A categorical semantics of quantum protocols

Samson Abramsky and Bob Coecke

Oxford University Computing Laboratory,
Wolfson Building, Parks Road, Oxford OX1 3QD, UK.
samson.abramsky · bob.coecke@comlab.ox.ac.uk

Abstract

We study quantum information and computation from a novel point of view. Our approach is based on recasting the standard axiomatic presentation of quantum mechanics, due to von Neumann [28]*, at a more abstract level, of compact closed categories with biproducts. We show how the essential structures found in key quantum information protocols such as teleportation* [5]*, logic-gate teleportation* [12]*, and entanglement swapping* [29] *can be captured at this abstract level. Moreover, from the combination of the — apparently purely qualitative — structures of compact closure and biproducts there emerge 'scalars' and a 'Born rule'. This abstract and structural point of view opens up new possibilities for describing and reasoning about quantum systems. It also shows the degrees of axiomatic freedom: we can show what requirements are placed on the (semi)ring of scalars* $\mathbf{C}(\mathrm{I}, \mathrm{I})$*, where* $\mathbf{C}$ *is the category and* I *is the tensor unit, in order to perform various protocols such as teleportation. Our formalism captures both the information-flow aspect of the protocols* [8, 9]*, and the branching due to quantum indeterminism. This contrasts with the standard accounts, in which the classical information flows are 'outside' the usual quantum-mechanical formalism.*

We give detailed formal descriptions and proofs of correctness of the example protocols.

1. Introduction

Quantum information and computation is concerned with the use of quantum-mechanical systems to carry out computational and information-processing tasks [20]. In the few years that this approach has been studied, a number of remarkable concepts and results have emerged. Our particular focus in this paper is on *quantum information protocols*, which exploit quantum-mechanical effects in an essential way. The particular examples we shall use to illustrate our approach will be *teleportation* [5], *logic-gate teleportation* [12], and *entanglement swapping* [29]. The ideas illustrated in these protocols form the basis for novel and potentially very important applications to secure and fault-tolerant communication and computation [7, 12, 20].

We now give a thumbnail sketch of teleportation to motivate our introductory discussion. (A more formal 'standard' presentation is given in Section 2. The — radically different — presentation in our new approach appears in Section 9.) Teleportation involves using an entangled pair of qubits (q_A, q_B) as a kind of communication channel to transmit an unknown qubit q from a source A ('Alice') to a remote target B ('Bob'). A has q and q_A, while B has q_B. We firstly entangle q_A and q at A (by performing a suitable unitary operation on them), and then perform a measurement on q_A and q.[1] This forces a 'collapse' in q_B because of its entanglement with q_A. We then send two classical bits of information from A to B, which encode the four possible results of the measurement we performed on q and q_A. Based on this classical communication, B then performs a 'correction' by applying one of four possible operations (unitary transformations) to q_B, after which q_B *has the same state that* q *had originally*. (Because of the measurement, q no longer has this state — the information in the source has been 'destroyed' in transferring it to the target). It should be born in mind that the information required to specify q is an arbitrary pair of complex numbers (α, β) satisfying $|\alpha|^2 + |\beta|^2 = 1$, so achieving this information transfer with just two classical bits is no mean feat!

Teleportation is simply the most basic of a family of quantum protocols, and already illustrates the basic ideas, in particular the use of *preparations of entangled states* as carriers for information flow, performing *measurements* to propagate information, using *classical information* to control branching behaviour to ensure the required behaviour despite quantum indeterminacy, and performing lo-

[1] This measurement can be performed in the standard 'computational basis'. The combination of unitary and measurement is equivalent to measurement in the 'Bell basis'.

cal data transformations using *unitary operations*. (Local here means that we apply these operations only at A or at B, which are assumed to be spatially separated, and not simultaneously at both).

Our approach is based on recasting the standard axiomatic presentation of Quantum Mechanics, due to von Neumann [28], at a more abstract level, of *compact closed categories with biproducts*. Remarkably enough, all the essential features of quantum protocols mentioned above find natural counterparts at this abstract level — of which the standard von Neumann presentation in terms of Hilbert spaces is but one example. More specifically:

- The basic structure of a symmetric monoidal category allows *compound systems* to be described in a resource-sensitive fashion (cf. the 'no cloning' and 'no deleting' theorems of quantum mechanics [20]).
- The compact closed structure allows *preparations and measurements of entangled states* to be described, and their key properties to be proved.
- Biproducts allow *indeterministic branching, classical communication and superpositions* to be captured.

We are then able to use this abstract setting to give precise formulations of teleportation, logic gate teleportation, and entanglement swapping, and to prove correctness of these protocols — for example, proving correctness of teleportation means showing that the final value of q_B equals the initial value of q. Moreover, from the combination of the—apparently purely qualitative—structures of compact closure and biproducts there emerge *scalars* and a *Born rule*.

One of our main concerns is to replace ad hoc calculations with bras and kets, normalizing constants, unitary matrices etc. by conceptual definitions and proofs. This allows general underlying structures to be identified, and general lemmas to be proved which encapsulate key formal properties. The compact-closed level of our axiomatization allows the key *information-flow properties* of entangled systems to be expressed. Here we are directly abstracting from the more concrete analysis carried out by one of the authors in [8, 9]. The advantage of our abstraction is shown by the fact that the extensive linear-algebraic calculations in [8] are replaced by a few simple conceptual lemmas, valid in an arbitrary compact closed category. We are also able to reuse the template of definition and proof of correctness for the basic teleportation protocol in deriving and verifying logic-gate teleportation and entanglement swapping.

The compact-closed level of the axiomatization allows information flow along any branch of a quantum protocol execution to be described, but it does not capture the *branching* due to measurements and quantum indeterminism. The biproduct structure allows this branching behaviour to be captured. Since biproducts induce a (semi)additive structure, the superpositions characteristic of quantum phenomena can be captured at this abstract level. Moreover, the biproduct structure interacts with the compact-closed structure in a non-trivial fashion. In particular, the *distributivity* of tensor product over biproduct allows classical communication, and the dependence of actions on the results of previous measurements (exemplified in teleportation by the dependence of the unitary correction on the result of the measurement of q and q_A), to be captured within the formalism. In this respect, our formalism is *more comprehensive* than the standard von Neumann axiomatization. In the standard approach, the use of measurement results to determine subsequent actions is left informal and implicit, and hence not subject to rigorous analysis and proof. As quantum protocols and computations grow more elaborate and complex, this point is likely to prove of increasing importance.

Another important point concerns the *generality* of our axiomatic approach. The standard von Neumann axiomatization fits Quantum Mechanics perfectly, with no room to spare. Our basic setting of compact closed categories with biproducts is general enough to allow very different models such as $\mathbf{Rel}$, the category of sets and relations. When we consider specific protocols such as teleportation, a kind of 'Reverse Arithmetic' (by analogy with Reverse Mathematics [26]) arises. That is, we can characterize what requirements are placed on the 'semiring of scalars' $\mathbf{C}(\mathrm{I}, \mathrm{I})$ (where I is the tensor unit) in order for the protocol to be realized. This is often much less than requiring that this be the field of complex numbers (but in the specific cases we shall consider, the requirements are sufficient to exclude $\mathbf{Rel}$). Other degrees of axiomatic freedom also arise, although we shall not pursue that topic in detail in the present paper.

The remainder of the paper is structured as follows. Section 2 contains a rapid review of the standard axiomatic presentation of Quantum Mechanics, and of the standard presentations of our example protocols. Section 3 introduces compact closed categories, and presents the key lemmas on which our analysis of the information-flow properties of these protocols will be based. Section 4 relates this general analysis to the more concrete and specific presentation in [8]. Section 5 introduces biproducts. Sections 6 and 7 present our abstract treatments of scalars and adjoints. Section 8 presents our abstract formulation of quantum mechanics. Section 9 contains our formal descriptions and verifications of the example protocols. Section 10 concludes.

2. Quantum mechanics and teleportation

In this paper, we shall only consider *finitary* quantum mechanics, in which all Hilbert spaces are finite-dimensional. This is standard in most current discussions of quantum computation and information [20], and corresponds physically to considering only observables with finite spectra, such as *spin*. (We refer briefly to the extension of our approach to the infinite-dimensional case in the Conclusions.)

Finitary quantum theory has the following basic ingredients (for more details, consult standard texts such as [13]).

1. The *state space* of the system is represented as a finite-dimensional Hilbert space $\mathcal{H}$, *i.e.* a finite-dimensional complex vector space with an inner product written $\langle \phi \mid \psi \rangle$, which is conjugate-linear in the first argument and linear in the second. A *state* of a quantum system corresponds to a one-dimensional subspace $\mathcal{A}$ of $\mathcal{H}$, and is standardly represented by a vector $\psi \in \mathcal{A}$ of unit norm.

2. For informatic purposes, the basic type is that of *qubits*, namely 2-dimensional Hilbert space, equipped with a *computational basis* $\{|0\rangle, |1\rangle\}$.

3. *Compound systems* are described by tensor products of the component systems. It is here that the key phenomenon of *entanglement* arises, since the general form of a vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is

$$\sum_{i=1}^{n} \alpha_i \cdot \phi_i \otimes \psi_i$$

Such a vector may encode *correlations* between the first and second components of the system, and cannot simply be resolved into a pair of vectors in the component spaces.

The *adjoint* to a linear map $f : \mathcal{H}_1 \to \mathcal{H}_2$ is the linear map $f^\dagger : \mathcal{H}_2 \to \mathcal{H}_1$ such that, for all $\phi \in \mathcal{H}_2$ and $\psi \in \mathcal{H}_1$,

$$\langle \phi \mid f(\psi) \rangle_{\mathcal{H}_2} = \langle f^\dagger(\phi) \mid \psi \rangle_{\mathcal{H}_1} .$$

Unitary transformations are linear isomorphisms

$$U : \mathcal{H}_1 \to \mathcal{H}_2$$

such that

$$U^{-1} = U^\dagger : \mathcal{H}_2 \to \mathcal{H}_1 .$$

Note that all such transformations *preserve the inner product* since, for all $\phi, \psi \in \mathcal{H}_1$,

$$\langle U(\phi) \mid U(\psi) \rangle_{\mathcal{H}_2} = \langle (U^\dagger U)(\phi) \mid \psi \rangle_{\mathcal{H}_1} = \langle \phi \mid \psi \rangle_{\mathcal{H}_1} .$$

Self-adjoint operators are linear transformations

$$M : \mathcal{H} \to \mathcal{H}$$

such that $M = M^\dagger$.

4. The *basic data transformations* are represented by unitary transformations. Note that all such data transformations are necessarily *reversible*.

5. The *measurements* which can be performed on the system are represented by self-adjoint operators.

The act of measurement itself consists of two parts:

5a. The observer is informed about the measurement outcome, which is a value x_i in the spectrum $\sigma(M)$ of the corresponding self-adjoint operator M. For convenience we assume $\sigma(M)$ to be *non-degenerate* (linearly independent eigenvectors have distinct eigenvalues).

5b. The state of the system undergoes a change, represented by the action of the *projector* P_i arising from the *spectral decomposition*

$$M = x_1 \cdot \mathrm{P}_1 + \ldots + x_n \cdot \mathrm{P}_n$$

In this spectral decomposition the projectors $\mathrm{P}_i : \mathcal{H} \to \mathcal{H}$ are idempotent and self-adjoint,

$$\mathrm{P}_i \circ \mathrm{P}_i = \mathrm{P}_i \quad \text{and} \quad \mathrm{P}_i = \mathrm{P}_i^\dagger,$$

and mutually orthogonal:

$$\mathrm{P}_i \circ \mathrm{P}_j = 0, \qquad i \neq j.$$

This spectral decomposition always exists and is unique by the *spectral theorem* for self-adjoint operators. By our assumption that $\sigma(M)$ was non-degenerate each projector P_i has a one-dimensional subspace of $\mathcal{H}$ as its fixpoint set (which equals its image).

The probability of $x_i \in \sigma(M)$ being the actual outcome is given by the *Born rule* which does not depend on the value of x_i but on P_i and the system state ψ, explicitly

$$\mathsf{Prob}(\mathrm{P}_i, \psi) = \langle \psi \mid \mathrm{P}_i(\psi) \rangle .$$

The status of the Born rule within our abstract setting will emerge in Section 8. The derivable notions of *mixed states* and *non-projective measurements* will not play a significant rôle in this paper.

The values $x_1, \ldots, x_n$ are in effect merely labels distinguishing the projectors $\mathrm{P}_1, \ldots, \mathrm{P}_n$ in the above sum. Hence we can abstract over them and think of a measurement as a list of n mutually orthogonal projectors $(\mathrm{P}_1, \ldots, \mathrm{P}_n)$ where n is the dimension of the Hilbert space.

Although real-life experiments in many cases destroy the system (e.g. any measurement of a photon's location destroys it) measurements always have the same shape in the quantum formalism. When distinguishing between 'measurements which preserve the system' and 'measurements which destroy the system' it would make sense to decompose a measurement explicitly in two components:

- *Observation* consists of receiving the information on the outcome of the measurement, to be thought of as specification of the index i of the outcome-projector P_i in the above list. Measurements which destroy the system can be seen as 'observation only'.
- *Preparation* consists of producing the state $\mathrm{P}_i(\psi)$.

