically represented as



- Given A and B, a component of the symmetry natural isomorphism $\sigma_{A,B} : A \otimes B \to B \otimes A$ and the dagger of a morphism $f : A \to B$ are depicted as

that is, $(-)^{\dagger}$ is graphically represented by 'vertical reflection'.
- Finally, for $g \circ f$ and $f \otimes g$ as above, $(g \circ f)^{\dagger}$ and $(f \otimes g)^{\dagger}$ are depicted as



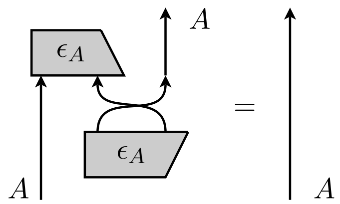
2.2 Dagger compact structure

The following definition of †-compact structure 'localizes' the †-compact categories that are key to Abramsky and Coecke's derivation of quantum teleportation in [1].

Definition 2.2 A †-*compact structure* in a †-SMC is a pair $(A, \epsilon_A : A \otimes A^* \to I)$ such that

$$(\epsilon_A \otimes 1_A) \circ (1_A \otimes \sigma_{A,A^*}) \circ (1_A \otimes \epsilon_A^\dagger) = 1_A$$

or, graphically,



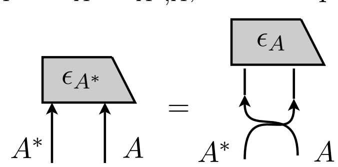
Example 2.3 The *conjugate Hilbert space* $\mathcal{H}^*$ of a Hilbert space $\mathcal{H}$ is the Hilbert space with the same vectors as $\mathcal{H}$ but with scalar multiplication and inner-product conjugated, that is, explicitly,

$$c \bullet_{\mathcal{H}^*} \psi = \bar{c} \bullet_{\mathcal{H}} \psi \qquad \text{and} \qquad \langle \psi \mid \phi \rangle_{\mathcal{H}^*} = \langle \phi \mid \psi \rangle_{\mathcal{H}} \,.$$

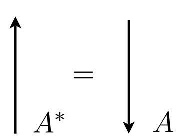
In **FdHilb**, for any $\mathcal{H} \in |\mathbf{FdHilb}|$, $(\mathcal{H}, \epsilon_{\mathcal{H}} : \mathcal{H} \otimes \mathcal{H}^* \to \mathbb{C})$ is a †-compact structure where $\mathcal{H}^*$ is the conjugate space of $\mathcal{H}$, and

$$\epsilon_{\mathcal{H}} : \mathcal{H} \otimes \mathcal{H}^* \to \mathbb{C} :: e_i \otimes \bar{e}_j \mapsto \langle e_i | e_j \rangle \ .$$

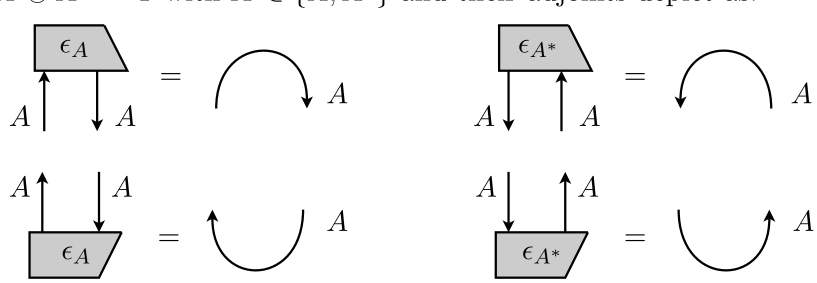
Definition 2.4 A †-*compact category* is a †-SMC where each object A comes with a †-compact structure, and where the †-compact structures on an object A and its *dual* A^* are connected by $\epsilon_{A^*} = \epsilon_A \circ \sigma_{A^*,A}$, which depicts as



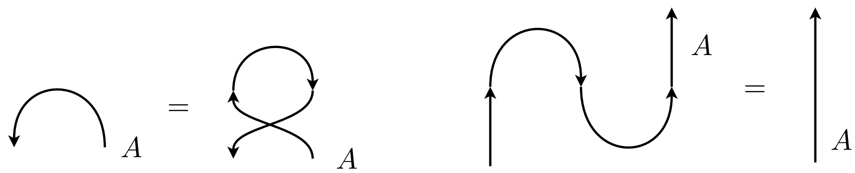
The graphical language of †-SMCs can be extended to †-compact categories as follows [20]. The identity 1_{A^*} is represented as an arrow with opposite orientation and labeled by A:



and $\epsilon_X : X \otimes X^* \to I$ with $X \in \{A, A^*\}$ and their adjoints depict as:



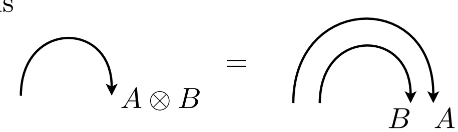
The axiomatic requirements for †-compact categories depict as:



Definition 2.5 A †-compact category is *strict* if $(A \otimes B)^* = B^* \otimes A^*$ and

$$\epsilon_{A\otimes B} = \epsilon_A \circ (1_A \otimes \epsilon_B \otimes 1_{A^*})\,,$$

