Université de Montréal

Categorical quantum computation

par
Éric Oliver Paquette

Département d'informatique et de recherche opérationelle
Faculté des arts et des sciences

Thèse présentée à la faculté des études supérieures et postdoctorales en vue de l'obtention du grade de Philosophiæ Doctor (Ph. D.) en informatique

septembre 2008

Résumé

L'informatique quantique est un sous-domaine de l'informatique qui étudie le calcul fait en utilisant certaines propriétés de la mécanique quantique telles que l'intrication et le principe de superposition quantique. Les travaux présentés dans cette thèse s'inscrivent dans un programme de recherche initié par S. Abramsky et B. Coecke qui vise à établir les fondements du calcul quantique dans le contexte de la théorie des catégories.

L'axiomatisation catégorique usuelle du calcul quantique utilise la notion de biproduit afin d'exprimer le fragment classique de la théorie qui comprend, par exemple, le résultat d'une mesure ou le contrôle classique. En se basant sur les travaux de S. Abramsky et B. Coecke et ceux de P. Selinger pour l'aspect quantique ainsi que sur les travaux de B. Coecke et de D. Pavlovic pour l'aspect classique, nous présenterons une sémantique catégorielle complète pour le calcul quantique qui comprend à la fois le fragment classique et le fragment quantique de la théorie. Pour ce faire, nous introduirons la notion d'interface classique-quantique qui est suffisamment générale pour traiter de ces deux fragments. De plus, le fragment classique sera axiomatisé exclusivement à l'aide de la structure tensorielle *i.e.*, sans utiliser la notion de biproduit. Une telle approche permet, entre autres, l'utilisation d'un calcul graphique intuitif et rigoureux comme technique de preuve qui est souvent plus facile à manipuler que les expressions algébriques usuelles. De surcroît, nous verrons que l'axiomatisation des structures de bases desquelles sont dérivées la notion de transformation classique permet aussi la définition de plusieurs familles de transformations classiques telles que les relations, les fonctions, les bijections et les applications stochastiques et bistochastiques; les trois dernières étant spécialement souhaitables dans le contexte du calcul quantique. Finalement, nous présenterons quelques protocoles quantiques et prouverons certains résultats liés à ceux-ci à l'aide du calcul graphique développé pour la sémantique afin de démontrer le bien-fondé et l'utilité de la présentation.

Mots clés: Calcul quantique. Contrôle classique. Théorie des catégories. Catégories compactes closes. Catégories †-monoidales. Catégories †-compactes closes. Interfaces classiques-quantiques.

Abstract

Quantum computation is a sub-discipline of computer science that studies computation performed using quantum-mechanical phenomena such as entanglement and the principle of quantum superposition. The work presented in this dissertation is part of a program of research initiated by S. Abramsky and B. Coecke that aims to establish a categorical foundation for quantum computation.

The usual axiomatisation of quantum computation uses the biproduct structure to express the classical fragment of the theory that comprises, for instance, the result of a measurement or classical control. Following the work of S. Abramsky and B. Coecke, that of P. Selinger for the quantum aspect, and that of B. Coecke and D. Pavlovic for the classical aspect, we will introduce a complete categorical semantics for quantum computation that includes both the classical and the quantum fragments of the theory. In order to do so, we will introduce the notion of classical-quantum interface, which is sufficiently general to include the two fragments of the theory. Moreover, the classical fragment will be axiomatised exclusively with respect to the tensorial structure, *i.e.*, without using biproducts. In particular, such an approach enables the use of an intuitive and rigorous graphical calculus as a proof technique which is often easier to use than the usual algebraic techniques. Moreover, we will see that the axiomatisation of basis structures from which is derived the notion of classical transformation also enables the definition of many families of classical transformations such as relations, functions, bijections, and stochastic and bistochastic transformations; the latter three being especially suitable in the context of quantum computation. Finally, we will present some quantum protocols and prove some results concerning these, using a graphical calculus developed for the categorical semantics in order to illustrates the usefulness and the well-foundedness of the theory .

Key words: Quantum computation. Classical control. Category theory. Compact closed categories. †-monoidal categories. †-compact categories. Classical-quantum interfaces.

Acknowledgement

Je tiens d'abord à remercier Michel Boyer pour son soutien tout au long de mes études doctorales, pour ses commentaires, son temps, nos discussions et ses critiques au sujet de mon travail qui m'ont toujours poussé à faire mieux; Gilles Brassard pour son soutien académique, financier et pour plusieurs discussions qui m'ont aidé à approfondir ma compréhension de l'informatique quantique.

Beaucoup de résultats présentés dans cette thèse proviennent de mes collaborations avec Bob Coecke, Dusko Pavlovic, Prakash Panangaden et Simon Perdrix. Je ne peux que souligner le travail exceptionnel et les contributions de toutes ces personnes.

Merci aussi a Samson Abramsky et Bob Coecke pour m'avoir invité à des sessions de travail à l'Université d'Oxford et pour croire en mon potentiel.

Je me dois aussi de souligner la patience de tous mes collègues du LITQ pour avoir enduré mes "absconseries" durant ces quatre années.

Merci à Frédéric Dupuis, Yannick Delbecque et Ross Duncan pour leurs commentaires sur des parties de cette thèse et à Yan Thériault ainsi qu'à James Vicary pour avoir révisé le texte.

À Caroline

There is no knowledge, no attainment, no realisation...

– Maka hannya haramita shingyo

Contents

1 Introduction

Quantum computation is a sub-discipline of computer science that relies on quantum mechanical properties such as quantum entanglement and quantum superposition to realise feats that are generally admitted – and often proven – to be impossible for classical computers. For instance, quantum pseudotelepathy games [15] or Shor's integer factorisation algorithm [63], a quantum algorithm which is exponentially faster than the best classical algorithm known to date, the general number field sieve [60].

As compared to quantum mechanics, the usual mathematical theory of quantum computation is fairly simple. Indeed, while the mathematical formulation of quantum mechanics relies on linear algebra, differential equations, harmonic and functional analysis, quantum computation can be understood via the basic notions of finite-dimensional Hilbert spaces. However, the advent of quantum computation changed the perspective relative to some concepts prevalent in quantum mechanics. For instance, as noted by S. Abramsky and B. Coecke in [7], quantum entanglement was reduced to a paradox by Einstein, Podolsky and Rosen [44] in the thirties. In the sixties, Bell formulated its celebrated theorem [20] about entanglement. Then, with the advent of quantum computing, it became a feature as, for instance, in the quantum teleportation [13] and superdense coding [14] protocols. More recently, it even became an informatic resource [10]. All in all, quantum computation—despite its simple mathematical formalism—remains a fertile ground to reason about quantum phenomena.

The results of this thesis aren't described in the language of Hilbert spaces—or even C^* algebras, another formalism sometimes used—but in terms of categories. Category theory is, broadly speaking, a theory of structures and relations between them. Following this, a categorical axiomatisation of quantum computing brings the most fundamental structures needed for quantum computation to the forefront and studies how they interact. Such a framework of study brings in new tools for the study of quantum information such as:

1. *Graphical calculus.* The categorical axiomatisation used in this thesis enables a rigorous graphical calculus which is, in the author's opinion, easier to manipulate than the usual algebraic expressions or even the $2^n \times 2^n$ matrices one usually works with in quantum computing. Moreover, such a graphical calculus can be used as a proof technique, and such graphical proofs are often more succinct and appealing than the usual algebraic proofs, as they provide a direct visual understanding of what a formula means in terms of information flow and the manipulations that one performs on such an expression.

2. *Models.* A categorical formulation of quantum computation may accommodate a wide range of models. The study of different models may shed some new light on the nature of quantum data which often behaves in an non-intuitive manner.

3. *Different views on quantum informatics.* There are a few, for instance:

i. The area of quantum programming languages has been a fertile area in the last few years. Many quantum λ-calculi where introduced [71,74], Selinger's QPL [66], T. Altenkirch and J. Grattage's QML [9] and so on. Such quantum programming languages are often described within a category-theoretic framework.

ii. Quantum games as introduced by Y. Delbecque in [41], [39] and [40] with P. Panangaden.

iii. Last but certainly not least, the categorical foundations of quantum computation in terms of †-compact categories, which is the context of this dissertation.

Hence, if we agree that quantum computing is—in particular—about understanding the nature of quantum information, category theory provides a new angle to such an understanding and is a topic worth studying.

The new results of this dissertation consist of a re-writing of a (strict) subset of the results found in the following papers:

1. Bob Coecke, Éric Oliver Paquette and Dusko Pavlovic, Classical and quantum structuralism. To appear in: *Semantic techniques in Quantum Computation.* S. Gay and I. Mackie, Eds. Cambridge University Press.

2. Bob Coecke, Éric O. Paquette and Dusko Pavlovic, *Classical and quantum structures.* Oxford University Computing Laboratory Research Report PRG-RR-08-02, 2008.

3. Bob Coecke and Éric Oliver Paquette, *POVMs and Naimark's theorem without sums.* Proceedings of the 4th International Workshop on Quantum Programming Languages (QPL'06). Electronic Notes in Theoretical Computer Science, Vol 210, pp. 123–137, 2008.

4. Bob Coecke, Éric Oliver Paquette and Simon Perdix, *Bases in diagrammatic quantum protocols.* Proceedings of the 24th Conference on the Mathematical Foundation of Programming Semantics (MFPS XXIV). Electronic Notes in Theoretical Computer Science, Vol. 218, pp. 131–152, 2008.

along with some comments and calculations taken from [35], an introduction to category theory that the author wrote with B. Coecke. All of these are part of a program initiated by S. Abramsky and B. Coecke in their seminal paper *A categorical semantics of quantum protocols* [5], which has become a very active field since its inception; see for instance, [1, 6, 2, 8, 30, 42] and [69] as well as the many papers cited throughout this dissertation. Such a program aims to recast the standard axiomatisation of quantum computing in terms of †-compact categories. Such an axiomatisation is given, broadly speaking and in the context of **FdHilb**—the category of finite-dimensional Hilbert spaces—, in terms of adjoints and maximally entangled states. It has been extended to categories of completely positive maps by P. Selinger in [68] in order to accommodate the notion of mixed states and superoperators. A remarkable feature of such an axiomatisation is that it does not rely on the notion of basis when one restricts oneself to the quantum fragment of the theory. The notion of basis can be abstracted in the categorical language as a biproduct structure; such an approach was taken in both [5] and [68].

The main contributions of this dissertation are as follows:

- Building upon the work of B. Coecke and D. Pavlovic in [36] where they developed the notion of classical objects which axiomatises orthonormal bases in **FdHilb** in pure tensorial terms, we will define the notion of basis structure on an object in a †-compact category which we call a *category of quantum structures* throughout this dissertation. As for classical objects, basis objects are defined in pure tensorial terms, *i.e.*, without any reference to biproducts. From this, we will define the notion of category of basis structures and inspect how the basis structures and the quantum structures interact therein.

- In such categories, maps built from tensoring and composing the structural morphisms of the basis structure and identities and whose graphical representation is connected—in a sense to be defined—admit a normal form. We will give an algorithm of reduction of any such connected map into normal form. Such a reduction simplifies calculations in a non-trivial manner.

- We will define the notion of classical maps in a category of basis structures and show that the subcategory of classical maps of a category of basis structures is again a category of basis structures. In the context of finite-dimensional Hilbert spaces, classical maps are those matrices with entries in $\mathbb{R}_+$ hence the name "classical". The structural morphisms of basis objects enable us to define many subclasses of classical maps such as relations, functions, bijections, stochastic and bistochastic maps.

- We will construct the category of classical-quantum interfaces of a category of quantum structures and show that this category is again a category of quantum structures. The morphisms of such a category comprise classical maps, quantum maps (actually, completely positive maps), controlled quantum maps, projective measurements and positive operator-valued measurements (POVMs). Moreover, we will see that both the category of completely positive maps and the category of classical maps embed faithfully in the category of interfaces.

- Finally, throughout this dissertation, we will make extensive use of graphical calculus. As we shall see in chapter 8 of this dissertation, it can be very handy in describing protocols and, among other things, proving their correctness. In that sense, it provides a suitable less "static" alternative to quantum circuits. Indeed, while there are some transformations possible on quantum circuits (see, for instance, [63] pp. 178–185), the graphical calculus that we will use is a powerful proof technique whose scope surpasses what one can do with quantum circuits with respect to algebraic (or operation) manipulations.

Another (albeit minor) result of this dissertation is that it has been written for a target audience of quantum computer scientists with no prior knowledge of category theory; this had two major consequences on the way it was written. First, when bringing up a new subject, we will usually start by discussing the corresponding concept in the category **FdHilb** of finite dimensional Hilbert spaces rather than by introducing the concepts in categorical terms first. Since the latter was the usual approach taken in the papers cited above, it seemed appropriate to proceed the other way around for the targeted audience. Second, it should be noted that some constructions and definitions given throughout this dissertation can be seriously shortened using the advanced machinery of category theory. However, we did not do so in order to keep the discussion at a reasonable level of abstraction; for instance, all questions related to monads, Eilenberg-Moore algebras, Kleisli categories, adjunctions and bicategories have been avoided but are discussed in the papers cited above.

The plan of this dissertation is as follows:

Chapter 2 is a brief introduction to Hilbert spaces and quantum computing.

Chapter 3 is a standard introduction to category theory where we define the notions of categories, functors, quotient categories and natural transformations.

Chapter 4 is about †-monoidal categories. We will discuss the notion of monoidal category, which is central to the whole dissertation. Such categories, as mentioned above, are equipped with a product which is a suitable abstraction of the tensor product of vector spaces. In addition, we will introduce the notions of traced monoidal categories, internal monoids, internal comonoids and scalars. We will then introduce the graphical calculus for monoidal categories. Further, we will define the notion of †-monoidal category which will give us the necessary formalism to describe adjoints and related concepts. Finally, we will extend the graphical calculus for monoidal categories to †-monoidal categories.

Chapter 5 discusses the notion of quantum structures, categories of quantum structures, and how the latter constitutes a suitable framework for quantum computation. Moreover, we will introduce the category of completely positive maps of a category of quantum structures; the morphisms of such a category will allow us to handle mixed states and superoperators.

Chapter 6 is about basis structures and classical maps. First, we will need to define the notion of basis structure as a complement of a quantum structure. From there, we will inspect how the basis structures interact with quantum structures. Finally, we will define classical maps and study their properties.

In chapter 7, we give the main construction of this dissertation: we define the notion of classical-quantum interfaces and we construct the category of classical-quantum interfaces of a category of quantum structures; moreover, we show that such a category is again a category of quantum structures. Such a construction allows us to give a formal semantics for all data comprising both the quantum and the classical fragment of the theory together with non-trivial interfaces such as controlled operations and measurements. Some important results will be stated and proved such as, for instance, a classification of the different types of classical maps and a categorical (and purely graphical) proof of Naimark's theorem for POVMs.

In chapter 8, we will discuss protocols using the language of a category of classical-quantum interfaces. Among other things, we will prove correctness of the quantum teleportation protocol and superdense coding, and relate both quantum teleportation with superdense coding and BB84 with BBM92 (a protocol akin to Ekert91 [43]) within our framework, which may suggest a new line of investigation concerning structural resources.

Finally, in chapter 9, we will give some concluding remarks and discuss future work.

2 Quantum computing

This chapter intends to cover briefly the basic notions of quantum computation and Hilbert spaces. As the results of this dissertation are built upon the standard mathematical presentation of quantum mechanics, we will only recall the important concepts and results of quantum computation and Hilbert spaces from a mathematical standpoint. In other words, we won't give any interpretation as to why or how quantum mechanical phenomena occur. The intent is not to give a complete introduction but to recall most of the concepts that will be used in this dissertation.

This chapter consists of two sections. The first one introduces the notions of Hilbert space, of tensor product of Hilbert spaces and finally, discusses the notion of vector and matrices relative to a chosen basis. The second section introduces the basic notions of quantum computation and discusses quantum states, transformations of quantum states, measurements and open systems via mixed states and superoperators.

2.1 Hilbert spaces

The formalism of quantum computing heavily relies on linear algebra. Thus, we make use of this section to recall some important concepts and to fix the notation. Moreover, as we will often use the category of Hilbert spaces and bounded linear operator as an example and since an important part of the theory we will introduce in the forthcoming chapters is basis-independent, we will introduce most concepts in the most general way here. The following presentation is standard; for instance, see [61] where—unless otherwise specified—all the results and definitions from this section are taken.

2.1.1 Hilbert spaces

The goal of this subsection is to rigorously define the notion of Hilbert space; this is the most fundamental notion in quantum mechanics and quantum computation, as the state vector which completely describes the state of a quantum system is but a unit vector in a Hilbert space. All along, we will work with *complex vector spaces*, *i.e.*, vector spaces where the field of scalars is $\mathbb{C}$, the complex field. Hence, when we speak of vector spaces, we mean complex vector spaces. We first define different types of transformations between complex vector spaces.

[**Linear and multilinear map**] Given two vector spaces V and W, a *linear map* is function $f : V \longrightarrow W$ such that for any $v, w \in V$ and $z \in \mathbb{C}$, we have

$$f(v + w) = f(v) + f(w) \qquad \text{and} \qquad f(z \cdot v) = z \cdot f(x).$$

Given vector spaces $V_1, \cdots, V_n$ and W, a *multilinear map* or *n-linear map* is a function $f : V_1 \times \cdots \times V_n \longrightarrow W$ which is linear in each variable.

A particular instance of bilinear map is a *(bilinear) form* which is just a bilinear map of type $V \times V \longrightarrow \mathbb{C}$.

[**Antilinear map**] Given two vector spaces V and W, an *antilinear map* is a function $f : V \longrightarrow W$ such that for any $v, w \in V$ and $z \in \mathbb{C}$, we have

$$f(v + w) = f(v) + f(w) \qquad \text{and} \qquad f(z \cdot v) = \overline{z} \cdot f(x)$$

where $\overline{z}$ is the complex conjugate of z.

[**Inner product and inner product space**] A map $\phi : V \times V \longrightarrow \mathbb{C}$ is a *sesquilinear form* on a complex vector space V if for all $v, w, x, y \in V$ and $z_1, z_2 \in \mathbb{C}$,

1. $\phi(v + w, x + y) = \phi(v, x) + \phi(v, y) + \phi(w, x) + \phi(w, y)$ and

2. $\phi(z_1 \cdot v, z_2 \cdot w) = \overline{z_1} z_2 \phi(v, w)$.

A sesquilinear form is *Hermitian* if for all $v, w \in V$,

$$\phi(v, w) = \overline{\phi(w, v)}.$$

A form ϕ is *positive definite* if for all $v \in V$,

$$\phi(v, v) \geq 0 \quad \text{and} \quad \phi(v, v) = 0 \text{ implies } v = 0.$$

An *inner product* on V is a positive-definite Hermitian form $\langle -, - \rangle : V \times V \longrightarrow \mathbb{C}$ and an *inner product space* is a vector space that comes equipped with an inner product.

Inner products enable the following notions:

[**Orthogonal vectors**] Let V an inner product space, then $v, w \in V$ are *orthogonal* if $\langle v, w \rangle = 0$.

[**Norm**] The *norm* induced by an inner product $\langle -, - \rangle$ is

$$\| - \| := \sqrt{\langle -, - \rangle}.$$

Note that $\| v \|$ is a positive real number, since $\langle -, - \rangle$ is positive definite.

[**Bounded linear operator**] A linear operator $f : V \longrightarrow W$ between inner product spaces is *bounded* if there exists a $c > 0$ such that for all $v \in V$,

$$\| f(v) \|_W \leq c \| v \|_V .$$

We will denote the set of bounded operators of type $V \longrightarrow V$ by $L(V)$ and the set of those of type $V \longrightarrow W$ by $L(V, W)$.

Now,

[**Hilbert space**] A *Hilbert space* $\mathcal{H}$ is a complex vector space with a inner product $\langle -, - \rangle$ which is complete under the norm $\| - \|$ that is, every Cauchy sequence in $\mathcal{H}$ converges in $\mathcal{H}$ under $\| - \|$.

Example 2.1.1 For any n, the vector space $\mathbb{C}^n$ is a Hilbert space when equipped with the dot product as inner product (see p. 13).

[**Adjoint**] If it exists, the *adjoint* of a linear operator $f : \mathcal{H} \to \mathcal{H}'$ is a linear operator $f^\dagger : \mathcal{H}' \to \mathcal{H}$ such that for all $\psi \in \mathcal{H}$ and $\phi \in \mathcal{H}'$,

$$\langle f^\dagger \phi, \psi \rangle_{\mathcal{H}} = \langle \phi, f\psi \rangle_{\mathcal{H}'}.$$

Theorem 2.1.2 Let $f : \mathcal{H} \to \mathcal{H}'$ be a bounded operator, then there exists a unique bounded operator $f^\dagger$ such that for all $\phi, \psi \in \mathcal{H}$,

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

Hence, all bounded operators admit a unique adjoint.

Proof: See [61].

□

Theorem 2.1.3 If f and g both admit an adjoint, then

i. $(f^\dagger)^\dagger = f$.

ii. $(f + g)^\dagger = f^\dagger + g^\dagger$.

iii. For any $z \in \mathbb{C}$, $(z \cdot f)^\dagger = \overline{z} \cdot f^\dagger$.

iv. Finally, if the composite $g \circ f$ is defined, $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$.

Proof: See [61].

□

The notion of adjoint enables us to define many concepts crucial in quantum mechanics and quantum computation.

[**Self-adjoint operator**] An operator f is *self-adjoint* if $f^\dagger = f$.

Self-adjoint operators arise in quantum mechanics as physical observables. For instance, angular momentum, position and spin are all represented by self-adjoint operators on a Hilbert space.

[**Positive operator**] A self-adjoint operator f is *positive* if for all x,

$$\langle fx, x \rangle = \langle x, fx \rangle \geq 0.$$

Notation. We will denote that an operator f is positive by $f \geq 0$.

[**Unitary operator**] A *unitary operator* is a bounded linear operator $U : \mathcal{H} \to \mathcal{H}'$ such that

$$U^\dagger \circ U = 1_{\mathcal{H}} \quad \text{and} \quad U \circ U^\dagger = 1_{\mathcal{H}'}$$

where $1_{\mathcal{H}}$ (resp. $1_{\mathcal{H}'}$) denotes the identity on $\mathcal{H}$ (resp. $\mathcal{H}'$).

Unitary transformations describe the evolution of a particular class of quantum systems.

The following notion will be important when we define the category of finite dimensional Hilbert spaces:

[Conjugate space] The *conjugate space* of a Hilbert space $\mathcal{H}$ is a Hilbert space $\mathcal{H}^*$ with the same underlying set of vectors as $\mathcal{H}$ but where

- The scalar multiplication of $z \in \mathbb{C}$ with $\psi \in \mathcal{H}^*$ is $\bar{z} \cdot \psi$ taken as in $\mathcal{H}$ and

- The inner product $\langle \phi, \psi \rangle_{\mathcal{H}^*}$ is defined as $\langle \psi, \phi \rangle_{\mathcal{H}}$.

Remark 2.1.4 Note that the map

$$\mathcal{H} \to \mathcal{H}^* :: \phi \mapsto \phi$$

is an antilinear isomorphism.

2.1.2 Tensor product

As we will see in section 2.2, if two quantum systems are described by the state vectors $\phi \in \mathcal{H}$ and $\psi \in \mathcal{H}'$, then their compound system is described by the state vector $\phi \otimes \psi \in \mathcal{H} \otimes \mathcal{H}'$.

[Tensor product] The *tensor product* of two vector spaces V_1 and V_2 is a vector space $V_1 \otimes V_2$ together with a bilinear map

$$\otimes : V_1 \times V_2 \to V_1 \otimes V_2 :: (v_1, v_2) \mapsto v_1 \otimes v_2$$

such that for any space W and any bilinear map $f : V_1 \times V_2 \to W$, there is a unique linear map $\hat{f}$ satisfying for any pair $(v, v') \in V_1 \times V_2$,

$$f(v, v') = \hat{f}(v \otimes v').$$

In terms of commutative diagram, the defining condition can be expressed as

$$\begin{tikzcd}
V_1 \times V_2 \arrow[r, "\otimes"] \arrow[dr, "f"'] & V_1 \otimes V_2 \arrow[d, "\hat{f}"] \\
& W
\end{tikzcd}$$

While this defines the tensor product, it does not proves its existence. The standard construction is as follows:

- Consider the free vector space $F(V \times W)$ generated by $V \times W$ *i.e.*, the vector space of linear combinations of pairs of elements $e \otimes f := (f, g)$ with $e \in V$ and $f \in W$.

- Define R as the vector space spanned by elements of the form

  - $(\alpha_1 e_1 + \alpha_2 e_2) \otimes f - \alpha_1 e_1 \otimes f - \alpha_2 e_2 \otimes f$ and

  - $e \otimes (\alpha_1 f_1 + \alpha_2 f_2) - \alpha_1 e \otimes f_1 - \alpha_2 e \otimes f_2$.

The tensor product of V and W is then

$$V \otimes W := V \times W/R.$$

The tensor product extends to linear maps as follows:

Proposition 2.1.5 [55] Given linear maps $f : V \to W$ and $g : V' \to W'$, there is a unique linear map $f \otimes g : V \otimes V' \to W \otimes W'$ such that for any $v \in V$ and $v' \in V'$,

$$(f \otimes g)(v \otimes v') = f(v) \otimes g(v').$$

Proof: See [55].

□

Finally,

[Tensor product of Hilbert spaces] Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces with inner products $\langle -, - \rangle_1$ and $\langle -, - \rangle_2$ respectively. The tensor product of $\mathcal{H}_1$ and $\mathcal{H}_2$ is the vector space $\mathcal{H}_1 \otimes \mathcal{H}_2$—taken as a tensor product of vector spaces—with inner product $\langle -, - \rangle$ defined by linearly extending

$$\langle \phi_1 \otimes \phi_2, \psi_1 \otimes \psi_2 \rangle := \langle \phi_1, \psi_1 \rangle_1 \langle \phi_2, \psi_2 \rangle_2 \quad \text{for all } \phi_1, \psi_1 \in \mathcal{H}_1 \text{ and } \phi_2, \psi_2 \in \mathcal{H}_2$$

to the whole vector space $\mathcal{H}_1 \otimes \mathcal{H}_2$.

2.1.3 Basis

The notion of basis offers a specification of quantum states by means of a fixed reference relative to which we work. For instance, in quantum computing, we usually take the so-called standard (or computational) basis (see below) for fixed reference for the Hilbert space $\mathbb{C}^2$. The initial state in which the computation starts is a vector in that basis and evolution of the system is formulated as a unitary transformation with respect to that basis.

[Basis] Let $\mathcal{H}$ be a Hilbert space. An *orthonormal basis* for $\mathcal{H}$ is a family $B := \{e_i\}_i$ of vectors in $\mathcal{H}$ such that

- The elements of B are pairwise orthogonal *i.e.*: $\langle e_i, e_j \rangle = 0$ when $i \neq j$
- Any $e_i \in B$ satisfies $\| e_i \| = 1$.
- The linear span of B is dense in $\mathcal{H}$.

We say that a Hilbert space $\mathcal{H}$ is *finite-dimensional* if it admits a basis B which is finite.

Remark 2.1.6 Whenever $\mathcal{H}$ is finite-dimensional, B forms a spanning set for $\mathcal{H}$.

From now on, we will work on finite-dimensional Hilbert spaces. Thus, when we will speak of a Hilbert space, we implicitly mean a finite-dimensional Hilbert space.

Theorem 2.1.7 Every Hilbert space admits an orthonormal basis.

Proof: See [61].

□

Example 2.1.8 The set of n-tuples of complex numbers

$$e_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad e_2 := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad \cdots \quad e_n := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

defines an orthonormal basis for $\mathbb{C}^n$ called the *standard basis.*

Proposition 2.1.9 Let $\mathcal{H}$ and $\mathcal{H}'$ be finite-dimensional Hilbert spaces. Then any linear operator $f : \mathcal{H} \to \mathcal{H}'$ is bounded.

Proof: See [61].

□

In particular, this entails that $L(\mathcal{H})$ contains all the linear operators of type $\mathcal{H} \to \mathcal{H}$ when $\mathcal{H}$ is finite-dimensional.

Once we have chosen an orthonormal basis $B = \{\phi_i\}_i$ for $\mathcal{H}$, every vector $\phi \in \mathcal{H}$ can be written as a unique linear combination of the ϕ_i's *i.e.*,

$$\phi = \sum_i z_i' \phi_i \quad \text{where} \quad z_i' := \langle \phi_i, \phi \rangle.$$

If the basis B contains n elements, the n-tuple

$$[\phi]_B := \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix}$$

such that $\phi = \sum_{i=1}^n z_i \phi_i$ is the *coordinate-vector of ϕ relative to the basis B*. It is not hard to see that there is a bijection between the vectors of $\mathcal{H}$ and the n-tuples of $\mathbb{C}^n$.

Now, given a basis $B = \{\phi_1, \cdots, \phi_m\}$ and $B' = \{\psi_1, \cdots, \psi_n\}$ for $\mathcal{H}$ and $\mathcal{H}'$ respectively and a linear operator $f : \mathcal{H} \to \mathcal{H}'$, then for all i, $f(\phi_i) \in \mathcal{H}'$ and hence can be written as a linear combinaison of the ψ_i's:

$$\begin{aligned} f(\phi_1) &= z_{11}\psi_1 + z_{21}\psi_2 + \ldots + z_{n1}\psi_n \\ f(\phi_2) &= z_{12}\psi_1 + z_{22}\psi_2 + \ldots + z_{n2}\psi_n \\ \vdots \quad & \vdots \qquad\qquad \vdots \\ f(\phi_m) &= z_{1m}\psi_1 + z_{2m}\psi_2 + \ldots + z_{nm}\psi_n \end{aligned}$$

The table of complex numbers

$$[f]_B^{B'} := \begin{pmatrix} z_{11} & z_{12} & \cdots & z_{1m} \\ z_{21} & z_{22} & \cdots & z_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ z_{n1} & z_{n2} & \cdots & z_{nm} \end{pmatrix}$$

is called the *matricial representation of f relative to B and B'*. From this, we may denote the entry z_{ij} of a matrix $M : \mathbb{C}^n \to \mathbb{C}^m$ simply by M_{ij}. Again, we see that we have a bijection between the linear operators $f \in L(\mathcal{H})$ and the matrices in $\mathbb{C}^{n \times m}$. Now that we have a matricial representation for linear operators, we can recast the concepts of the two preceding sections in terms of matrices.

The tensor product of matrices admits a simple form:

[Kronecker product] The *Kronecker product* $M \otimes N$ of two matrices M and N is given as first taking

$$M \otimes N := \sum_{i,j} (M)_{ij} \cdot N$$

abd then removing the parenthesis from the expression. Thus, if M is of dimension $n \times m$ and N of dimension $n' \times m'$, $M \otimes N$ can be seen as a block matrix of matrices of dimension $nn' \times mm'$ where the block i, j with $1 \leq i \leq n$ and $1 \leq j \leq m$ is $(M)_{ij} \cdot N$.

Example 2.1.10 The Kronecker product

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes M = \begin{pmatrix} a \cdot M & b \cdot M \\ c \cdot M & d \cdot M \end{pmatrix}$$

thus a matrix of four blocks of dimension equal to the dimension of M.

[Hermitian transpose of a matrix] Let $(-)^T$ denote the transposition and $\overline{(-)}$ pointwise complex conjugation. The *hermitian transpose* $M^\dagger$ of a complex matrix M is

$$M^\dagger := (\overline{M})^T = \overline{(M^T)}.$$

The dagger notation for the Hermitian transpose seems to clash with the notation for the adjoint. We will address this issue below.

Theorem 2.1.11 Let $U : \mathcal{H} \to \mathcal{H}$ be a linear operator, then the following are equivalent:

i. $U^\dagger = U^{-1}$, *i.e.*, U is unitary,

ii. For any $\phi, \psi \in \mathcal{H}$, $\langle U\phi, U\psi \rangle = \langle \phi, \psi \rangle$.

iii. For any $\phi \in \mathcal{H}$, $\| U\phi \| = \| \phi \|$.