In our abstract setting these arise naturally as the two 'building blocks' which are used to construct projectors and measurements.

We now discuss some important quantum protocols which we chose because of the key rôle entanglement plays in them — they involve both initially entangled states, and measurements against a basis of entangled states.

2.1 Quantum teleportation

The quantum teleportation protocol [5] (see also [8] §2.3 and §3.3) involves three qubits a, b and c (corresponding to q, q_A and q_B respectively in our preliminary sketch in the Introduction). Qubit a is in a state $|\phi\rangle$ and qubits b and c form an 'EPR-pair', that is, their joint state is $|00\rangle + |11\rangle$. After spatial relocation (so that a and b are positioned at the source A, while c is positioned at the target B), one performs a *Bell-base measurement* on a and b, that is, a measurement such that each P_i projects on one of the one-dimensional subspaces spanned by a vector in the *Bell basis*:

$$b_1 := \tfrac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle) \qquad b_2 := \tfrac{1}{\sqrt{2}} \cdot (|01\rangle + |10\rangle)$$

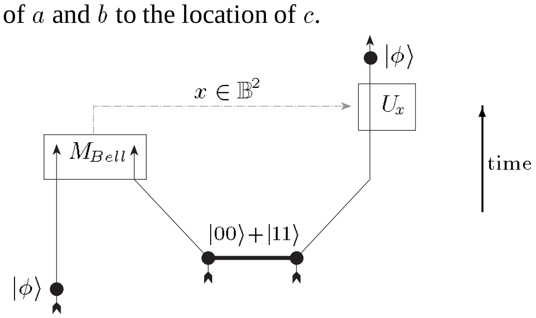
$$b_3 := \tfrac{1}{\sqrt{2}} \cdot (|00\rangle - |11\rangle) \qquad b_4 := \tfrac{1}{\sqrt{2}} \cdot (|01\rangle - |10\rangle)\,.$$

This measurement can be of the type 'observation only'. We observe the outcome of the measurement and depending on it perform one of the unitary transformations

$$\beta_1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \beta_2 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\beta_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \beta_4 := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

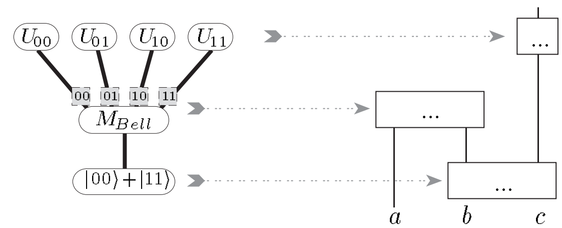
on c — $\beta_1, \beta_2, \beta_3$ are all self-inverse while $\beta_4^{-1} = -\beta_4$. Physically, this requires transmission of two classical bits, recording the outcome of the measurement, from the location of a and b to the location of c.



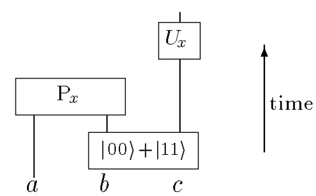
The final state of c proves to be $|\phi\rangle$ as well. We will be able to derive this fact in our abstract setting.

Since a continuous variable has been transmitted while the actual *classical communication* involved only two bits, besides this *classical information flow* there has to exist a *quantum information flow*. The nature of this quantum flow has been analyzed by one of the authors in [8, 9], building on the joint work in [2]. We recover those results in our abstract setting (see Section 4), which also reveals additional 'fine structure'. To identify it we have to separate it from the classical information flow. Therefore we decompose the protocol into:

1. a *tree* with the operations as nodes, and with *branching* caused by the indeterminism of measurements;
2. a *network* of the operations in terms of the order they are applied and the subsystem to which they apply.



The nodes in the tree are connected to the boxes in the network by their temporal coincidence. Classical communication is encoded in the tree as the dependency of operations on the branch they are in. For each path from the root of the tree to a leaf, by 'filling in the operations on the included nodes in the corresponding boxes of the network', we obtain an *entanglement network*, that is, a network



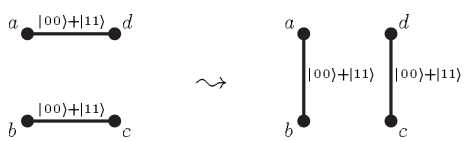
for each of the four values x takes. A component P_x of an observation will be referred to as an *observational branch*. It will be these networks, from which we have removed the classical information flow, that we will study in Section 4. (There is a clear analogy with the idea of unfolding a Petri net into its set of 'processes' [21]). The classical information flow will be reintroduced in Section 9.

2.2 Logic gate teleportation

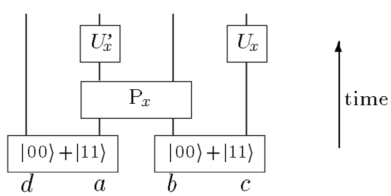
Logic gate teleportation [12] (see also [8] §3.3) generalizes the above protocol in that b and c are initially not necessarily an EPR-pair but may be in some other (not arbitrary) entangled state $|\Psi\rangle$. Due to this modification the final state of c is not $|\phi\rangle$ but $|f_\Psi(\phi)\rangle$ where f_Ψ is a linear map which depends on Ψ. As shown in [12], when this construction is applied to the situation where a, b and c are each a pair of qubits rather than a single qubit, it provides a universal quantum computational primitive which is moreover fault-tolerant [25] and enables the construction of a quantum computer based on single qubit unitary operations, Bell-base measurements and only one kind of prepared state (so-called GHZ states). The connection between Ψ, f_Ψ and the unitary corrections $U_{\Psi,x}$ will emerge straightforwardly in our abstract setting.

2.3 Entanglement swapping

Entanglement swapping [29] (see also [8] §6.2) is another modification of the teleportation protocol where a is not in a state $|\phi\rangle$ but is a qubit in an EPR-pair together with an ancillary qubit d. The result is that after the protocol c forms an EPR-pair with d. If the measurement on a and b is non-destructive, we can also perform a unitary operation on a, resulting in a and b also constituting an EPR-pair. Hence we have 'swapped' entanglement:



In this case the entanglement networks have the shape:



Why this protocol works will again emerge straightforwardly from our abstract setting, as will generalizations of this protocol which have a much more sophisticated compositional content (see Section 4).

3. Compact closed categories

Recall that a *symmetric monoidal category* consists of a category $\mathbf{C}$, a bifunctorial *tensor*

$$-\otimes- : \mathbf{C}\times\mathbf{C}\to\mathbf{C}\,,$$

a *unit* object I and natural isomorphisms

$$\lambda_A : A \simeq \mathrm{I}\otimes A \qquad\qquad \rho_A : A\simeq A\otimes \mathrm{I}$$

$$\alpha_{A,B,C} : A\otimes(B\otimes C)\simeq (A\otimes B)\otimes C$$

$$\sigma_{A,B} : A\otimes B\simeq B\otimes A$$

which satisfy certain coherence conditions [17]. A category $\mathbf{C}$ is $*$-*autonomous* [4] if it is symmetric monoidal, and comes equipped with a full and faithful functor

$$(\ )^* : \mathbf{C}^{op}\to\mathbf{C}$$

such that a bijection

$$\mathbf{C}(A\otimes B, C^*)\simeq \mathbf{C}(A,(B\otimes C)^*)$$

exists which is natural in all variables. Hence a $*$-autonomous category is closed, with

$$A\multimap B := (A\otimes B^*)^*\,.$$

These $*$-autonomous categories provide a categorical semantics for the multiplicative fragment of linear logic [23].

A *compact closed category* [15] is a $*$-autonomous category with a self-dual tensor, i.e. with natural isomorphisms

$$u_{A,B} : (A\otimes B)^*\simeq A^*\otimes B^* \qquad\quad u_{\mathrm{I}} : \mathrm{I}^*\simeq \mathrm{I}\,.$$

It follows that

$$A\multimap B\simeq A^*\otimes B\,.$$

3.1 Definitions and examples

A very different definition arises when one considers a symmetric monoidal category as a one-object bicategory. In this context, compact closure simply means that every object A, qua 1-cell of the bicategory, has an adjoint [16].

Definition 3.1 (Kelly-Laplaza) A *compact closed category* is a symmetric monoidal category in which to each object A a *dual object* A^*, a *unit*

$$\eta_A : \mathrm{I}\to A^*\otimes A$$

and a *counit*

$$\epsilon_A : A\otimes A^*\to \mathrm{I}$$

are assigned in such a way that the diagram

$$\begin{tikzcd}
A \arrow[r, "\rho_A"] \arrow[d, "1_A"'] & A\otimes \mathrm{I} \arrow[r, "1_A\otimes\eta_A"] & A\otimes(A^*\otimes A) \arrow[d, "\alpha_{A,A^*,A}"] \\
A & \mathrm{I}\otimes A \arrow[l, "\lambda_A^{-1}"] & (A\otimes A^*)\otimes A \arrow[l, "\epsilon_A\otimes 1_A"]
\end{tikzcd}$$

and the dual one for A^* both commute.

The monoidal categories $(\mathbf{Rel},\times)$ of sets, relations and cartesian product and $(\mathbf{FdVec}_{\mathbb{K}},\otimes)$ of finite-dimensional vector spaces over a field $\mathbb{K}$, linear maps and tensor product are both compact closed. In $(\mathbf{Rel},\times)$, taking a one-point set $\{*\}$ as the unit for $\times$, and writing $R^{\cup}$ for the converse of a relation R:

$$\eta_X = \epsilon_X^{\cup} = \{(*, (x,x)) \mid x \in X\}\,.$$

The unit and counit in $(\mathbf{FdVec}_{\mathbb{K}}, \otimes)$ are

$$\eta_V : \mathbb{K} \to V^* \otimes V :: 1 \mapsto \sum_{i=1}^{i=n} \bar{e}_i \otimes e_i$$
$$\epsilon_V : V \otimes V^* \to \mathbb{K} :: e_i \otimes \bar{e}_j \mapsto \bar{e}_j(e_i)$$

where n is the dimension of V, $\{e_i\}_{i=1}^{i=n}$ is a basis of V and $\bar{e}_i$ is the linear functional in V^* determined by $\bar{e}_j(e_i) = \delta_{ij}$.

Definition 3.2 The *name* $\ulcorner f \urcorner$ and the *coname* $\llcorner f \lrcorner$ of a morphism $f : A \to B$ in a compact closed category are

$$\begin{tikzcd} A^*\otimes A \arrow[r, "1_{A^*}\otimes f"] & A^*\otimes B \\ \mathrm{I} \arrow[u, "\eta_A"] \arrow[ur, "\ulcorner f \urcorner"'] & \end{tikzcd} \qquad \begin{tikzcd} & \mathrm{I} \\ A\otimes B^* \arrow[ur, "\llcorner f \lrcorner"] \arrow[r, "f\otimes 1_{B^*}"'] & B\otimes B^* \arrow[u, "\epsilon_B"'] \end{tikzcd}$$

For $R \in \mathbf{Rel}(X,Y)$ we have

$$\ulcorner R \urcorner = \{(*, (x,y)) \mid xRy, x \in X, y \in Y\}$$
$$\llcorner R \lrcorner = \{((x,y), *) \mid xRy, x \in X, y \in Y\}$$

and for $f \in \mathbf{FdVec}_{\mathbb{K}}(V,W)$ with (m_{ij}) the matrix of f in bases $\{e_i^V\}_{i=1}^{i=n}$ and $\{e_j^W\}_{j=1}^{j=m}$ of V and W respectively:

$$\ulcorner f \urcorner : \mathbb{K} \to V^* \otimes W :: 1 \mapsto \sum_{i,j=1}^{i,j=n,m} m_{ij} \cdot \bar{e}_i^V \otimes e_j^W$$
$$\llcorner f \lrcorner : V \otimes W^* \to \mathbb{K} :: e_i^V \otimes \bar{e}_j^W \mapsto m_{ij}\,.$$

3.2 Some constructions

Given $f : A \to B$ in any compact closed category $\mathbf{C}$ we can define $f^* : B^* \to A^*$ as follows [16]:

$$\begin{tikzcd} B^* \arrow[r, "\lambda_{B^*}"] \arrow[d, "f^*"'] & \mathrm{I}\otimes B^* \arrow[r, "\eta_A \otimes 1_{B^*}"] & A^*\otimes A\otimes B^* \arrow[d, "1_{A^*}\otimes f \otimes 1_{B^*}"'] \\ A^* & A^*\otimes \mathrm{I} \arrow[l, "\rho_{A^*}^{-1}"] & A^*\otimes B\otimes B^* \arrow[l, "1_{A^*}\otimes \epsilon_B"] \end{tikzcd}$$

This operation $(\ )^*$ is functorial and makes Definition 3.1 coincide with the one given at the beginning of this section. It then follows by

$$\mathbf{C}(A \otimes B^*, \mathrm{I}) \simeq \mathbf{C}(A,B) \simeq \mathbf{C}(I, A^* \otimes B)$$

that every morphism of type $\mathrm{I} \to A^* \otimes B$ is the name of some morphism of type $A \to B$ and every morphism of type $A \otimes B^* \to \mathrm{I}$ is the coname of some morphism of type $A \to B$. In the case of the unit and the counit we have

$$\eta_A = \ulcorner 1_A \urcorner \qquad \text{and} \qquad \epsilon_A = \llcorner 1_A \lrcorner\,.$$

For $R \in \mathbf{Rel}(X,Y)$ the dual is the converse, $R^* = R^{\cup} \in \mathbf{Rel}(Y,X)$, and for $f \in \mathbf{FdVec}_{\mathbb{K}}(V,W)$, the dual is

$$f^* : W^* \to V^* :: \phi \mapsto \phi \circ f\,.$$

In any compact closed category, there is a natural isomorphism $d_A : A^{**} \simeq A$.