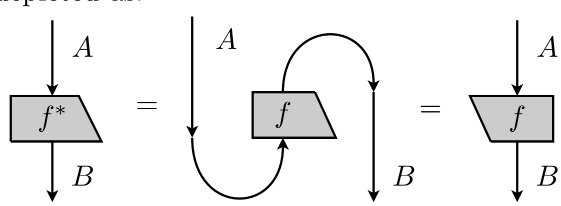
diagrammatically this is



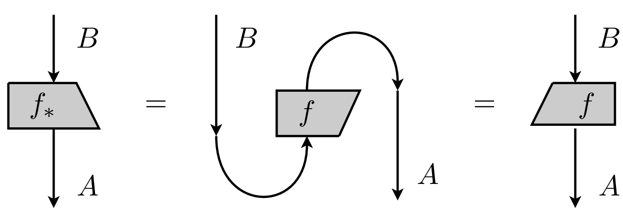
In any compact category, the assignment $(-)^*$ on objects can be extended to a contravariant functor whose assigment on morphisms maps $f : A \to B$ to

$$f^* : B^* \to A^* := (1_{A^*} \otimes \epsilon_B) \circ (1_{A^*} \otimes f \otimes 1_{B^*}) \circ (\eta_A \otimes 1_{B^*})\,.$$

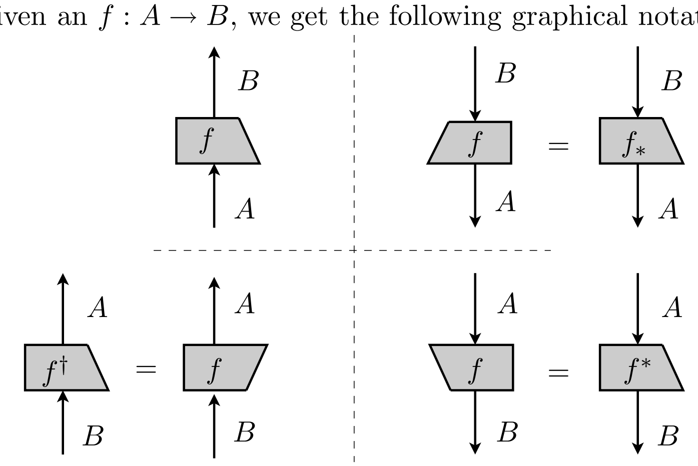
Such a mapping is depicted as:



Moreover, we can define a covariant functor $(-)_* := (-)^{\dagger *} = (-)^{*\dagger}$ whose assignment on morphisms is given by



Thus, given an $f : A \to B$, we get the following graphical notation [20]:



that is, $(-)_*$ is graphically represented by horizontal reflection and $(-)^*$ by 180° rotation. This captures $(-)^\dagger = ((-)^*)_*$ and similar equations.

3 Bases axiomatisation

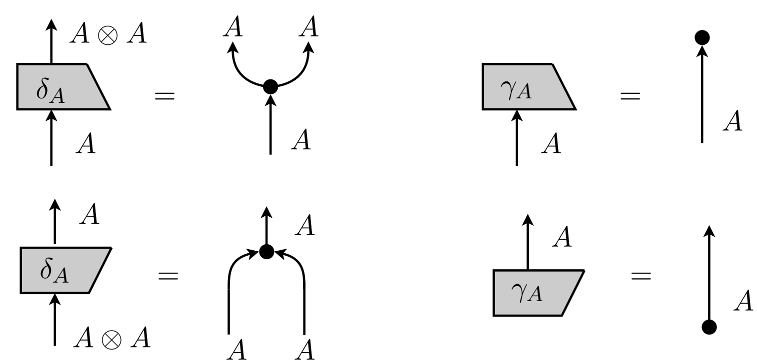
3.1 Cloning vs copying

The no-cloning theorem [21], a well-known result of quantum information theory, states that for any Hilbert space of finite dimension greater than two, there is no quantum evolution $f : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ such that for any $|\phi\rangle \in \mathcal{H}$, $f(|\phi\rangle) = |\phi\rangle \otimes |\phi\rangle$. Despite of the no-cloning theorem, *copying* is allowed by quantum mechanics: for a given orthonormal base $\{e_k, k \in K\}$, the linear operator $\delta : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H} :: e_k \mapsto e_k \otimes e_k$ is an isometry (i.e. $\delta^\dagger \circ \delta = 1_{\mathcal{H}}$), thus a valid quantum evolution. Here, the only vectors that are truly copied are the base vectors. Coecke and Pavlovic [8] relied on this fact when axiomatising bases as †-Frobenius structures.

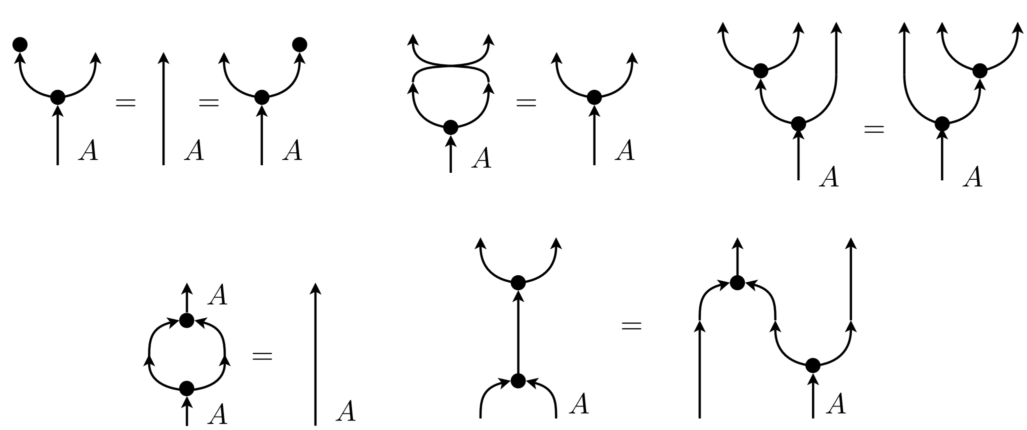
Definition 3.1 A †-*Frobenius structure* in a †-SMC is an internal co-commutative comonoid $(A, \delta_A : A \to A \otimes A, \gamma_A : A \to I)$ such that

$$\delta_A^\dagger \circ \delta_A = 1_A \qquad \text{and} \qquad \delta_A \circ \delta_A^\dagger = (\delta_A^\dagger \otimes 1_A) \circ (1_A \otimes \delta_A)\,.$$