Proof: See [61].

□

Thus, as unitary transformations preserve the inner products, it follows that they preserve all the structures of a Hilbert space. Moreover

Theorem 2.1.12 Given any two orthonormal bases $B = \{\psi_1, ..., \psi_n\}$ and $B' = \{\phi_1, ..., \phi_n\}$ of a Hilbert space $\mathcal{H}$, then there exists a unique unitary transformation $U : \mathcal{H} \to \mathcal{H}$ such that $\phi_j = \sum_i U_{ij} \psi_i$; $j = 1, ..., n$.

Proof: See [61].

□

Thus, we may think of a unitary transformation as an operator that "rotates" the basis. Following this, for any fixed basis B for $\mathcal{H}$, the dot product of ϕ and $\psi \in \mathcal{H}$ is given by

$$\phi \bullet \psi = [\phi]_B^\dagger \, [\psi]_B$$

where $[\phi]_B^\dagger$ is the Hermitian transpose of $[\phi]_B$. Routine verification shows that the dot product is an inner product and, moreover, that the adjoint of the matricial representation of an operator is given by its Hermitian transpose. This inner product is the one commonly used in quantum computation thus, from now on, we assume that our Hilbert spaces are equipped with the dot product as inner product which we will denote $\langle -, - \rangle$ to align with Dirac notation that we will introduce in the next section.

[**Trace**] The *trace* of a square matrix $M = (M)_{ij}$ is defined as the sum of its diagonal elements i.e.,

$$tr(M) := \sum_i (M)_{ii}.$$

Obviously, the trace is a linear operator. It satisfies the following

Lemma 2.1.13 The trace is cyclic i.e., for any $M : \mathbb{C}^n \to \mathbb{C}^m$ and $N : \mathbb{C}^m \to \mathbb{C}^n$, we have

$$Tr(MN) = Tr(NM).$$

Proof: See [61].

□

In particular, the previous lemma says that for any M and any invertible P,

$$Tr(PMP^{-1}) = Tr(P^{-1}PM) = Tr(M).$$

From this, we see that the trace does not depend upon the choice of basis and we can speak of the trace of a linear operator $f \in L(\mathcal{H})$ *i.e.*, $tr(f) = tr([f]_B)$ for any B.

[**Partial trace**] Let $M : \mathbb{C}^n \otimes \mathbb{C}^m \to \mathbb{C}^n \otimes \mathbb{C}^m$, then

$$M = (M)_{kl,ij} \quad 1 \leq k, i \leq m, \quad 1 \leq l, j \leq n.$$

The *partial trace* of M over $\mathbb{C}^n$ is defined by

$$\left[Tr^{\mathbb{C}^n}(M)\right]_{k,i} = \sum_{j=1}^{n} (M)_{kj,ij}.$$

Again, the partial trace can be defined without references to the basis, *i.e.*, as the unique linear operator

$$Tr^{\mathcal{H}'} : L(\mathcal{H} \otimes \mathcal{H}') \to L(\mathcal{H})$$

such that for all $f \in L(\mathcal{H})$ and $g \in \mathcal{H}'$,

$$Tr^{\mathcal{H}'}(f \otimes g) = Tr(g) \cdot f.$$

Now, for any $m \times n$ matrix M, we have

$$Tr(M^\dagger M) = \sum_{ij} ||M_{ij}||^2 \geq 0 \quad \text{and} \quad Tr(M^\dagger M) = 0 \ \text{ implies } \ M = 0.$$

The assignment

$$Tr : \mathbb{C}^{m \times n} \times \mathbb{C}^{m \times n} \to \mathbb{C} :: (A, B) \mapsto Tr(A^\dagger B)$$

yields an inner product on the space of complex $m \times n$ matrices. More generally, as the trace can be defined without any reference to the basis, it follows that $L(\mathcal{H}, \mathcal{H}')$ is also a Hilbert space when equipped with the trace as inner product.

The following notions will be needed to define the most general type of operation one can apply on quantum states.

[Trace preserving operator] An operator $F : L(\mathcal{H}) \rightarrow L(\mathcal{H}')$ is *trace-preserving* if for any $f \in L(\mathcal{H})$, $Tr(f) = Tr(F(f))$.

[Completely positive operator] An operator $F : L(\mathcal{H}) \rightarrow L(\mathcal{H}')$ is *completely positive* if

i. For any $f \in L(\mathcal{H})$ s.t. $f \geq 0$, $F(f) \geq 0$.

ii. For any $\mathcal{H}'$ and any $f \in L(\mathcal{H} \otimes \mathcal{H}')$ s.t. $f \geq 0$, $(F \otimes 1_{L(\mathcal{H}')})(f) \geq 0$.

2.2 Quantum computing

We now bring in the notion of quantum computation, that is, computing using quantum mechanical phenomena such as superposition and entanglement. As we mentioned in the introduction of this chapter, the intent is not to give a complete introduction. Most of the definitions and results presented below are covered in [55] and [63] where the reader is referred for a more detailed introduction to the subject.

2.2.1 States, state spaces and transformations

In this subsection, we will introduce the concepts needed to describe pure states—a state which can't be described as a statistical mixture of other states—evolving in closed quantum systems—systems which are decoupled from the environment. It is only in the third subsection that we will introduce mixed states—statistical mixtures of states—and superoperators which are needed to describe evolution in open quantum systems—quantum systems that interact with a larger environment.

Heuristically, one can think of a classical computer as a device that operates on states built from a finite number of bits, *i.e.*, the *state* of a classical computer is an element of $\mathbb{B}^n := \{0, 1\}^n$. Such a set is finite and has cardinality 2^n. In contrast, a quantum computer works with a set of

[Qubits] A *qubit* is a vector $|\psi\rangle \in \mathbb{C}^2$ (which is Dirac notation for a vector and $|\psi\rangle$ reads "ket-ψ") *i.e.*,

$$|\psi\rangle = \sum_{i \in \mathbb{B}} \alpha_i |i\rangle; \quad \sum_{i \in \mathbb{B}} |\alpha_x|^2 = 1.$$

where $\{|0\rangle, |1\rangle\}$ is an orthonormal basis called the *computational basis* of the *state space* $\mathbb{C}^2$. Moreover the coefficients α_i are called *amplitudes*.

Thus, in contrast to classical bits, qubits admit an infinite number of states. Of notable importance are the states $|0\rangle$ and $|1\rangle$ *i.e.*, the elements of the computational basis. Indeed, as we shall see later, if we measure (or observe) a qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ in the computational basis, then we will obtain $|i\rangle$ with probability $|\alpha_i|^2$. Note that this entails that two states differing by any complex phase $e^{i\theta}$ are indistinguishable, thus are physically the same.

We say that a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and different from $\alpha|0\rangle$ and $\beta|1\rangle$ is in a *superposition* of the states $|0\rangle$ and $|1\rangle$.

As we have seen, the computational basis on $\mathbb{C}^2$ induces an inner product given by the dot product. Indeed, given a $|\psi\rangle \in \mathbb{C}^2$ its adjoint $\langle\psi| := (|\psi\rangle)^\dagger$ (read "bra-ψ") is the Hermitian transpose of $|\psi\rangle$. The inner product of $|\psi\rangle$ and $|\phi\rangle$ is then written as

$$\langle\phi|\psi\rangle := \langle\phi||\psi\rangle,$$

the "braket" of ϕ and ψ. In particular, the states of a qubit are those $|\psi\rangle \in \mathbb{C}^2$ which have norm 1 under this inner product.

Another major difference between classical and quantum computers is the set of transformations they can apply on their states. While a classical computer operates on states via functions, the transformations on the state of a quantum computer are given by unitary transformations. As such, a transformation that preserves the norm of a vector: it maps quantum states on quantum states.

Example 2.2.1 The *Pauli matrices*

$$\sigma_I := \begin{pmatrix}1&0\\0&1\end{pmatrix} \quad , \quad \sigma_X := \begin{pmatrix}0&1\\1&0\end{pmatrix} \quad , \quad \sigma_Y := \begin{pmatrix}0&-i\\i&0\end{pmatrix} \quad \text{and} \quad \sigma_Z := \begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

are all unitary transformations. The **CNOT** gate

$$\mathbf{CNOT} := \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

is a unitary transformation.

A compound system of n qubits is a normalised vector of $\mathbb{C}^{2^n}$ which is usually represented as the n-fold tensor product of $\mathbb{C}^2$ *i.e.*,

$$\mathbb{C}^{2^n} \simeq (\mathbb{C}^2)^{\otimes n} := \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 \quad n \text{ times}.$$

On such a space, the computational basis becomes $\{|i\rangle \mid i \in \mathbb{B}^n\}$. Interestingly, it is not true that every compound system of n qubits can be written as an n-fold tensor product of qubits. Indeed, consider the *Bell state*:

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathbb{C}^2 \otimes \mathbb{C}^2,$$

then there exist no $|\phi\rangle$ and $|\phi'\rangle$ such that $|\psi\rangle = |\phi\rangle \otimes |\phi'\rangle$. A state having this property is said to be *entangled*. More generally,

[Entangled state] A quantum state $|\psi\rangle$ is *entangled* if it can't be written as a tensor product of states of its components system.

The notion of quantum entanglement is crucial in quantum computing. It implies strong correlations between qubits (we will clarify this when we speak of quantum measurements). In particular, it enables quantum teleportation [13], super-dense coding [14], quantum pseudotelepathy games [15], BBM92 [12], etc. Depending on the number of subsystems, one may speak of *bipartite*, *tripartite* or even *n-partite* entanglement.

Example 2.2.2 The *Bell basis* is a basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ consisting of four entangled states

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\Phi^-\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\Psi^+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$\text{and } |\Psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Note that each of these states is equal (up to a phase factor) to $(1 \otimes \sigma)|\Psi^-\rangle$ where σ is some Pauli matrix.

2.2.2 Quantum measurements

At the end of a computation, one must measure the state of the system; contrary to what happens in the deterministic case, a quantum state undergoes a change when measured and the state of the system immediately after the measurement is determined by the observed value. A first example of an observable is provided by projector-valued spectra which we now introduce. In chapter 7, we will consider a generalisation of quantum measurements called Positive Operator Valued Measurement (POVM) which are described by non-negative self-adjoint operators.

[Projector] A *projector* P is a self-adjoint idempotent operator.

In particular, the operators $|i\rangle\langle i|$—the composition of the adjoint of $|i\rangle$ and $|i\rangle$ itself—are projectors and are seen to be self-adjoint and idempotent. Every projector defines an orthogonal projection to some subspace. For instance, consider the projector $P := |00\rangle\langle 00| + |01\rangle\langle 01|$, it projects orthogonally every vector in $\mathbb{C}^2 \otimes \mathbb{C}^2$ to the subspace spanned by the vectors $|00\rangle$ and $|01\rangle$.

Suppose that the state of n qubits is given by

$$|\psi\rangle = \sum_i \alpha_i |i\rangle.$$

When a measurement occurs, the probability of finding the system in the state $|i\rangle$ is given by the square of the absolute value of the amplitude α_i. Now, any state $|\psi\rangle \in \mathbb{C}^n$ can be written as

$$|\psi\rangle = 1_{\mathbb{C}^n}|\psi\rangle = \left(\sum_i |i\rangle\langle i|\right)|\psi\rangle = \sum_i \langle i|\psi\rangle|i\rangle.$$

Setting $\alpha_i := \langle i|\psi\rangle$, we have written the state $|\psi\rangle$ in the basis $\{|i\rangle\}_i$.

[Projector-valued spectrum] A *projector-valued spectrum* is a set $\{P_i\}$ consisting of self-adjoint and mutually orthogonal operators that form a partition of the identity. That is

- For all i, $P_i^\dagger = P_i$,
- For all i and j, $P_iP_j = \delta_{ij}P_i$ where δ_{ij} is the Kronecker delta *i.e.*, $\delta_{ij} = 1$ when $i = j$ and is equal to 0 otherwise, and
- $\sum_i P_i = 1$.

As a particular case, the set $\{P_i \mid P_i := |i\rangle\langle i|\}_i$ is a projector-valued spectrum. In fact, it is easy to see that *any* orthonormal basis $\{|\psi_i\rangle\}_i$ gives rise to a projector-valued spectrum $\{|\psi_i\rangle\langle\psi_i|\}_i$.

Example 2.2.3 As we mentioned above, quantum entanglement can be thought of as correlations between quantum states. Indeed, suppose we measure the leftmost qubit in the Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

using a projector-valued spectrum in the standard basis, *i.e.*, the projectors are respectively $P_0 := |0\rangle\langle 0|$ and $P_1 := |1\rangle\langle 1|$. Then, as the second qubit is unaffected by the measurement, we may measure 0 with probability

$$\frac{1}{2}\langle 00|(P_0 \otimes I)(P_0 \otimes I)|00\rangle = \frac{1}{2}$$

and 1 with the same probability. However, the following interesting phenomenon occurs: if we measure 0, then the state after the measurement is $|00\rangle$; otherwise it is $|11\rangle$. Thus, both qubits are now in the same state and this, despite the fact that we did not measure the second qubit.

2.2.3 Mixed states and superoperator

So far, we spoke of the evolution of closed quantum systems, it might occur that a quantum system leaks information to the environment in an irreversible manner. An extreme case of this is called *quantum decoherence* where the system undergoes an irreversible degradation so that it becomes some basis state with a given classical probability—this in contrast with the probability given by the amplitudes of a quantum state that we could refer to as "quantum". Therefore, it makes sense to define a generalisation of the notion of state described by a probabilistic mixture of quantum states.

[Ensemble of pure states] An *ensemble of pure states* is a set $\{(p_i, |\psi_i\rangle)\}_i$ where $\{p_i\}$ is a set of probabilities with $\sum_i p_i = 1$ and for all i, $|\psi_i\rangle$ is a state vector.

From this, it is possible to give an operator describing such an ensemble. Indeed,

[Density operator] Given an ensemble of pure states $\{p_i, |\psi_i\rangle\}$, the *density operator* (or *density matrix*) ρ associated to $\{p_i, |\psi_i\rangle\}$ is

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

We can interpret a density operator as a probabilistic mixture of the states $|\psi_i\rangle$. In that sense, a state described by a density operator is called a *mixed state* and a density operator of rank 1, *i.e.*, that can be written as $|\psi\rangle\langle\psi|$ for some state $|\psi\rangle$, is called a *pure state.*

Proposition 2.2.4 Density operators are positive self-adjoint operators of unit trace.

Proof: See [63].

□

A unitary transformation still gives the evolution of a system described by a density operator; it acts on a density operator $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ as

$$\sum_i p_i |\psi_i\rangle\langle\psi_i| \quad \overset{U}{\mapsto} \quad \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger.$$

If ρ describes a system where we have $|\psi_j\rangle$ with probability p_j, then after applying U, the system is in the state $U|\psi_j\rangle$ with probability p_j.

For measurements, a projector valued spectrum $\mathcal{P} = \{P_i\}$ acts on a density operator ρ as

$$\rho \quad \overset{\mathcal{P}}{\mapsto} \quad \sum_i P_i \rho P_i^\dagger = \sum_i P_i \rho P_i.$$

Now, unitary transformations and measurements are but two instances of a more general kind of transformation that one can apply on a mixed state. These transformations, known as superoperators, consist of all the physically realisable operations one can apply on a mixed state. Formally,

[Superoperator] A *superoperator* is a linear map $F : L(\mathcal{H}) \to L(\mathcal{H}')$ which satisfies the following two equivalent conditions:

1. F is a trace-preserving completely positive map,
2. there exists a set of matrices $\{F_i : \mathcal{H} \to \mathcal{H}'\}_i$—the *Kraus operators*—such that $\sum_i F_i^\dagger F_i = 1_\mathcal{H}$ and
$$F(\rho) := \sum_i F_i \rho F_i^\dagger$$
for all $\rho : \mathcal{H} \to \mathcal{H}$.

The partial trace is another instance of a superoperator [66]. Suppose that a mixed state is described by a density operator on $\mathcal{H} \otimes \mathcal{H}'$, then the restriction of ρ on the subsystem $\mathcal{H}$ is given by

$$\rho^\mathcal{H} = tr_{\mathcal{H}'}\rho.$$

Another instance of a superoperator that we shall see in the forthcoming chapters is quantum decoherence [78]. As mentioned above, such a phenomenon describes the irreversible transformation of a quantum state into a state in the basis of the decoherence caused by the interaction of the quantum state with the environment. Such a process can be thought of as a measurement where the observer forgets about the outcome. Formally, decoherence acts on a density operator as follows:

$$\rho = \sum_{i,j} \alpha_{i,j} |i\rangle\langle j| \mapsto \sum_i \alpha_{ii} |i\rangle\langle i|.$$

Such an action is described by the following sequence of operations:

1. First, we assign an ancilla to ρ. This ancilla is thought of as the state of the environment.
$$\rho \mapsto \rho \otimes |0\rangle\langle 0|.$$
2. We apply a **CNOT** to couple ρ with the environment. This is
$$\rho \otimes |0\rangle\langle 0| \mapsto \sum_{i,j} \alpha_{i,j} |ii\rangle\langle jj|.$$
3. Finally, we trace out the environment, as it is essentially inaccessible in terms of measurements. This gives
$$\sum_k \alpha_{kk} |k\rangle\langle k|.$$

Remark 2.2.5 The operation that we use to couple the density operator with the environment is not a cloning operation. It duplicates only the basis vector. In other words, it can be thought of as an isometry of the form

$$\sum_i |ii\rangle\langle i|.$$

[Completely mixed state] The *completely mixed state* on $\mathbb{C}^n$ is the density operator $\perp_n := n^{-1} \sum_i |i\rangle\langle i|$.

Remark 2.2.6 The completely mixed state is diagonal in all bases, *i.e.*, for any unitary transformation U, $U(\perp)U^\dagger = \perp$ hence, it makes sense to speak of the completely mixed state of $L(\mathcal{H})$ even if $\mathcal{H}$ is not equipped with a basis.

[Maximally entangled state] A state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ is *maximally entangled* if

$$(1_\mathcal{H} \otimes tr_\mathcal{H})(|\psi\rangle\langle\psi|) = \perp_\mathcal{H}.$$

Indeed, such a definition makes sense; as entanglement stands for strong correlations between qubits and tracing out a qubit is essentially the same as discarding it, we can infer that given two maximally entangled qubits, if we trace one of the two, the outcomes on the remaining qubit are all equally likely. Thus, we obtain the completely mixed state. Such a fact is easily seen to generalise to qupits *i.e.*, p-level quantum states.

3 Category theory

In this chapter, we introduce the basic notions of category theory: the notions of category, functors and natural transformations. This introduction is fairly concise; for a more complete introduction, the reader is referred to [58], the standard reference, or to [35] which the author wrote with B. Coecke which is intended for physicists.

The definition of a category is quite simple but requires a different standpoint from the one we may be used to: Indeed, most mathematical concepts are usually defined as a structure on some set; for instance:

- A *group* is a set G closed under an associative binary operation

  $$\cdot : G \times G \to G$$

  possessing a two-sided identity element for $\cdot$ and where each element is invertible with respect to $\cdot$.

- A *vector space V over a field* $\mathbb{K}$ is a set equipped with two binary operations, addition and scalar multiplication, and whose elements satisfy the usual axioms.

However, in category theory, the definitions are centred around the notion of transformation of structures usually called *morphisms* or *arrows*. For instance, paralleling the two examples above, the main defining ingredient of the categories of groups and the category of vector spaces would respectively be

- Homomorphisms between groups.

- Linear transformations between vector spaces.

From the notion of transformation of structure, it is natural to take an operational standpoint from which it is quite simple to understand the essence of a category.

3.1 Categories

First, to describe a category $\mathbf{C}$, we need the notion of structure, or operationally speaking, systems to transform; let us label the collection of such systems by $|\mathbf{C}|$ and individual systems therein by $A, B, C, ...$ which are called *objects.*
Next, we need the notion of transformation between objects. Let us denote a transformation f *from* the object A *to* the object B by $f : A \to B$. Further, one can apply sequentially the

transformations $f : A \to B$ and $g : B \to C$ yielding the composite transformation $g \circ f : A \to B \to C$. Also, in each of our two motivating examples, for any object A there is a trivial transformation, the *identity on A* denoted as

$$1_A : A \to A.$$

It acts as an identity on arrows *i.e.*, for $f : A \to B$ and $g : C \to A$, we have

$$f = f \circ 1_A : A \to B \quad \text{and} \quad g = 1_A \circ g : C \to A.$$

We have just introduced the notion of *composition* via sequentiality and, more subtly, the notion of *types*. Indeed, the objects can be used as types for the arrows thus, for instance, an arrow $f : A \to B$ has type $A \to B$. Types prevent silly mistakes: for instance, consider the arrow $g' : C \to D$, in this case, the composition $g' \circ f$ makes no sense because it means that one is trying to apply the transformation g' with inpu—*domain*—C on the output—*codomain*—of the transformation f which is B. These two systems might be of very different nature as the types mismatch; hence, this composition is not valid. Thus, we require that composition makes sense, meaning that $g \circ f$ holds whenever the codomain of f is the same as the domain of g. Thus, a morphism f is really a triple consisting of f its domain and its codomain.

Also, in a category, we require the composition to be associative: This means that if $f : A \to B$, $g : B \to C$ and $h : C \to D$, then

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Now, while outlining some expected properties of transformations, we have stated informally the definition of a category. In formal terms:

[Category] A *category* **C** consists of

1. A class $|\mathbf{C}|$ of *objects*.
2. For any $A, B \in |\mathbf{C}|$, a set $\mathbf{C}(A, B)$ of *morphisms from A to B*.
3. For any $A, B, C \in |\mathbf{C}|$ a *composition law*.

$$\circ : \mathbf{C}(A,B) \times \mathbf{C}(B,C) \to \mathbf{C}(A,C); (f,g) \mapsto g \circ f$$

satisfying:

i. *Identity for the composition:* For any $A \in |\mathbf{C}|$, there exists a morphism $1_A \in \mathbf{C}(A, A)$ called the *identity morphism for A* such that for every $f : A \to B$ and $g : C \to A$,

$$f = f \circ 1_A : A \to B \quad \text{and} \quad g = 1_A \circ g : C \to A.$$

ii. *Associativity of the composition:* For any $f \in \mathbf{C}(A, B)$, $g \in \mathbf{C}(B, C)$ and $h \in \mathbf{C}(B, C)$,

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Let us now give a few concrete examples of the rather abstract previous definition:

Example 3.1.1 The category **Set** of sets and functions, has

1. For objects, the members of the class $|\mathbf{Set}|$ of all sets,
2. Functions as morphisms and
3. The composition law is given by the composition of functions and satisfies all the defining axioms of a category:

   i. For any set X, there is an identity function $1_X : X \to X$.

   ii. The composition of function is associative.

Thus, **Set** is a category.

Example 3.1.2 The category **FdVect** of *finite dimensional vector spaces over* $\mathbb{C}$, has

1. For objects, the members of the class $|\mathbf{FdVect}|$ of all complex vectors spaces,
2. For morphisms all linear maps between such vector spaces,
3. The composition is just the regular composition of linear maps. Again, we just need to check that all conditions of definition of a category are satisfied. Indeed, the composition of two linear maps is again linear. Moreover,

   i. There is an identity map 1_V for any complex vector space $V \in |\mathbf{FdVect}|$ satisfying the obvious properties.

   ii. The composition of linear maps is—of course—associative.

Since all requirements of definition of a category are satisfied, **FdVect** is, indeed, a category.

Example 3.1.3 The category **Grp** of groups and group homomorphisms, with:

1. $|\mathbf{Grp}|$ as the class of all groups,
2. Group homomorphisms between them as morphisms and
3. The composition is given as the regular composition of group homomorphism with identities given by the identity homomorphisms. The defining axioms of a category are evidently satisfied.

Example 3.1.4 A single group $\langle G, \cdot, 1\rangle$ can also be seen as a category $\mathbf{G}$. Indeed, it suffices to consider a category with a single object denoted $*$ and each $g \in G$ becomes a morphism $g : * \to *$ in $\mathbf{G}$. The group operation $\cdot : G \times G \to G$ becomes the composition $\circ : \mathbf{G} \times \mathbf{G} \to \mathbf{G}$. By definition, G has a two-sided identity 1 for the operation $\cdot$ which becomes the identity morphism $1_* : * \to *$ in $\mathbf{G}$ and the group operation is associative, thus making the composition in $\mathbf{G}$ associative. It follows that $\mathbf{G}$ is indeed a category.

Example 3.1.5 The category **Hilb** of Hilbert spaces:

1. Its objects are the members of the class $|\mathbf{Hilb}|$ of all Hilbert spaces,

2. Bounded linear maps between them as morphisms and

3. The identity is a bounded linear map and the composition is just the regular composition of linear maps. The defining axiom of a category are again obviously satisfied.

Example 3.1.6 The category $\mathbf{Mat}_{\mathbb{R}}$ with natural numbers as objects and matrices with real values as morphisms. A morphism of type $n \longrightarrow m$ therein is simply an $m \times n$ real matrix. The identity for n is given by the $n \times n$ identity matrix and composition by matrix multiplication.

We now introduce our second[1] main example, the category **Rel** of sets and relations. As we assume that the reader is already acquainted with finite dimensional Hilbert spaces, we will use this category to introduce most notions with detailed calculations.

Recall that a *relation* $R : X \longrightarrow Y$ between the sets X and Y is a subset of the set of all their pairs *i.e.*, $R \subseteq X \times Y$. Given element (x, y) of that subset, we say that $x \in X$ is *related* to $y \in Y$ and we denote this as xRy. Typically, we will denote a relation R by its graph:

$$R := \{(x, y) \mid xRy\}.$$

Example 3.1.7 The category **Rel** of sets and relations with:

1. Objects, the members of the class $|\mathbf{Rel}|$ of sets,

2. As morphisms relations between sets and

3. Given two relations $R_1 : X \longrightarrow Y$ and $R_2 : Y \longrightarrow Z$, their composite $R_2 \circ R_1 \subseteq X \times Z$ is defined as

$$R_2 \circ R_1 := \{(x, z) \mid \text{there exists a } y \in Y \text{ such that } xR_1y \text{ and } yR_2z]\}.$$

Moreover

i. For any set $X \in |\mathbf{Rel}|$, we have an identity relation

$$1_X := \{(x, x) \mid x \in X\}.$$

ii. This composition is manifestly associative.

We can already define some morphisms having special properties. For instance, we can define the notion of *isomorphism*:

[Isomorphism] Given a category $\mathbf{C}$. Two objects $A, B \in |\mathbf{C}|$ are *isomorphic* if there exists morphisms $f \in \mathbf{C}(A, B)$ and $g \in \mathbf{C}(B, A)$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. The morphism f is then called an *isomorphism* and its inverse g is denoted as f^{-1}.

The singleton $\{*\} \in |\mathbf{Set}|$—unique up to isomorphism—has an interesting property; given a set $A \in |\mathbf{Set}|$, a function $f : A \longrightarrow \{*\}$ must map all the elements of A unto $*$, the unique element

[1] The first being the category **FdHilb** yet to be introduced!

of $\{*\}$. It follows that f is unique or, in other terms, $\mathbf{C}(A, \{*\})$ is a singleton for any set A. Generalising the concept to an arbitrary category, we have

[**Terminal object**] An object $\top \in |\mathbf{C}|$ is *terminal* in $\mathbf{C}$ if for any $A \in |\mathbf{C}|$, the set $\mathbf{C}(A, \top)$ is a singleton.

The notion of terminal object enables in its turn the notion of element. Before defining this, let us note that given a set $X \in |\mathbf{Set}|$ and some fixed element $x \in X$, a function $x : \{*\} \to X$ maps the unique element of $\{*\}$ unto a unique element—say x—of X. Hence, if X contains n elements, there are n functions of type $\{*\} \to X$ each corresponding to the element to which $*$ is mapped. In more general terms, if a category $\mathbf{C}$ has a terminal object $\top$, then a map $\top \to A$ in $\mathbf{C}$ is called an *element* of A. However, one must be careful with this: an object in $\mathbf{C}$ is not necessarily determined by its elements.

We can also introduce the concept dual to the one of terminal object, *i.e.*, the notion of an *initial object*. Consider the empty set $\emptyset \in |\mathbf{Set}|$ then, for every set A there is a unique function $\emptyset \to A$ whose graph is $\emptyset = \emptyset \times A$, the *empty function*. Generalising, one gets the notion of

[**Initial object**] An object $\bot \in |\mathbf{C}|$ is *initial* in $\mathbf{C}$ if for any $A \in |\mathbf{C}|$, the set $\mathbf{C}(\bot, A)$ is a singleton.

3.2 Quotient category

Given an equivalence relation $\sim$ on a set X, we can define the set of all equivalence classes of X. The resulting set, usually denoted $X/\sim$ is then called the *quotient set of X by $\sim$*. For instance the set of integers modulo 2 consists of two equivalence classes: the sets of even numbers and of odd numbers. In category theory, a *quotient category* is obtained from a category by identifying morphisms through a congruence relation therein. Such a construction will be used only once in this dissertation so we will give a swift introduction to the concept.

First we need the notion of congruence relation. This is just an equivalence relation compatible with some structure; in our case, it needs to be compatible with the categorical structure.

[**Congruence relation**] Let $\mathbf{C}$ be a category. A *congruence relation* R on $\mathbf{C}$ consists of an equivalence relation $R_{A,B}$ on $\mathbf{C}(A, B)$ for any $A, B \in |\mathbf{C}|$ such that if

- $f, f' : A \to B$ are such that $f R_{A,B} f'$ and
- $g, g' : B \to C$ are such that $g R_{B,C} g'$,

then $g \circ f R_{A,C} g' \circ f'$.

Having a congruence relation, we may define

[**Quotient category**] Given a congruence relation R on $\mathbf{C}$, the *quotient category* $\mathbf{C}/R$ is the category with the same objects as $\mathbf{C}$ and whose morphisms are the equivalence classes of morphisms of $\mathbf{C}$ with respect to R *i.e.*, for any $A, B \in |\mathbf{C}|$,

$$\mathbf{C}/R(A, B) := \mathbf{C}(A, B)/R_{A,B}.$$

Example 3.2.1 We know that a group G can be seen as a category $\mathbf{G}$ with one object. If we are given a congruence relation R on G, then the congruence is determined by those elements congruent to the identity so that R a normal subgroup of G. Lifting the notion to categories, the morphisms of the quotient category of $\mathbf{G}/R$ are the equivalence classes of the morphisms which are the equivalence classes of G modulo R.

3.3 Functors

Clearly, a category is itself a mathematical structure. Hence, one may consider transformations between categories. These transformations, called *functors*, must preserve identities and composition which is nothing but the structure of a category.

We will introduce the notion of functors via the example of linear representation; it is, in fact, more than 'just' a functor, but it is good enough for our purposes. A *representation* of a group G on a vector space V—say, over $\mathbb{C}$—is a group homomorphism from G to $\mathrm{GL}(V)$, the general linear group on V i.e, the group of all automorphisms of V. That is a map

$$\rho : G \to \mathrm{GL}(V)$$

such that

$$\rho(g_1 \cdot g_2) = \rho(g_1) \circ \rho(g_2), \text{ for all } g_1, g_2 \in G.$$

The passage from this definition to a category theoretic one is quite smooth using examples 3.1.2 and 3.1.4. Indeed, consider G as the category $\mathbf{G}$ and the following morphism of categories (functor):

$$R_\rho : \mathbf{G} \to \mathbf{FdVect}.$$

In order to be consistent with group representations, R_ρ must

1. Select an object $V \in \mathbf{FdVect}$ and map $*$ on V thus defining a mapping

   $$R_\rho : |\mathbf{G}| \to |\mathbf{FdVect}|; * \mapsto V$$

   between the objects of the two categories.

2. It must also define a group homomorphism $G \to GL(V)$ which maps every morphism $g \in \mathbf{G}(*, *)$ to an invertible linear transformation of V that is, an automorphism of V^2. This yields a map

   $$R_\rho : \mathbf{G}(*, *) \to \mathbf{FdVect}(R_\rho(*), R_\rho(*)); g \mapsto \rho(g)$$

   between the morphisms of the two categories.