The following holds by general properties of adjoints and the fact that the tensor is symmetric [16].

Proposition 3.3 *In a compact closed category* $\mathbf{C}$ *we have*

$$\begin{tikzcd} \mathrm{I} \arrow[r, "\eta_{A^*}"] \arrow[d, "\eta_A"'] & A^{**}\otimes A^* \arrow[d, "d_A \otimes 1_{A^*}"] \\ A^*\otimes A \arrow[r, "\sigma_{A^*,A}"'] & A\otimes A^* \end{tikzcd} \qquad \begin{tikzcd} A^*\otimes A \arrow[r, "\sigma_{A^*,A}"] \arrow[d, "1_{A^*}\otimes d_A^{-1}"'] & A\otimes A^* \arrow[d, "\epsilon_A"] \\ A^*\otimes A^{**} \arrow[r, "\epsilon_{A^*}"'] & \mathrm{I} \end{tikzcd}$$

for all objects A of $\mathbf{C}$.

3.3 Key lemmas

The following Lemmas constitute the core of our interpretation of entanglement in compact closed categories.

Lemma 3.4 (absorption) *For*

$$A \xrightarrow{f} B \xrightarrow{g} C$$

we have that

$$(1_{A^*} \otimes g) \circ \ulcorner f \urcorner = \ulcorner g \circ f \urcorner.$$

Proof: Straightforward by Definition 3.2. □

Lemma 3.5 (compositionality) *For*

$$A \xrightarrow{f} B \xrightarrow{g} C$$

we have that

$$\lambda_C^{-1} \circ (\llcorner f \lrcorner \otimes 1_C) \circ (1_A \otimes \ulcorner g \urcorner) \circ \rho_A = g \circ f\,.$$

Proof: See the diagram in the appendix to this paper which uses bifunctoriality and naturality of ρ and λ. □

Lemma 3.6 (compositional CUT) *For*

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

we have that

$$(\rho_A^{-1}\otimes 1_{D^*})\circ(1_{A^*}\otimes \llcorner g\lrcorner\otimes 1_D)\circ(\ulcorner f\urcorner\otimes\ulcorner h\urcorner)\circ\rho_I = \ulcorner h\circ g\circ f\urcorner.$$

Proof: See the diagram in the appendix to this paper which uses Lemma 3.5 and naturality of ρ and λ. □

On the right hand side of Lemma 3.5 we have $g \circ f$, that is, we first apply f and then g, while on the left hand side we first apply the coname of g, and then the coname of f. In Lemma 3.6 there is a similar, seemingly 'acausal' inversion of the order of application, as g gets inserted between h and f.

For completeness we add the following 'backward' absorption lemma, which again involves a reversal of the composition order.

Lemma 3.7 (backward absorption) *For*

$$C \xrightarrow{g} A \xrightarrow{f} B$$

we have that

$$(g^* \otimes 1_{A^*}) \circ \ulcorner f\urcorner = \ulcorner f \circ g\urcorner.$$

Proof: This follows by unfolding the definition of g^*, then using naturality of λ_{A^*}, $\lambda_{\mathrm{I}} = \rho_{\mathrm{I}}$, and finally Lemma 3.6. □

The obvious analogues of Lemma 3.4 and 3.7 for conames also hold.

4. Abstract entanglement networks

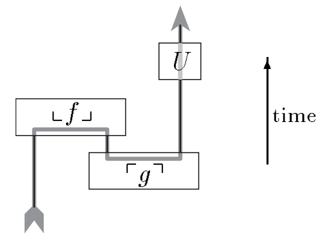
We claim that Lemmas 3.4, 3.5 and 3.6 capture the quantum information flow in the (logic-gate) teleportation and entanglement swapping protocols. We shall provide a full interpretation of finitary quantum mechanics in Section 8 but for now the following rule suffices:

- We interpret *preparation* of an entangled state as a *name* and an *observational branch* as a *coname*.

For an entanglement network of teleportation-type shape (see the picture below) applying Lemma 3.5 yields

$$U \circ \left(\lambda_C^{-1} \circ (\llcorner f\lrcorner \otimes 1)\right) \circ ((1 \otimes \ulcorner g\urcorner) \circ \rho_A) = U \circ g \circ f\ .$$

Note that the quantum information seems to flow 'following the line' while being acted on by the functions whose name or coname labels the boxes (and this fact remains valid for much more complex networks [8]).



Teleporting the input requires $U \circ g \circ f = 1_A$ — we assume all functions have type $A \to A$. Logic-gate teleportation of $h : A \to B$ requires $U \circ g \circ f = h$.

We calculate this explicitly in **Rel**. For initial state $x \in X$ after preparing

$$\ulcorner S\urcorner \subseteq \{*\} \times (Y \times Z)$$

we obtain

$$\{x\} \times \{(y, z) \mid *\ulcorner S\urcorner(y, z)\}$$

as the state of the system. For observational branch

$$\llcorner R\lrcorner \subseteq (X \times Y) \times \{*\}$$

we have that $z \in Z$ is the output iff $\llcorner R\lrcorner \times 1_Z$ receives an input $(x, y, z) \in X \times Y \times Z$ such that $(x, y)\llcorner R\lrcorner *$. Since

$$*\ulcorner S\urcorner(y, z) \Leftrightarrow ySz \quad \text{and} \quad (x, y)\llcorner R\lrcorner * \Leftrightarrow xRy$$

we indeed obtain $x(R; S)z$. This illustrates that the compositionality is due to a mechanism of imposing constraints between the components of the tuples.

In $\mathbf{FdVec}_{\mathbb{C}}$ the vector space of all linear maps of type $V \to W$ is $V \multimap W$ and hence by

$$V^* \otimes W \simeq V \multimap W$$

we have a bijective correspondence between linear maps $f : V \to W$ and vectors $\Psi \in V^* \otimes W$ (see also [8, 9]):

$$\sqrt{2} \cdot \Psi_f = \ulcorner f\urcorner(1) \qquad\qquad \llcorner f\lrcorner = \langle\sqrt{2} \cdot \Psi_f|-\rangle\ .$$

In particular we have for the Bell base:

$$\sqrt{2} \cdot b_i = \ulcorner \beta_i\urcorner(1) \qquad\qquad \llcorner \beta_i\lrcorner = \langle\sqrt{2} \cdot b_i|-\rangle\ .$$

Setting

$$g := \beta_1 = 1_V\ , \quad f := \beta_i\ , \quad U := \beta_i^{-1}$$

indeed yields

$$\beta_i^{-1} \circ 1_A \circ \beta_i = 1_A\ ,$$

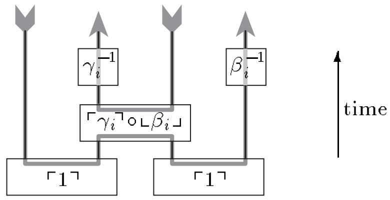
which expresses the correctness of the teleportation protocol along each branch.

Setting $g := h$ and $f := \beta_i$ for logic-gate teleportation requires U_i to satisfy $U_i \circ h \circ \beta_i = h$ that is

$$h \circ \beta_i = U^\dagger \circ h$$

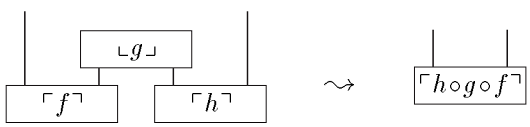
(since U has to be unitary). Hence we have derived the laws of logic-gate teleportation — one should compare this calculation to the size of the calculation in Hilbert space.

Deriving the swapping protocol using Lemma 3.4 and Lemma 3.6 proceeds analogously to the derivation of the teleportation protocol. We obtain two distinct flows due to the fact that a non-destructive measurement is involved.



How γ_i has to relate to β_i such that they make up a true projector will be discussed in Section 8.

For a general entanglement network of the swapping-type (without unitary correction and observational branching) by Lemma 3.6 we obtain the following 'reduction':



This picture, and the underlying algebraic property expressed by Lemma 3.5, is in fact directly related to *Cut-Elimination* in the logic corresponding to compact-closed categories. If one turns the above picture upside-down, and interprets names as Axiom-links and conames as Cut-links, then one has a normalization rule for proof-nets. This perspective is developed in [11].

5. Biproducts

Biproducts have been studied as part of the structure of Abelian categories. For further details, and proofs of the general results we shall cite in this Section, see e.g. [19].

A *zero object* in a category is one which is both initial and terminal. If $\mathbf{0}$ is a zero object, there is an arrow

$$0_{A,B} : A \longrightarrow \mathbf{0} \longrightarrow B$$

between any pair of objects A and B. Let $\mathbf{C}$ be a category with a zero object and binary products and coproducts. Any arrow

$$A_1 \coprod A_2 \to A_1 \prod A_2$$

can be written uniquely as a matrix (f_{ij}), where $f_{ij} : A_i \to A_j$. If the arrow

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is an isomorphism for all A_1, A_2, then we say that $\mathbf{C}$ has *biproducts*, and write $A \oplus B$ for the biproduct of A and B.

Proposition 5.1 (Semi-additivity) *If $\mathbf{C}$ has biproducts, then we can define an operation of addition on each hom-set $\mathbf{C}(A, B)$ by*

$$\begin{tikzcd} A \arrow[r, "f+g"] \arrow[d, "\Delta"'] & B \\ A\oplus A \arrow[r, "f\oplus g"'] & B\oplus B \arrow[u, "\nabla"'] \end{tikzcd}$$

for $f, g : A \to B$, where

$$\Delta = \langle 1_A, 1_A\rangle \qquad \text{and} \qquad \nabla = [1_B, 1_B]$$

are respectively the diagonal and codiagonal. This operation is associative and commutative, with 0_{AB} as an identity. Moreover, composition is bilinear with respect to this additive structure. Thus $\mathbf{C}$ is enriched over abelian monoids.

Proposition 5.2 *If $\mathbf{C}$ has biproducts, we can choose projections $p_1, \ldots, p_n$ and injections $q_1, \ldots, q_n$ for each $\bigoplus_{k=1}^{k=n} A_k$ satisfying*

$$p_j \circ q_i = \delta_{ij} \qquad \text{and} \qquad \sum_{k=1}^{k=n} q_k \circ p_k = 1_{\bigoplus_k A_k}$$

where $\delta_{ii} = 1_{A_i}$, and $\delta_{ij} = 0_{A_i, A_j}$, $i \neq j$.

Proposition 5.3 (Distributivity of $\otimes$ over $\oplus$) *In monoidal closed categories there are natural isomorphisms*

$$\tau_{A,B,C} : A \otimes (B \oplus C) \simeq (A \otimes B) \oplus (A \otimes C)\,,$$

explicitly,

$$\tau_{A,\cdot,\cdot} = \langle 1_A \otimes p_1, 1_A \otimes p_2\rangle \qquad \tau^{-1}_{A,\cdot,\cdot} = [1_A \otimes q_1, 1_A \otimes q_2]\,.$$

A left distributivity isomorphism

$$\upsilon_{A,B,C} : (A \oplus B) \otimes C \simeq (A \otimes C) \oplus (A \otimes C)$$

can be defined similarly.

Proposition 5.4 (Self-duality of $\oplus$ for $(\,)^*$) *In any compact closed category there are natural isomorphisms*

$$\nu_{A,B} : (A \oplus B)^* \simeq A^* \oplus B^* \qquad \nu_{\mathrm{I}} : \mathbf{0}^* \simeq \mathbf{0}\,.$$

Writing $n \cdot X$ for $\bigoplus_{i=1}^{i=n} X$ it follows by self-duality of the tensor unit I that

$$\nu^{-1}_{\mathrm{I},\ldots,\mathrm{I}} \circ (n \cdot u_{\mathrm{I}}) \;:\; n \cdot \mathrm{I} \simeq (n \cdot \mathrm{I})^*\,.$$

Matrix representation. We can write any arrow of the form $f : A \oplus B \to C \oplus D$ as a matrix

$$M_f := \begin{pmatrix} p_1^{C,D} \circ f \circ q_1^{A,B} & p_1^{C,D} \circ f \circ q_2^{A,B} \\ p_2^{C,D} \circ f \circ q_1^{A,B} & p_2^{C,D} \circ f \circ q_2^{A,B} \end{pmatrix}.$$

The sum $f + g$ of such morphisms corresponds to the matrix sum $M_f + M_g$ and composition $g \circ f$ corresponds to matrix multiplication $M_g \cdot M_f$. Hence categories with biproducts admit a matrix calculus.