The structural morphisms therein are diagrammatically represented as [6]:



and their axiomatic conditions depict as:



Example 3.2 Let $\{|0\rangle, |1\rangle\}$ be the so-called standard basis of $\mathcal{H}_2$, the Hilbert space

of dimension 2. Let

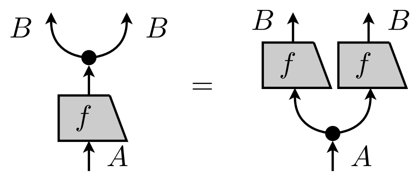
$$\delta_{std} : \mathcal{H}_2 \to \mathcal{H}_2 \otimes \mathcal{H}_2 :: |j\rangle \mapsto |jj\rangle \qquad \text{and} \qquad \gamma_{std} : \mathcal{H}_2 \to \mathbb{C} :: |j\rangle \mapsto 1\,. \qquad (1)$$

Then $(\mathcal{H}_2, \delta_{std}, \gamma_{std})$ is a †-Frobenius structure in **FdHilb**.

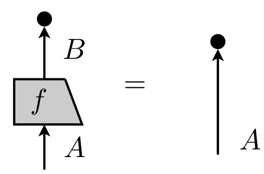
Theorem 3.3 [9] *There is a one-to-one correspondence between †-Frobenius structure and orthonormal bases in* **FdHilb***; this correspondence is established by eqs.*(1).

Thus, †-Frobenius structures truly axiomatise orthonormal bases.

Definition 3.4 Let (A, δ_A, γ_A) and (B, δ_B, γ_B) be two †-Frobenius structures, then $f : A \to B$ is a *partial map* if $\delta_B \circ f = (f \otimes f) \circ \delta_A$, diagrammatically



Moreover, it is a *total map* if also $\gamma_B \circ f = \gamma_A$, which depicts as



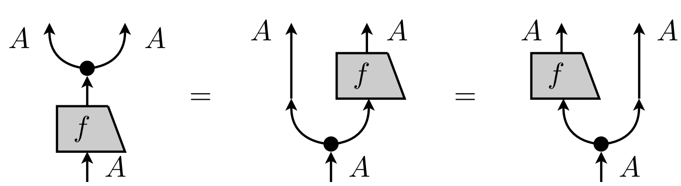
Finally, it is a *permutation* if, in addition to the previous, f is unitary.

Carboni and Walters showed in [3] that in the category of finite sets, relations and the cartesian product, for a 'suitably restricted' notion of †-Frobenius structures, these partial and total maps, and permutations, correspond to the usual notion. As a consequence of Theorem 3.3, for arbitrary †-Frobenius structures, in **FdHilb** these partial and total maps, and permutations, correspond to the usual notion – a simple computation easily demonstrates this. They map the base vectors of one classical structure on the base vectors of the other classical structure.

Definition 3.5 Let (A, δ_A, γ_A) be a †-Frobenius structure, then a unitary morphism $f : A \to A$ is a *phase map* if

$$(f \otimes 1_A) \circ \delta_A = \delta_A \circ f = (1_A \otimes f) \circ \delta_A\,,$$

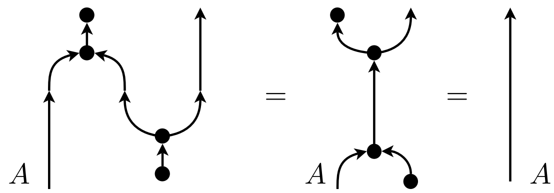
this is



In **FdHilb** the equality $(f \otimes 1_{\mathcal{H}}) \circ \delta_{\mathcal{H}} = \delta_{\mathcal{H}} \circ f$ implies for $f = \sum_{ij} f_{ij}|i\rangle\langle j|$ that $\sum_i f_{ij}|ik\rangle = \sum_i f_{ij}|ii\rangle$ for all k, hence $((f_{ij})_{ij})$ must be diagonal. Unitarity assures that all these diagonal elements are of the form $e^{i\theta}$, hence the name 'phase map'.

Lemma 3.6 [7] *In a †-SMC, whenever (A, δ_A, γ_A) is a †-Frobenius structure, then $(A, \epsilon_A := \gamma_A \circ \delta_A^\dagger)$ is a †-compact structure, with $A^* = A$.*

Proof.



□

So †-Frobenius structure 'factorizes' †-compact structure. However, this forces $A^* = A$.[8] As a consequence, a †-compact category in which the †-compact structure factorizes as †-Frobenius structure cannot be strict! (in the sense of Definition 2.5)

Lemma 3.7 *In a †-SMC, if (A, δ_A, γ_A) is a †-Frobenius structure, and $U : A \to A$ is unitary, then $(A, (U \otimes U) \circ \delta_A \circ U^\dagger, \gamma_A \circ U^\dagger)$ is also a †-frobenius structure. These two †-frobenius structure induce the same †-compact structure if and only if $U_* = U$.*

In **FdHilb** the equation $U_* = U$ implies that the matrix representation of U only involves real numbers. It then easily follows that the X-, Y- and Z-bases, i.e.,

$$\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\} \qquad \{|0\rangle + i|1\rangle, |0\rangle - i|1\rangle\} \qquad \{|0\rangle, |1\rangle\}$$

cannot be cast as †-Frobenius structures which share the same compact structure, since transforming them in each other requires complex matrix entries.