Note that since this mapping is a group homomorphism, it must preserve the composition: from group multiplication in $\mathbf{G}$ to composition of linear maps in $\mathbf{FdVect}$. It must also preserve the identities *i.e.*, $1_* \mapsto 1_V$. All in all, it preserves the categorical structure.

Having this example in mind, we infer that a functor must consist of two mappings, one on the objects and the other on the morphisms. Moreover, the latter mapping must preserve both the identities and the composition. We get:

[2] This is where R_ρ isn't 'just' a functor as we said above. Indeed, if it were just a functor, it would have to send the group elements to linear maps *i.e.*, not necessarily to invertible ones.

[Functor] Let $\mathbf{C}$ and $\mathbf{D}$ be categories, a *functor* $F : \mathbf{C} \to \mathbf{D}$ consists of

1. A mapping

$$|\mathbf{C}| \to |\mathbf{D}|; A \mapsto F(A)$$

2. For any $A, B \in |\mathbf{C}|$, a mapping

$$\mathbf{C}(A, B) \to \mathbf{D}(F(A), F(B)); f \mapsto F(f)$$

subject to

i. *Preservation of the composition:* For any $f \in \mathbf{C}(A, B)$ and $g \in \mathbf{C}(B, C)$,

$$F(g \circ f) = F(g) \circ F(f)$$

ii. *Preservation of identities:* For any $A \in |\mathbf{C}|$,

$$F(1_A) = 1_{F(A)}$$

Remark 3.3.1 To avoid cluttering the notation, we now drop the parentheses unless they are necessary. For instance, $F(A)$ and $F(f)$ will be denoted simply as FA and Ff.

Manifestly, the composition of functors is a functor; such a composition is associative and to each category, one can define an identity functor. Using this, we can define another category:

[Cat] The category **Cat** has for class of objects all (small[3]) categories and for morphisms, functors between them.

Functors enable us to define the notion of *isomorphism of categories* in an obvious sense *i.e.*, an isomorphism of categories is a functor $F : \mathbf{C} \to \mathbf{D}$ for which there is a functor $G : \mathbf{D} \to \mathbf{C}$ such that

$$G \circ F = 1_{\mathbf{C}} \quad \text{and} \quad F \circ G = 1_{\mathbf{D}}$$

where $1_{\mathbf{C}} : \mathbf{C} \to \mathbf{C}$ and $1_{\mathbf{D}} : \mathbf{D} \to \mathbf{D}$ are identity functors. In such a case, the functor G is a two-sided inverse for F and is denoted as F^{-1}. Equivalently, one could say that an isomorphism of categories is a functor $F : \mathbf{C} \to \mathbf{D}$ which is a bijection on both objects and morphisms. We may also define weaker notions. For instance the two following definitions describe functors whose morphism assignments are injective and surjective respectively.

[Faithful functor] A functor $F : \mathbf{C} \to \mathbf{D}$ is *faithful* if for any pair $A, B \in |\mathbf{C}|$ and any pair $f, f' : A \to B$, $Ff = Ff' : FA \to FB$ implies $f = f'$.

[Full functor] A functor $F : \mathbf{C} \to \mathbf{D}$ is *full* if for any pair $A, B \in |\mathbf{C}|$ and any $g : FA \to FB$, there exists an $f : A \to B$ such that $Ff = g$.

[Subcategory] A subcategory $\mathbf{D}$ of $\mathbf{C}$ is a collection of objects and morphisms of $\mathbf{C}$ such that

[3] There are cardinality issues here. Without going into the details, a *small category* $\mathbf{C}$ is a category where both $|\mathbf{C}|$ and the collection of arrows are sets. We prefer to avoid such issues here; for more details, the reader is referred to [58] pp. 22–24.

i. For every morphism $f : A \longrightarrow B$ in $\mathbf{D}$, both A and $B \in |\mathbf{D}|$,

ii. For every $A \in |\mathbf{D}|$, 1_A is in $\mathbf{D}$ and

iii. For every pair of composable morphisms f and g in $\mathbf{D}$, $g \circ f$ is in $\mathbf{D}$.

The conditions in the previous definition manifestly insure that $\mathbf{D}$ is itself a category. The inclusion functor $F : \mathbf{D} \longrightarrow \mathbf{C}$ defined by

- $A \mapsto FA = A$ and
- $f \mapsto Ff = f$

is faithful. If in addition F is full, then we say that $\mathbf{D}$ is a *full subcategory* of $\mathbf{C}$.

Before giving another example of functor, we need to introduce yet another concept which is, simply put, the process of reversing the arrows of a given category $\mathbf{C}$. We start by an example to illustrate the need of such a process:

Consider the operation of transposition in $\mathbf{Mat}_{\mathbb{R}}$:

1. It preserves the identities as they are equal to their transpose,
2. It reverses the arrow as if $M : m \longrightarrow n$, then M^T has type $n \longrightarrow m$ and
3. It preserves the composition "up to" reversal of the arrows as for any real matrix $M : m \longrightarrow n$ and $N : n \longrightarrow p$,
$$(N \circ M)^T = M^T \circ N^T : p \longrightarrow m.$$

In fact, this sort of behaviours define a special type of morphism of categories called *contravariant functors*, *i.e.*, functors preserving composition *up to* reversal of the arrows.

To formally define the notion of "reversal of arrows", we introduce the notion of

[Opposite category] Give a category $\mathbf{C}$, its *opposite category* $\mathbf{C}^{op}$ has:

1. The same objects as $\mathbf{C}$,
2. The morphisms $\mathbf{C}^{op}$ are in one-to-one correspondence with the morphisms $\mathbf{C}$. In details, given any $f \in \mathbf{C}(A, B)$, then we have a corresponding $f^{op} \in \mathbf{C}^{op}(B, A)$ which is called the *opposite morphism* to f in $\mathbf{C}$.
3. The composition in $\mathbf{C}^{op}$ is defined as the opposite composition defined in $\mathbf{C}$ that is, if $g \circ f$ is defined in $\mathbf{C}$ then:
$$(g \circ f)^{op} = f^{op} \circ g^{op}$$
is defined in $\mathbf{C}^{op}$ making it a category.

Of course, the operation $(-)^{op}$ is self-inverse—reversing the arrows twice is the same as doing nothing.

Remark 3.3.2 The process of reversing the arrows is sometimes indicated by the prefix "co" (*e.g.*: comonoid) indicating that the defining equations for those structures are the same as the defining equations for the original structure (*e.g.*: monoid) but with arrows reversed. The process of reversing arrows is called *categorical dualisation* [58].

Following this, we can define a contravariant functor as a functor that reverses the arrows and the order of the composition with respect to its domain category, thus formally defining the concept that we outlined for real matrices.

[Contravariant functor] A *contravariant functor* $F : \mathbf{C} \to \mathbf{D}$ associates

1. To each $A \in |\mathbf{C}|$ an object $FA \in |\mathbf{D}|$ and
2. To each $f \in \mathbf{C}(A, B)$ a morphism $Ff \in \mathbf{D}(FB, FA)$ such that
   i. $F(g \circ f) = Ff \circ Fg \in \mathbf{D}(FC, FA)$ for all $f \in \mathbf{C}(A, B)$ and $g \in \mathbf{C}(B, C)$ and
   ii. $F1_A = 1_{FA}$ for every $A \in |\mathbf{C}|$.

As opposed to contravariant functors, ordinary functors are often called *covariant functors*; in what follows, we will generally denote contravariant functors $\mathbf{C} \to \mathbf{D}$ as covariant functors of type

$$\mathbf{C}^{op} \to \mathbf{D}.$$

Example 3.3.3 Another example of contravariant functor is the identity-on-objects functor "dagger" that maps every bounded linear map on its adjoint. Indeed, it is a functor

$$\dagger : \mathbf{Hilb}^{op} \to \mathbf{Hilb}$$

which acts as:

1. An identity-on-objects that is

$$\dagger : |\mathbf{Hilb}|^{op} \to |\mathbf{Hilb}|; \mathcal{H} \mapsto \mathcal{H} \text{ for all } \mathcal{H} \in |\mathbf{Hilb}|^{op}$$

2. To each $f \in \mathbf{Hilb}(\mathcal{H}, \mathcal{H}')$ it associates its *adjoint* $\dagger(f) := f^\dagger \in \mathbf{Hilb}(\mathcal{H}', \mathcal{H})$. Such an assignment satisfies:
   i. $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$ for all $f \in \mathbf{Hilb}(\mathcal{H}, \mathcal{H}')$ and $g \in \mathbf{Hilb}(\mathcal{H}', \mathcal{H}'')$,
   ii. $1_{\mathcal{H}}^\dagger = 1_{\mathcal{H}}$ for every $\mathcal{H} \in |\mathbf{Hilb}|$.

3.4 Natural transformations

Before carrying on with natural transformations—and as it will be used extensively here and after—we introduce the important notion of *Commutative diagrams.* These diagrams constitute a convenient visual aid for equations and become powerful tools when they are used in a technique of proof called *diagram chasing* that we will use below. Given an equation, say

$$g \circ f = h \text{ with } f : A \to B,\ g : B \to C \text{ and } h : A \to C$$

the corresponding commutative diagram is

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \\
 & C
\end{tikzcd}$$

which says that if we compose the arrow f with the arrow g, it is equal to the arrow h; in fact, the *commutation* of the diagram is insured by the equality $g \circ f = h$ in that case. Formally,

[Commutative diagram] A *commutative diagram* is a diagram of objects and morphisms such that any directed path consisting of compositions of morphisms between any two chosen objects of the diagram are equal under composition.

Using this, we can now speak of transformation between functors. These transformations are called *natural transformations*. In order to introduce these, let us return to our motivating example for functors namely: group representations. Given vector spaces V and W, two representations

$$\rho_1 : G \longrightarrow \mathrm{GL}(V) \qquad \text{and} \qquad \rho_2 : G \longrightarrow \mathrm{GL}(W)$$

are *equivalent* if there exists an isomorphism $\tau : V \longrightarrow W$ so that for all $g \in G$, $\tau \circ \rho_1(g) = \rho_2(g) \circ \tau$. It turns out that this isomorphism is an example of a natural transformation. Taking the functorial point of view for the two representations above, we get two functors

$$R_{\rho_1} : \mathbf{G} \longrightarrow \mathbf{FdVect} \qquad \text{and} \qquad R_{\rho_2} : \mathbf{G} \longrightarrow \mathbf{FdVect}$$

where R_{ρ_1} applies $*$ on V and R_{ρ_2} applies $*$ on W and morphisms are transformed in the same manner as ρ_1 and ρ_2 dictates. The defining condition for the equivalence condition reduces to the commutation of the following diagram:

$$\begin{tikzcd}
R_{\rho_1}(*) \arrow[r, "\tau_*"] \arrow[d, "R_{\rho_1} g"'] & R_{\rho_2}(*) \arrow[d, "R_{\rho_2} g"] \\
R_{\rho_1}(*) \arrow[r, "\tau_*"'] & R_{\rho_2}(*)
\end{tikzcd}$$

It should be noted that although this natural transformation is also an isomorphism, this may not be the case in general. Also, note that the domain and the codomain—categories—of both functors coincide and that the natural transformation is a function $\tau : R_{\rho_1} \Rightarrow R_{\rho_2}$ *i.e.*, it maps one functor to the other while respecting the composition of morphisms; for this reason, natural transformations are sometimes called *morphisms of functors*. The formal definition is as follows:

[Natural transformation] Let $F, G : \mathbf{C} \longrightarrow \mathbf{D}$ be functors. A *natural transformation* $\tau : F \Rightarrow G$ associates to any $A \in \mathbf{C}$ a morphism

$$\tau_A : FA \longrightarrow GA \tag{3.1}$$

in $\mathbf{D}$, the *component of* τ *at* A, such that for any $f \in \mathbf{C}(A, B)$, the diagram

$$\begin{tikzcd} FA \arrow[r, "\tau_A"] \arrow[d, "Ff"'] & GA \arrow[d, "Gf"] \\ FB \arrow[r, "\tau_B"'] & GB \end{tikzcd} \tag{3.2}$$

commutes. Moreover, we say that a natural transformation τ is a *natural isomorphism* if its components are isomorphisms.

Example 3.4.1 For every $V \in \mathbf{FdVect}$ with V^* the dual of V, the map

$$\Phi : V \longrightarrow V^{**}$$

defined by $(\Phi(-))(\phi) = \phi(-)$ for all linear functional $\phi \in V^*$ is a natural isomorphism $\phi : 1 \Rightarrow (-)^{**}$ from the identity functor to the double dual functor. Importantly, note that this map does not depend on a choice of basis on V.

Example 3.4.2 Along the same line, a non-example: Every finite dimensional vector space is isomorphic to its dual; however, an isomorphism $\psi : V \longrightarrow V^*$ can't be natural: it relies on an (arbitrary) choice of basis which means that (3.2) will not be satisfied, in contrast to the natural transformation ϕ of the preceding example.

Remark 3.4.3 Although we have used double arrows to describe a natural transformation $\tau : F \Rightarrow G$, in what follows we may denote it only as $\tau : F \longrightarrow G$ if the context is clear.

4 †-Monoidal categories

The notions presented in the preceding chapter are not rich enough for our context. For instance, these are not sufficient to express the notion of compound system or the notion of adjoints. The bulk of this chapter is used to introduce monoidal categories together with the associated notions that we will use later in this dissertation. The plan is as follows:

First, we will define formally the product of categories in order to introduce the notion of monoidal categories; that is, a category that comes equipped with a bifunctor that provides a categorical notion of tensor product. Such a notion is the second most fundamental concept in our exposition after the notion of category. The notion of monoidal product is broad enough to axiomatise the tensor product of vector spaces, of modules and other notions of tensor products.

The notion of monoidal category is a fairly complicated one, in the sense that we have to take in account a few natural isomorphisms and coherence conditions. Fortunately, however, every monoidal category is equivalent to a strict monoidal category where these natural isomorphisms are identities. We will give the necessary definitions and state the results that provide us with this equivalence. This will enables us to work in "strict" monoidal categories in the following chapter, that is, a monoidal category where most of the coherence conditions hold trivially.

We will then introduce the notion of traced monoidal categories, this is, a monoidal category that comes with a family of functions acting on the homsets that provide a generalisation of the standard trace in linear algebra.

Next, we will introduce two internal structures that might exist in a monoidal category *i.e.*, the notion of internal monoid and the notion of internal comonoid. These two structures will be used extensively when we will define the notion of basis objects in chapter 6.

The sixth section of this chapter discusses the monoid of scalars in a monoidal category and its properties; the notion of scalar is essential in our context as it provides us with a quantitative aspect to our theory. For instance, as we shall see later, the structural witnesses of the quantum structure aren't normalised even in **FdHilb**. Therefore, when we will expose protocols, scalars will enable us to normalise states in the same way as in conventional quantum computation.

Then, we will introduce the notion of †-monoidal categories. The dagger structure is an involutive, identity-on-objects contravariant functor that coherently preserves the monoidal structure. The operation that associates to each bounded linear map $f \in$ **Hilb** its adjoint $f^\dagger$ is an instance of dagger structure turning **Hilb** into a †-monoidal category.

Moreover, we will introduce the graphical calculus we spoke of in the introduction. First, we will introduce the graphical calculus for monoidal category, then, at the end of the chapter, we will enrich it with the suitable notions to accommodate †-monoidal categories.

Again, for the first half of the chapter, we follow the standard presentation. For more details, we refer the reader to [58] or [35].

4.1 Product of categories

Before we actually get to new structures within categories, we need to introduce one at the level of categories themselves.

[Product of categories] Let $\mathbf{C}$ and $\mathbf{D}$ be categories. The *product of $\mathbf{C}$ and $\mathbf{D}$* is the category $\mathbf{C} \times \mathbf{D}$ which consists of

- *Objects:* Ordered pairs (C, D) with $C \in |\mathbf{C}|$ and $D \in |\mathbf{D}|$
- *Morphisms:* Ordered pairs $(f, g) : (C, D) \rightarrow (C', D')$, with $f : C \rightarrow C'$ in $\mathbf{C}$ and $g : D \rightarrow D'$ in $\mathbf{D}$. Identities are given by $1_{(A,B)} := (1_A, 1_B)$ and the composition of morphisms is defined pointwise *i.e.*,

$$(f', g') \circ (f, g) := (f' \circ f, g' \circ g).$$

We will also encounter functors of type

$$F : \mathbf{C} \times \mathbf{D} \rightarrow \mathbf{E}.$$

Such functors are called *bifunctors i.e.*, functors in each of their arguments.

4.2 Monoidal categories

In this section, we introduce one of the most basic product structure that a category can have: the monoidal product. The categorical notion of product, coproduct and biproduct are particular instances of monoidal products with some extra structure (see [58] and [35]).

In order to introduce the notion of monoidal category, we will again start by working with an example: the tensor product of Hilbert spaces[4]. We will argue in broad terms that the assignments

$$(\mathcal{H}, \mathcal{H}') \mapsto \mathcal{H} \otimes \mathcal{H}' \qquad \text{and} \qquad (f, g) \mapsto f \otimes g$$

defines a bifunctor

$$\otimes : \mathbf{FdHilb} \times \mathbf{FdHilb} \rightarrow \mathbf{FdHilb}.$$

Consider the Hilbert spaces $\mathcal{H}_a$ and $\mathcal{H}_b$ associated to two quantum particles a and b and the Hilbert space $\mathcal{H}_a \otimes \mathcal{H}_b$ which describes the compound system of a and b. Suppose we apply some unitary transformation $U_a : \mathcal{H}_a \rightarrow \mathcal{H}_a$ on the particle a and the unitary transformation $U_b : \mathcal{H}_b \rightarrow \mathcal{H}_b$ on the particle b, then this is the same thing as applying the transformation

$$U_a \otimes U_b : \mathcal{H}_a \otimes \mathcal{H}_b \rightarrow \mathcal{H}_a \otimes \mathcal{H}_b$$

[4] Strictly speaking, we will only speak of the tensor product of vector spaces here but we make the abuse of language to stay within our context, the notion of pairing being introduced in the next chapter.

on the compound system of the two particles. Now, note that applying U_a first and then U_b second or *vice versa* is the same as applying $U_a \otimes U_b$ simultaneously; this yield the following well known identity:

$$U_a \otimes U_b = (1_{\mathcal{H}_a} \otimes U_b) \circ (U_a \otimes 1_{\mathcal{H}_b}) = (U_a \otimes 1_{\mathcal{H}_b}) \circ (1_{\mathcal{H}_a} \otimes U_b)$$

showing some "atemporal" features—or *bifunctoriality*—of the tensor product. Thus, the tensor product may be seen as some kind of "lateral" composition or, in other words, a way to compose systems and the operations on them.

There are other things to expect from the tensor product. In the category of finite dimensional complex Hilbert spaces, the tensor product also has an identity, namely, the complex field. Indeed, for any Hilbert space $\mathcal{H}$, the following holds:

$$\mathcal{H} \simeq \mathcal{H} \otimes \mathbb{C} \simeq \mathbb{C} \otimes \mathcal{H}.$$

which states that $\mathbb{C}$ acts both as a left and a right unit for the tensor product of objects. In other words, for every $\mathcal{H}$, there is a pair of natural isomorphisms

$$\lambda_{\mathcal{H}} : \mathbb{C} \otimes \mathcal{H} \xrightarrow{\sim} \mathcal{H} \qquad \text{and} \qquad \rho_{\mathcal{H}} : \mathcal{H} \otimes \mathbb{C} \xrightarrow{\sim} \mathcal{H}.$$

Second, the tensor product has to be associative or else we would run into some serious problems. Categorically, this means that for each triple of objects $\mathcal{H}_1, \mathcal{H}_2$ and $\mathcal{H}_3$ there is a natural isomorphism

$$\alpha_{1,2;3} : (\mathcal{H}_1 \otimes \mathcal{H}_2) \otimes \mathcal{H}_3 \xrightarrow{\sim} \mathcal{H}_1 \otimes (\mathcal{H}_2 \otimes \mathcal{H}_3).$$

Finally, still in the category of finite dimensional Hilbert spaces, the tensor product is symmetric, which means that for any pair of objects $\mathcal{H}_1$ and $\mathcal{H}_2$, we have yet another natural isomorphism

$$\sigma_{1,2} : \mathcal{H}_1 \otimes \mathcal{H}_2 \xrightarrow{\sim} \mathcal{H}_2 \otimes \mathcal{H}_1.$$

Before giving a precise definition of a *monoidal category*, let us recall the set-theoretical notion of *monoid*: it is a set M equipped with an associative binary operation $\cdot : M \times M \to M$ and an identity e for that operation. For instance, given an alphabet $A = \{a, b, c, ...\}$, define $M = A^*$ as the set of all finite words on A, then M together with the concatenation for operation and the empty string ϵ acting as an identity is a monoid.

Lifting the notion to the level of category, a *monoidal category* is, broadly speaking, a monoid at the level of the objects and a sort of "typed" generalisation of a monoid at the level of morphisms. Formally,

[Monoidal category] A *monoidal category* $\langle \mathbf{C}, \otimes, I, \alpha, \lambda, \rho \rangle$ consists of

1. A category $\mathbf{C}$,
2. A bifunctor $\otimes : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$,
3. An object $I \in |\mathbf{C}|$ and
4. Three natural isomorphisms:

   i. Associativity isomorphism:

$$\alpha_{A,B;C} : A \otimes (B \otimes C) \xrightarrow{\sim} (A \otimes B) \otimes C$$

natural for all A, B and $C \in |\mathbf{C}|$, and such that the pentagon

$$\begin{tikzcd}
A \otimes (B \otimes (C \otimes D)) \arrow[r, "\alpha"] \arrow[d, "1\otimes\alpha"'] & (A \otimes B) \otimes (C \otimes D) \arrow[r, "\alpha"] & ((A \otimes B) \otimes C) \otimes D \\
A \otimes ((B \otimes C) \otimes D) \arrow[rr, "\alpha"'] & & (A \otimes (B \otimes C)) \otimes D \arrow[u, "\alpha\otimes 1"']
\end{tikzcd}$$

commutes for all A, B, C and $D \in |\mathbf{C}|$.

ii. Left unit:

$$\lambda : I \otimes A \xrightarrow{\sim} A$$

iii. Right unit:

$$\rho : A \otimes I \xrightarrow{\sim} A$$

both natural for all $A \in |\mathbf{C}|$ and such that the triangle

$$\begin{tikzcd}
A \otimes (I \otimes B) \arrow[r, "\alpha"] \arrow[dr, "1\otimes\lambda"'] & (A \otimes I) \otimes B \arrow[d, "\rho\otimes 1"] \\
& A \otimes B
\end{tikzcd}$$

commutes for all A and $B \in |\mathbf{C}|$.

iv. $\lambda_I = \rho_I : I \otimes I \to I$

Moreover, $\mathbf{C}$ is *symmetric* monoidal if for any pair of object $A, B \in |\mathbf{C}|$, there is a natural isomorphism

$$\sigma_{A,B} : A \otimes B \xrightarrow{\sim} B \otimes A$$

such that for all $A, B, C \in |\mathbf{C}|$,

$$\begin{tikzcd}
A \otimes B \arrow[r, "\sigma_{A,B}"] \arrow[dr, equal] & B \otimes A \arrow[d, "\sigma_{B,A}"] \\
& A \otimes B
\end{tikzcd} \quad , \quad \begin{tikzcd}
A \otimes I \arrow[r, "\sigma_{A,I}"] \arrow[dr, "\rho"'] & I \otimes A \arrow[d, "\lambda"] \\
& A
\end{tikzcd}$$

and

$$\begin{tikzcd}
A \otimes (B \otimes C) \arrow[r, "\alpha"] \arrow[d, "1_A\otimes\sigma_{B,C}"'] & (A \otimes B) \otimes C \arrow[r, "\sigma_{(A\otimes B),C}"] & C \otimes (A \otimes B) \arrow[d, "\alpha"] \\
A \otimes (C \otimes B) \arrow[r, "\alpha"'] & (A \otimes C) \otimes B \arrow[r, "\sigma_{A,B}\otimes 1_C"'] & (C \otimes A) \otimes B
\end{tikzcd}$$

commute.

Remark 4.2.1 Note that the defining diagrams of the previous definition spells out how the various natural isomorphisms relate coherently one with respect to the other.

[Strict monoidal category] A monoidal category $\langle \mathbf{C}, \otimes, I, \alpha, \lambda, \rho \rangle$ is *strict* if the natural isomorphisms α, λ and ρ are identities.

We shall see in the next section that every monoidal category is monoidally equivalent to a strict monoidal category *i.e.*, for all practical purposes, they are essentially the same.

Example 4.2.2 The category **FdVect** is symmetric monoidal. Indeed, the natural isomorphisms are:

- *Associativity:*

$$\alpha_{V_1,V_2;V_3} : (V_1 \otimes V_2) \otimes V_3 \xrightarrow{\sim} V_1 \otimes (V_2 \otimes V_3); (v' \otimes v'') \otimes v''' \mapsto v' \otimes (v'' \otimes v'''),$$

- *Left unit:*

$$\lambda_V : \mathbb{C} \otimes V \xrightarrow{\sim} V; z \otimes v \mapsto zv$$

and it's inverse is given by

$$\lambda_V^{-1} : V \xrightarrow{\sim} \mathbb{C} \otimes V; v \mapsto 1 \otimes v$$

- *Right unit:* is defined analogously to the left unit.

- *Symmetry:*

$$\sigma_{V_1,V_2} : V_1 \otimes V_2 \xrightarrow{\sim} V_2 \otimes V_1; v' \otimes v'' \mapsto v'' \otimes v'$$

The fact that they meet the requirement is obvious from the definitions.

The category **FdVect** is also a symmetric monoidal category with the direct sum as monoidal product and the 0 vector space as monoidal unit. For a detailed description of this fact see [35].

We can single out vectors in **FdVect**: consider a vector space $V \in |\mathbf{FdVect}|$ and a morphism

$$\psi : \mathbb{C} \to V. \tag{4.1}$$

This morphism ψ is a linear map with a precise image at 1, say $\psi(1) = v$. It turns out that this is the *unique* morphism that has this image; the reader can easily prove that there can't be two such morphisms using linearity. Hence, there is a bijection between the vectors of V and the linear maps of type $\mathbb{C} \to V$ and again, we can define concepts with the use of morphism without using elements themselves.

Remark 4.2.3 Even if we can single out elements with the tensor unit $\mathbb{C} \in |\mathbf{FdVect}|$, it is *not* a terminal object in that category and that in contrast with what we did in **Set** to single out elements.

Example 4.2.4 The category **Set** is a symmetric monoidal category with both the Cartesian product and $\{*\}$ as unit and the disjoint union with $\emptyset$ as unit. For a detailed description of these particular monoidal products, see [35].

The following example—and most examples concerning **Rel** that we will give—are taken from [35] that the author wrote with B. Coecke. These result aren't new but where part of the folklore so we felt that it was necessary to expose them.

Example 4.2.5 The category **Rel** has a monoidal product given by ×. Indeed, consider the relations

$$R_1 : X_1 \longrightarrow Y_1 \qquad \text{and} \qquad R_2 : X_2 \longrightarrow Y_2,$$

then,

$$R_1 \times R_2 := \{((x, x'), (y, y')) \mid xR_1x' \text{ and } yR_2y'\}$$

is a relation of type $X_1 \times X_2 \to Y_1 \times Y_2$.

Unit: The object $\{*\} \in |\mathbf{Rel}|$ acts as a unit for the monoidal product.

Natural isomorphisms: The three following natural isomorphisms

- *Associativity:* $\alpha_{X,Y;Z} : (X \times Y) \times Z \to X \times (Y \times Z)$ is defined as

$$\alpha_{X,Y;Z} := \{(((x, y), z), (x, (y, z))) \mid x \in X, y \in Y \text{ and } z \in Z\}.$$

- *Left identity:* $\lambda_X : \{*\} \times X \to X$ is defined as

$$\lambda_X := \{((*, x), x) \mid x \in X\}.$$

- *Right identity:* $\rho_X : X \times \{*\} \to X$ is defined as

$$\rho_X := \{((x, *), x) \mid x \in X\}.$$

make

(i) The pentagon

$$\begin{tikzcd}
W \times (X \times (Y \times Z)) \arrow[r, "\alpha"] \arrow[d, "1\times\alpha"'] & (W \times X) \times (Y \times Z) \arrow[r, "\alpha"] & ((W \times X) \times Y) \times Z \\
W \times ((X \times Y) \times Z) \arrow[rr, "\alpha"'] & & (W \times (X \times Y)) \times Z \arrow[u, "\alpha\times 1"']
\end{tikzcd}$$

commutes. Indeed, for the top part, we have

$$\alpha \circ \alpha : W \times (X \times (Y \times Z)) \to ((W \times X) \times Y) \times Z$$

which is, by definition, a subset of

$$(W \times (X \times (Y \times Z))) \times ((W \times X) \times Y) \times Z.$$

Explicitly,

$$\alpha \circ \alpha := \{((w, (x, (y, z))), (((w'', x''), y''), z'')) \mid \text{ there exists } ((w', x'), (y', z')) \text{ such that } ((w, (x, (y, z)))\alpha((w', x'), (y', z')) \text{ and } ((w', x'), (y', z'))\alpha(((w'', x''), y''), z'')\}.$$

By definition of α, the previous expression is simply

$$\alpha \circ \alpha = \{((w, (x, (y, z))), (((w, x), y), z)) \mid w \in W, x \in X, y \in Y \text{ and } z \in Z\}.$$

The bottom path is done analogously, from which both paths are equal to

$$\{((w,(x,(y,z))),(((w,x),y),z)) \mid w \in W, x \in X, y \in Y \text{ and } z \in Z\}$$

making the pentagon commute. The remaining diagrams commute using similar calculations.
(ii) The triangle

$$\begin{tikzcd}
X \times (\{*\} \times Y) \arrow[r, "\alpha"] \arrow[dr, "1\times\lambda"'] & (X \times \{*\}) \times Y \arrow[d, "\rho\times 1"] \\
& X \times Y
\end{tikzcd}$$

commutes as both paths are equal to

$$\{((x,(*,y)),(x,y)) \mid x \in X \text{ and } y \in Y\}.$$

This turns **Rel** into a monoidal category.

Symmetry: The natural isomorphism $\sigma_{X,Y} : X \times Y \to Y \times X$ defined as

$$\sigma_{X,Y} := \{((x,y),(y,x) \mid x \in X \text{ and } y \in Y\}$$

make

(i) The two triangles

$$\begin{tikzcd}
X \times Y \arrow[r, "\sigma_{X,Y}"] \arrow[dr, equal] & Y \times X \arrow[d, "\sigma_{Y,X}"] \\
& X \times Y
\end{tikzcd}
\quad , \quad
\begin{tikzcd}
X \times \{*\} \arrow[r, "\sigma_{\{*\},X}"] \arrow[dr, "\rho"'] & \{*\} \times X \arrow[d, "\lambda"] \\
& X
\end{tikzcd}$$

commute; both paths of the left triangle are equal to

$$\{((x,y),(x,y)) \mid x \in X \text{ and } y \in Y\}$$

while the paths of the left triangle are equal to

$$\{((x,*),x) \mid x \in X\}.$$

(ii) Both the following and its inverse hexagon

$$\begin{tikzcd}
X \times (Y \times Z) \arrow[r, "\alpha"] \arrow[d, "1_X \times \sigma_{Y,Z}"'] & (X \times Y) \times Z \arrow[r, "\sigma_{(X\times Y);Z}"] & Z \times (X \times Y) \arrow[d, "\alpha"] \\
X \times (Z \times Y) \arrow[r, "\alpha"'] & (X \times Z) \times Y \arrow[r, "\sigma_{X,Y}\times 1_Z"'] & (Z \times X) \times Y
\end{tikzcd}$$

commute as both paths are equal to

$$\{((x,(y,z)),((z,x),y)) \mid x \in X, y \in Y \text{ and } z \in Z\}.$$

This makes **Rel** a symmetric monoidal category as claimed.