Examples. The categories $(\mathbf{Rel}, \times, +)$ where the biproduct is the disjoint union and $(\mathbf{FdVec}_{\mathbb{K}}, \otimes, \oplus)$ where the biproduct is the direct sum are examples of compact closed categories with biproducts. More generally, the category of relations for a regular category with stable disjoint coproducts; the category of finitely generated projective modules over a commutative ring; the category of finitely generated free semimodules over a commutative semiring; and the category of free semimodules over a complete commutative semiring are all compact closed with biproducts. Compact closed categories with biproducts, with additional assumptions (e.g. that the category is abelian) have been studied in the mathematical literature on *Tannakian categories* [10]. They have also arisen in a Computer Science context in the first author's work on Interaction Categories [3].

6. Scalars

In any compact closed category we shall call endomorphisms $s : \mathrm{I} \to \mathrm{I}$ *scalars*. As observed in [16], in any monoidal category $\mathbf{C}$, the endomorphism monoid $\mathbf{C}(\mathrm{I}, \mathrm{I})$ is commutative. Any scalar s induces a natural transformation $s_A : A \to A$ by

$$A \xrightarrow{\ \lambda\ } \mathrm{I} \otimes A \xrightarrow{s \otimes 1_A} \mathrm{I} \otimes A \xrightarrow{\ \lambda^{-1}\ } A\,.$$

Here naturality means that all morphisms 'preserve scalar multiplication'. We write $s \bullet f$ for $f \circ s_A$, where s is a scalar and $f : A \to B$. If $\mathbf{C}$ moreover has biproducts, the scalars $\mathbf{C}(\mathrm{I}, \mathrm{I})$ form a commutative semiring.

Examples. In $\mathbf{FdVec}_{\mathbb{K}}$, linear maps $s : \mathbb{K} \to \mathbb{K}$ are uniquely determined by the image of 1, and hence correspond biuniquely to elements of $\mathbb{K}$; composition and addition of these maps corresponds to multiplication and addition of scalars. Hence in $\mathbf{FdVec}_{\mathbb{K}}$ the commutative semiring of scalars is the field $\mathbb{K}$. In $\mathbf{Rel}$, there are just two scalars, corresponding to the classical truth values. Hence in $\mathbf{Rel}$ the commutative semiring of scalars is the Boolean semiring $\{0, 1\}$.

7. Strong compact closure

In any compact closed category $\mathbf{C}$, there is a natural isomorphism $A \simeq A^{**}$. It will be notationally convenient to assume that $(\ )^*$ is strictly involutive, so that this natural isomorphism is the identity. The following definition allows the key example of (*complex*) Hilbert spaces to be accomodated in our setting.

Definition 7.1 A compact closed category $\mathbf{C}$ is *strongly compact closed* if the assignment on objects $A \mapsto A^*$ extends to a *covariant* functor, with action on morphisms $f_* : A^* \to B^*$ for $f : A \to B$, such that

$$f_{**} = f \qquad\qquad (f_*)^* = (f^*)_* : B \to A\,.$$

Examples. Any compact closed category such as $\mathbf{Rel}$, in which $(\ )^*$ is the identity on objects, is trivially strongly compact closed (we just take $f_* := f$). The category of finite-dimensional real inner product spaces and linear maps offers another example of this situation, where we take $A = A^*$, and define

$$\epsilon_A : \phi \otimes \psi \mapsto \langle \phi \mid \psi \rangle\,.$$

Our main intended example, $\mathbf{FdHilb}$, the category of finite-dimensional Hilbert spaces and linear maps, exhibits this structure less trivially, since the conjugate-linearity in the first argument of the inner product prevents us from proceeding as for real spaces. Instead, we define $\mathcal{H}^*$ as follows. The additive abelian group of vectors in $\mathcal{H}^*$ is the same as in $\mathcal{H}$. Scalar multiplication and the inner product are

$$\alpha \bullet_{\mathcal{H}^*} \phi := \bar{\alpha} \bullet_{\mathcal{H}} \phi \qquad \langle \phi \mid \psi \rangle_{\mathcal{H}^*} := \langle \psi \mid \phi \rangle_{\mathcal{H}}$$

where $\bar{\alpha}$ is the complex conjugate of α. The covariant action is then just $f_* = f$. Note that the identity map from $\mathcal{H}$ to $\mathcal{H}^*$ is a conjugate-linear isomorphism, but *not* linear — and hence does not live in the category $\mathbf{FdHilb}$! Importantly, however, $\mathcal{H}$ and $\mathcal{H}^*$ have the same orthonormal bases. Hence we can define

$$\eta_{\mathcal{H}} : 1 \mapsto \sum_{i=1}^{i=n} e_i \otimes e_i \qquad\qquad \epsilon_{\mathcal{H}} : \phi \otimes \psi \mapsto \langle \psi \mid \phi \rangle_{\mathcal{H}}$$

where $\{e_i\}_{i=1}^{i=n}$ is an orthonormal basis of $\mathcal{H}$.

7.1 Adjoints, unitarity and inner products

Each morphism in a strongly compact closed category admits an adjoint in the following sense.

Definition 7.2 We set

$$f^\dagger := (f_*)^* = (f^*)_*\,,$$

and call this the *adjoint* of f.

Proposition 7.3 *The assignments $A \mapsto A$ on objects, and $f \mapsto f^\dagger$ on morphisms, define a contravariant involutive functor:*

$$(f \circ g)^\dagger = g^\dagger \circ f^\dagger \qquad 1^\dagger = 1 \qquad f^{\dagger\dagger} = f.$$

In $\mathbf{FdHilb}$ and real inner product spaces, $f^\dagger$ is the usual adjoint of a linear map. In **Rel**, it is relational converse.

Definition 7.4 An isomorphism U is called *unitary* if its adjoint is its inverse ($U^\dagger = U^{-1}$).

Definition 7.5 Given $\psi, \phi : \mathrm{I} \to A$ we define their *abstract inner product* $\langle \psi \mid \phi \rangle$ as

$$\mathrm{I} \xrightarrow{\rho_\mathrm{I}} \mathrm{I}\otimes\mathrm{I} \xrightarrow{1_\mathrm{I}\otimes u_\mathrm{I}} \mathrm{I}\otimes\mathrm{I}^* \xrightarrow{\phi\otimes\psi_*} A\otimes A^* \xrightarrow{\epsilon_A} \mathrm{I}.$$

In $\mathbf{FdHilb}$, this definition coincides with the usual inner product. In **Rel** we have for $x, y \subseteq \{*\} \times X$:

$$\langle x \mid y \rangle = 1_\mathrm{I}, \quad x \cap y \neq \varnothing \qquad \langle x \mid y \rangle = 0_\mathrm{I}, \quad x \cap y = \varnothing.$$

Lemma 7.6 *If $\psi : \mathrm{I} \to A$, then $\psi^\dagger$ is given by*

$$A \xrightarrow{\rho_A} A\otimes\mathrm{I} \xrightarrow{1_A\otimes u_\mathrm{I}} A\otimes\mathrm{I}^* \xrightarrow{1_A\otimes\psi_*} A\otimes A^* \xrightarrow{\epsilon_A} \mathrm{I}.$$

Proof: See the diagram in the appendix to this paper, which uses Proposition 3.3 twice (with $d_A = 1_A$). □

Proposition 7.7 *For $\langle \psi \mid \phi \rangle$ as defined above we have*

$$\langle \psi \mid \phi \rangle = \psi^\dagger \circ \phi\,.$$

Proof: Using bifunctoriality of tensor and naturality of ρ, it is easy to see that $\langle \psi \mid \phi \rangle$ can be written as

$$\mathrm{I} \xrightarrow{\phi} A \xrightarrow{\rho_A} A\otimes\mathrm{I} \xrightarrow{1_A\otimes u_\mathrm{I}} A\otimes\mathrm{I}^* \xrightarrow{1_A\otimes\psi_*} A\otimes A^* \xrightarrow{\epsilon_A} \mathrm{I}\,.$$

We now apply Lemma 7.6 to conclude. □

Proposition 7.8 *For*

$$\psi : \mathrm{I} \to A \qquad \phi : \mathrm{I} \to B \qquad f : B \to A$$

we have

$$\langle f^\dagger \circ \psi \mid \phi \rangle_B = \langle \psi \mid f \circ \phi \rangle_A\,.$$

Proof: By Proposition 7.7,

$$\langle f^\dagger \circ \psi \mid \phi \rangle = (f^\dagger \circ \psi)^\dagger \circ \phi = \psi^\dagger \circ f \circ \phi = \langle \psi \mid f \circ \phi \rangle. \square$$

Proposition 7.9 *Unitary morphisms $U : A \to B$ preserve the inner product, that is for all $\psi, \phi : \mathrm{I} \to A$ we have*

$$\langle U \circ \psi \mid U \circ \phi \rangle_B = \langle \psi \mid \phi \rangle_A\,.$$

Proof: By Proposition 7.8,

$$\langle U \circ \psi \mid U \circ \phi \rangle_B = \langle U^\dagger \circ U \circ \psi \mid \phi \rangle_A = \langle \psi \mid \phi \rangle_A. \qquad \square$$

7.2 Bras and kets

By Proposition 7.8 we can interpret the Dirac notation (e.g. [20]) in our setting. For morphisms

$$\psi : \mathrm{I} \to A \qquad \phi : \mathrm{I} \to B \qquad f : B \to A$$

define

$$\langle \psi \mid f \mid \phi \rangle := \langle f^\dagger \circ \psi \mid \phi \rangle_B = \langle \psi \mid f \circ \phi \rangle_A.$$

By Proposition 7.7,

$$\langle \psi \mid f \mid \phi \rangle = \psi^\dagger \circ f \circ \phi\,.$$

7.3 Strong compact closure and biproducts

Proposition 7.10 *If $\mathbf{C}$ has biproducts, $(\ )^\dagger$ preserves them and hence is additive:*

$$(f+g)^\dagger = f^\dagger + g^\dagger \qquad\qquad 0^\dagger_{A,B} = 0_{B,A}\,.$$

If a category is both strongly compact closed and has biproducts, the adjoint acts as an involutive automorphism on the semiring of scalars $\mathbf{C}(\mathrm{I},\mathrm{I})$. For **Rel** and real inner product spaces it is the identity, while in the case of $\mathbf{FdHilb}$, it corresponds to *complex conjugation*.

We need a compatibility condition between the strong compact closure and the biproducts.

Definition 7.11 We say that a category **C** is a *strongly compact closed category with biproducts* iff

1. It is strongly compact closed;
2. It has biproducts;
3. The coproduct injections

$$q_i : A_i \to \bigoplus_{k=1}^{k=n} A_k$$

satisfy

$$q_j^\dagger \circ q_i = \delta_{ij}\,.$$

From this, it follows that we can require that the chosen projections and injections in Proposition 5.2 additionally satisfy $(p_i)^\dagger = q_i$.

Examples Finite-dimensional Hilbert spaces and real inner product spaces, categories of relations, and categories of free modules and semimodules are all examples of strongly compact closed categories with biproducts.

7.4 Spectral Decompositions

We define a *spectral decomposition* of an object A to be a unitary isomorphism

$$U : A \to \bigoplus_{i=1}^{i=n} A_i \,.$$

(Here the 'spectrum' is just the set of indices $1, \ldots, n$). Given a spectral decomposition U, we define morphisms

$$\begin{aligned} \psi_j &:= U^\dagger \circ q_j : A_j \to A \\ \pi_j &:= \psi_j^\dagger = p_j \circ U : A \to A_j \,, \end{aligned}$$

diagramatically

$$\begin{tikzcd} A_j \arrow[r, "\psi_j"] \arrow[d, "q_j"'] & A \arrow[d, "\pi_j"] \arrow[dl, shift left, "U"] \\ \bigoplus_{i=1}^{i=n} A_i \arrow[r, "p_j"'] \arrow[ur, shift left, "U^\dagger"] & A_j \end{tikzcd}$$

and finally *projectors*

$$\mathrm{P}_j := \psi_j \circ \pi_j : A \to A \,.$$

These projectors are *self-adjoint*

$$\mathrm{P}_j^\dagger = (\psi_j \circ \pi_j)^\dagger = \pi_j^\dagger \circ \psi_j^\dagger = \psi_j \circ \pi_j = \mathrm{P}_j$$

idempotent and *orthogonal*:

$$\mathrm{P}_i \circ \mathrm{P}_j = \psi_i \circ \pi_i \circ \psi_j \circ \pi_j = \psi_i \circ \delta_{ij} \circ \pi_j = \delta_{ij}^A \circ \mathrm{P}_i \,.$$

Moreover, they yield a *resolution of the identity*:

$$\begin{aligned} \sum_{i=1}^{i=n} \mathrm{P}_i &= \sum_{i=1}^{i=n} \psi_i \circ \pi_i \\ &= \sum_{i=1}^{i=n} U^\dagger \circ q_i \circ p_i \circ U \\ &= U^\dagger \circ (\sum_{i=1}^{i=n} q_i \circ p_i) \circ U \\ &= U^{-1} \circ 1_{\bigoplus_i A_i} \circ U = 1_A \,. \end{aligned}$$

7.5 Bases and dimension

A *basis* for an object A is a unitary isomorphism

$$\mathsf{base} : n \cdot \mathrm{I} \to A \,.$$

Given bases base_A and base_B for objects A and B respectively we can define the matrix (m_{ij}) of any morphism $f : A \to B$ in those two bases as the matrix of

$$\mathsf{base}_B^\dagger \circ f \circ \mathsf{base}_A : n_A \cdot \mathrm{I} \to n_B \cdot \mathrm{I}$$

as in Section 5.