3.2 Dagger dual Frobenius structure

We now introduce a different 'factorization' of compact structures, as †-*dual Frobenius structure*. This does not impose $A^* = A$. Intuitively, the axiomatisation of bases in a dagger compact category implies that every object A has two duals:

- First, the object A^* which comes from the †-compact structure and
- The object A itself as it is self-dual when equipped with a †-Frobenius structure (A, δ_A, γ_A) (see lemma 3.6).

These two duals of A are isomorphic [14]. Instead of requiring $A = A^*$ as was done in [8,7], we make this isomorphism – the *dualiser* between A and A^* – explicit.

Definition 3.8 A †-*dual Frobenius structure* in a †-SMC is a quadruple

$$(A, \delta_A : A \to A \otimes A, \gamma_A : A \to I, d_A : A \to A^*)$$

such that

- (A, δ_A, γ_A) is a †-Frobenius structure.
- d_A is unitary.

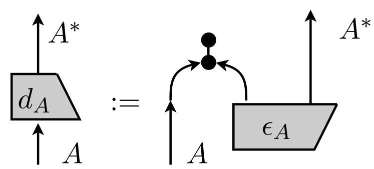
[8] Note that this does not obstruct modelling bases in **FdHilb**. The reason of this is that there is no unique dagger compact structure on **FdHilb** but that many different ones can be chosen. Those include the ones where we 'pick' $\mathcal{H}^*$ to be the conjugate space as well as the ones where we 'pick' $\mathcal{H}^*$ to be $\mathcal{H}$ itself.

Theorem 3.9 *For a given †-SMC,*

(i) *If* (A, δ_A, γ_A) *is a †-Frobenius structure and* (A, ϵ_A) *is a †-compact structure, then* $(A, \delta_A, \gamma_A, d_A)$ *is a †-dual Frobenius structure, where*

$$d_A := (\gamma_A^\dagger \otimes 1_{A^*}) \circ (\delta_A^\dagger \otimes 1_{A^*}) \circ (1_A \otimes \epsilon_A^\dagger)\,,$$

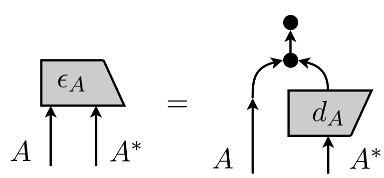
that is, graphically,



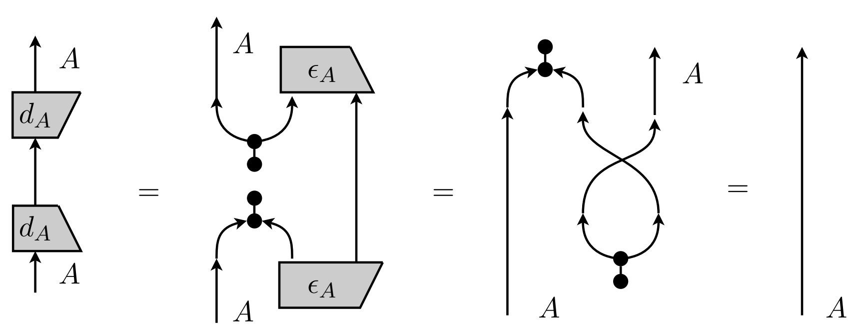
(ii) *If* $(A, \delta_A, \gamma, d_A)$ *is a †-dual Frobenius structure then* (A, δ_A, γ_A) *is a †-Frobenius structure and* (A, ϵ_A) *is a †-compact structure, where*

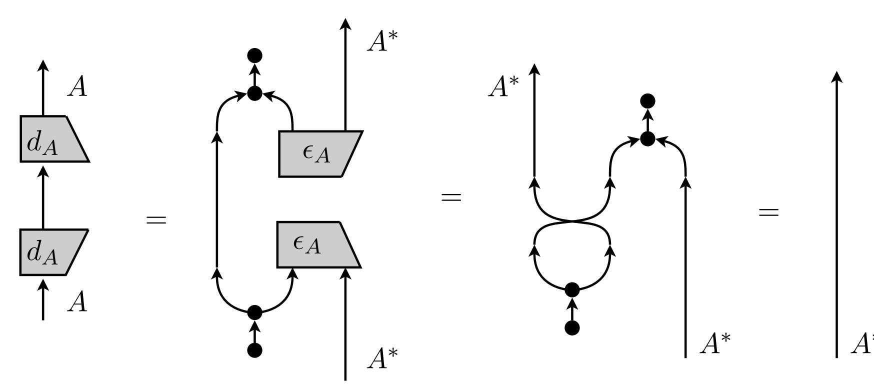
$$\epsilon_A := \gamma_A \circ \delta_A^\dagger \circ (1_A \otimes d_A^\dagger))$$

which is

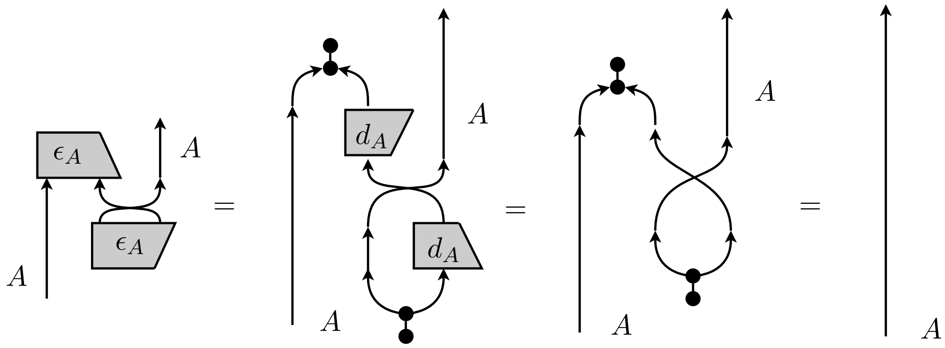


Proof. (i) Unitarity of d_A means $d_A^\dagger \circ d_A = 1_A$ and $d_A \circ d_A^\dagger = 1_{A^*}$ which holds since