The category **Rel** is also symmetric monoidal with the disjoint union as monoidal product and the empty set as monoidal unit. Again, for details see [35].

4.3 Strictification of monoidal categories

The definition of a monoidal category is quite heavy. It will be convenient to avoid working with the natural isomorphism α, λ and ρ. We will make use of this section to introduce two theorems stating that, for all practical purposes, we can assume that the category we work in is strict. Most of the concepts that follow are taken from [58] to which the reader is referred for more details.

[Equivalence of categories] A functor $F : \mathbf{C} \to \mathbf{D}$ is an *equivalence of categories* when there is a functor $G : \mathbf{D} \to \mathbf{C}$ and natural isomorphisms $G \circ F \xrightarrow{\sim} 1_{\mathbf{C}}$ and $F \circ G \xrightarrow{\sim} 1_{\mathbf{D}}$.

Theorem 4.3.1 [58] A functor $F : \mathbf{C} \to \mathbf{D}$ is an equivalence of categories if and only if F is full, faithful, and each object $A \in |\mathbf{C}|$ is isomorphic to FA' for some $A' \in |\mathbf{D}|$.

Proof: See [58].

□

Such a definition is weaker than the notion of an isomorphism of categories but it remains quite strong. Indeed, in the words of S. MacLane [58], "[equivalence of categories] allows us to compare categories which are "alike" but of very different "sizes" ".

Example 4.3.2 [58] The *skeleton* $\mathbf{D}$ of a category $\mathbf{C}$ is any full subcategory of $\mathbf{C}$ such that each object $A \in |\mathbf{C}|$ is isomorphic in $\mathbf{C}$ to exactly one object $A' \in |\mathbf{D}|$. The equivalence is then defined as follows: evidently, since $\mathbf{D}$ is a full subcategory of $\mathbf{C}$ there is an inclusion functor $F : \mathbf{D} \to \mathbf{C}$. Now, for any $A \in |\mathbf{C}|$, we choose an isomorphism $\tau_A : A \to GA$ where $GA \in |\mathbf{D}|$. From this, there is a unique way to define a functor $G : \mathbf{C} \to \mathbf{D}$ such that $\tau : I_{\mathbf{C}} \to FG$ is a natural isomorphism with inverse $\tau^{-1} : GF \to I_{\mathbf{D}}$. As particular instances:

1. The category **FinSet** of finite sets and functions is equivalent to the category with objects all finite ordinals *i.e.*: $0, 1, 2, \cdots, n, \cdots$.
2. The category $\mathbf{FdVect}(\mathbb{C})$ is equivalent to the category with objects $\mathbb{C}, \mathbb{C}^2, \cdots, \mathbb{C}^n, \cdots$. This is nothing but the category $\mathbf{Mat}(\mathbb{C})$ of matrices with entries in $\mathbb{C}$.

[Monoidal functor] Let $\langle \mathbf{C}, \otimes, I, \alpha_{\mathbf{C}}, \lambda_{\mathbf{C}}, \rho_{\mathbf{C}} \rangle$ and $\langle \mathbf{D}, \odot, J, \alpha_{\mathbf{D}}, \lambda_{\mathbf{D}}, \rho_{\mathbf{D}} \rangle$ be monoidal categories, then a *monoidal functor* is a functor $F : \mathbf{C} \to \mathbf{D}$ together with a natural transformation

$$\phi_{A,B} : FA \odot FB \to F(A \otimes B)$$

and a morphism

$$\phi : J \to FI$$

which are such that for every A, B and $C \in \mathbf{C}$, the diagrams

$$\begin{tikzcd}
(FA \odot FB) \odot FC \arrow[r, "\alpha_{\mathbf{D}}"] \arrow[d, "\phi_{A,B} \odot 1"'] & FA \odot (FB \odot FC) \arrow[d, "1 \odot \phi_{B,C}"] \\
F(A \otimes B) \odot C \arrow[d, "\phi_{A \otimes B, C}"'] & FA \odot F(B \otimes C) \arrow[d, "\phi_{A, B \otimes C}"] \\
F((A \otimes B) \otimes C) \arrow[r, "F\alpha_{\mathbf{C}}"'] & F(A \otimes (B \otimes C))
\end{tikzcd}$$

and

$$\begin{tikzcd}
FA \odot J \arrow[r, "1\odot\phi"] \arrow[d, "\rho_{\mathbf{D}}"'] & FA \odot FI \arrow[d, "\phi_{A,I}"] & , & J \odot FB \arrow[r, "\phi\odot 1"] \arrow[d, "\lambda_{\mathbf{D}}"'] & FI \odot FB \arrow[d, "\phi_{I,B}"] \\
FA & F(A\otimes I) \arrow[l, "F\rho_{\mathbf{C}}"] & & FB & F(I\otimes B) \arrow[l, "F\lambda_{\mathbf{C}}"]
\end{tikzcd}$$

Moreover, a monoidal functor between symmetric monoidal categories is *symmetric* if, in addition, the following diagram

$$\begin{tikzcd}
FA \odot FB \arrow[r, "\sigma_{FA,FB}"] \arrow[d, "\phi_{A,B}"'] & FB \odot FA \arrow[d, "\phi_{B,A}"] \\
F(A\otimes B) \arrow[r, "F\sigma_{A,B}"'] & F(B\otimes A)
\end{tikzcd}$$

commutes in $\mathbf{D}$. A monoidal functor is *strict* if the components of $\phi_{\_,\_}$ and the morphism ϕ are identities and it is *strong* if they are isomorphisms.

Theorem 4.3.3 [58] Every monoidal category $\mathbf{C}$ is equivalent, via strong monoidal functors $F : \mathbf{C} \to \mathbf{C}'$ and $G : \mathbf{C}' \to \mathbf{C}$, to a strict monoidal category $\mathbf{C}'$.

Proof: See [58].

□

Moreover,

Theorem 4.3.4 [53] Let $\mathbf{C}$ and $\mathbf{D}$ be monoidally equivalent to the strict categories $\mathbf{C}'$ and $\mathbf{D}'$ as in theorem 4.3.3. Then, every monoidal functor $F : \mathbf{C} \to \mathbf{D}$ induces a strict monoidal functor $F' : \mathbf{C}' \to \mathbf{D}'$.

Proof: See [53].

□

Thus, theorem 4.3.3 tells us that any diagram in a category $\mathbf{C}$ is equivalent to a diagram in $\mathbf{C}'$ where the components of α, λ and ρ are identities. Moreover, theorem 4.3.4 tells us that any diagram of monoidal categories and functors can be equivalently replaced by a diagram of strict monoidal category and strict monoidal functors between them.

Remark 4.3.5 In the strictification $\mathbf{C}'$ of a symmetric monoidal category $\mathbf{C}$, it is *only* the components of the natural isomorphism α, λ and ρ of $\mathbf{C}$ that becomes identities in $\mathbf{C}'$. The components of the symmetry σ are *not* taken as identities in $\mathbf{C}'$.

4.4 Traced monoidal categories

A traced (symmetric) monoidal category is a category equipped with a trace which is a generalisation of the common notion of (partial) trace found in linear algebra. Such a structure was introduced by A. Joyal, R. Street and D. Verity in [54]. Heuristically, one can think of a trace as structure which provides a notion of "feedback" (or "loop") in a symmetric monoidal category equipped with such structure. We introduce the notion mainly because the type of category we will work in (in the next chapter and those that follow) admit a trace structure. Formally and relying on strictification,

[Traced monoidal category] [54] A *traced symmetric monoidal category* consists of a symmetric monoidal category $\mathbf{C}$ together with a family of functions, the *trace*,

$$Tr^X_{A,B} : \mathbf{C}(A \otimes X, B \otimes X) \to \mathbf{C}(A, B)$$

such that

i. *Naturality in A:* For every $f : A \otimes X \to B \otimes X$ and $g : C \to A$,

$$Tr^X_{A,B}(f) \circ g = Tr^X_{C,B}(f \circ (g \otimes 1_X)).$$

ii. *Naturality in B:* For every $f : A \otimes X \to B \otimes X$ and $g : B \to C$,

$$g \circ Tr^X_{A,B}(f) = Tr^X_{C,B}((g \otimes 1_X) \circ f).$$

iii. *Dinaturality in X:* For every $f : A \otimes X \to B \otimes Y$ and $g : Y \to X$,

$$Tr^X_{A,B}((1_B \otimes g) \circ f) = Tr^Y_{A,B}(f \circ (1_A \otimes g)).$$

iv. *Vanishing 1:* For every $f : A \otimes I \to B \otimes I$,

$$Tr^I_{A,B}(f) = f.$$

v. *Vanishing 2:* For every $f : A \otimes X \otimes Y \to B \otimes X \otimes Y$,

$$Tr^{X \otimes Y}_{A,B}(f) = Tr^X_{A,B}(Tr^Y_{A \otimes X, B \otimes X}(f)).$$

vi. *Superposing:* For every $f : A \otimes X \to B \otimes X$ and $g : C \to D$,

$$g \otimes Tr^X_{A,B}(f) = Tr^X_{C \otimes A, D \otimes B}(g \otimes f).$$

vii. *Yanking:*

$$Tr^X_{X,X}(\sigma_{X,X}) = 1_X.$$

The first three points of the definition indicate that the trace can indeed be thought of as a loop while the remaining points ensure that it behaves coherently with the monoidal structure.

Example 4.4.1 The following examples are taken from [54] to which the reader is referred for more details:

1. The category **FdVect** admit a trace which is just the partial trace.
2. The category **Rel** is traced. Given a relation $R : X \times U \to Y \times U$, then $Tr^U_{X,Y}(R) : X \to Y$ is defined as

$$\{(x, y) \mid \text{There exists } u \in U \text{ such that } (x, u)R(y, u)\}.$$

4.5 Internal monoids and comonoids

We now formally define the notion of internal monoid and internal comonoid in a monoidal category. Again, the following definitions are taken from [58] to which the reader may refer for a more complete discussion on the subject.

Let us go back to the notion of monoid defined at the beginning of this chapter; we said that one of the simplest examples was to start from an alphabet A of symbols and take the set $M = A^*$ of words on A together with an associative operation $\cdot$ and a special symbol ϵ acting as an identity for this operation. Note that M is nothing more than a set, so we can formalise the concept of monoid as a set $M \in |\mathbf{Set}|$ together with some extra structure.

Now, suppose $M \in |\mathbf{Set}|$ in equipped with a function $\mu : M \times M \to M$ where $\times$ is the Cartesian product and such that

$$\begin{tikzcd}
M \times M \times M \arrow[r, "1_M \times \mu"] \arrow[d, "\mu \times 1_M"'] & M \times M \arrow[d, "\mu"] \\
M \times M \arrow[r, "\mu"'] & M
\end{tikzcd}$$

commutes. The previous diagram precisely states that μ is a binary operation which is associative.

Next, suppose that, in addition to μ above, there is also a morphism $e : \{*\} \to M$ such that

$$\begin{tikzcd}
 & M & \\
\{*\} \times M \arrow[ur, "\sim"] \arrow[r, "e \times 1_M"'] & M \times M \arrow[u, "\mu"] & M \times \{*\} \arrow[ul, "\sim"'] \arrow[l, "1_M \times e"]
\end{tikzcd}$$

commutes. Since $\{*\}$ is the singleton, the previous diagram says that e as picks an element in M that acts as an identity under the operation μ. We have thus defined the notion of an *internal monoid* in **Set** as $\langle M, \mu, e \rangle$.

Generally, internal monoids in **Set** exactly correspond to usual notion of monoids. Now, the notion of internal monoids in **Set** taking the Cartesian product as the monoidal product, can be generalised to arbitrary monoidal categories as follows:

[Internal monoid] Let $\langle \mathbf{C}, \otimes, I \rangle$ be a monoidal category. Then an *internal monoid* is an object $M \in |\mathbf{C}|$ together with a pair of morphisms

$$\begin{tikzcd}
M \otimes M \arrow[r, "\mu"] & M & I \arrow[l, "e"']
\end{tikzcd}$$

called *multiplication* and *unit* respectively, that are such that both

$$\begin{tikzcd}
M \otimes M \otimes M \arrow[r, "1_M \otimes \mu"] \arrow[d, "\mu \otimes 1_M"'] & M \otimes M \arrow[d, "\mu"] \\
M \otimes M \arrow[r, "\mu"'] & M
\end{tikzcd}$$

and

$$\begin{tikzcd}
 & M & \\
I \otimes M \arrow[ur, "\sim"] \arrow[r, "e \otimes 1_M"'] & M \otimes M \arrow[u, "\mu"] & M \otimes I \arrow[ul, "\sim"'] \arrow[l, "1_M \otimes e"]
\end{tikzcd}$$

commute. In addition, an internal monoid is *commutative*—or symmetric—when

$$\begin{tikzcd}
M \otimes M \arrow[r, "\sigma_{M,M}"] \arrow[dr, "\mu"'] & M \otimes M \arrow[d, "\mu"] \\
 & M
\end{tikzcd}$$

Of course, we can also dualise the notion, thus defining internal *comonoids* as follows:

[Internal comonoid] Let $\langle \mathbf{C}, \otimes, I\rangle$ be a monoidal category. Then an *internal comonoid* an object $C \in |\mathbf{C}|$ together with a pair of morphisms

$$\begin{tikzcd} C \otimes C & C \arrow[l, "\delta"'] \arrow[r, "\epsilon"] & I \end{tikzcd}$$

the *comultiplication* and the *counit*, that are such that both

$$\begin{tikzcd} C \arrow[r, "\delta"] \arrow[d, "\delta"'] & C \otimes C \arrow[d, "1_C \otimes \delta"] \\ C \otimes C \arrow[r, "\delta \otimes 1_C"'] & C \otimes C \otimes C \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} & C \arrow[dl, "\simeq"'] \arrow[d, "\delta"] \arrow[dr, "\simeq"] & \\ I \otimes C & C \otimes C \arrow[l, "\epsilon \otimes 1_C"] \arrow[r, "1_C \otimes \epsilon"'] & C \otimes I \end{tikzcd}$$

commute. Moreover, an internal comonoid is *cocommutative* when

$$\begin{tikzcd} C \arrow[r, "\delta"] \arrow[dr, "\delta"'] & C \otimes C \arrow[d, "\sigma_{M,M}"] \\ & C \end{tikzcd}$$

4.6 Scalars

In any category $\mathbf{C}$, the set of endomorphism $\mathbf{C}(A, A)$ of an object A is a monoid where the composition acts as monoid multiplication and $1_A : A \to A$ as identity. In this section, we will be interested in the monoid $\mathbf{C}(I, I)$ of a monoidal category $\mathbf{C}$. In many cases, such a monoid carries some explicit quantitative content.

Example 4.6.1 In the category **FdVect**, the set $\mathbf{FdVect}(\mathbb{C}, \mathbb{C})$ is isomorphic to $\mathbb{C}$, the base field.

In **Rel**, there are exactly two relations of type $\{*\} \to \{*\}$ that is, the identity and the empty relation. Thus the elements of $\mathbf{Rel}(*, *)$ can be thought of as truth values.

In the light of the previous examples, we will call $\mathbf{C}(I, I)$ the *monoid of scalars* of $\mathbf{C}$.

We have the following remarkable result:

Proposition 4.6.2 [57] Let $\mathbf{C}$ be a monoidal category, then the monoid of scalars is commutative.

Proof: The proof is given by the following commutative diagram:

$$\begin{tikzcd} I \arrow[r, "\simeq"] & I \otimes I \arrow[r, equal] & I \otimes I \arrow[r, equal] & I \otimes I \arrow[r, "\simeq"] & I \\ I \arrow[r, "\simeq"] \arrow[u, "t"] & I \otimes I \arrow[u, "1_I \otimes t"] & & I \otimes I \arrow[r, "\simeq"] \arrow[u, "s \otimes 1_I"] & I \arrow[u, "s"'] \\ I \arrow[r, "\simeq"'] \arrow[u, "s"] & I \otimes I \arrow[u, "s \otimes 1_I"] \arrow[r, equal] & I \otimes I \arrow[uu, "s \otimes t"] \arrow[r, equal] & I \otimes I \arrow[r, "\simeq"'] \arrow[u, "1_I \otimes t"] & I \arrow[u, "t"'] \end{tikzcd} \tag{4.2}$$

Equality of the two outer composites from the lower-left corner to the upper-right corner boils down to equality between:

i. The outer left/upper path which consists of $t \circ s$ and the composite of an isomorphism $I \simeq I \otimes I$ with its inverse so that $t \circ s$.

ii. Analogously , the outer lower/right path yields $s \circ t$.

Equalities between these two paths is obtained via

- Bifunctoriality of $\otimes$ which gives the commutation of the middle two rectangles and
- Naturality of the left- and right-unit isomorphisms gives the commutation of the four smaller squares,

as required.

□

Remark 4.6.3 The category at stake in the previous proposition is not necessarily symmetric. Therefore, since the monoidal structure is one of the most fundamental structures in our theory, the preceding result entails that models with non-commutative monoid of scalars can't be expressed within the theory. For instance, quaternionic quantum mechanics would not make sense in our context.

The right half of (4.2) is

$$s \circ t := I \xrightarrow{\simeq} I \otimes I \xrightarrow{s \otimes t} I \otimes I \xrightarrow{\simeq} I$$

which defines the multiplication of scalars.

We can also define what it means to multiply a morphism by a scalar. In $\mathbf{FdVect}(\mathbb{K})$, any scalar $z : \mathbb{C} \to \mathbb{C}$ gives rise to a natural transformation $z_V : V \to V$ as the composite

$$V \xrightarrow{\lambda_V^{-1}} \mathbb{C} \otimes V \xrightarrow{z \otimes 1_V} \mathbb{C} \otimes V \xrightarrow{\lambda_V} V.$$

This observation generalises to an arbitrary monoidal category. Indeed, we can define the *scalar multiples* of a morphism $f : A \to B$ as

$$s \cdot f := A \xrightarrow{\simeq} I \otimes A \xrightarrow{s \otimes f} I \otimes B \xrightarrow{\simeq} B.$$

Lemma 4.6.4 We have

$$(s \cdot f) \circ (t \cdot g) = (s \circ t) \cdot (f \circ g) \quad \text{and} \quad (s \cdot f) \otimes (t \cdot g) = (s \circ t) \cdot (f \otimes g).$$

Proof: We will prove only the first equation as the proofs by diagram chase for these equations are fairly complicated for the insight they bring. The equation

$$(s \circ t) \cdot (f \circ g) = (t \cdot f) \circ (s \cdot g)$$

for $f : A \to B$ and $g : B \to C$ is proven by commutation of:

$$\begin{tikzcd}
 & I\otimes B \arrow[rr, "\lambda_B"] \arrow[drr, "\rho_I^{-1}\otimes 1_B"] & & B \arrow[rr, "\lambda_B^{-1}"] & & I\otimes B \arrow[dr, "t\otimes g"] & \\
A\simeq I\otimes A \arrow[ur, "s\otimes f"] \arrow[dr, "\rho_I\otimes 1_A"'] & & & (I\otimes I)\otimes B \arrow[urr, "\lambda_I\otimes 1_B"] \arrow[drr, "(1_I\otimes t)\otimes g"] & & & I\otimes C\simeq C \\
 & (I\otimes I)\otimes A \arrow[urr, "(s\otimes 1_I)\otimes f"] \arrow[rrrr, "(s\otimes t)\otimes(g\circ f)"'] & & & & (I\otimes I)\otimes C \arrow[ur, "\lambda_I\otimes 1_C"'] &
\end{tikzcd}$$

The diamond on the left commutes by naturality of ρ_I. The top triangle commutes because both paths are equal to $1_{I\otimes B}$ as $\lambda_I = \rho_I$. The bottom triangle commute by (4.2) and bifunctoriality of the tensor product. Finally, the right diamond commutes by naturality of λ_I.

□

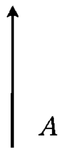
4.7 Graphical calculus for symmetric monoidal categories

We now introduce a useful graphical calculus for monoidal categories. Not only will such a calculus give us a neat way to figure what a formula means in operational terms, but it also will provide us with an elegant proof technique which is less tedious to read than diagram chasing. Diagrammatic proofs are often more illuminating than the algebraic proofs, as they subsume the notion of information flow implicit in the formalism and make it (visually) explicit.

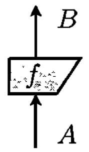
Such a graphical calculus can be traced back to the tensor diagram notation of Penrose for multilinear functions [65]. In the context of category theory, a graphical calculus has been introduced for symmetric monoidal categories by Joyal and Street in [52].

The basic building blocks of the graphical calculus for a symmetric monoidal category **C** are given as follows:

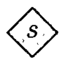
- The *identity on* $I \in |\mathbf{C}|$ is represented by the empty picture.
- The *identity on* $A \in |\mathbf{C}|$ different from I is represented by



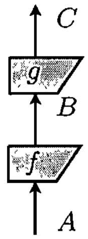
- A *morphism* $f : A \longrightarrow B$ is depicted as



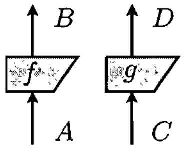
The trapezoid form for the boxes introduces an asymmetry that will be handy to distinguish f from its transposed, conjugate and adjoint as we shall see later. As an exception to this notation, a scalar $s : I \longrightarrow I$ is depicted as



- The *composition* of morphisms $f : A \to B$ and $g : B \to C$ is given by stacking the graphical representation of g above the one of f and connecting the arrows labeled by B, *i.e.*,



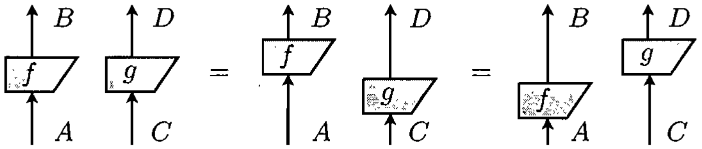
- The *tensor product* of morphisms $f : A \to B$ and $g : C \to D$ is given by aligning the graphical representation of and f and g side by side in the $f \otimes g$ order, *i.e.*,



Bifunctoriality of the tensor product, *i.e.*,

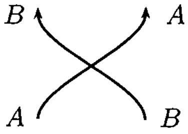
$$f \otimes g = (f \otimes 1_D) \circ (1_A \otimes g) = (1_B \otimes g) \circ (f \otimes 1_C)$$

becomes



which says that, in general, we can "slide" boxes along their wires.

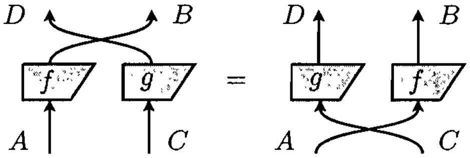
- The *symmetry* $\sigma_{AB} : A \otimes B \to B \otimes A$ is represented as



Naturality of the symmetry is

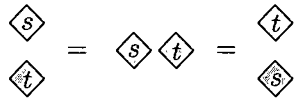
$$\begin{tikzcd}
A \otimes C \arrow[r, "\sigma_{A,C}"] \arrow[d, "f\otimes g"'] & C \otimes A \arrow[d, "g\otimes f"] \\
B \otimes D \arrow[r, "\sigma_{B,D}"'] & D \otimes B
\end{tikzcd}$$

which is depicted as



Hence, even in the presence of a symmetry, we can still slide the boxes along the wires.

Example 4.7.1 Commutation of the (strictified version of) diagram (4.2) is depicted as



In fact, as scalars aren't linked to any wires, the coherence condition for symmetric monoidal categories indicates that they may move freely in the picture.

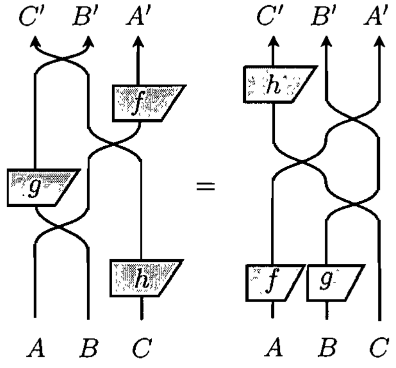
Example 4.7.2 Suppose that one wants to show that in **C**,

$$\begin{aligned}&(\sigma_{B',C'} \otimes f) \circ (g \otimes \sigma_{A,C'}) \circ (\sigma_{A,B} \otimes h)\\ =\quad &(h \otimes \sigma_{A',B'}) \circ (\sigma_{A',C} \otimes 1_{B'}) \circ (1_{A'} \otimes \sigma_{B',C}) \circ (f \otimes g \otimes 1_C)\end{aligned}$$

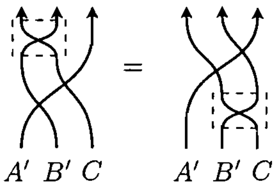
holds. Then, the proof by diagram chase and without bracketing—which the reader may skip—is

$$\begin{tikzcd}
A\otimes B\otimes C \arrow[rr, "1_{A\otimes B}\otimes h"] \arrow[drr, "\sigma_{A,B}\otimes 1_C"] \arrow[dd, "1_A\otimes g\otimes 1_C"] & & A\otimes B\otimes C' \arrow[r, "\sigma_{A,B}\otimes 1_{C'}"] & B\otimes A\otimes C' \arrow[dd, "g\otimes 1_{A\otimes C'}"] \\
 & & B\otimes A\otimes C \arrow[ur, "1_{B\otimes A}\otimes h"] \arrow[d, "g\otimes 1_{A\otimes C}"] & \\
A\otimes B'\otimes C \arrow[rr, "\sigma_{A,B'}\otimes 1_C"] \arrow[d, "f\otimes 1_{B'\otimes C}"] & & B'\otimes A\otimes C \arrow[r, "1_{B'\otimes A}\otimes h"] \arrow[dl, "1_{B'}\otimes f\otimes 1_C"] \arrow[d, "1_{B'}\otimes\sigma_{A,C}"] & B'\otimes A\otimes C' \arrow[d, "1_{B'}\otimes\sigma_{A,C'}"] \\
A'\otimes B'\otimes C \arrow[r, "\sigma_{A',B'}\otimes 1_C"] \arrow[d, "1_{A'}\otimes\sigma_{B',C}"] & B'\otimes A'\otimes C \arrow[dl, "\sigma_{B',A\otimes C}"] \arrow[dr, "1_{B'}\otimes\sigma_{A',C}"] & B'\otimes C\otimes A \arrow[r, "1_{B'}\otimes h\otimes 1_A"] \arrow[d, "1_{B'\otimes C}\otimes f"] & B'\otimes C'\otimes A \arrow[d, "1_{B'\otimes C'}\otimes f"] \\
A'\otimes C\otimes B' \arrow[d, "\sigma_{A',C}\otimes 1_{B'}"] & & B'\otimes C\otimes A' \arrow[r, "1_{B'}\otimes h\otimes 1_{A'}"] \arrow[dll, "\sigma_{B',C\otimes A'}"] \arrow[d, "\sigma_{B',C}\otimes 1_{A'}"] & B'\otimes C'\otimes A' \arrow[d, "\sigma_{B',C'}\otimes 1_{A'}"] \\
C\otimes A'\otimes B' \arrow[rr, "1_C\otimes\sigma_{A',B'}"'] & & C\otimes B'\otimes A' \arrow[r, "h\otimes 1_{B'\otimes A'}"'] & C'\otimes B'\otimes A'
\end{tikzcd}$$

On the other hand, the proof using the graphical calculus is

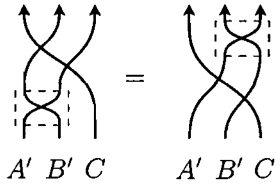


meaning to slide the boxes first and then rearrange the wires *i.e.*,



where we use naturality of the symmetry $\sigma_{A',B'\otimes C}$ to slide down the symmetry $\sigma_{B',C}$ which is in the dotted box in the above depiction.

Obviously, there is more than one way to proceed; we could have rearranged the wires first, then slid the boxes. We could also have proceeded using the naturality of $\sigma_{A'\otimes B',C}$ *i.e.*,



However, the only thing we are interested in is whether or not there exists a way to transform the initial picture into the final picture.

Now, one may doubt that a "graph isomorphism"[5] between two pictures *always* corresponds to an equation in the language of symmetric monoidal categories. The assurance that we have such a fact is given by the following result that we cite from [68] to ensure that the terminology is coherent with the other results that we will give for graphical calculi.

Theorem 4.7.3 A well-typed equation between morphisms in the language of symmetric monoidal categories follows from the axioms of symmetric monoidal categories if and only if it holds, up to graph isomorphism, in the graphical language.

Proof: See [52].

□

4.8 †-monoidal categories

We now introduce the notion of "dagger" structure [5]; concretely, such a structure gives a suitable abstraction of the notion of adjoint thus enabling the many notions defined with it.

[†-monoidal category] [68] A *†-(symmetric) monoidal category* is a symmetric monoidal category **C** equipped with an involutive, identity-on-objects, contravariant endofunctor $\dagger : \mathbf{C} \to \mathbf{C}$ such that, denoting $\dagger(f) := f^\dagger$,

i. For all $f : A \to B$ and $g : C \to D$, $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$,

ii. $\alpha^\dagger_{A,B;C} = \alpha^{-1}_{A,B;C}$

iii. $\lambda^\dagger_A = \lambda^{-1}_A$,

[5] Correspondence between two pictures is called *graph isomorphism* in the papers where this calculus was introduced. We keep the same terminology here and refer to the cited papers for a precise definition of *graph* and *graph isomorphism* in this context.

iv. $\rho_A^\dagger = \rho_A^{-1}$ and

v. $\sigma_{A,B}^\dagger = \sigma_{A,B}^{-1}$.

Given a morphism $f : A \to B$ in **C**, $f^\dagger : B \to A$ is called *the adjoint of f.*

[Self-adjoint and unitary morphism] Let **C** be a †-monoidal category. Then a morphism $f : A \to B$ is:

1. *Self-adjoint* if $f = f^\dagger$,

2. *Unitary* if $f^\dagger = f^{-1}$.

Example 4.8.1 The category **Hilb** of Hilbert spaces and bounded linear maps is †-monoidal. The dagger takes any bounded linear map f to its adjoint $f^\dagger$.

Example 4.8.2 [5] In **Rel**, we have an obvious candidate for the functor

$$\dagger : \mathbf{Rel}^{op} \to \mathbf{Rel}.$$

Indeed, given a relation $R : X \to Y$, the *converse relation* $R^c : Y \to X$ is defined as

$$R^{\cup} := \{(y, x) \mid xRy\}.$$

From this, we can define the functor † whose action on objects is trivial and on morphisms is described as taking the converse relation *i.e.*, $R^\dagger = R^{\cup}$.

[35] ***Rel*** *is †-monoidal:*

(i) $(R \otimes S)^\dagger = R^\dagger \times S^\dagger$. From the definition of the monoidal product of two relations $R_1 := \{(x, y) \mid xRy\}$ and $R_2 := \{(x', y') \mid xRy'\}$, we have that

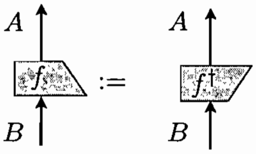
$$(R_1 \times R_2)^\dagger = \{((y, y'), (x, x')) \mid xR_1y \text{ and } x'R_2y'\} = R_1^\dagger \times R_2^\dagger$$

(ii) The fact that $\alpha^\dagger = \alpha^{-1}$, $\lambda^\dagger = \lambda^{-1}$, $\rho^\dagger = \rho^{-1}$ and $\sigma^\dagger = \sigma^{-1}$ is trivial as the inverse of all these morphism is the relational converse.

4.9 Graphical calculus for †-monoidal categories

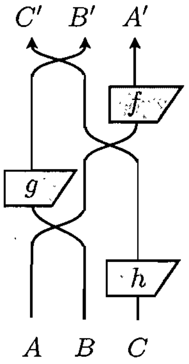
We may now enrich the graphical calculus for symmetric monoidal categories to †-monoidal categories. Such an enrichment was provided by P. Selinger in [68].

- Given a morphism $f : A \to B$ its *adjoint* $f^\dagger : B \to A$ depicts as

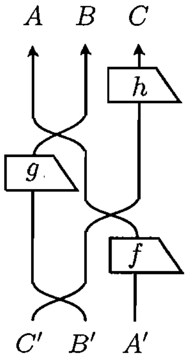


which is to reflect along the horizontal axis the depiction of f in the graphical language for symmetric monoidal categories while keeping the orientation of the wires from bottom to top.