Proposition 7.12 *Given $f : A \to B$ and*

$$\mathsf{base}_A : n_A \cdot \mathrm{I} \to A \quad \text{and} \quad \mathsf{base}_B : n_B \cdot \mathrm{I} \to A$$

the matrix (m'_{ij}) of $f^\dagger$ in these bases is the conjugate transpose of the matrix (m_{ij}) of f.

Proof: We have

$$\begin{aligned} m'_{ij} &= p_i \circ \mathsf{base}_A^\dagger \circ f^\dagger \circ \mathsf{base}_B \circ q_j \\ &= (p_j \circ \mathsf{base}_B^\dagger \circ f \circ \mathsf{base}_A \circ q_i)^\dagger \\ &= m_{ji}^\dagger \,. \end{aligned}$$

□

If in addition to the assumptions of Proposition 7.8 and Proposition 7.9 there exist bases for A and B, we can prove converses to both of them.

Proposition 7.13 *If there exist bases for A and B then $f : A \to B$ is the adjoint to $g : B \to A$ if and only if*

$$\langle f \circ \psi \mid \phi \rangle_B = \langle \psi \mid g \circ \phi \rangle_A$$

for all $\psi : \mathrm{I} \to A$ and $\phi : \mathrm{I} \to B$.

Proof: Let (m_{ij}) be the matrix of $f^\dagger$ and (m'_{ij}) the matrix of g in the given bases. By Proposition 7.7 we have

$$\begin{aligned} m_{ij} &= p_i \circ \mathsf{base}_A^\dagger \circ f^\dagger \circ \mathsf{base}_B \circ q_j \\ &= \langle f \circ \mathsf{base}_A \circ q_i \mid \mathsf{base}_B \circ q_j \rangle_B \\ &= \langle f \circ \psi \mid \phi \rangle_B = \langle \psi \mid g \circ \phi \rangle_A \\ &= \langle \mathsf{base}_A \circ q_i \mid g \circ \mathsf{base}_B \circ q_j \rangle_A \\ &= p_i \circ \mathsf{base}_A^\dagger \circ g \circ \mathsf{base}_B \circ q_j = m'_{ij} \,. \end{aligned}$$

Hence the matrix elements of g and $f^\dagger$ coincide so g and $f^\dagger$ are equal. The converse is given by Proposition 7.8. □

Proposition 7.14 *If there exist bases for A and B then a morphism $U : A \to B$ is unitary if and only if it preserves the inner product, that is for all $\psi, \phi : \mathrm{I} \to A$ we have*

$$\langle U \circ \psi \mid U \circ \phi \rangle_B = \langle \psi \mid \phi \rangle_A \,.$$

Proof: We have

$$\langle U^{-1} \circ \psi \mid \phi \rangle_A = \langle U \circ U^{-1} \circ \psi \mid U \circ \phi \rangle_B = \langle \psi \mid U \circ \phi \rangle_B$$

and hence by Proposition 7.13, $U^\dagger = U^{-1}$. The converse is given by Proposition 7.9. □

Note also that when a basis is available we can assign to $\psi^\dagger : A \to \mathrm{I}$ and $\phi : \mathrm{I} \to A$ matrices

$$\left(\begin{array}{ccc} \psi_1^\dagger & \cdots & \psi_n^\dagger \end{array} \right) \qquad\qquad \left(\begin{array}{c} \phi_1 \\ \vdots \\ \phi_n \end{array} \right)$$

respectively, and by Proposition 7.7, the inner product becomes

$$\langle \psi \mid \phi \rangle = \left(\begin{array}{ccc} \psi_1^\dagger & \cdots & \psi_n^\dagger \end{array} \right) \left(\begin{array}{c} \phi_1 \\ \vdots \\ \phi_n \end{array} \right) = \sum_{i=1}^{i=n} \psi_i^\dagger \circ \phi_i \, .$$

Interestingly, two different notions of dimension arise in our setting. We assign an *integer dimension* $\mathsf{dim}(A) \in \mathbb{N}$ to an object A provided there exists a base

$$\mathsf{base} : \mathsf{dim}(A) \cdot \mathrm{I} \to A \, .$$

Alternatively, we introduce the *scalar dimension* as

$$\mathsf{dim}_s(A) := \epsilon_A \circ \sigma_{A^*,A} \circ \eta_A \in \mathbf{C}(\mathrm{I}, \mathrm{I}).$$

We also have:

$$\mathsf{dim}_s(\mathrm{I}) = 1_{\mathrm{I}} \qquad\qquad \mathsf{dim}_s(A^*) = \mathsf{dim}_s(A)$$

$$\mathsf{dim}_s(A \otimes B) = \mathsf{dim}_s(A)\mathsf{dim}_s(B)$$

In $\mathbf{FdVec}_{\mathbb{K}}$ these notions of dimension coincide, in the sense that $\mathsf{dim}_s(V)$ is multiplication with the scalar $\mathsf{dim}(V)$. In $\mathbf{Rel}$ the integer dimension corresponds to the cardinality of the set, and is only well-defined for finite sets, while $\mathsf{dim}_s(X)$ always exists; however, $\mathsf{dim}_s(X)$ can only take two values, 0_{I} and 1_{I}, and the two notions of dimension diverge for sets of cardinality greater than 1.

8. Abstract quantum mechanics

We can identify the basic ingredients of finitary quantum mechanics in any strongly compact closed category with biproducts.

1. A *state space* is represented by an object A.

2. A *basic variable* ('type of qubits') is a state space Q with a given unitary isomorphism

$$\mathsf{base}_Q : \mathrm{I} \oplus \mathrm{I} \to Q$$

which we call the *computational basis* of Q. By using the isomorphism $n \cdot \mathrm{I} \simeq (n \cdot \mathrm{I})^*$ described in Section 5, we also obtain a computational basis for Q^*.

3. A *compound system* for which the subsystems are described by A and B respectively is described by $A \otimes B$. If we have computational bases base_A and base_B, then we define

$$\mathsf{base}_{A \otimes B} := (\mathsf{base}_A \otimes \mathsf{base}_B) \circ d_{nm}^{-1}$$

where

$$d_{nm} : n \cdot \mathrm{I} \otimes m \cdot \mathrm{I} \simeq (nm) \cdot \mathrm{I}$$

is the canonical isomorphism constructed using first the left distributivity isomorphism υ, and then the right distributivity isomorphism τ, to give the usual lexicographically-ordered computational basis for the tensor product.

4. Basic data transformations are unitary isomorphisms.

5a. A *preparation* in a state space A is a morphism

$$\psi : \mathrm{I} \to A$$

for which there exists a unitary $U : \mathrm{I} \oplus B \to A$ such that

$$\begin{tikzcd} \mathrm{I} \arrow[r, "\psi"] \arrow[d, "q_1"'] & A \\ \mathrm{I} \oplus B \arrow[ur, "U"'] & \end{tikzcd}$$

commutes.

5b. Consider a spectral decomposition

$$U : A \to \bigoplus_{i=1}^{i=n} A_i$$

with associated projectors P_j. This gives rise to the *non-destructive measurement*

$$\langle \mathrm{P}_i \rangle_{i=1}^{i=n} : A \to n \cdot A.$$

The projectors

$$\mathrm{P}_i : A \to A$$

for $i = 1, \ldots, n$ are called the *measurement branches*. This measurement is *non-degenerate* if $A_i = \mathrm{I}$ for all $i = 1, \ldots, n$. In this case we refer to U itself as a *destructive measurement* or *observation*. The morphisms

$$\pi_i = p_i \circ U : A \to \mathrm{I}$$

for $i = 1, \ldots, n$ are called *observation branches*. (We leave discussion of 'degenerate destructive measurements', along with other variant notions of measurement, to future work).

Note that the type of a non-destructive measurement makes it explicit that it is an operation which involves an indeterministic transition (by contrast with the standard Hilbert space quantum mechanical formalism).

6a. Explicit biproducts represent the *branching* arising from the indeterminacy of measurement outcomes.

Hence an operation f acting on an explicit biproduct $A \oplus B$ should itself be an explicit biproduct, *i.e.* we want

$$f = f_1 \oplus f_2 : A \oplus B \to C \oplus D\,,$$

for $f_1 : A \to C$ and $f_2 : B \to D$. The dependency of f_i on the branch it is in captures *local* classical communication. The full force of non-local classical communication is enabled by Proposition 5.3.

6b. Distributivity isomorphisms represent *non-local classical communication*.

To see this, suppose e.g. that we have a compound system $Q \otimes A$, and we (non-destructively) measure the qubit in the first component, obtaining a new system state described by $(Q \oplus Q) \otimes A$. At this point, we know 'locally', *i.e.* at the site of the first component, what the measurement outcome is, but we have not propagated this information to the rest of the system A. However, after applying the distributivity isomorphism

$$(Q \oplus Q) \otimes A \simeq (Q \otimes A) \oplus (Q \otimes A)$$

the information about the outcome of the measurement on the first qubit has been propagated globally throughout the system, and we can perform operations on A depending on the measurement outcome, e.g.

$$(1_Q \otimes U_0) \oplus (1_Q \otimes U_1)$$

where U_0, U_1 are the operations we wish to perform on A in the event that the outcome of the measurement we performed on Q was 0 or 1 respectively.

The Born rule

We now show how the *Born rule*, which is the key quantitative feature of quantum mechanics, emerges automatically from our abstract setting.

For a preparation $\psi : \mathrm{I} \to A$ and spectral decomposition

$$U : A \to \bigoplus_{i=1}^{i=n} A_i\,,$$

with corresponding non-destructive measurement

$$\langle \mathrm{P}_i \rangle_{i=1}^{i=n} : A \to n \cdot A\,,$$

we can consider the protocol

$$\mathrm{I} \xrightarrow{\ \psi\ } A \xrightarrow{\langle \mathrm{P}_i \rangle_{i=1}^{i=n}} n \cdot A\,.$$

We define scalars

$$\mathsf{Prob}(\mathrm{P}_i, \psi) := \langle \psi \mid \mathrm{P}_i \mid \psi \rangle = \psi^\dagger \circ \mathrm{P}_i \circ \psi\,.$$

Proposition 8.1 *With notation as above,*

$$\mathsf{Prob}(\mathrm{P}_i, \psi) = (\mathsf{Prob}(\mathrm{P}_i, \psi))^\dagger$$

and

$$\sum_{i=1}^{i=n} \mathsf{Prob}(\mathrm{P}_i, \psi) = 1\,.$$

Hence we think of the scalar $\mathsf{Prob}(\mathrm{P}_j, \psi)$ *as 'the probability of obtaining the* j*'th outcome of the measurement* $\langle \mathrm{P}_i \rangle_{i=1}^{i=n}$ *on the state* ψ*'.*

Proof: From the definitions of preparation and the projectors, there are unitaries U, V such that

$$\mathsf{Prob}(\mathrm{P}_i, \psi) = (V \circ q_1)^\dagger \circ U^\dagger \circ q_i \circ p_i \circ U \circ V \circ q_1$$

for each i. Hence

$$\begin{aligned}\sum_{i=1}^{i=n} \mathsf{Prob}(\mathrm{P}_i, \psi) &= \sum_{i=1}^{i=n} p_1 \circ V^\dagger \circ U^\dagger \circ q_i \circ p_i \circ U \circ V \circ q_1 \\ &= p_1 \circ V^\dagger \circ U^\dagger \circ \Big(\sum_{i=1}^{n} q_i \circ p_i\Big) \circ U \circ V \circ q_1 \\ &= p_1 \circ V^{-1} \circ U^{-1} \circ 1_{n\cdot \mathrm{I}} \circ U \circ V \circ q_1 \\ &= p_1 \circ q_1 = 1_{\mathrm{I}}\,. \end{aligned}$$

□

Moreover, since by definition $\mathrm{P}_j = \pi_j^\dagger \circ \pi_j$, we can rewrite the Born rule expression as

$$\begin{aligned}\mathsf{Prob}(\mathrm{P}_j, \psi) &= \psi^\dagger \circ \mathrm{P}_j \circ \psi \\ &= \psi^\dagger \circ \pi_j^\dagger \circ \pi_j \circ \psi \\ &= (\pi_j \circ \psi)^\dagger \circ \pi_j \circ \psi \\ &= s_j^\dagger \circ s_j\end{aligned}$$

for some scalar $s_j \in \mathbf{C}(\mathrm{I}, \mathrm{I})$. Thus s_j can be thought of as the 'probability amplitude' giving rise to the probability $s_j^\dagger \circ s_j$, which is of course self-adjoint. If we consider the protocol

$$\mathrm{I} \xrightarrow{\ \psi\ } A \xrightarrow{\langle \pi_i \rangle_{i=1}^{i=n}} n \cdot \mathrm{I}\,.$$

which involves an observation $\langle \pi_i \rangle_{i=1}^{i=n}$, then these scalars s_j correspond to the branches

$$\mathrm{I} \xrightarrow{\ \psi\ } A \xrightarrow{\ \pi_j\ } \mathrm{I}\,.$$

9. Abstract quantum protocols

We prove correctness of the example protocols.