(ii) We have †-compactness for (A, ϵ_A) since



□

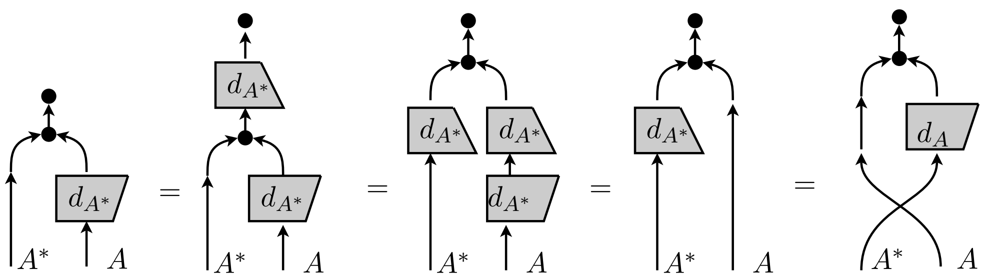
Definition 3.10 A †-*compact category with bases* is a †-SMC such that every object A comes with †-dual Frobenius structure

$$(A, \delta_A : A \to A \otimes A, \gamma_A : A \to I, d_A : A \to A^*)\,,$$

and where the †-dual Frobenius structures on object A and its dual A^* are connected by the fact that $d_{A^*} = d_A^\dagger$ and that d_A is a *permutation*.

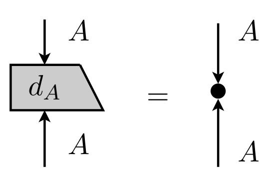
Lemma 3.11 *A †-compact category with bases is 'indeed' a †-compact category.*

Proof. For each object A, let $\epsilon_A := \gamma_A \circ \delta_A^\dagger \circ (1_A \otimes d_A^\dagger)$; according to Thm. 3.9 this entails that (A, ϵ_A) is a †-compact structure. Moreover, $\epsilon_{A^*} = \epsilon_A \circ \sigma_{A^*,A}$ since

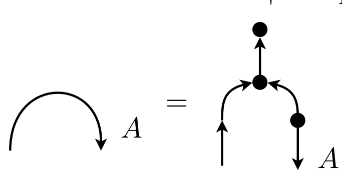


where the two first steps use the fact that d_{A^*} is a function and the third one uses unitarity of d_{A^*}. □

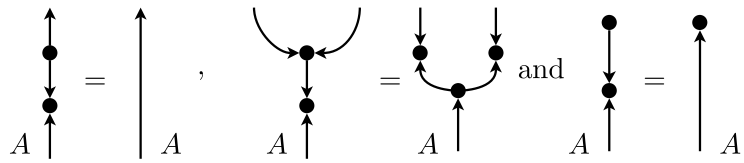
The graphical language for †-compact categories can now be extended to †-compact categories with bases:
- First, the dualiser depicts as:



- The †-dual Frobenius structure 'factorizes' the †-compact structure:



- Finally, the coherence conditions are those of the †-Frobenius structures and:



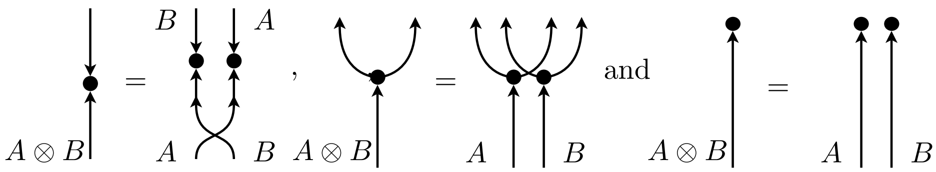
Definition 3.12 A *strict †-compact category with bases* is a †-compact category with bases which is such that for any objects A and B we have

$$d_{A\otimes B} = (d_B \otimes d_A) \circ \sigma_{A,B}$$

and also

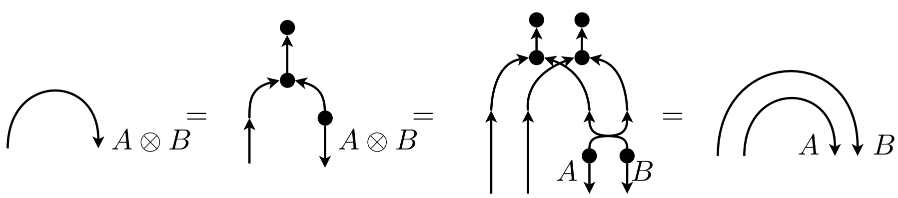
$$\delta_{A\otimes B} = (1_A \otimes \sigma_{A,B} \otimes 1_B) \circ (\delta_A \otimes \delta_B) \qquad \text{and} \qquad \gamma_{A\otimes B} = \gamma_A \otimes \gamma_B\,.$$

Graphically, these are



Lemma 3.13 *A strict †-compact category with bases is 'indeed' strict.*

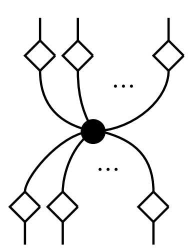
Proof. Since



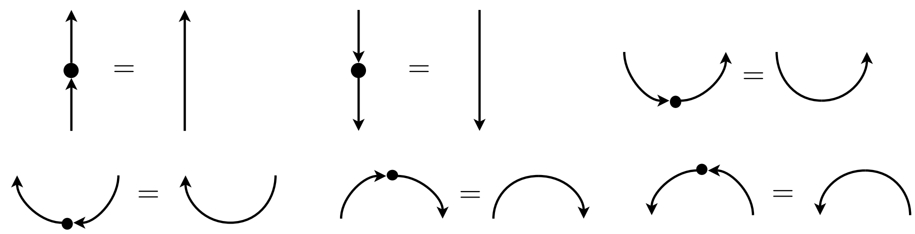
we indeed obtain strictness as in Defn. 2.5. □