Example 4.9.1 If $k = (\sigma_{B',C'} \otimes f) \circ (g \otimes \sigma_{A,C'}) \circ (\sigma_{A,B} \otimes h)$ that is



Then, the depiction of its adjoint $k^\dagger = (\sigma^\dagger_{A,B} \otimes h^\dagger) \circ (g^\dagger \otimes \sigma^\dagger_{A,C'}) \circ (\sigma^\dagger_{B',C'} \otimes f^\dagger)$ is



An analogous result to the one for symmetric monoidal categories holds here:

Theorem 4.9.2 [68] A well-typed equation between morphisms in the language of †-symmetric monoidal categories follows from the axioms of †-symmetric monoidal categories if and only if it holds, up to graph isomorphism, in the graphical language.

Proof: See [68]. □

5 Quantum structures

In this chapter, we introduce the quantum fragment of our theory via the notion of *quantum structure* in a †-monoidal category. From this, we will define the

1. *Category of quantum structures* $\mathbf{C}_q$ of a †-monoidal category $\mathbf{C}$ which is a suitable categorical context to work with pure states and unitary transformations. And

2. The *category of completely positive maps* $\mathbf{CP}(\mathbf{C}_q)$ of a category of quantum structures $\mathbf{C}_q$ which constitute a suitable categorical framework to work with mixed states and superoperators.

Importantly, a category of quantum structures is a †-compact[6] category as introduced in [5]. We use the terminology *quantum structures* to stress the distinction between these categories and the category $\mathbf{C}_c$ of classical maps that we introduce in chapter 6. Nonetheless, it should be understood that in the papers we cite, such a category might bear another name.

The approach of defining such a category by speaking of structures at the level of objects was the one taken in [32] which the author wrote with B. Coecke and D. Pavlovic. The presentation we give in this chapter contrasts with the one given there, since our definition of quantum structure does not require the objects to be self-dual and in that sense, is more general.

On the other hand, the category $\mathbf{CP}(\mathbf{C}_q)$ will be constructed from $\mathbf{C}_q$ in the same way that $\mathbf{CPM}(\mathbf{C})$ is constructed from a †-compact category $\mathbf{C}$ in Peter Selinger's paper [68] to which we refer the reader for more details. Aside from the general form of the discussion, the only discrepancies between the paper cited and our presentation are purely notational.

For the remainder of this dissertation, we assume that we work in a †-monoidal category $\mathbf{C}$ which is taken to be strict by convenience, *i.e.*, to avoid unnecessary complications in the presentation.

5.1 Compact structures

Compact categories provides a framework to handle duals such as, for instance, the dual space of a vector space. The bulk of this section is taken from [57] to which the reader is referred for more details.

We first define the notion of compact structure at the level of objects:

[6] Or *strongly compact closed* [5] or †-*compact closed* [68] depending on which fragment of the literature we refer to.

[Compact structure] Let $\mathbf{C}$ be a symmetric monoidal category. A *compact structure* on an $A \in |\mathbf{C}|$ is a quadruple

$$\langle A, A', \eta_A : I \to A' \otimes A, \epsilon_A : A \otimes A' \to I \rangle$$

where $A' \in |\mathbf{C}|$ is called a *dual of* A and such that the following diagrams commute

$$\begin{tikzcd} A \arrow[d, "1_A \otimes \eta_A"'] \arrow[dr, "1_A"] & \\ A \otimes A' \otimes A \arrow[r, "\epsilon_A \otimes 1_{A'}"'] & A \end{tikzcd} \qquad \begin{tikzcd} A' \arrow[r, "\eta_A \otimes 1_{A'}"] \arrow[dr, "1_{A'}"'] & A' \otimes A \otimes A' \arrow[d, "1_{A'} \otimes \epsilon_A"] \\ & A' \end{tikzcd} \tag{5.1}$$

Finally, a compact structure is *self-dual* whenever $A = A'$.

Example 5.1.1 A compact structure on a $V \in |\mathbf{FdVect}|$ is given by

$$\eta_V : \mathbb{C} \to V^* \otimes V :: 1 \mapsto \sum_{i=1}^{n} f_i \otimes e_i \tag{5.2}$$

where $n = \mathrm{Dim}(V)$, $\{e_i\}_{i=1}^n$ a basis of V and $f_i \in V^*$ is the linear functional such that for all i, j, $f_j(e_i) = \delta_{i,j}$. Now, with the same notation,

$$\epsilon_V : V \otimes V^* \to \mathbb{C} :: e_i \otimes f_j \mapsto f_j(e_i).$$

Lemma 5.1.2 [Dual of a morphism] Let $\mathbf{C}$ be symmetric monoidal category. If A is equipped with a compact structure $\langle A, A', \eta_A, \epsilon_A \rangle$ and B is equipped with $\langle B, B', \eta_B, \epsilon_B \rangle$ then, for any $f \in \mathbf{C}(A, B)$ there exists a unique $g \in \mathbf{C}(B', A')$ defined as

$$\begin{tikzcd} B' \arrow[r, "\eta_A \otimes 1_{B'}"] \arrow[d, "g"'] & A' \otimes A \otimes B' \arrow[d, "1_{A'} \otimes f \otimes 1_{B'}"] \\ A' & A' \otimes B \otimes B' \arrow[l, "1_B \otimes \epsilon_B"] \end{tikzcd}$$

The morphism g is called the *dual* of f.

Proof: See [57].

□

Lemma 5.1.3 [57] Let $\mathbf{C}$ be a monoidal category. The dual of an $A \in |\mathbf{C}|$ is unique up to a unique isomorphism compatible with the compact structure, *i.e.*, if A admits two compact structures $\langle A, A', \epsilon_A, \eta_A \rangle$ and $\langle A, A'', \epsilon'_A, \eta'_A \rangle$, there is a unique isomorphism $\phi : A' \to A''$ such that both

$$\begin{tikzcd} A' \otimes A \arrow[rr, "\phi \otimes 1_A"] & & A'' \otimes A \\ & I \arrow[ul, "\eta_A"] \arrow[ur, "\eta'_A"'] & \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} A \otimes A' \arrow[rr, "1_A \otimes \phi"] \arrow[dr, "\epsilon_A"'] & & A \otimes A'' \arrow[dl, "\epsilon'_A"] \\ & I & \end{tikzcd}$$

commute. Further, such an isomorphism is natural. Indeed, if $f : A \to B$ has duals $g : B' \to A'$ and $g' : B'' \to A''$ in the sense of lemma 5.1.2, then

$$\begin{tikzcd}
B' \arrow[r, "\phi"] \arrow[d, "g"'] & B'' \arrow[d, "g'"] \\
A' \arrow[r, "\phi'"'] & A''
\end{tikzcd}$$

commutes.

Proof: See [18].

□

[**Compact category**] A *compact category*—or *compact closed category*—**C** is a monoidal category where each $A \in |\mathbf{C}|$ comes with a compact structure $\langle A, A^*, \eta_A, \epsilon_A \rangle$.

Proposition 5.1.4 The operation $(-)^*$ taking A to its dual A^* and $f : A \to B$ to its dual $f^* : B^* \to A^*$ as in lemma 5.1.2 defines a contravariant functor.

Proof: See [57].

□

Lemma 5.1.5 Let **C** be a compact closed category. Then

i. The tensor unit I is self-dual,

ii. A is a dual of A^* and

iii. $B^* \otimes A^*$ is a dual of $A \otimes B$.

Proof: See [57].

□

From the previous lemma and since by lemma 5.1.3 duals are unique up to a natural isomorphism compatible with the compact structure, we have:

i. $I^* \simeq I$,

ii. $A^{**} \simeq A$ and

iii. $(A \otimes B)^* \simeq B^* \otimes A^*$.

[**Strict compact closed category**] A compact closed category **C** is *strict* if, in addition to being a strict monoidal category, we have

i. $I = I^*$,

ii. $A = A^{**}$ and

iii. $(A \otimes B)^* = B^* \otimes A^*$.

Theorem 5.1.6 [57] Any compact closed category **C** is equivalent to a strict compact closed category $\mathbf{C}'$.

Proof: See [57].

□

5.2 Quantum structures

The notion of category of quantum structures enables the axiomatisation of a large fragment of quantum mechanics in terms of adjoints and bipartite entanglement. As we shall see in the concluding remarks of this section, the formalism of such categories enables an abstraction of Dirac notation, of unitary and self-adjoint operators among other things. Most of the material of this section is derived from [5] and [68].

[Quantum structure] A *quantum structure*

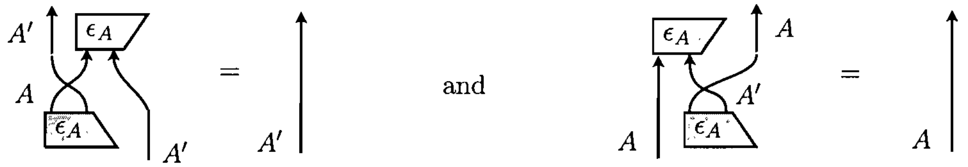
$$\langle A, \epsilon_A : A \otimes A' \to I \rangle \tag{5.3}$$

is a compact structure $\langle A, A', \eta_A, \epsilon_A \rangle$ such that

$$\begin{tikzcd} I \arrow[r, "\epsilon_A^\dagger"] \arrow[dr, "\eta_A"'] & A \otimes A' \arrow[d, "\sigma_{A,A'}"] \\ & A' \otimes A \end{tikzcd} \tag{5.4}$$

We call η_A the *unit* (of the quantum structure) and ϵ_A the *counit*. Finally, we will make an abuse of terminology saying that the support A of a quantum structure $\langle A, \epsilon_A \rangle$ is a *quantum object*.

Taking in account the constraint of equation (5.4), compactness (eq. (5.2)) of the quantum structure depicts in the graphical language of †-monoidal categories as



Now, we have an analogue of lemma 5.1.3 for quantum structures:

Lemma 5.2.1 The dual of a quantum object is unique up to a unique unitary isomorphism compatible with the quantum structure, *i.e.*, if $A \in |\mathbf{C}|$ admits two quantum structures, $\langle A, \epsilon_A \rangle$ with dual A' and $\langle A, \epsilon'_A \rangle$ with dual A'', then there exists a unique unitary transformation $u : A' \to A''$ such that

$$\begin{tikzcd} A \otimes A' \arrow[rr, "1_A \otimes u"] \arrow[dr, "\epsilon_A"'] & & A \otimes A'' \arrow[dl, "\epsilon'_A"] \\ & I & \end{tikzcd} \tag{5.5}$$

The proof of this lemma is postponed to the next chapter as it is included in the proof of theorem 6.3.3.

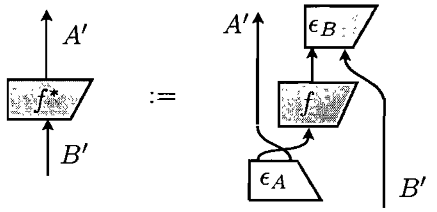
[Category of quantum structures] A category of *of quantum structures* $\mathbf{C}_q$ is a †-monoidal category $\mathbf{C}$ where every object A comes with a specified quantum structure $\langle A, \epsilon_A \rangle$ and where A relates to its dual A' via $\epsilon_{A'} = \epsilon_A \circ \sigma_{A,A'}$.

Remark 5.2.2 The constraint $\epsilon_{A'} = \epsilon_A \circ \sigma_{A,A'}$ entails that the double dual of A is A.

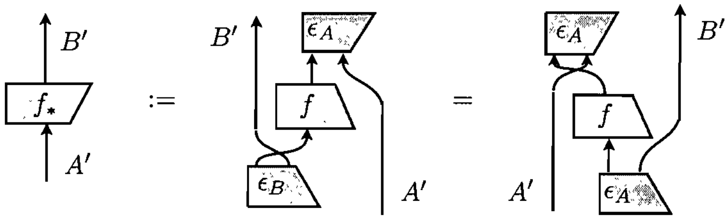
Proposition 5.2.3 The quantum structures in $\mathbf{C}_q$ induces two functors

$$(-)^* : \mathbf{C}_q^{op} \to \mathbf{C}_q \quad \text{and} \quad (-)_* : \mathbf{C}_q \to \mathbf{C}_q \tag{5.6}$$

whose actions on objects are $A \mapsto A'$ where A' is the dual of A in $\mathbf{C}_q$. For morphisms, given an $f : A \to B$ where A has dual A' and B has dual B' then, their actions on f are respectively given by

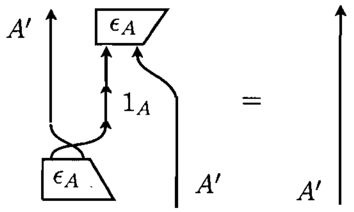


and

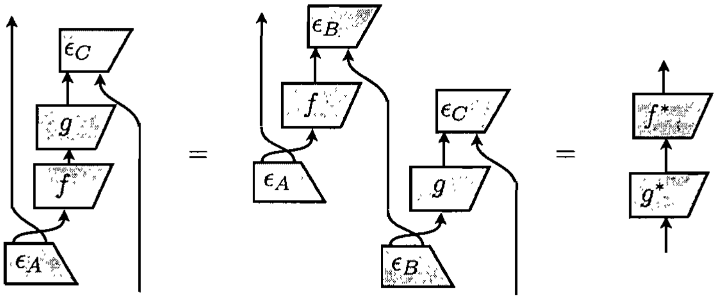


i.e., $(-)_* := (-)^{\dagger *} = (-)^{*\dagger}$.

Proof: The fact that $(-)^*$ is a functor is almost trivial using the graphical calculus. Indeed, for any $A \in |\mathbf{C}_q|$, $(1_A)^* = 1_{(A)^*} = 1_{A'}$ as



For the composition, let $f : A \to B$ and $g : B \to C$ then $(g \circ f)^*$ is given by



where the second expression is obtained from the first using the dual compactness equation on B and we get from the second to the third simply by definition of $(-)^*$.

One gets functoriality of $(-)_*$ in in an analogous manner using the definition of $(-)_*$.

□

Terminology. We say that f^* is the *transpose* of f and f_* its *conjugate*. Moreover, in light of the previous proposition, we will denote the chosen dual of A in $\mathbf{C}_q$ as A^*.

Remark 5.2.4 The previous result says that, indeed, the category $\mathbf{C}_q$ is a †-compact category as was defined in [5].

Moreover, taken that a category of quantum structures is also a compact closed category, *i.e.*, a monoidal category where each object comes with a compact structure, we have:

Lemma 5.2.5 **[Canonical trace]** Every category of quantum structures admits a trace—in the sense of the definition given in section 4.4. Given an $f : A \otimes C \to B \otimes C$, the *canonical trace* of f is given by

$$Tr^C_{A,B}(f) := (1_B \otimes \epsilon_C) \circ (f \otimes C^*) \circ (A \otimes \eta_{C^*}) : A \to B$$

Proof: Since a category of quantum structures is an instance of compact closed category, the proof can be found in [54].

□

Example 5.2.6 The full subcategory **FdHilb** of **Hilb** of finite-dimensional Hilbert spaces and (bounded) linear maps is a category of quantum structures when

- The dual $\mathcal{H}^*$ of an $\mathcal{H} \in |\mathbf{FdHilb}|$ is the conjugate space.
- The counit of the quantum structure is given as

$$\epsilon_{\mathcal{H}} : \mathbb{C} \to \mathcal{H} \otimes \mathcal{H}^* :: \phi \otimes \psi \mapsto \phi^\dagger \circ \psi = \langle \phi, \psi \rangle.$$

It is easy to see that the constraint equation given in (5.3) is satisfied.

In **FdHilb**, the dagger corresponds to "taking the adjoint", the upper-star functor can be thought of as transposition and finally, the lower-star functor can be thought of as complex conjugation thus the name of f^* and f_*. Indeed, for the lower-star functor, its action on objects is given by $\mathcal{H} \mapsto \mathcal{H}^*$ where $\mathcal{H}^*$ is the conjugate space while its action on an $f : \mathcal{H} \to \mathcal{H}'$ is $f \mapsto (f)_* = f : \mathcal{H}^* \to \mathcal{H}'^*$; indeed, by definition of the scalar product in the conjugate space, this ensures that $(f_*)^* = (f^*)_* = f^\dagger$.

Remark 5.2.7 From this example, we can see that in a category of quantum structure, we have a notion of inner product given through the counit and the †-structure. This underlines a fundamental difference between compact categories and categories of quantum structures which is crucial for our purposes.

Remark 5.2.8 The counit $\epsilon_{\mathcal{H}}$ and the unit $\eta_{\mathcal{H}}$ are basis independent. For instance, the unit is the image of $1_{\mathcal{H}}$ under the natural isomorphism

$$\mathbf{FdHilb}(\mathcal{H}, \mathcal{H}) \simeq \mathbf{FdHilb}(\mathbb{C}, \mathcal{H}^* \otimes \mathcal{H}).$$

Remark 5.2.9 The reader may wonder why we didn't define the notion of quantum structures for the whole category **Hilb**. First, such a definition is irrelevant in the context of quantum computation albeit a very interesting question in general. Second, this is a very subtle issue. For results in that direction, we refer the reader to [3].

Example 5.2.10 [5,35] We will specify the notion of quantum structure in **Rel**. Since we defined **Rel** as a "non-strict" symmetric monoidal category, we will give the non-strict definition of compact and quantum structure so that we can proceed with this non-strict case.

Take $X^* = X$ for any $X \in |\mathbf{Rel}|$ making the objects self dual. Define

- The counit of any $X \in |\mathbf{Rel}|$ as:

$$\epsilon_X : X \otimes X \to \{*\} := \{((x,x),*) \mid x \in X\}$$

- and the unit as the converse relation of ϵ_X *i.e.*:

$$\eta_X : \{*\} \to X \otimes X := \{(*,(x,x)) \mid x \in X\}$$

We show that these morphisms make

$$\begin{tikzcd}
X \arrow[r, "\rho_X"] \arrow[d, "1_X"'] & X \otimes \{*\} \arrow[r, "1_X \otimes \eta_X"] & X \otimes (X \otimes X) \arrow[d, "\alpha"] \\
X & \{*\} \otimes X \arrow[l, "\lambda_X^{-1}"] & (X \otimes X) \otimes X \arrow[l, "\epsilon_X \otimes 1_X"]
\end{tikzcd}$$

—the non-strict analogue of the diagram given in (5.2)—and its dual both commute:

a) The composite

$$(1_X \otimes \eta_X) \circ \rho_X : X \to X \otimes (X \otimes X)$$

is the set of tuples $\{(x,(x',(x'',x''')))\} \subseteq X \otimes (X \otimes (X \otimes X))$ such that there exists an $(x'''',*) \in X \otimes \{*\}$ with $x\rho_X(x'''',*)$ and $(x'''',*)1_X \otimes \eta_X(x',(x'',x'''))$. By definition of ρ, 1_X and the product of relations, this entails that x, x'''' and x' are all equal. Moreover, by definition of η_X and the product of relation, we have that x'' and x''' are equal. Thus,

$$(1_X \otimes \eta_X) \circ \rho_X := \{(x,(x,(x',x'))) \mid x,x' \in X\}.$$

b) We compute the composite

$$\alpha \circ ((1_X \otimes \eta_X) \circ \rho) : X \to (X \otimes X) \otimes X.$$

By definition of α, it is directly seen that

$$\alpha \circ ((1_X \otimes \eta_X) \circ \rho) := \{(x,((x,x'),x') \mid x,x' \in X\}$$

c) Again, the composite

$$(\epsilon_X \otimes 1_X) \circ (\alpha \circ (1_X \otimes \eta_X) \circ \rho) : X \to \{*\} \otimes X$$

is a set of tuples $\{(x,(*,x'))\} \subseteq X \otimes (\{*\} \otimes X)$ such that there exists an $((x'',x'''),x^{iv}) \in (X \otimes X) \otimes X$ with $x(\alpha \circ (1_X \otimes \eta_X) \circ \rho)((x'',x'''),x'''')$ and $((x'',x'''),x'''')(\epsilon_X \otimes 1_X)(*,x')$. By the computation in b), $x = x''$ and $x''' = x''''$. By definition of ϵ_X, 1_X and the product of relations, $x'' = x'''$ and $x'''' = x'$. All this together yields $x = x'' = x''' = x'''' = x'$ and hence,

$$(\epsilon_X \otimes 1_X) \circ (\alpha \circ (1_X \otimes \eta_X) \circ \rho) := \{(x,(*,x)) \mid x \in X\}.$$

d) The last step is trivial. Composing the previous composite with λ_X^{-1} yields a morphism of type $X \to X$ defined as

$$\lambda_X^{-1} \circ (\epsilon_X \otimes 1_X) \circ \alpha \circ (1_X \otimes \eta_X) \circ \rho := \{(x,x) \mid x \in X\}$$

which is nothing but the relation 1_X as required. Commutation of the dual diagram is done analogously.

These compact structures are quantum structures:

We have to check that for any X,

$$\begin{tikzcd} \{*\} \arrow[r, "\epsilon_X^\dagger"] \arrow[dr, "\eta_X"'] & X \otimes X \arrow[d, "\sigma_{X,X}"] \\ & X \otimes X \end{tikzcd}$$

commute. If $\epsilon_X := \{((x,x),*) \mid x \in X\}$ then $\epsilon_X^\dagger := \{(*,(x,x)) \mid x \in X\}$ and $\sigma \circ \epsilon_X^\dagger = \epsilon_X^\dagger$ which is equal to η_X as required.

Upper- and Lower-star functors: Now, recall that for a relation $R : X \to Y$, $R^\dagger$ is the converse relation of R. Now, $R^* = R^\dagger$; indeed, given a relation $R : X \to Y$, then

$$R^* = (1_X \otimes \epsilon_Y) \circ (1_X \otimes R \otimes 1_Y) \circ (\eta_X \otimes 1_Y) = R^\dagger$$

follows by routine calculations. This makes the functor

$$(-)_* = (-)^{*\dagger} = (-)^{\dagger *} : \mathbf{Rel} \to \mathbf{Rel}$$

an identity.

Remark 5.2.11 Both **Rel** and **FdHilb** are categories of quantum structures thus, we have $A^{**} = A$ for any object in these categories. However, they are not strict: for instance, $(A \otimes B)^* \neq B^* \otimes A^*$. However, since every category of quantum structures is equivalent to a strict category of quantum structures by theorem 5.1.6 we shall assume that categories of quantum structure are strict in what follows.

As was noted in [5], categories of quantum structures come with an abstract version of the inner product and Dirac notation:

Indeed, in $\mathbf{C}_q$ the notion of inner product is given by

$$\langle f | g \rangle := f^\dagger \circ g.$$

for $f, g : I \to A$. From there we can show many known identities which remain true in the general case. For instance; let $\psi : I \to A$, $\phi : I \to B$ and $f : B \to A$, then

$$\begin{aligned} \langle f^\dagger \circ \psi | \phi \rangle &= (f^\dagger \circ \psi)^\dagger \circ \phi \\ &= \psi^\dagger \circ f \circ \phi \\ &= \langle \psi | f \circ \phi \rangle. \end{aligned}$$

Also, we can show that unitary transformations preserve the inner product. Indeed, let $\psi, \phi : I \to A$ and $U : A \to A$ be unitary, then

$$\begin{aligned}\langle U \circ \psi | U \circ \phi \rangle &= \langle U^\dagger \circ U \circ \psi | \phi \rangle \\ &= \langle \psi | \phi \rangle.\end{aligned}$$

It remains to generalise Dirac notation by defining

$$\langle \psi | f | \phi \rangle := \langle f^\dagger \circ \psi | \phi \rangle = \langle \psi | f \circ \phi \rangle.$$

Thus, many notions we defined in chapter 2 are recovered in categories of quantum structures.

Example 5.2.12 We can define an abstract ket in **Rel** as a relation $|\psi\rangle : \{*\} \to X$; the type of such a ket is similar to the kets in **FdHilb** as it has for domain the tensor unit and any object for codomain. A $|\psi\rangle$ in **Rel** is a set of tuples of the form $\{(*, x) \mid * \, \psi \, x\}$. An abstract bra is defined as the adjoint of some ket, *i.e.*, a set of tuples of the form $\langle \psi | := \{(x, *) \mid * \, \psi \, x\}$. We can also form an abstract inner product therein: for $\psi, \phi : \{*\} \to X$,

$$\langle \phi | \psi \rangle = \mathbf{1} \text{ if } |\phi\rangle \cap |\psi\rangle \neq \emptyset \qquad \text{and} \qquad \langle \phi | \psi \rangle = \mathbf{0} \text{ if } |\psi\rangle \cap |\phi\rangle = \emptyset$$

where $\mathbf{0}$ and $\mathbf{1}$ are the two scalars in $\mathbf{Rel}(I, I)$—see example 4.6.1.

In conclusion, a category of quantum structures is sufficiently rich to abstract the following concepts [5]:

- Pure states as morphisms of type $\psi : I \to A$.
- Pure costates as adjoints of pure states *i.e.*, $\psi^\dagger : A \to I$.
- The notion of an inner product via the composition of states and costates: $\phi^\dagger \circ \psi := \langle \phi | \psi \rangle$. From this, a state is *normalised* if $\psi^\dagger \circ \psi = 1_I$.
- Via the first three and the dagger, the notion of adjoints:

$$\langle \phi | f \circ \psi \rangle = \phi^\dagger \circ (f \circ \phi) = (\phi^\dagger \circ f) \circ \phi = (f^\dagger \circ \phi)^\dagger \circ \psi = \langle f^\dagger \circ \phi | \psi \rangle$$

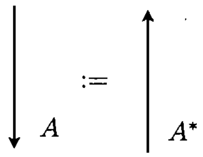
- The notion of unitary maps as morphisms such that $U^\dagger = U^{-1}$.
- The notion of bipartite entanglement via the coparings of the quantum structure, *i.e.*, $\eta_A : I \to A^* \otimes A$.
- The notion of observable as self-adjoint morphisms, *i.e.*, $f = f^\dagger$.

5.3 Graphical calculus for categories of quantum structures

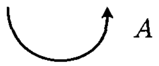
We now enrich the graphical calculus for †-monoidal categories to categories of quantum structure. Technically speaking, we should perhaps give the graphical calculus for compact categories first and the graphical calculus for categories of quantum structures after since the latter is built upon the former. However, since we won't use the graphical calculus for compact categories, we will give both at once.

The graphical calculus for monoidal categories has been extended to compact categories by Joyal and Street in [52] and the graphical calculus for categories of quantum structures has been formalised by P. Selinger in [68]. In order to be able to depict an expression from the language of categories of quantum structures in the graphical language, we must add the following building blocks:

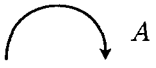
- The identity of the dual A^* of A is represented as:



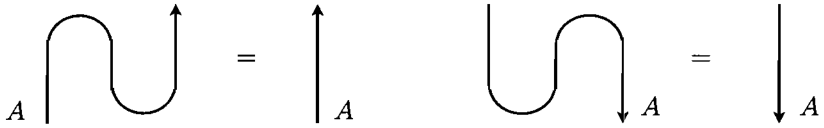
- Given an object A, the unit $\eta_A : I \to A^* \otimes A$ and the counit $\epsilon_A : A \otimes A^* \to I$ of the compact structure are represented respectively as



and

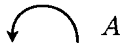


The defining equations of the compact structure then depict as

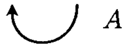


hence, we can straighten the wires.

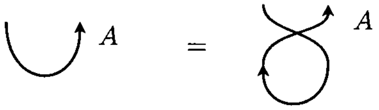
- For any $A \in |\mathbf{C}|$, the adjoints of the units and counits of the compact structure *i.e.*, $\eta_A^\dagger : A^* \otimes A \to I$ and $\epsilon_A^\dagger : I \to A \otimes A^*$ depict as



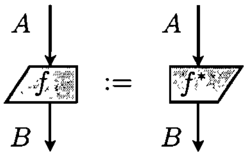
and



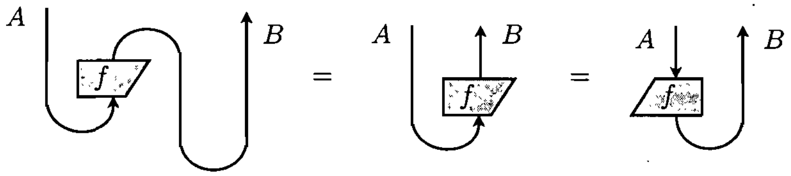
respectively. The constraint equation $\sigma_{A,A^*} \circ \epsilon_A^\dagger = \eta_A$ on the unit of a quantum structure depicts as



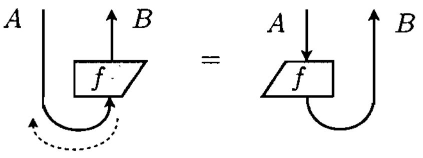
- Given a morphism $f : A \to B$, its transpose $f^* : B^* \to A^*$ depicts as



Recall that an arrow with downward orientation is the identity on the dual object. Now, the reason for this orientation with respect to the sharp side of the trapezoid is best understood via

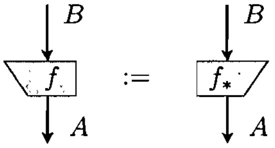


where for the first equality one just uses the compactness relations and yanks the wire, while the second equality is obtained from the leftmost expression via the definition of f^*. Thus, the orientation is taken from the idea that while sliding the box along the wires, we get



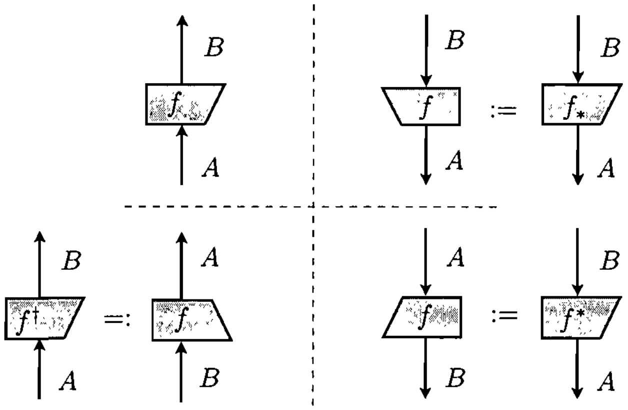
The graphical notation is then just an extension of the fact that we can slide boxes along wires. The orientation of the trapezoid keeps track of whether we have f or f^*. From this, we also see that the graphical representation of f^* is a rotation by 180° of the graphical representation for f.

- Finally, given an f as above, its conjugate $f_* : A^* \longrightarrow B^*$ depicts as



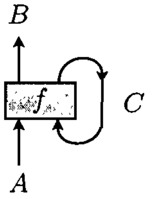
Again, such an orientation for the trapezoid is taken from the definition $(-)_* := (-)^{\dagger *}$ using an analogue argument as for the transpose.

Remark 5.3.1 Thus, all in all, given an $f : A \longrightarrow B$ in **C**, the graphical representations for f^*, f_* and $f^\dagger$ are given [5,4,50] and [68]:



which captures the equation $(-)^*_* = (-)^\dagger$ and other variations.

Example 5.3.2 The canonical trace (c.f. lemma 5.2.5) of an $f : A \otimes C \longrightarrow B \otimes C$ depicts as



Finally, these additions still provide a graphical calculus coherent with the language of categories of quantum structures:

Theorem 5.3.3 [68] A well-typed equation between morphisms in the language of categories of quantum structures follows from the axioms of the categories of quantum structures if and only if it holds up to graph isomorphism in the graphical language.

Proof: See [68].

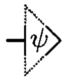
□

Graphical notations

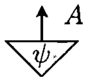
We now introduce a few more graphical notations that will be used later:

A *state* or an *abstract ket* is a morphism $\psi : I \longrightarrow A$ and is depicted as

$|\psi\rangle \quad \rightsquigarrow$



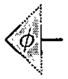
$\rightsquigarrow$



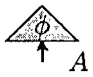
.