9.1 Quantum teleportation

Definition 9.1 A *teleportation base* is a scalar s together with a morphism

$$\mathsf{prebase}_{\mathrm{T}} : 4 \cdot \mathrm{I} \to Q^* \otimes Q$$

such that:

- $\mathsf{base}_{\mathrm{T}} := s \bullet \mathsf{prebase}_{\mathrm{T}}$ is unitary.
- the four maps $\beta_j : Q \to Q$, where β_j is defined by

  $$\ulcorner \beta_j \urcorner := \mathsf{prebase}_{\mathrm{T}} \circ q_j \,,$$

  are unitary.
- $2s^\dagger s = 1$.

The morphisms $s \bullet \ulcorner \beta_j \urcorner$ are the *base vectors* of the teleportation base. A teleportation base is a *Bell base* when the *Bell base maps*

$$\beta_1, \beta_2, \beta_3, \beta_4 : Q \to Q$$

satisfy[2]

$$\beta_1 = 1_Q \qquad \beta_2 = \sigma_Q^{\oplus} \qquad \beta_3 = \beta_3^\dagger \qquad \beta_4 = \sigma_Q^{\oplus} \circ \beta_3$$

where

$$\sigma_Q^{\oplus} := \mathsf{base}_Q \circ \sigma_{\mathrm{I},\mathrm{I}}^{\oplus} \circ \mathsf{base}_Q^{-1} \,.$$

A teleportation base defines a *teleportation observation*

$$\langle s^\dagger \bullet \llcorner \beta_i \lrcorner \rangle_{i=1}^{i=4} : Q \otimes Q^* \to 4 \cdot \mathrm{I} \,.$$

To emphasize the identity of the individual qubits we label the three copies of Q we shall consider as Q_a, Q_b, Q_c. We also use labelled identities, e.g. $1_{bc} : Q_b \to Q_c$, and labelled Bell bases. Finally, we introduce

$$\Delta_{ac}^4 := \langle s^\dagger s \bullet 1_{ac} \rangle_{i=1}^{i=4} : Q_a \to 4 \cdot Q_c$$

as the *labelled, weighted diagonal*. This expresses the intended behaviour of teleportation, namely that the input qubit is propagated to the output along each branch of the protocol, with 'weight' $s^\dagger s$, corresponding to the probability amplitude for that branch. Note that the sum of the corresponding probabilities is

$$4(s^\dagger s)^\dagger s^\dagger s = (2s^\dagger s)(2s^\dagger s) = 1 \,.$$

[2] This choice of axioms is sufficient for our purposes. One might prefer to axiomatize a notion of Bell base such that the corresponding Bell base maps are exactly the Pauli matrices — note that this would introduce a coefficient i in β_4.

Theorem 9.2 *The following diagram commutes.*

$$\begin{tikzcd}
Q_a \arrow[r, equal] \arrow[dddddd, "\Delta_{ac}^4"'] & Q_a \arrow[d, "\rho_a"', "\textbf{import unknown state}"] \\
& Q_a \otimes \mathrm{I} \arrow[d, "1_a \otimes (s \bullet \ulcorner 1_{bc} \urcorner)"', "\textbf{produce EPR-pair}"] \\
& Q_a \otimes (Q_b^* \otimes Q_c) \arrow[d, "\alpha_{a,b,c}"', "\textbf{spatial delocation}"] \\
& (Q_a \otimes Q_b^*) \otimes Q_c \arrow[d, "\langle s^\dagger \bullet \llcorner \beta_i^{ab} \lrcorner \rangle_{i=1}^{i=4} \otimes 1_c"', "\textbf{teleportation observation}"] \\
& (4 \cdot \mathrm{I}) \otimes Q_c \arrow[d, "(4 \cdot \lambda_c^{-1}) \circ \upsilon_c"', "\textbf{classical communication}"] \\
& 4 \cdot Q_c \arrow[d, "\bigoplus_{i=1}^{i=4} (\beta_i^c)^{-1}"', "\textbf{unitary correction}"] \\
4 \cdot Q_c \arrow[r, equal] & 4 \cdot Q_c
\end{tikzcd}$$

The right-hand-side of the above diagram is our formal description of the teleportation protocol; the commutativity of the diagram expresses the correctness of the protocol. Hence any strongly compact closed category with biproducts admits quantum teleportation provided it contains a teleportation base. If we do a Bell-base observation then the corresponding unitary corrections are

$$\beta_i^{-1} = \beta_i \quad \textit{for} \quad i \in \{1, 2, 3\} \quad \textit{and} \quad \beta_4^{-1} = \beta_3 \circ \sigma_Q^{\oplus} \,.$$

Proof: For a proof of the commutativity of this diagram see the Appendix – it uses the universal property of the product, Lemma 3.5, naturality of λ and the explicit form of

$$\upsilon_c := \langle p_i^{\mathrm{I}} \otimes 1_c \rangle_{i=1}^{i=4} \,.$$

In the specific case of a Bell-base observation we use

$$1_Q^\dagger = 1_Q \,, \quad (\sigma_Q^{\oplus})^\dagger = \sigma_Q^{\oplus}$$

and

$$(\sigma_Q^{\oplus} \circ \beta_3)^\dagger = \beta_3^\dagger \circ (\sigma_Q^{\oplus})^\dagger = \beta_3 \circ \sigma_Q^{\oplus} \,.$$

$\square$

Although in **Rel** teleportation works for 'individual observational branches' it fails to admit the full teleportation protocol since there are only two automorphisms of Q (which is just a two-element set, *i.e.* the type of 'classical bits'), and hence there is no teleportation base.

We now consider sufficient conditions on the ambient category $\mathbf{C}$ for a teleportation base to exist. We remark firstly that if $\mathbf{C}(\mathrm{I}, \mathrm{I})$ contains an additive inverse for 1, then it is a ring, and moreover all additive inverses exist in each hom-set $\mathbf{C}(A, B)$, so $\mathbf{C}$ is enriched over Abelian groups. Suppose then that $\mathbf{C}(\mathrm{I}, \mathrm{I})$ is a ring with $1 \neq -1$. We can define a morphism

$$\mathsf{prebase}_{\mathrm{T}} = \mathsf{base}_{Q^* \otimes Q} \circ M : 4 \cdot \mathrm{I} \to Q^* \otimes Q$$

where M is the endomorphism of $4 \cdot \mathrm{I}$ determined by the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

The corresponding morphisms β_j will have 2×2 matrices determined by the columns of this 4×4 matrix, and will be unitary. If $\mathbf{C}(\mathrm{I}, \mathrm{I})$ furthermore contains a scalar s satisfying $2s^\dagger s = 1$, then $s \bullet \mathsf{prebase}_{\mathrm{T}}$ is unitary, and the conditions for a teleportation base are fulfilled. Suppose we start with a ring R containing an element s satisfying $2s^2 = 1$. (Examples are plentiful, e.g. any subring of $\mathbb{C}$, or of $\mathbb{Q}(\sqrt{2})$, containing $\frac{1}{\sqrt{2}}$). The category of finitely generated free R-modules and R-linear maps is strongly compact closed with biproducts, and admits a teleportation base (in which s will appear as a scalar with $s = s^\dagger$), hence realizes teleportation.

9.2 Logic-gate teleportation

Logic gate teleportation of qubits requires only a minor modification as compared to the teleportation protocol.

Theorem 9.3 *Let unitary morphism $f : Q \to Q$ be such that for each $i \in \{1, 2, 3, 4\}$ a morphism $\varphi_i(f) : Q \to Q$ satisfying*

$$f \circ \beta_i = \varphi_i(f) \circ f$$

exists. The diagram of Theorem 9.2 with the modifications made below commutes.

$$\begin{tikzcd}[column sep=large]
{} \arrow[dddd, dotted, no head] & {} \arrow[d, dotted] & \\
 & Q_a \otimes \mathrm{I} \arrow[d, "1_a \otimes (s \bullet \ulcorner f \urcorner)"'] & \textbf{produce } f\textbf{-state} \\
 & Q_a \otimes (Q_b^* \otimes Q_c) \arrow[d, dotted] & \\
 & 4 \cdot Q_c \arrow[d, "\bigoplus_{i=1}^{i=4}(\varphi_i(f))^{-1}"'] & \textbf{unitary correction} \\
4 \cdot Q_c \arrow[r, equal] & 4 \cdot Q_c &
\end{tikzcd}$$

with the left vertical arrow labelled $\Delta^4_{ac} \circ f$.

The right-hand-side of the diagram is our formal description of logic-gate teleportation of $f : Q \to Q$; the commutativity of the diagram under the stated conditions expresses the correctness of logic-gate teleportation for qubits.

Proof: See the diagram in the appendix. $\square$

This two-dimensional case does not yet provide a universal computational primitive, which requires teleportation of $Q \otimes Q$-gates [12]. We present the example of teleportation of a CNOT gate [12] (see also [8] Section 3.3).

Given a Bell base we define a CNOT gate as one which acts as follows on tensors of the Bell base maps[3]:

$$\begin{aligned}
\mathrm{CNOT} \circ (\sigma_Q^{\oplus} \otimes 1_Q) &= (\sigma_Q^{\oplus} \otimes \sigma_Q^{\oplus}) \circ \mathrm{CNOT} \\
\mathrm{CNOT} \circ (1_Q \otimes \sigma_Q^{\oplus}) &= (1_Q \otimes \sigma_Q^{\oplus}) \circ \mathrm{CNOT} \\
\mathrm{CNOT} \circ (\beta_3 \otimes 1_Q) &= (\beta_3 \otimes 1_Q) \circ \mathrm{CNOT} \\
\mathrm{CNOT} \circ (1_Q \otimes \beta_3) &= (\beta_3 \otimes \beta_3) \circ \mathrm{CNOT}
\end{aligned}$$

It follows from this that

$$\begin{aligned}
\mathrm{CNOT} \circ (\beta_4 \otimes 1_Q) &= (\beta_4 \otimes \sigma_Q^{\oplus}) \circ \mathrm{CNOT} \\
\mathrm{CNOT} \circ (1_Q \otimes \beta_4) &= (\beta_3 \otimes \beta_4) \circ \mathrm{CNOT}
\end{aligned}$$

from which in turn it follows by bifunctoriality of the tensor that the required unitary corrections factor into single qubit actions, for which we introduce a notation by setting

$$\begin{aligned}
\mathrm{CNOT} \circ (\beta_i \otimes 1_Q) &= \varphi_1(\beta_i) \circ \mathrm{CNOT} \\
\mathrm{CNOT} \circ (1_Q \otimes \beta_i) &= \varphi_2(\beta_i) \circ \mathrm{CNOT}
\end{aligned}$$

[3] One could give a more explicit definition of a CNOT gate, e.g. by specifying the matrix. However, our generalized definition suffices to provide the required corrections. Moreover, this example nicely illustrates the attitude of 'focussing on the essentials by abstracting'.

The reader can verify that for

$$4^2\cdot(Q_{c_1}\otimes Q_{c_2}) := 4\cdot(4\cdot(Q_{c_1}\otimes Q_{c_2}))$$

and

$$\Delta^{4^2}_{ac} := \langle s^\dagger s\bullet\langle s^\dagger s\bullet 1_{ac}\rangle_{i=1}^{i=4}\rangle_{i=1}^{i=4} : Q_{a_1}\otimes Q_{a_2}\to 4^2\cdot(Q_{c_1}\otimes Q_{c_2})$$

the following diagram commutes.