3.3 Spider theorem for base structures

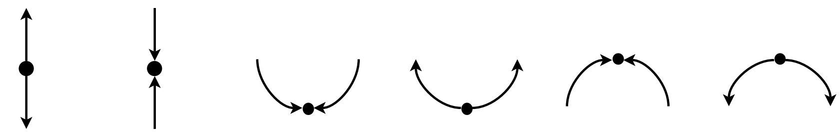
The spider theorem for †-Frobenius structures of [6] also holds in †-compact categories with bases provided we allow the spider's legs to be directed. Hence a spider now takes the form



where the diamonds either represent an up- or a down-arrow. There are six special cases, namely



in which we can drop the dot. However, in the six cases



the presence of the dot is essential.

Theorem 3.14 (oriented spider) *Let A and A^* be objects in a †-compact category with bases. Then, in the graphical representation, each 'connected' diagram Ξ obtained from †-SMC structure and the †-dual Frobenius structure both on A and A^* is equal to a 'spider with directed legs', of which the inputs/outputs have the same orientation as the inputs/outputs of Ξ.*

Hence, every such 'connected' diagram only depends on its number of inputs, it's number of outputs, and the directions of the arrows at these inputs and outputs.

4 Protocols

4.1 The quantum teleportation protocol

The quantum teleportation protocol [2] involves three qubits a, b, c and two parties Alice and Bob. At the start of the protocol:

- The pair (a, b) is in state $|00\rangle + |11\rangle$, and qubit a is in Alice's possession while qubit b is in Bob's possession.
- Qubit c is in an unknown state $|\phi\rangle$ and in Alice's possession.

To realise the protocol, the following steps are taken:

(i) Alice performs a Bell base measurement on her pair of qubits (c, a),

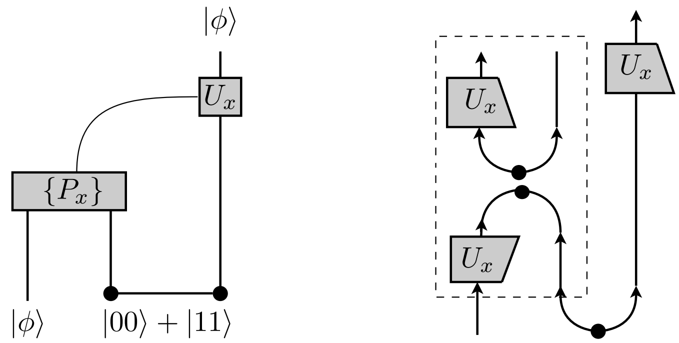
(ii) Alice sends the classical outcome x of this measurement to Bob, and,

(iii) Bob applies a particular – on x depending – unitary operation U_x.

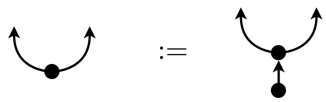
As a result qubit b will now be the unknown state $|\phi\rangle$. The unitary transformation U_x applied by Bob is one of the Pauli operators, and the Bell measurement applied by Alice is composed of four projectors $\{P_x\}_{x=0..3}$, such that for any x,

$$P_x = (U_x \otimes 1_{\mathcal{H}}) \circ (\delta_{std} \circ \gamma_{std}^{\dagger}) \circ (\gamma_{std} \circ \delta_{std}^{\dagger}) \circ (U_x^{\dagger} \otimes 1_{\mathcal{H}})$$

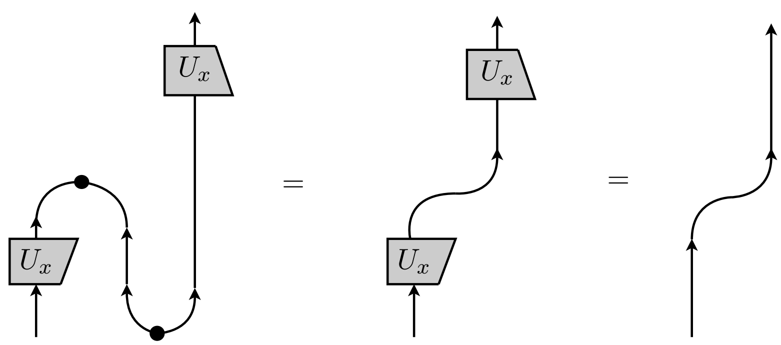
Thus, the protocol of teleportation can be described in the graphical language of †-SMC with †-Frobenius structures:



where we used following diagrammatic notation:



Note here in particular, as compared to the presentation in [1], that all arrows point in the direction of the actual physical flow of time. It are the 'dots' (= dualizers) which enable it. Lemma 3.6 provides a both intuitive and rigourous proof of correctness for teleportation:



This diagrammatic proof very much resembles 'yanking a rope' as it was the case in the original diagrammatic proof in [1] for correctness of the teleportation protocool, with as only difference the 'anihilation' of the two dots involved (see §4.4 below). Formally however, our proof is not based on †-compact structures but on †-Frobenius structures. This presentation enables easy comparison of the teleportation protocol with the following one.

4.2 The quantum state transfer protocol

The state transfer involves only two qubits (a, b). At the start of the protocol:

- Qubit a is an unknown state $|\phi\rangle$, and,
- Qubit b is in state $|0\rangle + |1\rangle$.

To realise the protocol, the following steps are taken:

(i) Qubits a and b are measured according to the parity measurement,

(ii) Qubit a is measured in the diagonal basis, and,

(iii) A unitary operation U_{xy} is applied on qubit b, depending on the classical outcomes x, y of the previous two measurements.