A *co-state* or *abstract bra* is a morphism $\phi : A \longrightarrow I$ which depicts as

$\langle\phi| \quad \rightsquigarrow$

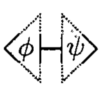


$\rightsquigarrow$

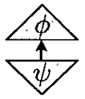


Moreover, one can compose a state with a co-state and obtain a scalar—a morphism $I \longrightarrow I$—as

$\langle\phi|\psi\rangle \quad \rightsquigarrow$

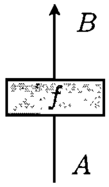


$\rightsquigarrow$



Thus, not only can we abstract Dirac notation in a category of quantum structures, but our representation of states within the graphical calculus for monoidal categories also allows such an abstraction in a clear visual way. Of course, in adopting this notation, we lose the asymmetrical notation introduced for general morphisms. However, the transpose or the conjugate of a given state can still be identified via the orientation of the wires along with the identification ψ_* or ψ^* in the triangles. We will do analogously for scalars.

Remark 5.3.4 In the following sections and chapters, there might be some places where it would be odd to orient the boxes for reasons that will be obvious then. In such cases, we may use a rectangular box to depict $f : A \longrightarrow B$ as in



5.4 The category $\mathbf{CP}(\mathbf{C}_q)$ of completely positive maps

The purpose of this section is to introduce the category of completely positive maps of a category of quantum structures as given in [68]. As superoperators are completely positive applications with some normalisation condition, a category of completely positive maps provides us with the right context to handle not only these but also density matrices that will be described as morphisms of type $I \longrightarrow A$. All categorical definitions and results from this section are taken from [68] with perhaps minor modifications; the reader is referred there for proofs and a complete introduction to the subject.

As a starting point, we know that a mixed state in **FdHilb** is a self-adjoint—or positive—operator $\rho : \mathcal{H} \longrightarrow \mathcal{H}$ of unit trace. Let us relax the normalisation condition, then—according to the spectral theorem [61]—a positive operator is an operator for which there exists a basis where the operator is diagonal with only non-negative entries *i.e.*:

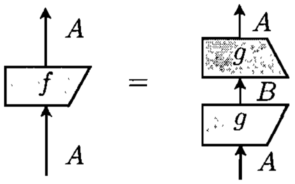
$$\rho = U^{\dagger} \circ \Lambda \circ U$$

where Λ is a diagonal matrix with non-negative entries and U is a unitary transformations. We can take the square root of Λ and obtain

$$\begin{aligned}\rho &= U^{\dagger} \circ \Lambda^{1/2} \circ \Lambda^{1/2} \circ U \\ &= (\Lambda^{1/2} \circ U)^{\dagger} \circ (\Lambda^{1/2} \circ U) \\ &= g^{\dagger} \circ g.\end{aligned}$$

Now, lifting this notion to a category of quantum structures we get

[Positive morphism] A morphism $f : A \to A$ in $\mathbf{C}_q$ is *positive* if it factors as a composition of the form $g^{\dagger} \circ g$ for some $g : A \to B$. That is:



We have the following

Lemma 5.4.1 Let $f : A \to A$ and $g : B \to B$ be positive in $\mathbf{C}_q$, then

a. For any $h : C \to A$, $h^{\dagger} \circ f \circ h$ is positive,

b. For any $A \in \mathbf{C}$, 1_A is positive,

c. The tensor product $f \otimes g$ is positive,

d. $f^{\dagger} = f$ and

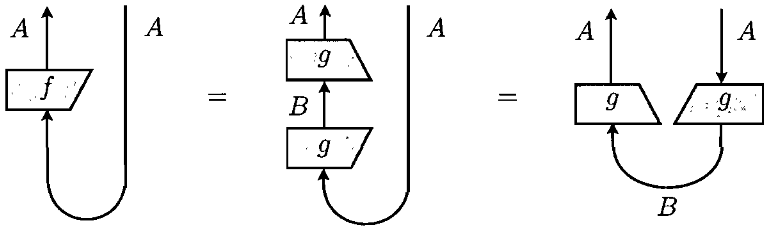
e. The morphism $f^* : A^* \to A^*$ is positive.

Proof: See [68].

□

In quantum computing, a superoperator F is usually given in its Kraus decomposition with components in $\{A_i\}_i$. When composing such an operator with a density operator, we obtain a composite of the form $\sum_i A_i^{\dagger} \rho A_i$. This is a correct point of view but, for our purpose, instead of seeing density operators as maps of type $\mathcal{H} \to \mathcal{H}$—which is the point of view taken when working with Kraus operators—, we will see them as maps of type $\mathbb{C} \to L(\mathcal{H})$. Adopting such a type system, superoperators becomes maps of type $F : L(\mathcal{H}) \to L(\mathcal{H}')$ so that the composite $F \circ \rho$ makes sense. Such a change of point of view is given by the following operation in $\mathbf{C}_q$:

Given a positive $f : A \to A$ and considering the composite $(f \otimes 1_A) \circ \eta_A$, we have



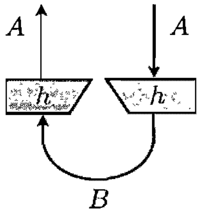
The category $\mathbf{CP}(\mathbf{C}_q)$ of completely positive maps

This indeed recasts the positive morphism f as a map of type $I \longrightarrow A \otimes A^*$ in $\mathbf{C}_q$. From where,

[**Positive element**] A *positive element*[7] in $\mathbf{C}_q$ is morphism $\rho : I \longrightarrow A \otimes A^*$ for which there exists a $B \in |\mathbf{C}_q|$ and an $h : B \longrightarrow A$ such that

$$\rho = (h \otimes h_*) \circ \eta_B$$

that is, graphically,



Of course, the given depiction of a positive element is obtained from the one before the definition setting $h = g^\dagger$.

As we relaxed the normalisation condition for density operators, we also do so for superoperators. That is, a superoperator is a completely positive operator normalised in such a way that it applies density operators to density operators (see chapter 2). Relaxing the normalisation condition means that we will categorify only the notion of complete positivity. Recall that a linear map $F : L(\mathcal{H}) \longrightarrow L(\mathcal{H}')$ is *completely positive* if

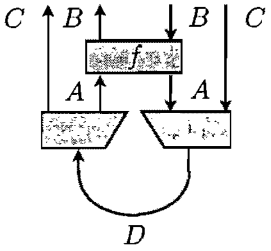
1. $F(f)$ is positive for all $f \geq 0$ and
2. $[F \otimes 1_{L(\mathcal{H})}](f)$ is positive for all $\mathcal{H}$ and $f \geq 0$.

The two notions are recast in $\mathbf{C}_q$ as the notion of

[**Completely positive map**] A morphism $f : A \otimes A^* \longrightarrow B \otimes B^*$ in $\mathbf{C}_q$ is *completely positive* if for all $C \in |\mathbf{C}_q|$ and all positive elements

$$I \simeq I \otimes I^* \longrightarrow C \otimes A \otimes A^* \otimes C^*,.$$

the composite



is positive.

A characterisation of completely positive maps in linear algebra is given by

Theorem 5.4.2 [**Choi's theorem**] [21] The linear map $f : \mathbb{C}^{n\times n} \longrightarrow \mathbb{C}^{m\times m}$ is completely positive if and only if the matrix $(f(E_{ij}))_{ij} : \mathbb{C} \rightarrow \mathbb{C}^{nm\times nm}$ is positive. There, E_{ij} is a $n \times n$ matrix with zero's everywhere except at the entry ij where it is 1.

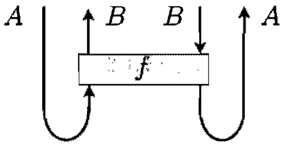
[7] In [68], such a morphism is called a *positive matrix*.

Proof: See [21].

□

An abstract analogue of this theorem is

Theorem 5.4.3 A morphism $f : A \otimes A^* \to B \otimes B^*$ in $\mathbf{C}_q$ is completely positive if and only if



is a positive element.

Proof: See [68].

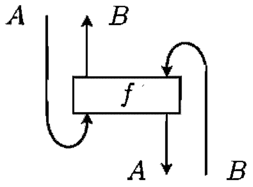
□

Using this result in conjunction with the definition of completely positive maps, one can show using the graphical calculus the following result:

Corollary 5.4.4 The following are equivalent:

a. The morphism $f : A \otimes A^* \to B \otimes B^*$ is completely positive.

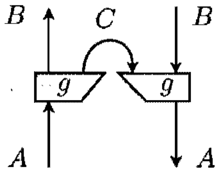
b. The morphism



is positive.

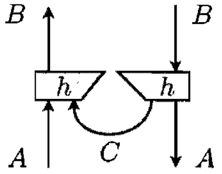
c. There exists an object C and a morphism $g : A \to B \otimes C$ such that

f =



d. There exists an object C and a morphism $h : C \otimes A \to B$ such that

f =



Proof: See [68].

□

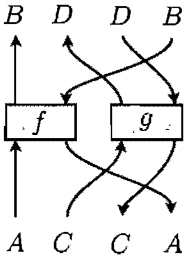
We also have the following

Lemma 5.4.5

1. For any $A \in |\mathbf{C}_q|$, the identity map $1_{A \otimes A^*}$ is completely positive.

2. The composition of completely positive maps is completely positive.

3. If $f : A \otimes A^* \to B \otimes B^*$ and $g : C \otimes C^* \to D \otimes D^*$ are completely positive then



is completely positive.

4. For any $f \in \mathbf{C}$, $f \otimes f_*$ is completely positive.

Proof: See [68].

□

This lemma tells us, in particular, that the collection of completely positive maps satisfies the axioms of a category. Following this,

[$\mathbf{CP}(\mathbf{C}_q)$ construction] Given a category of quantum structures $\mathbf{C}_q$, define a new category $\mathbf{CP}(\mathbf{C}_q)$ whose objects are the same as the objects of $\mathbf{C}_q$. A morphism $f : A \to B$ in $\mathbf{CP}(\mathbf{C}_q)$ is a completely positive map $f : A \otimes A^* \to B \otimes B^*$ in $\mathbf{C}_q$. Composition of morphism is as in $\mathbf{C}_q$.

Lemma 5.4.6 The mapping $F : \mathbf{C}_q \to \mathbf{CP}(\mathbf{C}_q)$ given by $F(A) = A$ and $F(f) = f \otimes f_*$ is functorial.

Proof: That it preserves the identity is evident. That it preserves composition is given by bifunctoriality of the tensor in $\mathbf{C}_q$ and functoriality of $(-)_*$. Indeed, since $F(g \circ f)$ is $(g \circ f) \otimes (g \circ f)_*$ in $\mathbf{C}_q$, we get

$$(g \circ f) \otimes (g \circ f)_* = (g \circ f) \otimes (g_* \circ f_*) = (g \otimes g_*) \circ (f \otimes f_*)$$

which is $F(g) \circ F(f)$. Hence we conclude that F is indeed a functor.

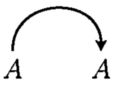
□

Theorem 5.4.7 The category $\mathbf{CP}(\mathbf{C}_q)$ is again a category of quantum structures. The tensor product on objects is inherited from $\mathbf{C}_q$, on morphisms it is given by lemma 5.4.5-3. The natural isomorphism $\sigma^{\mathbf{CP}(\mathbf{C}_q)}$, the units and counits of the quantum structures are given by their respective images under F. If $f : A \otimes A^* \to B \otimes B^*$ is in $\mathbf{CP}(\mathbf{C}_q)$, then $f^\dagger$ in $\mathbf{CP}(\mathbf{C}_q)$ is given by $f^\dagger : B \otimes B^* \to A \otimes A^*$ in $\mathbf{C}_q$. The functor $F : \mathbf{C}_q \to \mathbf{CP}(\mathbf{C}_q)$ preserves the quantum structures.

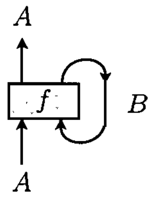
Proof: See [68].

□

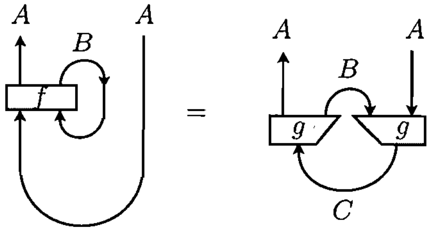
Now, a few remarks are required. First, for any $A \in |\mathbf{CP}(\mathbf{C}_q)|$, the map $tr_A : A \to I$ corresponding to the completely positive map ϵ_A in $\mathbf{C}_q$



is, of course, no longer the counit of the quantum structure on A. In fact, it can be thought of as a (perhaps partial) trace over positive elements. Indeed, start with a positive map $f : A \otimes B \longrightarrow A \otimes B$ in $\mathbf{C}_q$. Then, its partial trace (via the canonical trace) over B is given by

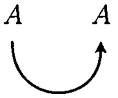


Applying the construction we gave for positive elements yields

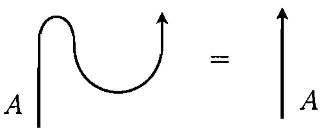


from which it is seen that the trace of a morphism in $\mathbf{C}_q$ becomes the morphism tr_B in $\mathbf{CP}(\mathbf{C}_q)$ and this, because of the particular form of the morphism of $\mathbf{CP}(\mathbf{C}_q)$ as morphisms in $\mathbf{C}_q$. It is a remarkable fact that the trace is no longer an operation on homsets but rather a morphism within the category $\mathbf{CP}_q(\mathbf{C})$. In that sense, one could say that the $\mathbf{CP}(\mathbf{C}_q)$ construction "internalises" the trace[8].

Next, for any $A \in |\mathbf{CQ}_q(\mathbf{C})|$, the element $m_A : I \longrightarrow A$ corresponding to the completely positive map η_A in $\mathbf{C}_q$ *i.e.*,

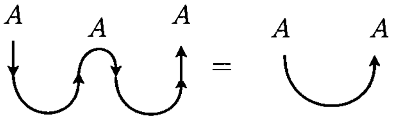


can be thought of as an unnormalised form of completely mixed state. Indeed, reversing the construction we gave for positive elements, *i.e.*,



yields the identity which, in $\mathbf{CP}(\mathbf{FdHilb})$, is the completely mixed state up to a normalisation factor. Interestingly enough, we have seen in chapter 2 that a maximally entangled state is a bipartite entangled state $\psi : \mathbb{C} \longrightarrow \mathcal{H} \otimes \mathcal{H}$ such that its partial trace over either of the two $\mathcal{H}$ in its codomain is the completely mixed state. Interpreting $\eta_A : I \longrightarrow A^* \otimes A$ as an unnormalised Bell state—an instance of maximally entangled state—its partial trace over A yields

[8] Some unsuccessful attempts have been made by Yannick Delbecque, Prakash Panangaden and myself to give a proper axiomatisation of the notion of internal trace as originally suggested by Y. Delbecque. The main problem is that the dinaturality of the usual trace seems to have no common analogue in the context of internal traces. Thus, the attempted axiomatisations are simply too degenerate to give any conclusive results. This remains an interesting open question.



which is m_A, our unnormalised maximally mixed state.

Remark 5.4.8 The reader may have noticed that when depicting a morphism of $\mathbf{CP}(\mathbf{C}_q)$, we do so with respect to the completely positive map in $\mathbf{C}_q$. From now on and without further remark we will always do so and that in $\mathbf{CP}(\mathbf{C}_q)$ as well as in other categories that we will define in the following chapters. Since we always work "relative to" a category of quantum structures, such a depiction will always make sense.

In conclusion, $\mathbf{CP}(\mathbf{C}_q)$ is rich enough to abstract the following concepts:

- Since $\mathbf{CP}(\mathbf{C}_q)$ is a category of quantum structures, we recover the concepts of pure states and costates, bipartite entangled states and unitary transformation in $\mathbf{CP}(\mathbf{C}_q)$ as their respective images under the functor $F : \mathbf{C} \to \mathbf{CP}(\mathbf{C}_q)$. As an example, a pure state $\psi : I \to A$ in $\mathbf{CP}(\mathbf{C}_q)$ is a completely positive map $\psi \otimes \psi_* : I \otimes I^* \to A \otimes A^*$ in $\mathbf{C}_q$ *mutans mutandis* for pure costates, bipartite entangled states and unitary transformations.

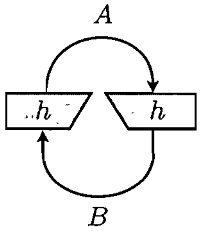
- If ρ is a positive element, then $tr \circ \rho$ is a categorical analogue of the trace norm.

- Mixed states are normalised elements of type $I \to A$,

- Superoperators are normalised completely positive maps $f : A \to B$.

Normalisation conditions are now depicted with respect to the trace. Indeed, a positive element $\rho : I \to A$ is normalised if

$tr_A \circ \rho$ =

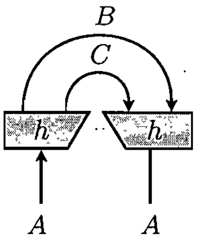


=

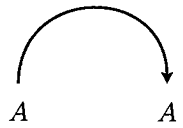
that is, if it is equal to the empty picture, the identity 1_I.

A completely positive map $f : A \to B$ is normalised and hence, a superoperator, if

$tr_B \circ f$ =

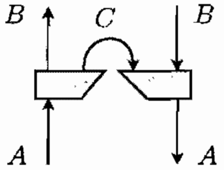


=

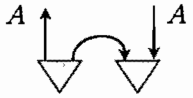


which is an abstract analogue of the normalisation condition contained in the Kraus decomposition of a superoperator. Note that in what follows, we will not assume that everything is normalised. As we work mainly at the level of the structures, such an assumption would be too restrictive for our purposes.

Remark 5.4.9 We introduced many different notations for completely positive maps. Unless otherwise specified, a completely positive map will be depicted as



and a positive element of $\mathbf{CP}(\mathbf{C}_q)$ as



6 Basis structures and classical maps

In the last chapter, we introduced the quantum fragment of our theory. Although it can stand alone, it will be handy to introduce the notion of classical data in order to speak of measurements and controlled operations. Before we can do so, we need to introduce an abstract analogue of the basis. Indeed, as we shall see in the last section of this chapter, the notion of classical morphism in **FdHilb** coincides with matrices with entries in the involutive semiring $\mathbb{R}_+$. Of course, to isolate such morphisms one needs first to equip objects with a basis so that the very notion of classical morphism makes sense. Thus, the purpose of this chapter is to introduce the concept of basis structure and of classical morphisms. To do so, building upon the work of B. Coecke and D. Pavlovic in [36] we will equip some objects of $\mathbf{C}_q$ with a †-Frobenius structure. Such structures are, in **FdHilb**, in one-to-one correspondence with orthonormal bases as was shown by Coecke, Pavlovic and J. Vicary in [38]. Further, we will define the notion of basis structure, whose specification corresponds in **FdHilb** to a choice of basis. Such a basis structure consists of the initial quantum structure of an object in addition to a †-Frobenius structure which makes the object self-dual; thus, the object now come with two perhaps distinct duals, one of which is the object itself. Duals being unique up to a unique unitary transformation, we will make this unitary transformation between the object and its dual explicit. We will then restrict ourselves to the category of basis structure where each object now comes with these two structures and study its properties. Finally, we will define the notion of classical map, inspect the properties of such morphisms and define a category of classical maps which defines the classical fragment of the theory. These results are taken from [34] which the author wrote with B. Coecke and S. Perdrix.

In addition, sections 2 and 4 of this chapter states two important results of reduction in normal form for a particular type of morphism involving the structural witnesses of the †-Frobenius and the basis structures.

6.1 †-Frobenius structures

Discussion aside, most of the results given in this section are taken from [36] with appropriate changes to fit our context. Other works will be cited as needed.

Quantum information is subject to two important theorems, that is: the no-cloning [77] and the no-deleting [64] theorems, in contrast with classical information which can generally be duplicated and deleted. Consider the following two cases where we have an interface between classical and quantum data:

1. A quantum state is measured with an apparatus: the state undergoes a change, but also, the apparatus indicates the result of the measurement. Hence, the type of a quantum measurement is

   $$\text{Initial quantum state} \ \longrightarrow\ \text{Final quantum state} \otimes \text{Classical output.}$$

   where the classical output is correlated with the final quantum state.

2. A set of transformations $\{U_i\}$ can be applied to a quantum state: The type of such an operation is

   $$\text{Initial quantum state} \otimes \text{Choice of transformation} \ \longrightarrow\ \text{Final quantum state.}$$

In fact, these two operations—when taken in **FdHilb** and once we have chosen an orthonormal basis $\{|i\rangle\}$ for the measurement—can be written as

$$|\psi\rangle = \sum_i \langle i|\psi\rangle|i\rangle \mapsto \sum_i \langle i|\psi\rangle|i\rangle \otimes |i\rangle_c \qquad \text{and} \qquad |\psi\rangle \otimes |i\rangle_c \mapsto U_i|\psi\rangle$$

respectively. There, we used the subscript c to denote classical data.

Remark 6.1.1 The operation on the left is not quite a measurement, as the system is still in coherent superposition, but it illustrates enough for our actual purpose, that is:

In the context of Hilbert spaces, we will consider basis vectors as classical data.

Following this, it is possible to define operators in **FdHilb** that will take care both of copying and deleting of classical states. Indeed, let $\{|i\rangle\}_i$ be the canonical basis for $\mathbb{C}^n \in |\textbf{FdHilb}|$. Then,

1. Any $|\phi\rangle \in \{|i\rangle\}_i$ is duplicated by the isometry

   $$\delta_{\mathbb{C}^n} := \sum_i |ii\rangle\langle i| : \mathbb{C}^n \to \mathbb{C}^n \otimes \mathbb{C}^n.$$

   It is important to stress that such an isometry *does not* duplicate all $|\psi\rangle \in \mathbb{C}^n$ thus, it is *not* a cloning machine.

2. Any $|\phi\rangle \in \{|i\rangle\}_i$ is deleted by the operator

   $$\mu_{\mathbb{C}^n} := \sum_i \langle i| : \mathbb{C}^n \to \mathbb{C}.$$

   Again, such an operator is not a deleting machine.

Remark 6.1.2 For the remainder of the discussion, we will drop the subscript $\mathbb{C}^n$ for δ and μ in order to lighten the notation.

These two morphisms together satisfy the operational properties we would expect from them, that is:

a. If we duplicate some data and erase either one of the two outputs, it is the same as doing nothing. This is:

$$(\mu \otimes 1) \circ \delta = (1 \otimes \mu) \circ \delta = \sum_i |i\rangle\langle i| = 1.$$

b. If we duplicate some data, then duplicating either of the two outputs is the same. This is:

$$(1 \otimes \delta) \circ \delta = (\delta \otimes 1) \circ \delta = \sum_i |iii\rangle\langle i|.$$

c. If we duplicate some data, then swap the outputs, it is the same as just duplicating the data. This is:

$$\sigma \circ \delta = \left(\sum_{i,j} |ji\rangle\langle ij|\right) \circ \left(\sum_k |kk\rangle\langle k|\right) = \sum_i |ii\rangle\langle i|.$$

Such equations precisely state that $\langle \mathbb{C}^n, \delta, \mu\rangle$ is an internal cocommutative comonoid in the category **FdHilb**. Since this category comes equipped with a dagger, not only $\delta^\dagger$ and $\mu^\dagger$ are defined but the triple $\langle \mathbb{C}^n, \delta^\dagger, \mu^\dagger\rangle$ is an internal commutative monoid, the defining equations of the later being dual to those of the former. The defining morphisms of this monoid can be interpreted as follows:

1. $\delta^\dagger$ stands for comparing as

$$(|i\rangle \otimes |i'\rangle) \circ \delta^\dagger = \begin{cases} |i\rangle & \text{if } i = i' \\ \mathbf{0} & \text{if } i \neq i' \end{cases}$$

where $\mathbf{0}$ is the zero vector of $\mathbb{C}^n$.

2. $\mu^\dagger$ is an unnormalised generalisation of the vector $|+\rangle$ to arbitrary dimensions, hence, some quantum analogue of a completely random state.

Finally, the morphisms δ and $\delta^\dagger$ together satisfies the following two equations:

1. δ has for left-inverse $\delta^\dagger$ *i.e.*:

$$\delta^\dagger \circ \delta = 1$$

2. They satisfy the *Frobenius condition* that is

$$(\delta^\dagger \otimes 1) \circ (1 \otimes \delta) = (1 \otimes \delta^\dagger) \circ (\delta \otimes 1) = \delta \circ \delta^\dagger = \sum_i |ii\rangle\langle ii|.$$

These two conditions together with the defining equations of the monoid and the comonoid say that the quintuple

$$\langle \mathbb{C}^n, \delta, \delta^\dagger, \mu, \mu^\dagger\rangle$$

is a †-*Frobenius structure* in **FdHilb**, a concept that we will formally define below. The justification for such a structure is given by the following

Theorem 6.1.3 [38] There is a one-to-one correspondence between †-Frobenius structures and orthonormal bases in **FdHilb** which is established by the equations

$$\delta_{\mathcal{H}} : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}; |i\rangle \mapsto |ii\rangle \quad \text{and} \quad \mu_{\mathcal{H}} : \mathcal{H} \to \mathbf{C}; |i\rangle \mapsto 1.$$

From which we see that †-Frobenius structures truly axiomatise the notion of orthonormal basis.

Proof: See [38].

□

[**†-Frobenius structure**] A *†-Frobenius structure* in $\mathbf{C}_q$ is a †-Frobenius structure *i.e.*, a quintuple

$$\langle X, \delta_X : X \to X \otimes X, m_X : X \otimes X \to X, \mu_X : X \to I, u_X : I \to X \rangle \tag{6.1}$$

such that

1. $m_X = \delta_X^\dagger$,
2. $u_X = \mu_X^\dagger$,
3. $\langle X, \delta_X, \mu_X \rangle$ is an internal cocommutative comonoid,
4. $\langle X, \delta_X^\dagger, \mu_X^\dagger \rangle$ is an internal commutative monoid,
5. The following diagram defining the *Frobenius condition* commute:

$$\begin{tikzcd}
X \otimes X \arrow[rr, "\delta_X \otimes 1_X"] \arrow[dd, "1_X \otimes \delta_X"'] \arrow[dr, "\delta_X^\dagger"] & & X \otimes X \otimes X \arrow[dd, "1_X \otimes \delta_X^\dagger"] \\
& X \arrow[dr, "\delta"] & \\
X \otimes X \otimes X \arrow[rr, "\delta_X^\dagger \otimes 1_X"'] & & X \otimes X
\end{tikzcd} \tag{6.2}$$

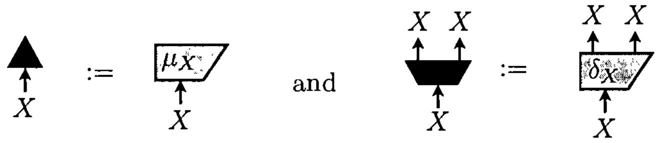
6. Finally, the †-Frobenius object is *special*[9] that is

$$\delta_X^\dagger \circ \delta_X = 1_X. \tag{6.3}$$

Remark 6.1.4 The previous definition could be reduced in length by saying that a †-Frobenius structure is a comonoid $\langle X, \delta_X, \mu_X \rangle$ such that it admits a special Frobenius structure in an obvious way. However, as the notion of Frobenius structure has not been defined elsewhere in this dissertation, we gave this definition so that the notion is at least implicitly defined.

In the graphical language for †-compact categories the notions of the previous definition depict as follows:

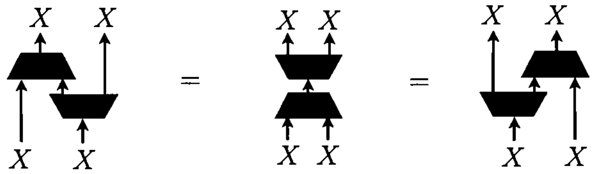
- The comultiplication δ_X and the counit μ_X are depicted as



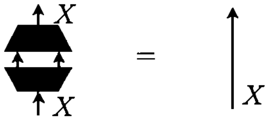
[9] Sometimes called *separable*

respectively.

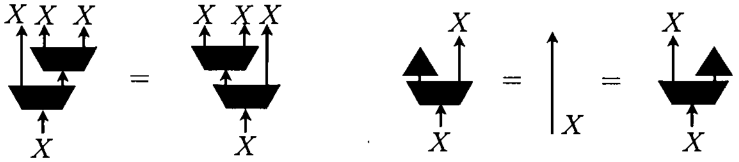
- Using these notations, the Frobenius condition depicts as



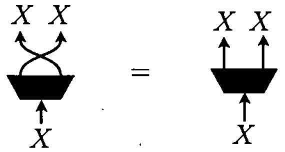
- Speciality as



Since a †-Frobenius structure consists of a monoid and a comonoid, identities defining those can also be translated within the graphical calculus. Coassociativity and counit conditions for the comonoid are depicted respectively as



Cocommutativity depicts as

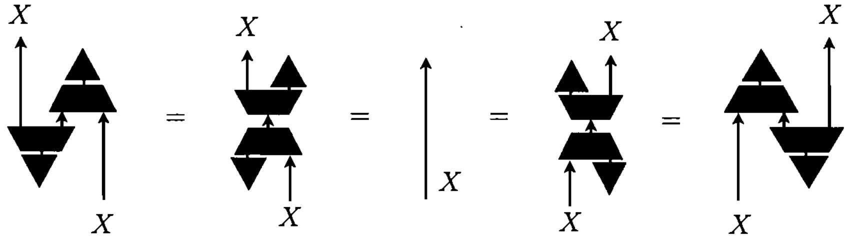


We will not depict the multiplication, the unit, the associativity and the commutativity for the monoid as they are given by "daggering" the preceding pictures *i.e.*, taking the them upside-down while keeping the orientation of the wires.

Proposition 6.1.5 Every †-Frobenius structure $\langle X, \delta_X, \mu_X\rangle$ on $X \in |\mathbf{C}_q|$ induces a quantum structure

$$\langle X, \nu_X\rangle \quad \text{where} \quad \nu_X := \mu_X \circ \delta_X^\dagger : X \otimes X \to I.$$

Proof: We have



Thus, $\langle X, X, \nu_X, \nu_X^\dagger\rangle$ is a compact structure on X. Moreover, by symmetry of the comultiplication, $\sigma_{X,X} \circ \nu_X^\dagger = \nu_X^\dagger$ so that $\langle X, \nu_X\rangle$ is a quantum structure for X.

□

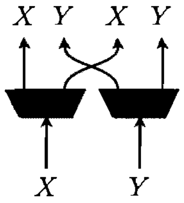
Remark 6.1.6 Note that X is self-dual relative to this quantum structure.

Remark 6.1.7 Since we are working in $\mathbf{C}_q$, the previous proposition concretely says that if an $X \in |\mathbf{C}_q|$ is equipped with a †-Frobenius structure, then there are two (perhaps distinct) quantum structures on X, that is, the one with which X is equipped because it is an object of $\mathbf{C}_q$ and the other one induced by the †-Frobenius structure. We will study what this entails in section 6.3 below.