$$\begin{tikzcd}
Q_{a_1}\otimes Q_{a_2} \arrow[r, equal] \arrow[ddddddddd, "\Delta^{4^2}_{ac}\circ\mathrm{CNOT}"'] & Q_{a_1}\otimes Q_{a_2} \arrow[d, "\rho_a"', "\textbf{import unknown state}"] \\
& (Q_{a_1}\otimes Q_{a_2})\otimes \mathrm{I} \arrow[d, "1_a\otimes(s^2\bullet\ulcorner\mathrm{CNOT}\urcorner)"', "\textbf{produce CNOT-state}"] \\
& (Q_{a_1}\otimes Q_{a_2})\otimes((Q_{b_1}\otimes Q_{b_2})^*\otimes(Q_{c_1}\otimes Q_{c_2})) \arrow[d, "(\alpha,\sigma)\circ(1_a\otimes(u_b\otimes 1_c))"', "\textbf{spatial delocation}"] \\
& ((Q_{a_1}\otimes Q^*_{b_1})\otimes(Q_{c_1}\otimes Q_{c_2}))\otimes(Q_{a_2}\otimes Q^*_{b_2}) \arrow[d, "(\langle s^\dagger\bullet\llcorner\beta_i^{a_1b_1}\lrcorner\rangle_{i=1}^{i=4}\otimes 1_c)\otimes 1_2"', "\textbf{1st observation}"] \\
& ((4\cdot\mathrm{I})\otimes(Q_{c_1}\otimes Q_{c_2}))\otimes(Q_{a_2}\otimes Q^*_{b_2}) \arrow[d, "((4\cdot\lambda_c^{-1})\circ\upsilon_c)\otimes 1_2"', "\textbf{1st communication}"] \\
& (4\cdot(Q_{c_1}\otimes Q_{c_2}))\otimes(Q_{a_2}\otimes Q^*_{b_2}) \arrow[d, "\left(\bigoplus_{i=1}^{i=4}(\varphi_1^c(\beta_i))^{-1}\right)\otimes 1_2"', "\textbf{1st correction}"] \\
& (4\cdot(Q_{c_1}\otimes Q_{c_2}))\otimes(Q_{a_2}\otimes Q^*_{b_2}) \arrow[d, "(4\cdot 1_c)\otimes\langle s^\dagger\bullet\llcorner\beta_i^{a_2b_2}\lrcorner\rangle_{i=1}^{i=4}"', "\textbf{2nd observation}"] \\
& (4\cdot(Q_{c_1}\otimes Q_{c_2}))\otimes(4\cdot\mathrm{I}) \arrow[d, "(4\cdot\rho_{4c}^{-1})\circ\tau_{4c}"', "\textbf{2nd communication}"] \\
& (4\cdot(4\cdot(Q_{c_1}\otimes Q_{c_2}))) \arrow[d, "\bigoplus_{i=1}^{i=4}(4\cdot\varphi_2^c(\beta_i))^{-1}"', "\textbf{2nd correction}"] \\
4^2\cdot(Q_{c_1}\otimes Q_{c_2}) \arrow[r, equal] & 4^2\cdot(Q_{c_1}\otimes Q_{c_2})
\end{tikzcd}$$

9.3 Entanglement swapping

Theorem 9.4 *Setting*

$$\begin{aligned}
\gamma_i &:= (\beta_i)_* \\
\mathrm{P}_i &:= s^\dagger s\bullet(\ulcorner\gamma_i\urcorner\circ\llcorner\beta_i\lrcorner) \\
\zeta_i^{ac} &:= \bigoplus_{i=1}^{i=4}\left((1_b^*\otimes\gamma_i^{-1})\otimes(1_d^*\otimes\beta_i^{-1})\right) \\
\Theta_{ab} &:= 1_d^*\otimes\langle\mathrm{P}_i\rangle_{i=1}^{i=4}\otimes 1_c \\
\Omega_{ab} &:= \langle s^\dagger s^3\bullet(\ulcorner 1_{ba}\urcorner\otimes\ulcorner 1_{dc}\urcorner)\rangle_{i=1}^{i=4}
\end{aligned}$$

the following diagram commutes.

$$\begin{tikzcd}
\mathrm{I}\otimes\mathrm{I} \arrow[r, equal] \arrow[ddddd, "\Omega_{ab}"'] & \mathrm{I}\otimes\mathrm{I} \arrow[d, "s^2\bullet(\ulcorner 1_{da}\urcorner\otimes\ulcorner 1_{bc}\urcorner)"', "\textbf{produce EPR-pairs}"] \\
& (Q_d^*\otimes Q_a)\otimes(Q_b^*\otimes Q_c) \arrow[d, "\alpha"', "\textbf{spatial delocation}"] \\
& Q_d^*\otimes(Q_a\otimes Q_b^*)\otimes Q_c \arrow[d, "\Theta_{ab}"', "\textbf{Bell-base measurement}"] \\
& Q_d^*\otimes(4\cdot(Q_a\otimes Q_b^*))\otimes Q_c \arrow[d, "(4\cdot(\alpha,\sigma))\circ(\tau,\upsilon)"', "\textbf{classical communication}"] \\
& 4\cdot((Q_b^*\otimes Q_a)\otimes(Q_d^*\otimes Q_c)) \arrow[dl, "\zeta_i^{ac}"', "\textbf{unitary correction}"] \\
4\cdot((Q_b^*\otimes Q_a)\otimes(Q_d^*\otimes Q_c)) &
\end{tikzcd}$$

The right-hand-side of the above diagram is our formal description of the entanglement swapping protocol.

Proof: See the diagram in the appendix — it uses Lemma 3.4 and Lemma 3.6. □

We use $\gamma_i = (\beta_i)_*$ rather than β_i to make P_i an endomorphism and hence a projector. The general definition of a 'bipartite entanglement projector' is

$$\mathrm{P}_f := \ulcorner f\urcorner\circ\llcorner f_*\lrcorner = \ulcorner f\urcorner\circ\llcorner f^\dagger\lrcorner\circ\sigma_{A^*,B} : A^*\otimes B\to A^*\otimes B$$

for $f : A\to B$, so in fact $\mathrm{P}_i = \mathrm{P}_{(\beta_i)_*}$.

10. Conclusion

Other work. Birkhoff and von Neumann [6] attempted to capture quantum behavior abstractly in lattice-theoretic terms — see also Mackey [18] and Piron [22]. The weak spot of this programme was the lack of a satisfactory treatment of compound systems — whereas in our approach the tensor $\otimes$ is a primitive. Different kinds of lattices do arise naturally in our setting, but we leave a discussion of this to future work.

Isham and Butterfield [14] have reformulated the Kochen-Specker theorem in a topos-theoretic setting. On the one hand, assuming that the tensor in a compact closed category is the categorical product leads to triviality—the category is then necessarily equivalent to the one-object one-arrow category—and in this sense the compact closed and topos axioms are not compatible. On the other hand, each topos yields a strongly compact closed category with biproducts as its category of relations.

The recent papers [24, 27] use categorical methods for giving semantics to a quantum programming language, and a quantum lambda calculus, respectively. In both cases, the objectives, approach and results are very different to those of the present paper. A more detailed comparison must again be left to future work.

Further Directions. This work has many possible lines for further development. We mention just a few.

- Our setting seems a natural one for developing type systems to control quantum behaviour.
- In order to handle protocols and quantum computations more systematically, it would be desirable to have an effective syntax, whose design should be guided by the categorical semantics.
- The information flow level of analysis using only the compact-closed structure allows some very elegant and convenient 'qualitative' reasoning, while adding biproducts allows very fine-grained modelling and analysis. The interplay between these two levels merits further investigation.
- We have not considered mixed states and non-projective measurements in this paper, but they can certainly be incorporated in our framework.
- In this paper, we have only studied finitary Quantum Mechanics. A significant step towards the infinite dimensional case is provided by the previous work on *nuclear ideals in tensored $*$-categories* [1]. The 'compactness' axiom for nuclear ideals (see Definition 5.7 in [1]) corresponds to our Compositionality Lemma 3.4. One of the main intended models of nuclear ideals is given by the category of all Hilbert spaces and bounded linear maps.
- Another class of compact closed categories with biproducts are the Interaction Categories introduced by one of the authors [3]. One can consider linear-algebraic versions of Interaction Categories — 'matrices extended in time' rather than 'relations extended in time' as in [3]. Does this lead to a useful notion of quantum concurrent processes?

Acknowledgements

Rick Blute and Prakash Panangaden suggested some improvements to an earlier version of this paper.

References

[1] S. Abramsky, R. Blute, and P. Panangaden. Nuclear and trace ideals in tensored $*$-categories. *Journal of Pure and Applied Algebra*, 143:3–47, 1999.

[2] S. Abramsky and B. Coecke. Physical traces: Quantum vs. classical information processing. In *Proceedings of Category Theory and Computer Science 2002 (CTCS'02)*, volume 69 of *Electronic Notes in Theoretical Computer Science*. Elsevier Science, 2003. arXiv:cs/0207057.

[3] S. Abramsky, S. J. Gay, and R. Nagarajan. Interaction categories and foundations of typed concurrent programming. In *Deductive Program Design: Proceedings of the 1994 Marktoberdorf International Summer School*, NATO Advanced Science Institutes Series F, pages 35–113. Springer-Verlag, 1995.

[4] M. Barr. *$*$-Autonomous Categories*, volume 752 of *Lecture Notes in Mathematics*. Springer-Verlag, 1979.

[5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wooters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[6] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. *Annals of Mathematics*, 37:823–843, 1936.

[7] D. Bouwmeester, A. Ekert, and A. Zeilinger, editors. *The physics of quantum information*. Springer-Verlag, Berlin, 2001.

[8] B. Coecke. The logic of entanglement. An invitation. Technical Report PRG-RR-03-12, Oxford University, 2003. web.comlab.ox.ac.uk/oucl/publications/tr/rr-03-12.html.

[9] B. Coecke. The logic of entanglement. arXiv:quant-ph/0402014, 2004.

[10] P. Deligne. Catégories tannakiennes. In *The Grothendieck Festschrift Volume II*, volume 87 of *Progress in Mathematics*, pages 111–196. Birkhäuser, 1990.

[11] R. Duncan. Quantum entanglement and multiplicative linear logic. Transfer Report Oxford University, November 2003.

[12] D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. *Nature*, 402:390–393, 1999. arXiv:quant-ph/9908010.

[13] C. Isham. *Lectures on Quantum Theory*. Imperial College Press, 1995.

[14] C. J. Isham and J. Butterfield. A topos perspective on the Kochen-Specker theorem I: Quantum states as generalized valuations. *International Journal of Theoretical Physics*, 37:2669–2733, 1998.

[15] G. M. Kelly. An abstract approach to coherence. *Lecture Notes in Mathematics*, 281:106–147, 1972.

[16] G. M. Kelly and M. L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[17] S. Mac Lane. *Categories for the Working Mathematician*. Springer-Verlag, 1971.

[18] G. M. Mackey. *The mathematical foundations of quantum mechanics*. W. A. Benjamin, 1963.

[19] B. Mitchell. *Theory of Categories*. Academic Press, 1965.

[20] M. A. Nielsen and L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[21] C. A. Petri. Non-sequential processes. Technical Report ISF-77-5, GMD, St-Augustin, Germany, 1977.

[22] C. Piron. *Foundations of quantum physics*. W. A. Benjamin, 1976.

[23] R. A. G. Seely. Linear logic, $*$-autonomous categories and cofree algebras. In *Categories in Computer Science and Logic*, volume 92 of *Contemporary Mathematics*, pages 371–382, June 1987, Boulder, Colorado, 1989.

[24] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 2004. To appear.

[25] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37nd Annual Symposium on Foundations of Computer Science*, pages 56–65. IEEE Computer Society Press, 1996.

[26] S. G. Simpson. *Subsystems of Second-Order Arithmetic*. Springer-Verlag, 1999.

[27] A. van Tonder. Quantum computation, categorical semantics, and linear logic. arXiv:quant-ph/0312174, 2003.

[28] J. von Neumann. *Mathematische grundlagen der quantenmechanik*. Springer-Verlag, Berlin, 1932. Translation, *Mathematical foundations of quantum mechanics*, Princeton University Press, 1955.

[29] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. Event-ready-detectors' Bell experiment via entanglement swapping. *Physical Review Letters*, 71:4287–4290, 1993.

Appendix: Diagramatic proofs

Proof of Lemma 3.5 (compositionality). The top trapezoid is the statement of the Lemma.

$$
\begin{tikzcd}
A \arrow[rrrrrr, "g \circ f"] \arrow[dddd, "f"'] \arrow[dr, "\rho_A"] & & & & & & C \\
& A \otimes \mathrm{I} \arrow[rr, "1_A \otimes \ulcorner g \urcorner"] \arrow[dr, "1_A \otimes \eta_B"'] \arrow[dd, "f \otimes 1_{\mathrm{I}}"'] & & A \otimes B^* \otimes C \arrow[rr, "\llcorner f \lrcorner \otimes 1_C"] \arrow[dr, "f \otimes 1_{B^* \otimes C}"'] \arrow[u, phantom, "\textbf{Lemma 3.5}"] & & \mathrm{I} \otimes C \arrow[ur, "\lambda_C^{-1}"] & \\
& & A \otimes B^* \otimes B \arrow[ur, "1_{A \otimes B^*} \otimes g"'] \arrow[dr, "f \otimes 1_{B^* \otimes B}"'] & & B \otimes B^* \otimes C \arrow[ur, "\epsilon_B \otimes 1_C"'] & & \\
& B \otimes \mathrm{I} \arrow[rr, "1_B \otimes \eta_B"'] & & B \otimes B^* \otimes B \arrow[ur, "1_{B^* \otimes B} \otimes g"'] \arrow[rr, "\epsilon_B \otimes 1_B"'] \arrow[d, phantom, "\textbf{Compact closedness}"] & & \mathrm{I} \otimes B \arrow[uu, "1_{\mathrm{I}} \otimes g"'] \arrow[dr, "\lambda_B^{-1}"] & \\
B \arrow[ur, "\rho_B"] \arrow[rrrrrr, equal] & & & & & & B \arrow[uuuu, "g"']
\end{tikzcd}
$$

Proof of Lemma 3.6 (compositional CUT). The top trapezoid is the statement of the Lemma.