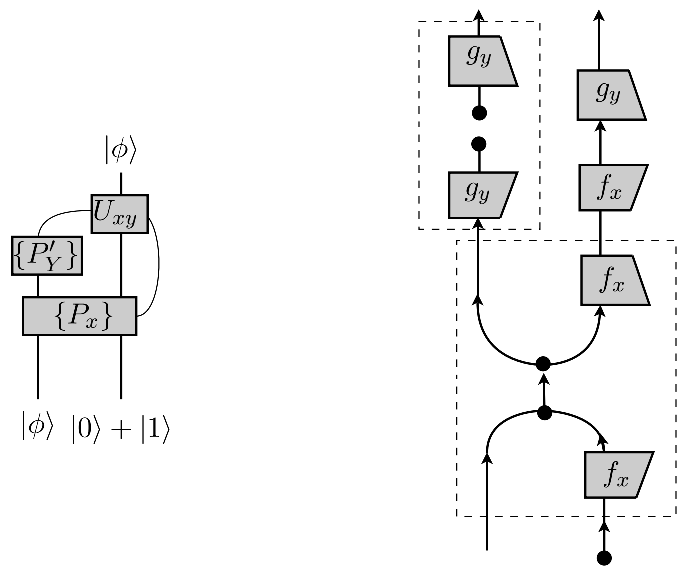
As a result qubit b will now be the unknown state $|\phi\rangle$. A parity measurement is a partial measurement. The state of the measured 2-qubit system is not projected on a vector, but on a plane: either on the *even plane* spanned by $|00\rangle$ and $|11\rangle$ or on the *odd plane* spanned by $|01\rangle$ and $|10\rangle$. The projectors are, for $x \in \{0, 1\}$,

$$\pi_x = (1_{\mathcal{H}} \otimes f_x) \circ \delta_{std} \circ \delta_{std}^{\dagger} \circ (1_{\mathcal{H}} \otimes f_x^{\dagger})$$

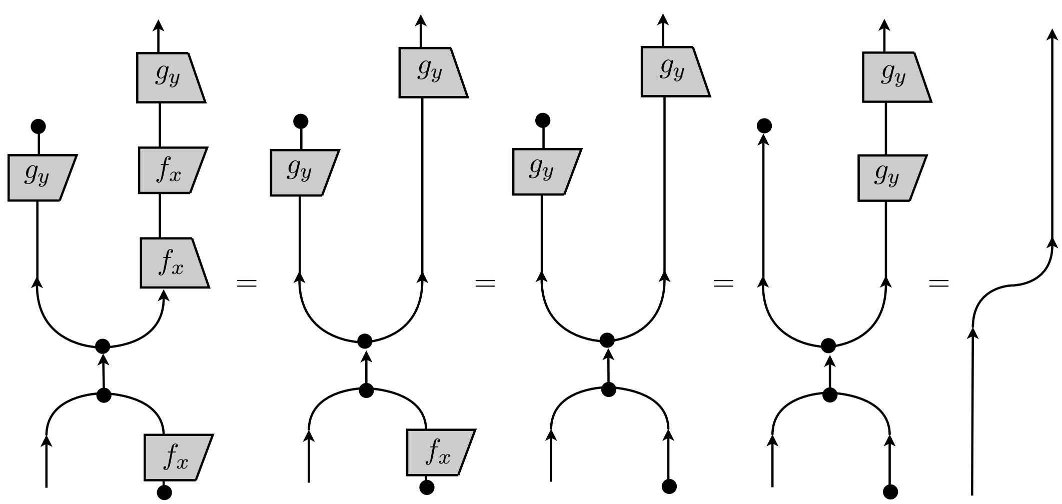
where f_x is a *permutation*. A diagonal basis measurement is a 1-qubit measurement described by the following projectors, for $y \in \{0, 1\}$ and g_y unitary *phase maps*,

$$P'_y = g_y \circ \gamma_{std}^{\dagger} \circ \gamma_{std} \circ g_y^{\dagger}\,.$$

In the graphical language of †-SMC with †-Frobenius structures we obtain:

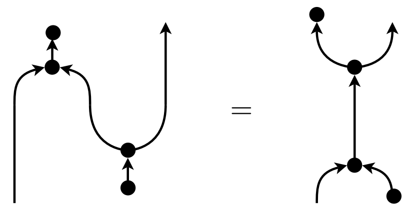


The †-Frobenius structure and the properties of the permutations and phase morphisms provide a diagrammatic proof of the state transfer:



4.3 Unifying state transfer and teleportation

In sections 4.1 and 4.2, the graphical calculus for †-SMC with †-Frobenius structures has been used to give a diagrammatic representation and proof of both teleportation and state transfer. State transfer was initially introduced to optimise the resources of measurement-only quantum computation [18]: while teleportation requires three qubits state transfer requires only two qubits. The diagrammatic representation of these two protocols leads to a better understanding of the foundational structures of measurement-only quantum computation: one can transform teleportation into state transfer and vice versa just by applying the Frobenius equation as it is illustrated in the following diagram



where, for reasons of clarity, all unitary transformations are taken to be identity.

While state transfer requires less ancillary qubits than teleportation, it needs more *structural resources* in the sense that the unitary transformations f_x and g_y have to be permutations and phase morphisms respectively. Also, while for teleportation we could rely on compact structure only, as in [1], for state transfer, even in post-selected form, the use of Frobenius structures (= a *base*) is *essential*.