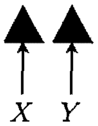
Proposition 6.1.8 If X and $Y \in |\mathbf{C}_q|$ are equipped with a †-Frobenius structure, then so is $X \otimes Y$ with

$$\delta_{X\otimes Y} := (1_X \otimes \sigma_{X,Y} \otimes 1_Y) \circ (\delta_X \otimes \delta_Y) \quad \text{and} \quad \mu_{X\otimes Y} := \mu_X \otimes \mu_Y$$

which depict respectively as



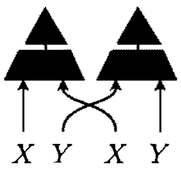
and



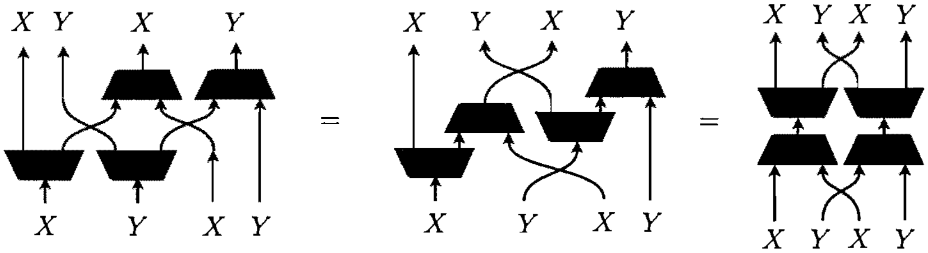
Moreover, the †-Frobenius structure on $X \otimes Y$ induces a quantum structure

$$(X \otimes Y, \nu_{X\otimes Y}) \quad \text{where} \quad \nu_X := \mu_{X\otimes Y} \circ \delta^\dagger_{X\otimes Y} \tag{6.4}$$

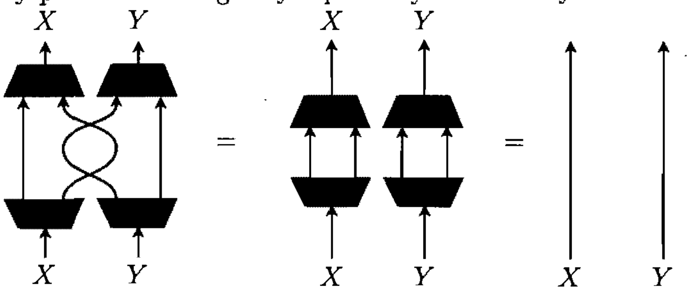
which depicts as



Proof: That $\delta_{X\otimes Y}$ and $\mu_{X\otimes Y}$ define a cocommutative comonoid is immediate using the graphical calculus. That $\delta_{X\otimes Y}$ and $\delta^\dagger_{X\otimes Y}$ satisfy the Frobenius condition is given by

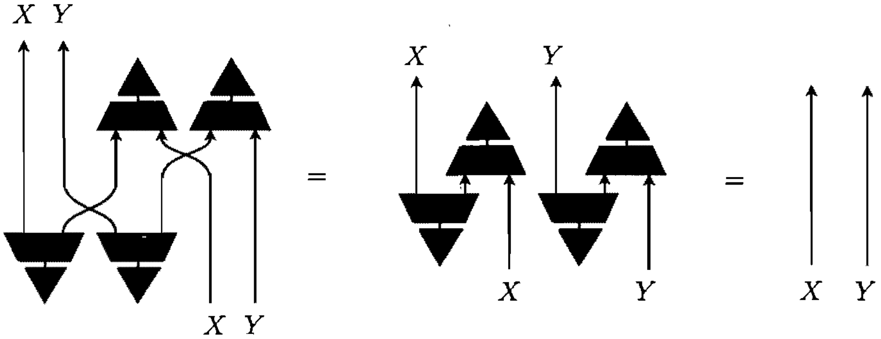


and the other equality proceeds analogously. Speciality is shown by

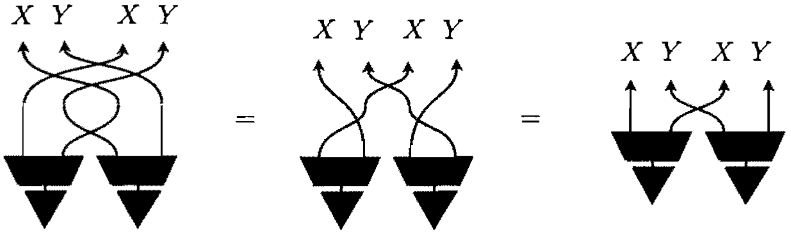


Thus, $(X \otimes Y, \delta_{X\otimes Y}, \mu_{X\otimes Y})$ is a †-Frobenius structure.

To see that $\nu_{X\otimes Y}$ defines a quantum structure, we first show that $\nu_{X\otimes Y}$ together with $\nu^{\dagger}_{X\otimes Y}$ define a compact structure. This is



To see that this compact structure is a quantum structure, we have to verify the constraint equation $\sigma_{X\otimes Y, X\otimes Y} \circ \nu^{\dagger}_{X\otimes Y} = \nu_{X\otimes Y}$. This is the case as



where we obtained the first equality by cancelling the symmetry and the second using the fact that the comultiplication is cocommutative.

□

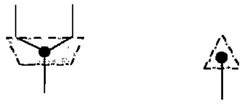
6.2 Normal form

We now provide a normal form result for expressions involving the structural witnesses of the †-Frobenius structure. Such a result is "new" and was published in [31]. The quotation mark around new indicates that we didn't know when we discovered this that an analogue result existed in the context of topological quantum field theories, where Frobenius algebras arise in the 2 dimensional case. It was J. Kock that pointed out this fact by referring us to his book [56]. However, there are enough discrepancies between our presentation and the one given in the cited book to present it here in details. Among these, a formal definition of connectedness, the fact that †-Frobenius structures are special and the details of the proof albeit there [56]—perhaps unsurprisingly—the idea of the proof remains the same.

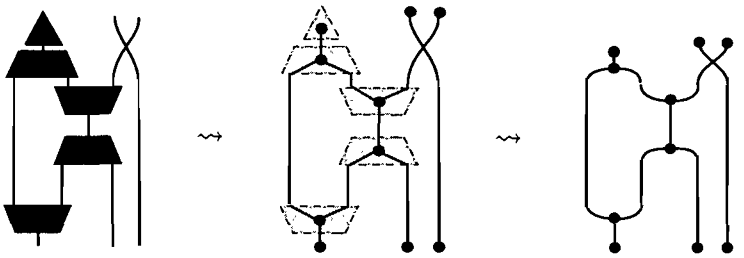
Remark 6.2.1 As †-Frobenius structures on X entail that X is self-dual relative to the quantum structure induced by the †-Frobenius structure and since, the depictions do not take into account X^*, the non-trivial dual of X relative to its quantum structure in $\mathbf{C}_q$, we will drop the arrows from our graphical notation in what follows. Moreover, if our graphical depictions involve only one type, we will not label the wires since there are no risks of confusion.

[Classical network] A *classical network* in $\mathbf{C}_q$ is a morphism obtained by composing terms obtained by tensoring of δ's, μ's (and hence also of ν's) symmetries, identities and their adjoints.

Let us introduce the following notations for δ and μ respectively:



Consider the graphical representation of a classical network f, then by using the notation above, dismissing the gray box and adding black dots to each input and each output, we obtain an undirected graph, the *underlying graph* of f. As an example, consider



Classical network Underlying graph

Clearly, this consists of two connected components. We will build on this intuition to define the notion of

[Connectedness] Let X be a classical object, $X^{\otimes k}$ denote the k-fold monoidal product of X and $X^{\otimes 0} := I$, the monoidal unit. A classical network is *connected* if it is equal to a classical network constructed from the following recursive definition:

[Basic clauses] The morphisms

$$(A1)\ \ 1_X : X \to X,\ (A2)\ \ \delta_X : X \to X \otimes X,\ (A3)\ \ \delta_X^\dagger : X \otimes X \to X,$$
$$(A4)\ \ \mu_X : X \to I \qquad \text{and} \qquad (A5)\ \ \mu_X^\dagger : I \to X$$

are connected classical networks.

[Inductive clauses] If $f : X^{\otimes m} \to X^{\otimes n}$ and $f' : X^{\otimes m'} \to X^{\otimes n'}$ are connected classical networks, $S : X^{\otimes m+m'} \to X^{\otimes m+m'}$ and $S' : X^{\otimes n+n'} \to X^{\otimes n+n'}$ are morphisms obtained by composing and tensoring identities and symmetries then

$$(B1)\ \ (f \otimes f') \circ S \circ (1_{X^{\otimes i}} \otimes \delta_X \otimes 1_{X^{\otimes j}})$$

is connected if

1. i and j are any values such that $i + j + 2 = m + m'$ and

2. δ_X composes with both f and f'; that is, if $\sigma^{(m+m')}_{n,n+1}$ denotes the symmetry applied to the n-th and $n+1$-th then, as a particular case,

$$(f \otimes f') \circ S \circ (\delta_X \otimes 1_{X^{\otimes(m+m'-2)}})$$

is connected if $\sigma^{(m+m')}_{m,m+1} \circ S \circ \sigma^{(m+m')}_{1,2} = S$. This, in fact, connects the first wire to either m or $m+1$ and the second wire to either m or $m+1$ depending which is connected with the first. In the general case described by the clause $(B1)$ we just need to replace $\sigma^{m+m'}_{1,2}$ by $\sigma^{m+m'}_{i,i+1}$ and f by $(f \circ T)$ and f' by $(f' \circ T')$ for some appropriate permutations T and T' so that we connect with the right inputs via an analogue argument.

Also,

Normal form

$$(B2)\quad (1_{X^{\otimes i'}}\otimes\delta_X^\dagger\otimes 1_{X^{\otimes j'}})\circ S'\circ(f\otimes f').$$

is connected if

1. i' and j' are any values such that $i'+j'+2=n+n'$ and
2. Both f and f' composes with $\delta_X^\dagger$; an analogous argument as for $(B1)$ applies.

It remains to handle the cases of a well-defined composition of a connected f with a structural morphism from the †-Frobenius structure. In details, if a classical network

$$f: X^{\otimes m}\to X^{\otimes n}$$

is connected then so are

$$\begin{array}{lll}
(C1)\ f\circ(1_{X^{\otimes i}}\otimes\delta_X\otimes 1_{X^{\otimes j}}), & & (C2)\ (1_{X^{\otimes i'}}\otimes\delta_X\otimes 1_{X^{\otimes j'}})\circ f,\\
(C3)\ f\circ(1_{X^{\otimes i''}}\otimes\delta_X^\dagger\otimes 1_{X^{\otimes j''}}), & & (C4)\ (1_{X^{\otimes i'''}}\otimes\delta_X^\dagger\otimes 1_{X^{\otimes j'''}})\circ f,\\
(C5)\ f\circ(1_{X^{\otimes i}}\otimes\sigma_{X,X}\otimes 1_{X^{\otimes j}}), & & (C6)\ (1_{X^{\otimes i'''}}\otimes\sigma_{X,X}\otimes 1_{X^{\otimes j'''}})\circ f.\\
(C7)\ f\circ(1_{X^{\otimes k}}\otimes\mu_X^\dagger\otimes 1_{X^{\otimes k}}), & \text{and} & (C8)\ (1_{X^{\otimes k'}}\otimes\mu_X\otimes 1_{X^{\otimes l'}})\circ f,
\end{array}$$

For any values of i, j, i', j', i'', j'', i''', j'''. k, l, k' and l'—depending on the clause—such that

$$i+j+2=m,\qquad i'+j'+1=n,\qquad i''+j''+1=m,\qquad i'''+j'''+2=n,$$
$$k+l+1=m\quad\text{or } k'+l'+1=n.$$

[Extremal clause] Nothing else is a connected classical network.

Moreover, a classical network is *totally disconnected* if it is equal to

$$s_1\otimes s_2\otimes\ldots\otimes s_i\otimes\ldots\otimes s_n\quad\text{for }\ n\geq 2\ \text{ and for all } i\qquad s_i\in\{\nu_X,\nu_X^\dagger,\sigma_{X,X},1_X\}$$

where $n\geq 2$. Finally, a classical network which is neither connected nor totally disconnected is *disconnected*.

Remark 6.2.2 We did not include ν_X and $\nu_X^\dagger$ into our definition of connectedness; as these factor as composites $\mu_X\circ\delta_X^\dagger$ and $\delta_X\circ\mu_X^\dagger$ respectively, such an addition would have been redundant.

[Normal form] Let $\delta_0:=\mu_X^\dagger$, $\delta_1:=1_X$ and for $n\geq 2$,

$$\delta_n:=(\delta_X\otimes 1_{X^{\otimes n-2}})\circ(\delta_X\otimes 1_{X^{\otimes n-3}})\circ\ldots\circ(\delta_X\otimes 1_X)\circ\delta_X. \tag{6.5}$$

A connected classical network $f: X^{\otimes m}\to X^{\otimes n}$ is in *normal form* if

$$f=\delta_n\circ\delta_m^\dagger: X^{\otimes m}\to X^{\otimes n}. \tag{6.6}$$

Lemma 6.2.3 A non-empty connected classical network f containing only δ's and identities can be brought in normal form.

Proof: By induction on the number of δ's, we find:

Case $i=0$:

In this case, by connectedness, f consists only of an identity which is in normal form.

Case $i = n$ is assumed to be true.

Case $i = n + 1$:

As f consists only of δ's and identities, using bifunctoriality of the tensor product, we have

$$f = (1_{X^{\otimes p}} \otimes \delta_X \otimes 1_{X^{\otimes q}}) \circ f'$$

with $p + q + 1 = i$—indeed, this is of the form given by clause ($C2$). Now, by the induction hypothesis, f' can be brought into normal form. It remains to get the δ_X we factored out to be the leftmost term in the tensor product. We can always do so by using coassociativity of the †-Frobenius structure thus obtaining a normal form.

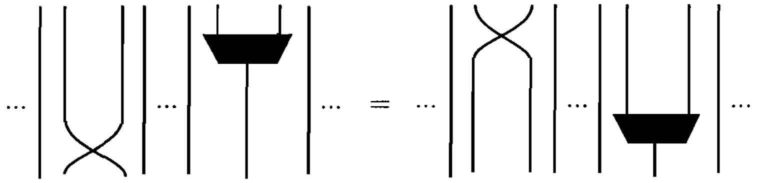
□

Lemma 6.2.4 Any non-empty classical network f consisting only of δ's, symmetries and identities factors as $S \circ D$ where S is a classical network containing only symmetries and identities while D contains only δ's and identities.

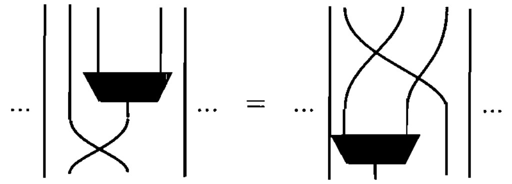
Proof: Let s denote a tensor product of a single symmetry and identities and d a tensor product of a single δ with identities. We first show that given s_1 and d_1,

$$d_1 \circ s_1 = s_2 \circ d_2.$$

This says that it is always possible to bring the term containing the symmetry after the term containing the δ in the compositional order. By cases, we have:



and the analogue when the symmetry is placed at the right of δ or



and the analogue when the symmetry is placed at the "right" of δ. As this exhausts all the cases, this proves our claim. The general result is true by extension on the size of f.

□

Lemma 6.2.5 Any non-empty classical network f containing only $\delta^\dagger$'s, symmetries and identities factors as $D \circ S$ where D is a classical network containing only $\delta^\dagger$'s and identities while S is a classical network containing only symmetries and identities.

Proof: The result is true by dualising the proof of lemma 6.2.4.

□

Proposition 6.2.6 Any non-empty connected classical network f consisting only of δ's, symmetries and identities can be brought into normal form.

Proof: First, apply lemma 6.2.4 so that $f = S \circ D$. Then, note that D satisfies the conditions of lemma 6.2.3 and hence can be brought into normal form that we denote D'. Now, as S is completely disconnected and it composes with D', every symmetry therein must compose with a set of δ's in D' and hence, up to a rearrangement of the δ's using coassociativity, it can be cancelled by cocommutativity. It remains to rearrange the terms so that we recover D' using coassociativity again.

□

Proposition 6.2.7 Any non-empty connected classical network f consisting only of $\delta^\dagger$'s, symmetries and identities can be brought into normal form.

Proof: Again, the result is true by dualising the proof of proposition 6.2.6.

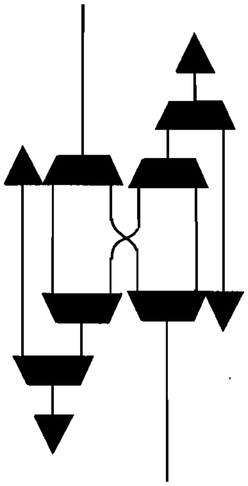
□

Theorem 6.2.8 **[Normalisation of classical networks]** Every connected classical network

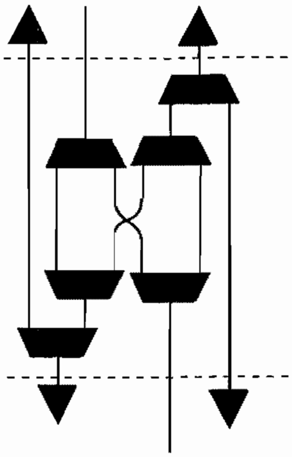
$$f : X^{\otimes m} \to X^{\otimes n}$$

admits a normal form.

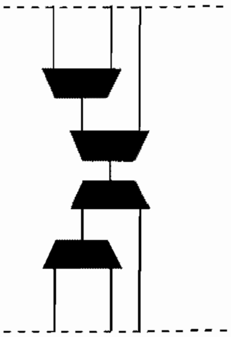
Before giving the proof, we will explain our strategy by giving an example of reduction in normal form. Consider the following connected classical network:



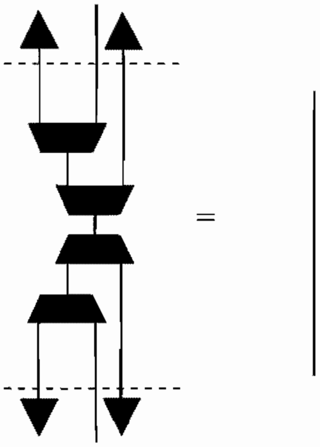
– Use bifunctoriality of the monoidal product to move all μ's and $\mu^\dagger$'s to the extremities of the network:



– The last step ensures that the expression in the middle consists only of δ's and $\delta^{\dagger}$'s and symmetries. The strategy is now to bring all the δ's after the $\delta^{\dagger}$'s using properties of the symmetric monoidal structure and of the †-Frobenius structure. In our case, the middle expression becomes:



– Finally, we bring back the μ and $\mu^{\dagger}$ and use the monoid and comonoid identities to obtain



where the identity is the normal form.

Proof of theorem 6.2.8: The steps of normalisations are:

1. Take every instance of ν_X and $\nu_X^\dagger$ and set them equal to $\mu_X \circ \delta_X^\dagger$ and $\delta_X \circ \mu_X^\dagger$ respectively. The process will eventually stop. Indeed, since f is finite, there are only a finite number of ν_X and $\nu_X^\dagger$. Let us denote the final expression from this step as f_1.

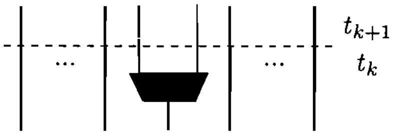
2. Using bifunctoriality of the tensor product, and naturality of the symmetry, factor out every μ_X and $\mu_X^\dagger$ so that
$$f_1 = M \circ f_2 \circ M'$$
where M is a tensor product of 1_X and μ_X's, M' is a tensor product of identities and $\mu_X^\dagger$'s and f_2 is a classical network consisting only of δ_X's, $\delta_X^\dagger$'s, symmetries and identities. Again, since there are only a finite number of μ_X's and $\mu_X^\dagger$'s as f is finite, the procedure must eventually halt.

3. Rewrite f_2 using bifunctoriality of the tensor as f_2', a composition of terms of the form
$$1_{X^{\otimes i}} \circ s \circ 1_{X^{\otimes j}},$$
where $s \in \{\delta_X, \delta_X^\dagger, \sigma_{X,X}\}$. We now "push" the δ_X's after the $\delta_X^\dagger$'s. As each term of the composition contains exactly one term different from the identity, this enables us to consider a set of identities involving the terms containing $\delta_X^\dagger$ and those appearing after in the composite f_2'. We read f_2' from right to left until we meet a term containing a δ_X, say the k-th term which we denote t_k. If the composition has k terms, then we are done and we proceed to the next step. Otherwise, we get into one the following subcases:

Simple cases:

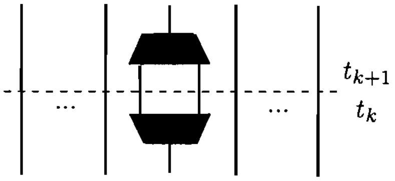
Consider $t_{k+1} \circ t_k$ then either

a. It is of the form



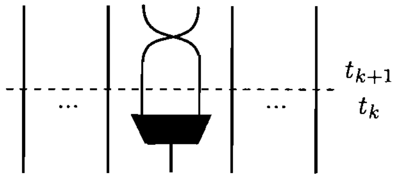
Meaning that the nontrivial term in t_{k+1} does not compose with δ_X, then, using bifunctoriality of the tensor product, apply
$$t_{k+1} \circ t_k = t_k \circ t_{k+1}$$

b. Of the form



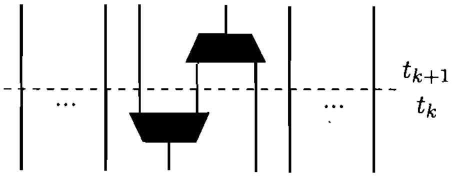
then apply speciality so that
$$\delta_X^\dagger \circ \delta_X = 1_X$$

c. Of the form

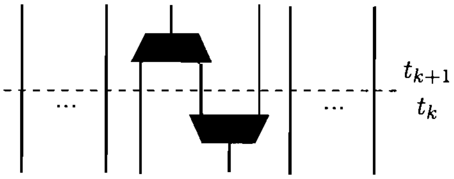


in which case we apply cocommutativity of δ_X to cancel out $\sigma_{X,X}$.

d. Or either of the forms



or

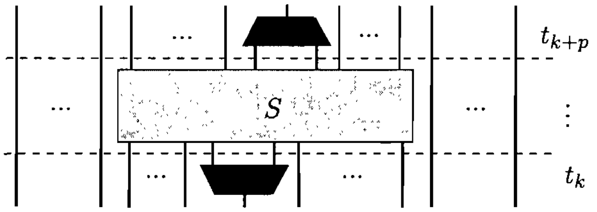


In either case we apply the Frobenius identity so that δ_X is brought in front of $\delta_X^\dagger$.

If $t_{k+1} \circ t_k$ was of none of the preceding form, it must interact with $\sigma_{X,X}$'s in which we fall in one of the following

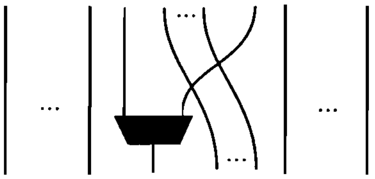
Non-simple cases:

Such cases involve considering composites in f_2' of the form $t_{k+p} \circ t_{k+(p-1)} \circ \cdots \circ t_k$ where t_k has a δ_X as non-trivial term, t_{k+p} has a $\delta_X^\dagger$ and the terms from t_{k+1} up to $t_{k+(p-1)}$ have a $\sigma_{X,X}$ as non-trivial term. We depict such a composite as



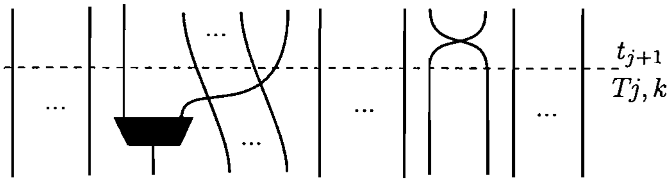
where S is a composite of tensor products of identities and symmetries.

Now, for some $j \geq k$, the composite $T_{j,k} := t_j \circ t_{j-1} \circ \cdots \circ t_k$ is represented without loss of generality as

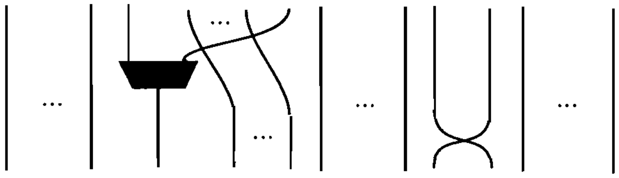


Indeed, if the term t_{k+1} has a symmetry on the left of δ_X, then there are no wires crossing the right leg of δ_X and $j = k$. From this, the composite $t_{j+1} \circ T_{j,k}$ is then

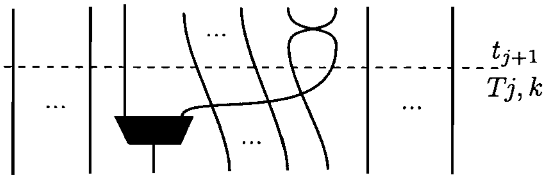
a. Of the form



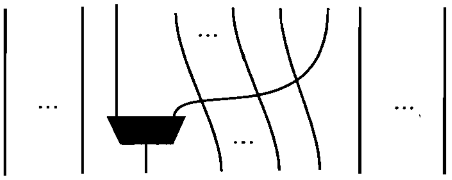
in which case we use bifunctoriality of the tensor product to get



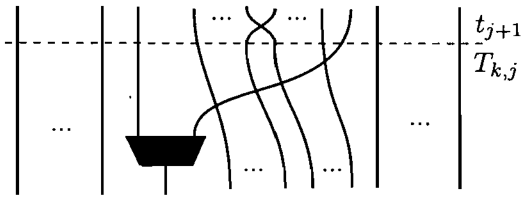
b. Of the form



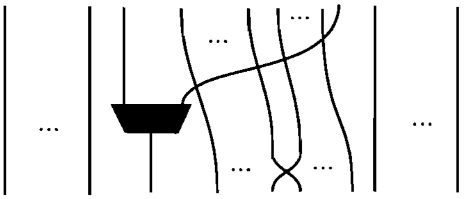
we then cancel out the symmetries to get



c. Of the form

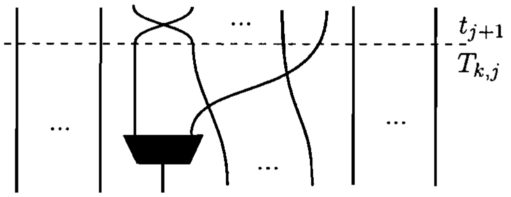


in which case we apply naturality of the symmetry in order to get

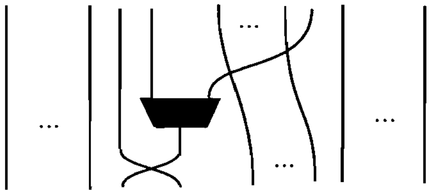


d. Of the form

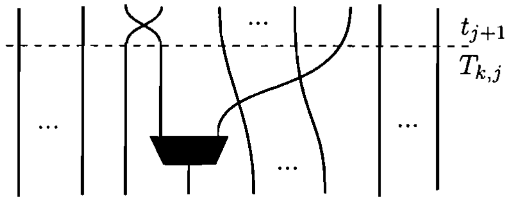
Normal form



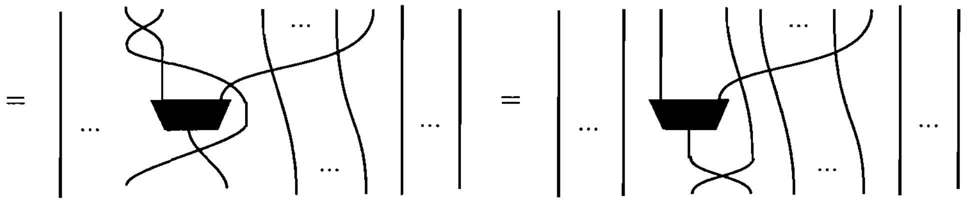
in which case we again apply naturality of the symmetry to get



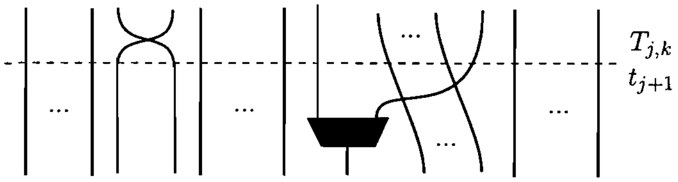
e. Of the form



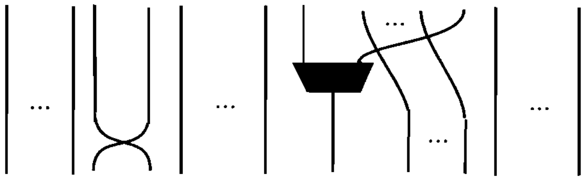
in which case we use



f. Or of the form



in which case we use bifunctoriality to get

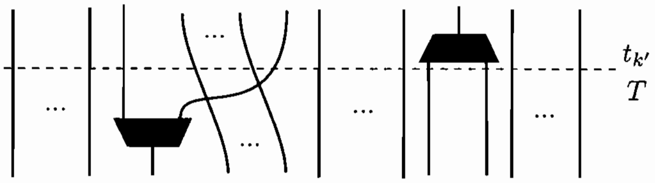


This step is repeated until we exhaust all the terms up to t_{k+p} in the original expression. Then, let us denote the composite of the terms from δ_X up to $\delta_X^\dagger$ but excluding the latter as T and the term containing $\delta_X^\dagger$ as $t_{k'}$.

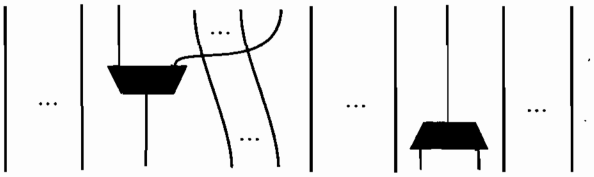
The composite $t_{k'} \circ T$ has now one of the following forms:

A. If the preceding transformations didn't leave any symmetries crossing the right leg of δ_X, we then fall back to a simple case and apply the corresponding identity.

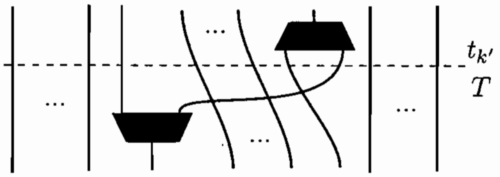
B. Of the form



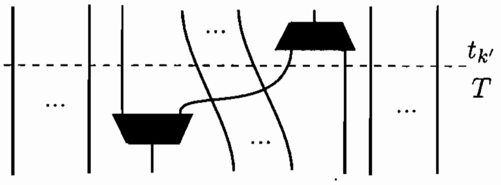
from which we get, via bifunctoriality,



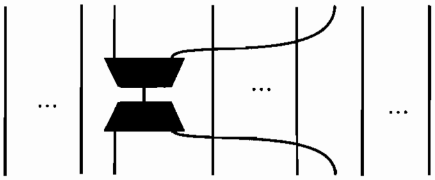
C. Of either of the forms



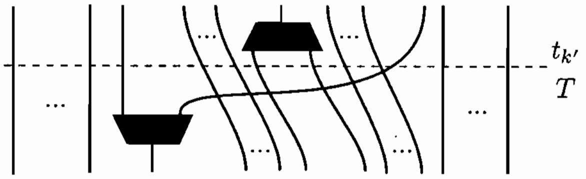
or



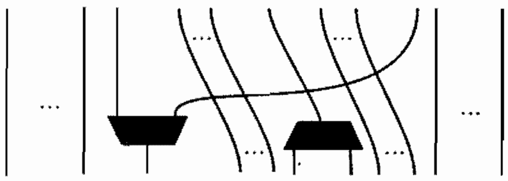
From there if we meet the first case, we cancel out the symmetry below $\delta_X^\dagger$, which enables us to consider the second case for both so that, via a graph isomorphism analogous to the one in case e. above, we can use the Frobenius identity to get



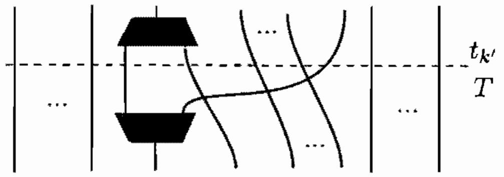
D. Of the form



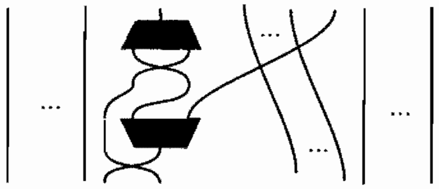
from which naturality of the symmetry yields



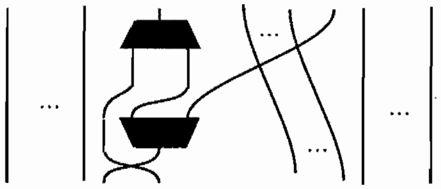
E. Of the form



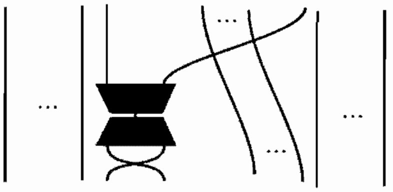
from which we use general properties of the symmetry to get to



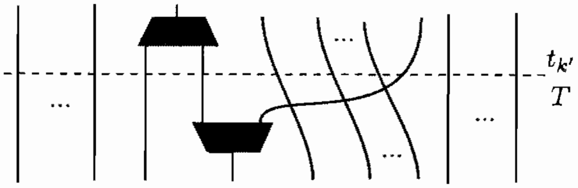
then, we use co-commutativity of $\delta_X^\dagger$ to get



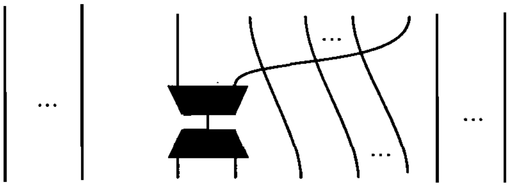
and finally, the Frobenius identity yields



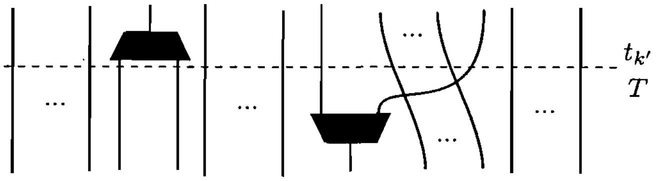
F. Of the form



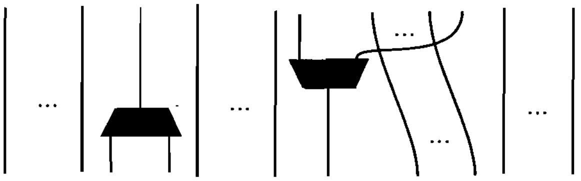
in which case we apply Frobenius identity to get



G. Or of the form



from which we get



using bifunctoriality.