$$
\begin{tikzcd}
\mathrm{I} \arrow[rrrr, "\ulcorner h \circ g \circ f \urcorner"] \arrow[ddd, "\eta_A"'] \arrow[dr, "\rho_{\mathrm{I}}"] & & & & A^* \otimes D \\
& \mathrm{I} \otimes \mathrm{I} \arrow[r, "\ulcorner f \urcorner \otimes \ulcorner h \urcorner"] \arrow[d, "\eta_A \otimes 1_{\mathrm{I}}"'] \arrow[dr, "\ulcorner f \urcorner \otimes 1_{\mathrm{I}}"] & A^* \otimes B \otimes C^* \otimes D \arrow[r, "1_{A^*} \otimes \llcorner g \lrcorner \otimes 1_D"] \arrow[u, phantom, "\textbf{Lemma 3.6}"] & A^* \otimes \mathrm{I} \otimes D \arrow[ur, "\rho_A^{-1} \otimes 1_{D^*} = 1_A \otimes \lambda_{D^*}^{-1}"] \arrow[d, phantom, "\textbf{Lemma 3.5}"] & \\
& A^* \otimes A \otimes \mathrm{I} \arrow[r, "1_{A^*} \otimes f \otimes 1_{\mathrm{I}}"] & A^* \otimes B \otimes \mathrm{I} \arrow[u, "1_{A^*} \otimes \ulcorner h \urcorner"] & A^* \otimes B \arrow[l, "\rho_{A^* \otimes B}"'] \arrow[uur, "1_{A^*} \otimes (h \circ g)"] & \\
A^* \otimes A \arrow[ur, "\rho_{A^* \otimes A}"'] \arrow[rrrr, equal] & & & & A^* \otimes A \arrow[ul, "1_{A^*} \otimes f"'] \arrow[uuu, "1_{A^*} \otimes (h \circ g \circ f)"']
\end{tikzcd}
$$

Proof of Lemma 7.6 (adjoints to points). The top trapezoid is the statement of the Lemma. The cell labelled **SMC** commutes by symmetric monoidal coherence.

$$
\begin{tikzcd}
A \arrow[rrrrr, "\psi^\dagger"] \arrow[d, "\lambda_A"'] \arrow[dr, "\rho_A"] & & \textbf{Lemma 7.6} & & & \mathrm{I} \arrow[dd, equal] \\
\mathrm{I}\otimes A \arrow[r, "\sigma_{\mathrm{I},A}"] \arrow[d, equal] \arrow[dr, "\eta_{\mathrm{I}}\otimes 1_A"] & A\otimes\mathrm{I} \arrow[r, "1_A\otimes u_{\mathrm{I}}"] \arrow[dr, "1_A\otimes\eta_{\mathrm{I}}"] & A\otimes\mathrm{I}^* \arrow[r, equal] & A\otimes\mathrm{I}^* \arrow[r, "1_A\otimes\psi_*"] & A\otimes A^* \arrow[ur, "\epsilon_A"] \arrow[dr, phantom, "\textbf{Prop. 3.3}"] & \\
\mathrm{I}\otimes A \arrow[dr, "\eta_{\mathrm{I}^*}\otimes 1_A"'] \arrow[dr, phantom, "\textbf{Prop. 3.3}"] & (\mathrm{I}^*\otimes\mathrm{I})\otimes A \arrow[r, "\sigma_{\mathrm{I}^*\otimes\mathrm{I},A}"'] \arrow[d, "\sigma_{\mathrm{I}^*,\mathrm{I}}\otimes 1_A"] & A\otimes(\mathrm{I}^*\otimes\mathrm{I}) \arrow[u, "1_A\otimes\rho_{\mathrm{I}}"'] \arrow[dr, phantom, "\textbf{SMC}"] & \mathrm{I}^*\otimes A \arrow[u, "\sigma_{\mathrm{I}^*,A}"'] \arrow[r, "\psi_*\otimes 1_A"] & A^*\otimes A \arrow[u, "\sigma_{A^*,A}"'] \arrow[r, "\epsilon_{A^*}"] & \mathrm{I} \\
 & (\mathrm{I}\otimes\mathrm{I}^*)\otimes A \arrow[r, "\alpha^{-1}_{\mathrm{I},\mathrm{I}^*,A}"'] & \mathrm{I}\otimes(\mathrm{I}^*\otimes A) \arrow[ur, "\lambda^{-1}_{\mathrm{I}^*\otimes A}"'] \arrow[r, "1_{\mathrm{I}}\otimes(\psi_*\otimes 1_A)"'] & \mathrm{I}\otimes A^*\otimes A \arrow[ur, "\lambda^{-1}_{A^*\otimes A}"'] \arrow[r, "1_{\mathrm{I}}\otimes\epsilon_{A^*}"'] & \mathrm{I}\otimes\mathrm{I} \arrow[ur, "\rho_{\mathrm{I}}^{-1}=\lambda_{\mathrm{I}}^{-1}"'] &
\end{tikzcd}
$$

Proof of Theorem 9.2 (quantum teleportation). For each $j \in \{1, 2, 3, 4\}$ we have a diagram of the form below. The top trapezoid is the statement of the Theorem. We ignore the scalars – which cancel out against each other – in this proof.

$$
\begin{tikzcd}
Q_a \arrow[rrrrrr, "\langle 1_{ac}\rangle_{i=1}^{i=4}"] \arrow[ddd, equal] \arrow[dr, "\rho_a"] & & & \textbf{Quantum teleportation} & & & 4\cdot Q_c \arrow[ddd, "p_j^{Q_c}"] \\
 & Q_a\otimes\mathrm{I} \arrow[r, "1_a\otimes\ulcorner 1_{bc}\urcorner"] \arrow[d, phantom, "\textbf{Lemma 3.5}"] & Q_a\otimes Q_b^*\otimes Q_c \arrow[r, "\langle\llcorner\beta_i^{ab}\lrcorner\rangle_{i=1}^{i=4}\otimes 1_c"] \arrow[dr, "\llcorner\beta_j^{ab}\lrcorner\otimes 1_c"'] & (4\cdot\mathrm{I})\otimes Q_c \arrow[r, "\langle p_i^{\mathrm{I}}\otimes 1_c\rangle_{i=1}^{i=4}"] \arrow[d, "p_j^{\mathrm{I}}\otimes 1_c"] & 4\cdot(\mathrm{I}\otimes Q_c) \arrow[r, "4\cdot\lambda_c^{-1}"] \arrow[d, "p_j^{\mathrm{I}\otimes Q_c}"] & 4\cdot Q_c \arrow[ur, "\bigoplus_{i=1}^{i=4}(\beta_i^c)_i^{-1}"] \arrow[d, "p_j^{Q_c}"] & \\
 & Q_c \arrow[rr, shift right, "\lambda_c"'] & & \mathrm{I}\otimes Q_c \arrow[ll, shift right, "\lambda_c^{-1}"'] \arrow[r, "1_{\mathrm{I}\otimes Q_c}"'] & \mathrm{I}\otimes Q_c \arrow[r, "\lambda_c^{-1}"'] & Q_c \arrow[dr, "(\beta_j^c)^{-1}"'] & \\
Q_a \arrow[ur, "\beta_j^{ac}"] \arrow[rrrrrr, "1_{ac}"'] & & & & & & Q_c
\end{tikzcd}
$$

Proof of Theorem 9.3 (logic-gate teleportation). The top trapezoid is the statement of the Theorem. The a, b and c-labels are the same as above. For each $j \in \{1,2,3,4\}$ we have a diagram of the form below. We ignore the scalars – which cancel out against each other – in this proof.

$$
\begin{tikzcd}
Q \arrow[rrrrrr, "\langle f\rangle_{i=1}^{i=4}"] \arrow[dd, equal] \arrow[dr, "\rho_Q"] & & & {} \arrow[d, phantom, "\textbf{Logic-gate teleportation}"] & & & 4\cdot Q \arrow[ddd, "p_j^Q"] \\
& Q\otimes\mathrm{I} \arrow[r, "1_Q\otimes\ulcorner f\urcorner"] \arrow[d, phantom, "\textbf{Lemma 3.5}"] & Q\otimes Q^*\otimes Q \arrow[r, "\langle\llcorner\beta_i\lrcorner\rangle_{i=1}^{i=4}\otimes 1_Q"] \arrow[dr, "\llcorner\beta_j\lrcorner\otimes 1_Q"'] & (4\cdot\mathrm{I})\otimes Q \arrow[r, "\langle p_i^{\mathrm{I}}\otimes 1_Q\rangle_{i=1}^{i=4}"] \arrow[d, "p_j^{\mathrm{I}}\otimes 1_Q"] & 4\cdot(\mathrm{I}\otimes Q) \arrow[r, "4\cdot\lambda_Q^{-1}"] \arrow[d, "p_j^{\mathrm{I}\otimes Q}"] & 4\cdot Q \arrow[ur, "\bigoplus_{i=1}^{i=4}\varphi_i(f)^{-1}"] \arrow[d, "p_j^Q"] & \\
Q \arrow[r, "f\circ\beta_j"'] \arrow[d, equal] & Q \arrow[rr, shift right, "\lambda_Q"'] & & \mathrm{I}\otimes Q \arrow[ll, shift right, "\lambda_Q^{-1}"'] \arrow[r, "1_{\mathrm{I}\otimes Q}"'] & \mathrm{I}\otimes Q \arrow[r, "\lambda_Q^{-1}"'] & Q \arrow[dr, "\varphi_j(f)^{-1}"'] & \\
Q \arrow[rrrrrr, "f"'] \arrow[ur, "\varphi_j(f)\circ f"] & & & & & & Q
\end{tikzcd}
$$

Proof of Theorem 9.4 (entanglement swapping). The top trapezoid is the statement of the Theorem. We have a diagram of the form below for each $j \in \{1,2,3,4\}$. To simplify the notation of the types we set (a^*, b, c^*, d) for $Q_a^* \otimes Q_b \otimes Q_c^* \otimes Q_d$ etc. We ignore the scalars – which cancel out against each other – in this proof.

$$
\begin{tikzcd}
\mathrm{I}\otimes\mathrm{I} \arrow[rrrrr, "\langle\ulcorner 1_{ba}\urcorner\otimes\ulcorner 1_{dc}\urcorner\rangle_{i=1}^{i=4}"] \arrow[dr, "\ulcorner 1_{da}\urcorner\otimes\ulcorner 1_{bc}\urcorner"] & & & {} \arrow[d, phantom, "\textbf{Entanglement swapping}"] & & 4\cdot(b^*,a,d^*,c) \arrow[ddd, "p_j^{(b^*,a,d^*,c)}"] \\
& (d^*,a,b^*,c) \arrow[r, "\Theta_{ab}"] \arrow[dr, "1_d^*\otimes\llcorner\beta_j\lrcorner\otimes 1_c"'] \arrow[d, phantom, "\textbf{Lemma 3.6}"] & (d^*,4\cdot(a,b^*),c) \arrow[r, "{(\tau,\upsilon)}"] \arrow[dr, "1_d^*\otimes p_j^{(a,b^*)}\otimes 1_c"'] & 4\cdot(d^*,a,b^*,c) \arrow[r, "4\cdot\sigma"] \arrow[d, "p_j^{(d^*,a,b^*,c)}"] & 4\cdot(b^*,a,d^*,c) \arrow[ur, "\bigoplus_{i=1}^{i=4}(1_b^*\otimes\gamma_i^{-1}\otimes 1_d^*\otimes\beta_i^{-1})"'] \arrow[d, "p_j^{(b^*,a,d^*,c)}"] & \\
& (d^*,c) \arrow[d, "\lambda_{d^*}\otimes 1_c"] & (d^*,\mathrm{I},c) \arrow[l, "\rho_{d^*}^{-1}\otimes 1_c"'] \arrow[r, "1_d^*\otimes\ulcorner\gamma_j\urcorner\otimes 1_c"'] \arrow[dl, "\sigma^{-1}"'] \arrow[d, "1_d^*\otimes\ulcorner 1_{ab}\urcorner\otimes\beta_j^{-1}"] \arrow[dr, phantom, "\textbf{Lemma 3.4}"] & (d^*,a,b^*,c) \arrow[r, "\sigma"'] \arrow[d, "1_d^*\otimes\gamma_j^{-1}\otimes 1_b^*\otimes\beta_j^{-1}"] & (b^*,a,d^*,c) \arrow[dr, "1_b^*\otimes\gamma_j^{-1}\otimes 1_d^*\otimes\beta_j^{-1}"'] & \\
\mathrm{I} \arrow[uuu, "\rho_{\mathrm{I}}"] \arrow[d, "\lambda_{\mathrm{I}}"] \arrow[ur, "\ulcorner\beta_j\urcorner"] & (\mathrm{I},d^*,c) \arrow[dr, "\ulcorner 1_{ba}\urcorner\otimes 1_d^*\otimes\beta_j^{-1}"] \arrow[d, phantom, "\textbf{Lemma 3.4}"] & (d^*,a,b^*,c) \arrow[r, equal] \arrow[d, "\sigma^{-1}"] & (d^*,a,b^*,c) \arrow[rr, "\sigma"'] & & (b^*,a,d^*,c) \\
\mathrm{I}\otimes\mathrm{I} \arrow[rr, "\ulcorner 1_{ba}\urcorner\otimes\ulcorner 1_{dc}\urcorner"'] & {} & (b^*,a,d^*,c) & & &
\end{tikzcd}
$$