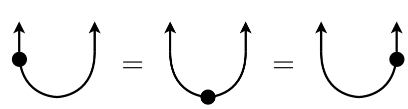
4.4 Flow of information

Our diagrammatic proofs of teleportation and state transfer rely on †-Frobenius structures in †-SMCs rather than on †-compact structure. However, compactness allows both Joyal, Street and Verity's construction of the trace [12] as well as Selinger's CPM construction [20]. One can use †-compact categories with bases in order to take advantage of both axiomatisations. In such a categorical framework the diagrammatic proofs of teleportation due to Abramsky and Coecke based on compact structure can be converted into the one presented in this paper using base structures, and vice versa.

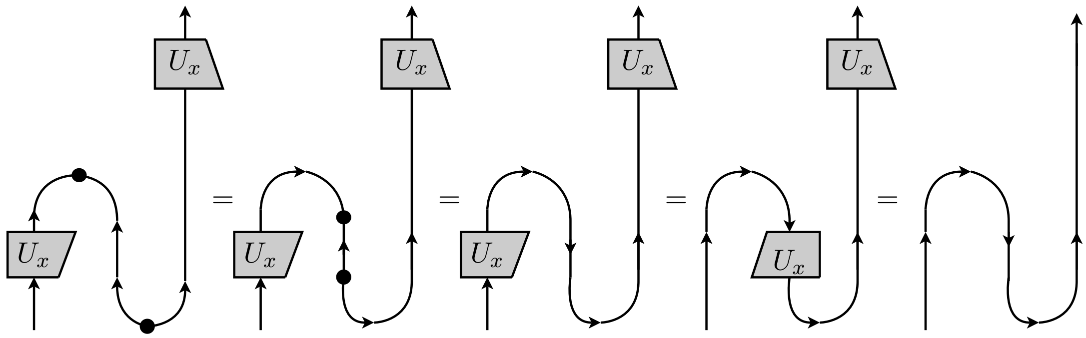
Lemma 4.1 *In a †-compact category with bases, for any object A we have*

$$(d_A^\dagger \otimes 1_A) \circ \epsilon_{A^*}^\dagger = \delta_A \circ \gamma_A^\dagger = (1_A \otimes d_A^\dagger) \circ \epsilon_A^\dagger$$

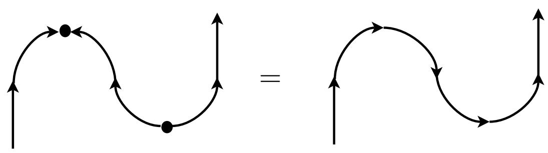
that is, graphically,



Note that while equality of the left and the right picture reflects a fact derivable in compact categories for arbitrary morphisms – involving the transposed $(-)^*$ – the picture in the middle can only be given meaning for base structure. We have:



Note in particular that in



the directions of the arrows in picture on the left can be interpreted as

- *the physical flow of information*,

since they respect causal ordering, while the directions of the arrows in picture on the right, which do not respect causal ordering, can be interpreted as

- *the logical flow of information.*

This logical flow of information guides the unknown input state to where it will end up at the end of the protocol. Having both compact structure and Frobenius structure available enables interchange between these two complementary views.

References

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

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[3] A. Carboni and R. F. C. Walters. Cartesian bicategories I. *Advances in Mathematics*, (49):11–32, 1987.

[4] B. Coecke. De-linearizing linearity: projective quantum axiomatics from strong compact closure. *Electronic Notes in Theoretical Computer Science*, 170:49–72, 2007. arXiv:quant-ph/0506134.v2.

[5] B. Coecke and R. Duncan. Interacting quantum observables. In *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP 2008*. Lecture Notes in Computer Science, 2008. to appear.

[6] B. Coecke and E. O. Paquette. Generalized measurements and Naimarks theorem without sums. In P. Selinger, editor, *Proceedings of Quantum Programming Languages IV*. arXiv:quant-ph/0608072.v2.

[7] B. Coecke, E. O. Paquette, and D. Pavlovic. Classical and quantum structures. 2007.

[8] B. Coecke and D. Pavlovic. *The Mathematics of Quantum Computation and Technology*, chapter Quantum measurements without sums. CRC Applied Mathematics Nonlinear Science, Taylor and Francis, 2007. arXiv:quant-ph/0608035.

[9] B. Coecke, D. Pavlovic, and J. Vicary. Commutative dagger Frobenius algebras in FdHilb are bases. Oxford University Computing Laboratory Research Report RR-08-03, 2008.

[10] Ph. Jorrand and S. Perdrix. Unifying quantum computation with projective measurements only and one-way quantum computation. In *Quantum Informatics 2004, Proceedings of the SPIE*, volume 5833, pages 44–51, 2005.

[11] A. Joyal and R. Street. The geometry of tensor calculus I. *Advances in Mathematics*, (88):55–112, 1991.

[12] A. Joyal, R. Street, and D. Verity. Traced monoidal categories. *Mathematical Proceedings of the Cambridge Philosophical Society*, (3):447–468, 1996.

[13] R. Jozsa. An introduction to measurement based quantum computation. arXiv:quant-ph/0508124v2.

[14] G. M. Kelly and M. L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, (19):194–213, 1980.

[15] J. Kock. *Frobenius Algebras and 2D Topological Quantum Field Theories*. Cambridge UP, 2003.

[16] S. Lack. Composing PROPs. *Theory and Applications of Categories*, (13):147–163, 2004.

[17] S. E. Morrison. *A diagrammatic category for the representation theory of* $U_q(sl_n)$. PhD thesis, University of California at Berkeley, 2007.

[18] S. Perdrix. State transfer instead of teleportation in measurement-based quantum computation. *International Journal of Quantum Information*, 3(1):219–223, 2005.

[19] S. Perdrix. Towards minimal resources of measurement-based quantum computation. *New Journal of Physics*, 9 206, June 2007.

[20] P. Selinger. Dagger compact closed categories and completely positive maps. In *Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL 2005), Chicago*, number 170, pages 139–163. ENTCS, 2007.

[21] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.