In each of these cases—aside those where we used speciality—, we brought δ_X after $\delta_X^\dagger$.

Following this, we begin this step anew until all δ_X's come after the $\delta_X^\dagger$'s.

Convergence of this step is ensured by the fact that we only have a finite number of δ_X's and $\delta_X^\dagger$'s. Denote the final expression obtained from this step by f_3.

4. Now, since all occurrences of $\delta_X^\dagger$'s occur before the occurrences of δ_X's, we may factor f_3 as

$$f'' \circ f' : X^{\otimes m} \to X^{\otimes j} \to X^{\otimes n}$$

where f' contains all the $\delta_X^\dagger$'s while f'' contains all the δ_X's.

We now shall argue that $j = 1$ and this will enable us to apply proposition 6.2.6 and proposition 6.2.7 to obtain a normal form. First, j can't be 0 since f_3 is connected. So, suppose that $j > 1$. We will show that such an assumption entails $f'' \circ f'$ is disconnected. To do so, we first show that f' is disconnected:

The composite f' can be factored as a composite of terms

$$1_{X^{\otimes k}} \otimes s \otimes 1_{X^{\otimes l}} \quad \text{where} \quad s \in \{\delta_X^\dagger, \sigma_{X,X}\} \tag{6.7}$$

for appropriate values of k and l. Now, the number of connected components in the first term of the composition term is at least $k + l + 1 \geq j > 1$, such a term is a disconnected classical network independently of whether s is a $\delta_X^\dagger$ or a symmetry. If there are no more terms, we are done. If not, there are two cases:

- The term that follows contains a symmetry, then the composite is still disconnected.
- The following term contains a $\delta_X^\dagger$ and this reduces the number of disconnected components by 1. Now, $k+l$ indicates the number of connected components in the term containing the

$\delta_X^\dagger$ which is again at least j so that the number of connected components is $k + l \geq j > 1$ and the composite is again disconnected.

By induction, it follows that f' is disconnected.

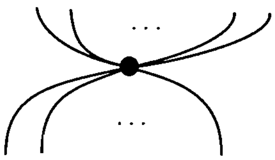
Now, for the composite $f'' \circ f'$ note that when composing f' with a term of f'' containing either a δ_X or a symmetry again leaves a disconnected classical network. Indeed, to connect the components of f' one would need the clause of connectedness ($B2$) but this can't happen as f' contains no $\delta_X^\dagger$. Thus, by induction, $f'' \circ f'$ is disconnected. As this can't happen—by assumption f_3 is connected—, $j = 1$ as claimed.

Following this, from f_3 we can apply proposition 6.2.6 and proposition 6.2.7 to obtain a normal form f_4. This step converges again by finiteness of f.

5. Finally, it just remains to bring in the μ_X and $\mu_X^\dagger$ which we evacuated in step 2 and cancelling them against δ_X and $\delta_X^\dagger$ respectively using the comonoid and monoid identities. The resulting expression is still in normal form and is equal to f as required. Again, this step must eventually terminate.

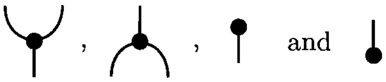
□

A classical network in normal form is completely determined by its number of inputs and outputs. For instance, the pair of input-output $(0, 1)$ defines $\mu^\dagger$, the pair $(1, 2)$ defines δ, the pair $(2, 2)$ defines $\delta \circ \delta^\dagger$ etc. Thus, when looking at a connected classical network, the only thing that we have to take care of is the number of inputs and outputs and then, we can write the corresponding normal form. Using this idea, we introduce the following unambiguous "spider" notation for a normal form $\delta_n \circ \delta_m^\dagger$:



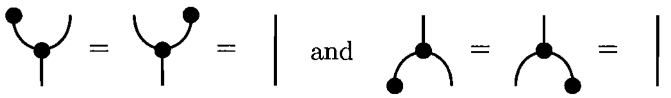
where the spider has m inputs and n outputs if they are not both equal to 1. In this particular case, the normal form is just an identity which we depict as a wire without dot as usual. A way to interpret such a reduction in normal form using the spider notation is to consider the usual normal form and then, we "contract" the dots from each components of the normal form into one while cancelling all the symmetries in between.

From now on, we will drop the trapezoids and triangle and depict δ_X, $\delta_X^\dagger$, μ_X and $\mu_X^\dagger$ as their corresponding spiders, that is

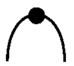
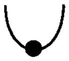


respectively.

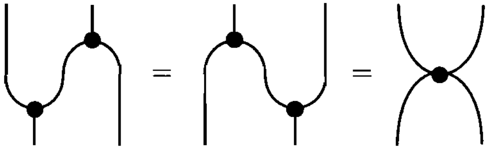
Incidentally, this notation gives us a better way to handle the properties of classical objects in the graphical calculus. Indeed, the comonoid and monoid identities now appear as



respectively. The counit ν_X of the quantum structure induced by the †-Frobenius structure together with its adjoint are depicted as

 and 

respectively. The Frobenius identities appear as



It is easy to see that this lemma induces a rewriting scheme for the "classical component of more general expressions", *i.e.*, the part only involving classical object structure, simply by normalising all (maximal) classical networks it comprises while considering the "boundary" of the classical component as its inputs and outputs.

Remark 6.2.9 Perhaps there is a more elegant proof than the one we gave, for instance via rewriting or structural induction. Whether such a proof already exists for Frobenius algebras isn't known to the author, and it remains an interesting open question for future work.

6.3 The category $\mathbf{C}_b$ of basis structures

In this section, we introduce the notion of category of basis structures. Given an object $\mathcal{H}$ in **FdHilb**, its specified dual related to the quantum structure is the conjugate space $\mathcal{H}^*$. However, nothing prevents us from choosing a basis for $\mathcal{H}$ that is via theorem 6.1.3, to equip $\mathcal{H}$ with a †-Frobenius structure. Having done so, the object $\mathcal{H}$ comes with two quantum structures:

- The first coming from the quantum structure of **FdHilb** with dual $\mathcal{H}^*$ while
- The second is the one induced by the †-Frobenius structure which is self-dual.

As we have seen in lemma 5.2.1, these two duals are isomorphic via a unique unitary transformation $d_X : \mathcal{H} \to \mathcal{H}^*$. But here, the second quantum structure is induced by a †-Frobenius object and this entails that d_X—*the dualiser of* $\mathcal{H}$—is a bijection.

The goal of this section is to introduce the notion of basis object which consists of an object of $\mathbf{C}_q$ equipped with a †-Frobenius structure. Then to make the dualiser explicit. To introduce the notion of a category of basis structures as a full subcategory of $\mathbf{C}_q$ where each object comes equipped with a basis structure. Finally, to study how the two quantum structures existing within such a category interact.

Such a construction is new and was first introduced in [34] which the author wrote with B. Coecke and S. Perdrix. There are, however, many discrepancies between that paper and what we present here. Among these, we stress the fact that the †-Frobenius structure of the basis structure is complementary to the quantum structure of the object of $\mathbf{C}_q$. This induces many changes in the statements of the results which are, sometimes, less general than what's presented in [34] but these are better suited for our needs. Finally, we make explicit the fact that the set of all dualisers in a category of basis structures defines a natural transformation between the two lower- and upper-star present functors present in a category of basis structures; such a result was not in the cited paper.

[Base structure] A *basis structure* on an $X \in |\mathbf{C}_q|$ is a quadruple

$$\langle X, \delta_X, \mu_X, \epsilon_X \rangle$$

where $\langle X, \delta_X, \mu_X \rangle$ is a †-Frobenius structure and $\langle X, \epsilon_X \rangle$ is the quantum structure of X in $\mathbf{C}_q$. Again, we will make the usual abuse of terminology saying that the support X of a basis structure $\langle X, \delta_X, \mu_X, \epsilon_X \rangle$ is a *basis object.*

Lemma 6.3.1 If X in $\mathbf{C}_q$ is equipped with a †-Frobenius structure, then so is X^* with

$$\langle X^*, (\delta_X)_*, (\mu_X)_* \rangle$$

.

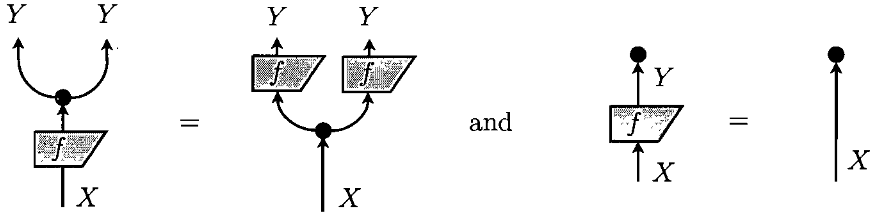
Proof: As $(-)_*$ is a functor such that for all f and g, $(f \otimes g)_* = g_* \otimes f_*$ (by our assumption on the strictness of $\mathbf{C}_q$), the result trivially holds. As an example, we show one of the two equations of the Frobenius condition on X^*:

$$\begin{aligned}((\delta_X)_*^\dagger \otimes 1_{X^*}) \circ (1_{X^*} \otimes (\delta_X)_*) &= ((\delta_X^\dagger)_* \otimes (1_X)_*) \circ ((1_X)_* \otimes (\delta_X)_*) \\ &= (1_X \otimes \delta_X^\dagger)_* \circ (\delta_X \otimes 1_X)_* \\ &= ((1_X \otimes \delta_X^\dagger) \circ (\delta_X \otimes 1_X))_* \\ &= (\delta_X \circ \delta_X^\dagger)_* \\ &= (\delta_X)_* \circ (\delta_X^\dagger)_* \\ &= (\delta_X)_* \circ (\delta_X)_*^\dagger .\end{aligned}$$

□

In order to prove the next result, we need the notion of

[Bijection] Let $X, Y \in |\mathbf{C}_q|$ be equipped with †-Frobenius structures. Then $f : X \to Y$ is a *bijection* if it is a unitary comonoid homomorphism. That is, in addition to being unitary, it is such that



Remark 6.3.2 In **FdHilb** the previous notion coincides with the usual notion of bijection. Indeed, if $f : X \to Y$ commutes with both δ and ϵ, then it must be a matrix of 0's and 1's. If in addition it is unitary, then it must be a bijection on the basis.

Theorem 6.3.3 [Dualiser] If $X \in |\mathbf{C}_q|$ is equipped with a basis structure

$$\langle X, \delta_X, \mu_X, \epsilon_X \rangle,$$

then there exists a unique bijection

$$d_X : X \to X^*,$$

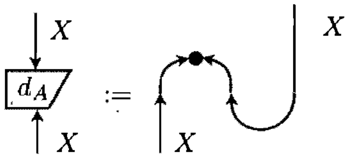
the *dualiser* of X, such that the counit of the quantum structure factors as

$$\begin{tikzcd}
X \otimes X^* \arrow[rr, "1_X \otimes d_X^\dagger"] \arrow[dr, "\epsilon_X"'] & & X \otimes X \arrow[dl, "\delta_X \circ \mu_X^\dagger"] \\
& I &
\end{tikzcd}$$

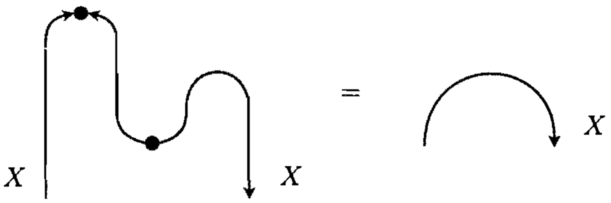
Proof: We first show that there exists a unique unitary d_X making the diagram commute. Let

$$d_X := (\mu_X \otimes 1_{X^*}) \circ (\delta_X^\dagger \otimes 1_{X^*}) \circ (1_X \otimes \epsilon_X^\dagger) \tag{6.8}$$

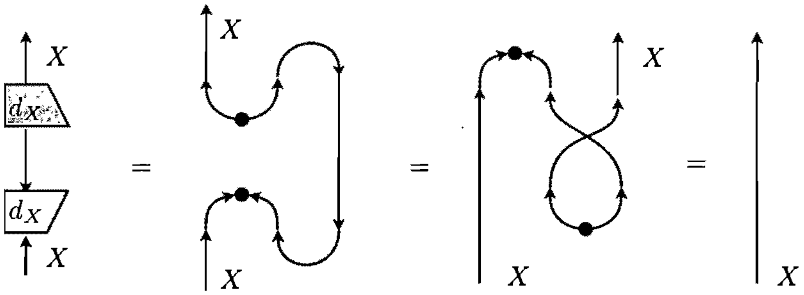
that is



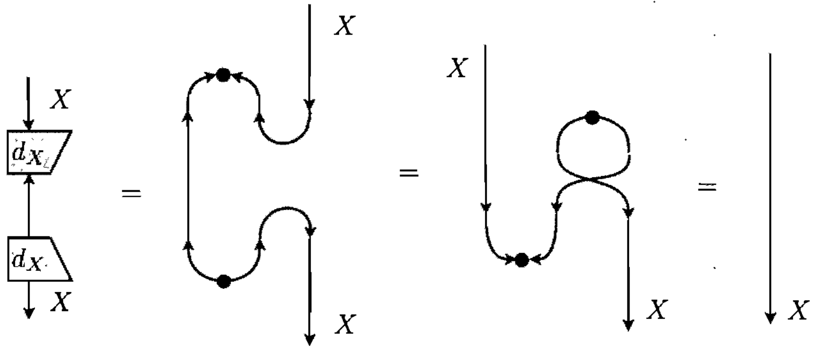
Then we have



making the diagram (5.5) commute. To show that this is a unitary transformation, observe that $d_X^\dagger \circ d_X = 1_X$ as

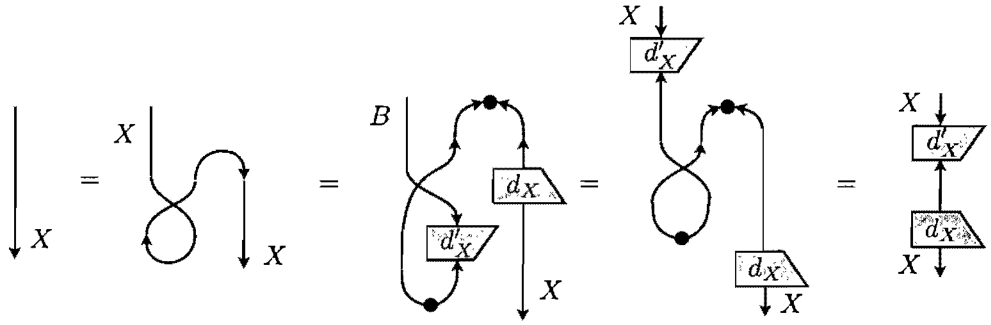


using simple isomorphisms of graph. For $d_X \circ d_X^\dagger = 1_{X^*}$,

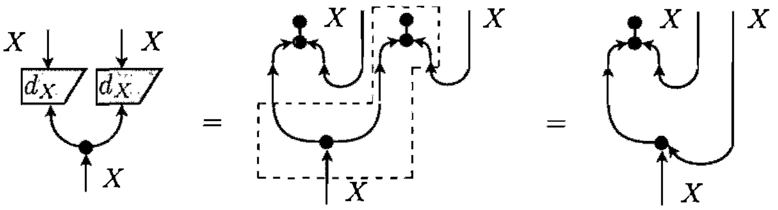


where the second equality is obtained by "sliding" ν_X and $\nu_X^\dagger$ along $\epsilon_X^\dagger$ and ϵ_X in the obvious way.

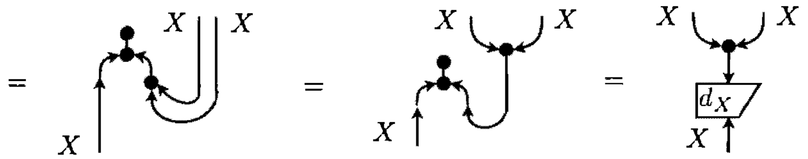
To show that d_X is unique, we suppose that there are two such unitaries d_X and d'_X making (5.2.1) commute. Then,



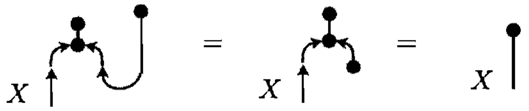
So we must have $d'_X \circ d^\dagger_X = 1_{X^*}$. Since d_X is unitary, it follows that $d'_X = d_X$, thus, d_X is unique. It remains to show that it is a bijection. To show that it commutes with δ_X, consider



The second equality is obtained by applying the normalisation theorem to the classical network within the dotted shape. Then we apply associativity to swap the two $\delta^\dagger_X$'s; this yields



There, the second equality is obtained by sliding $\delta^\dagger_X$ along $\epsilon^\dagger_{X\otimes X}$. To show that it commutes with μ_X is given by



Thus, d_X is a bijection.

□

From this,

[Category of basis structures] A *category of basis structures* $\mathbf{C}_b$ of a category of quantum structures $\mathbf{C}_q$ is any full subcategory of $\mathbf{C}_q$ such that every object $X \in \mathbf{C}_b$ comes with basis structure

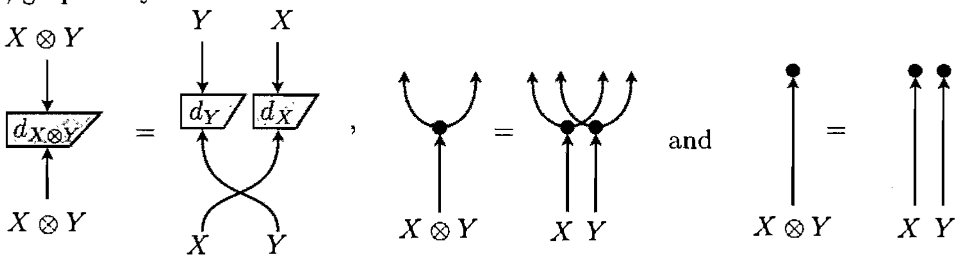
$$\langle X, \delta_X, \mu_X, \epsilon_X \rangle$$

and where

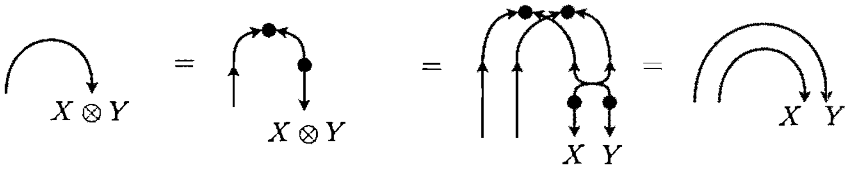
1. For any $X \in |\mathbf{C}_b|$, $d^\dagger_X = d_{X^*}$,
2. For any $X, Y \in |\mathbf{C}_b|$, we have

$$\delta_{X\otimes Y} = (1_X \otimes \sigma_{X,Y} \otimes 1_Y)\circ(\delta_X \otimes \delta_Y) \quad \mu_{X\otimes Y} = \mu_X \otimes \mu_Y \quad \text{and} \quad d_{X\otimes Y} = (d_X \otimes d_Y)\circ\sigma_{X,Y}$$

The category $\mathbf{C}_b$ of basis structures that is, graphically:



The constraint on the dualiser simply states that the choice of basis should be coherent with respect to both the basis structures of X and X^*. In details: the first condition on the dualisers insures that the basis structures on X and its dual X^* are properly connected one with respect to the other. The second one insures that that the dualiser behaves well when factoring the counit of a compound object in the sense that it preserves the strictness of the quantum structures, *i.e.*, we have:



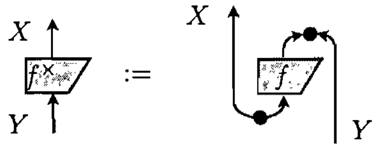
Example 6.3.4 In the category **FdHilb** if X is equipped with a basis structure $\langle X, \delta_X, \mu_X, \epsilon_X\rangle$ with induced basis $\{|\phi_i\rangle\}$, then the conjugate space X^* has the same basis. The dualiser is the unitary transformation

$$d_X = \sum_i |\phi_i\rangle\langle\phi_i| : X \to X^*.$$

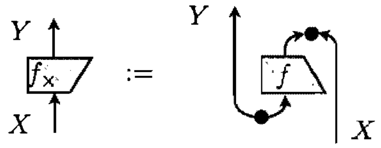
Proposition 6.3.5 Let $\mathbf{C}_b$ be a category of basis structures. The quantum structures induced by the †-Frobenius structures of the basis structures induce two identity-on-object functors

$$(-)^\times : \mathbf{C}_b^{op} \to \mathbf{C}_b \quad \text{and} \quad (-)_\times : \mathbf{C}_b \to \mathbf{C}_b$$

whose actions on an $f : X \to Y$ are given by



and



respectively.

Proof: The proof is analogous—simpler in fact—to the proof of proposition 5.2.3. □

The category $\mathbf{C}_b$ of basis structures

The previous proposition thus tells us that, in a category of basis structures, not only does each object come with two possibly distinct quantum structures, but also that if these two quantum structures are indeed distinct, they induces two distinct upper- and lower-star functors both factoring the dagger. The natural question now is: How do these two pairs of functors relate? Manifestly, the collection of all dualisers does not define a natural transformation from the identity functor to either $(-)_*$ or $(-)^*$. However, we have:

Proposition 6.3.6 Let $\mathbf{C}_b$ be a category of basis structures. The collection of all dualisers

$$\{d_X : X \to X^* \mid X \in |\mathbf{C}_b|\}$$

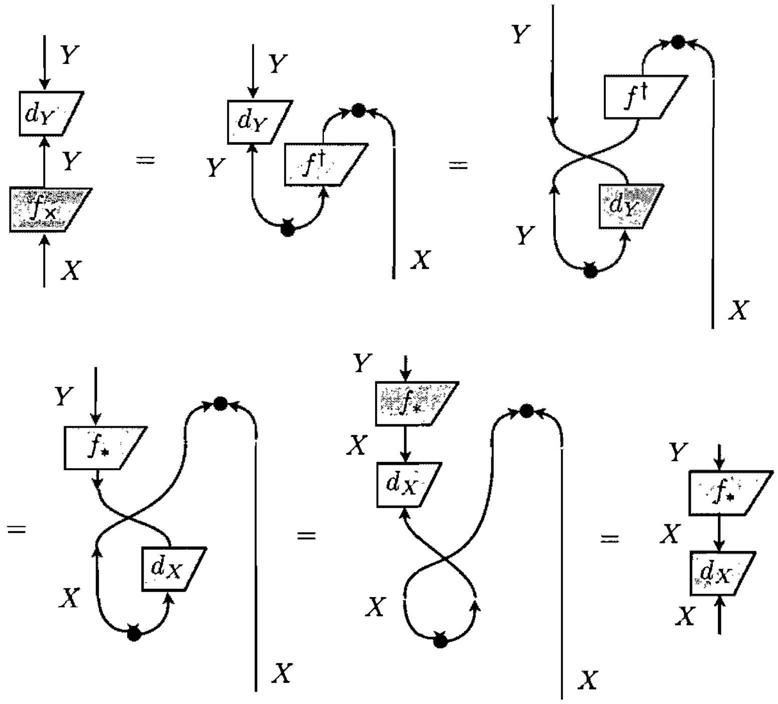
defines two natural isomorphisms

$$d^\bullet : (-)^\times \to (-)^* \quad \text{and} \quad d_\bullet : (-)_\times \to (-)_*$$

Proof: Since all the required equations are shown in an analogous manner, we will only show that given an $f : X \to Y$, then

$$\begin{tikzcd} X \arrow[r, "d_X"] \arrow[d, "f_\times"'] & X^* \arrow[d, "f_*"] \\ Y \arrow[r, "d_Y"'] & Y^* \end{tikzcd}$$

commutes. Indeed, the composite $d_Y \circ f_\times$ is



There, the first equality is taken from the definition of $f_\times$. The second equality by using the cocommutativity of the comultiplication and sliding the dualiser down. The third equality is obtained by sliding $f^\dagger$ along η_X which is factorised in the picture. The fourth equality is obtained by sliding the dualiser up. The final equality by compactness of the †-Frobenius structure. Thus, we indeed obtain

$$d_Y \circ f_\times = f_* \circ d_X$$

As required. Finally, that the components are (unitary) isomorphisms is already guaranteed by theorem 6.3.3.

□

6.4 Mixed normal form

The main result concerning the mixed normal form is new and was first stated in [34]. We give here for the first time a formal definition of connectedness and a complete proof based on the reduction of classical networks into normal form given in section 2 of this chapter.

We now generalise the normal form to objects in $\mathbf{C}_b$; that is, we add dual objects and dualisers to connectedness and the normal form theorem.

[**Mixed network**] A *mixed network* in $\mathbf{C}_b$ is a composition of terms obtained by tensoring of d's, δ's, μ's (and hence also of ϵ's and ν's) symmetries, identities and their adjoints.

[**Mixed connectedness**] Let $\mathcal{X}^n := X_1 \otimes X_2 \otimes \cdots \otimes X_n$ where for all i, $X_i \in \{X, X^*\}$ and $\mathcal{X}^0 := I$. Let X be an object equipped with a basis structure. A mixed network is *connected* if it is equal to a classical network constructed from the following definition:

[Basic clauses] These consist of the basic clause of connectedness $(A1) - (A7)$ for the structural morphisms of the †-Frobenius structure on X and their analogue $(A1^*) - (A7^*)$ for the structural morphisms of the †-Frobenius structure on X^* with, in addition the clauses

$$(A9)\ d_X : X \to X^*, \qquad \text{and} \qquad (A10)\ d_X^\dagger : X^* \to X$$

are connected mixed networks.

[Inductive clauses] Let

$$\mathcal{F} : \mathcal{X}^n \to \mathcal{X}^m \quad \text{and} \quad \mathcal{F}' : \mathcal{X}^{m'} \to \mathcal{X}^{n'},$$

be connected mixed networks and

$$\mathcal{S} : \mathcal{X}^{m+m'} \to \mathcal{X}^{m+m'} \quad \text{and} \quad \mathcal{S}' : \mathcal{X}^{n+n'} \to \mathcal{X}^{n+n'}$$

be composites of terms obtained by tensoring identities 1_X and 1_{X^*} and symmetries $\sigma_{X,X}$, σ_{X,X^*} its adjoint and σ_{X^*,X^*}. Now, with $\mathcal{F}$ instead of f, $\mathcal{F}'$ instead of f', $\mathcal{S}$ instead of S and $\mathcal{S}'$ instead of S', the inductive clauses consists of:

- The clauses of connectedness $(B1) - (B2)$ and $(C1) - (C8)$ for the structural morphisms of the †-Frobenius structure on X and that, whenever the composite of a given clause is defined[10].
- The analogue clauses $(B1^*) - (B2^*)$ and $(C1^*) - (C8^*)$ for the structural morphisms of the †-Frobenius structure on X^* whenever the composite of a given clause is defined.

In addition, if $\mathcal{F} : \mathcal{X}^n \to \mathcal{X}^m$ is a connected mixed network, then so are

[10] As we have two types in a mixed network: X and X^*.

$$(C9)\ \ (1_{\mathcal{X}^i} \otimes d_X \otimes 1_{\mathcal{X}^j}) \circ \mathcal{F}, \qquad (C10)\ (1_{\mathcal{X}^i} \otimes d_X^\dagger \otimes 1_{\mathcal{X}^j}) \circ \mathcal{F},$$
$$(C11)\ \mathcal{F} \circ (1_{\mathcal{X}^{i'}} \otimes d_X \otimes 1_{\mathcal{X}^{j'}}) \quad \text{and} \quad (C12)\ \mathcal{F} \circ (1_{\mathcal{X}^{i'}} \otimes d_X^\dagger \otimes 1_{\mathcal{X}^{j'}})$$

with all possible values of i and j with $i + j + 1 = n$ and possible values of i' and j' with $i' + j' + 1 = m$ again, whenever such a composite is defined.

[Extremal clause] Nothing else is a connected mixed network.

The generalisation of disconnectedness, and complete disconnectedness should be clear.

[**Mixed normal form**] A connected mixed network $f : \mathcal{X}^n \to \mathcal{X}^m$ is in *normal form* if

$$f = D \circ \delta_n \circ \delta_m^\dagger \circ D' : \mathcal{X}^n \to \mathcal{X}^m$$

where D is a tensor product of d_X's and 1_X's, and D' a tensor product of $d_X^\dagger$'s and 1_X's.

Theorem 6.4.1 Every connected mixed network

$$f : \mathcal{X}^n \to \mathcal{X}^m$$

admits a normal form.

Proof: The strategy for proving this theorem is analogous to that of the normal form theorem for classical network but we must take the presence of dualisers into account. The argument of convergence is the same as for each of the corresponding step in theorem 6.2.8 so we do not repeat it here.

1. Perform the same steps as in step 1 of the proof of theorem 6.2.8. In addition, take all instances of η_X and ϵ_X, and factor them in accordance to the form guaranteed by theorem 6.3.3 that is,

   $$\eta_X = (d_X \otimes 1_X) \circ \delta_X \circ \mu_X^\dagger \quad \text{and} \quad \epsilon_X = \mu_X \circ \delta_X^\dagger \circ (1_X \otimes d_X^\dagger).$$

   We do the same *mutatis mutandis* for η_{X^*} and ϵ_{X^*} and their adjoints. Denote the final expression from this step as f_1.

2. The principle of this step is the same as in step 2 of the proof of theorem 6.2.8. We use bifunctoriality of the tensor product to factor f_1 as

   $$f_1 = \mathcal{E} \circ f_2 \circ \mathcal{E}'$$

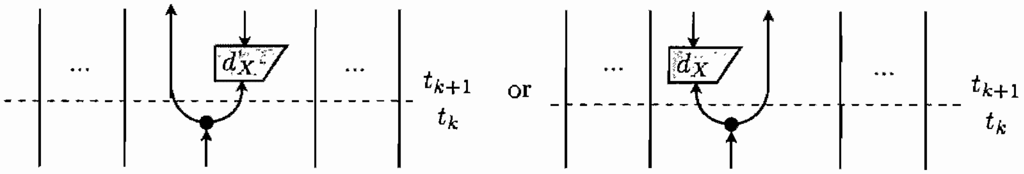
   where $\mathcal{E}$ is a tensor product of 1_X's, 1_{X^*}'s, μ_X's and μ_{X^*} and $\mathcal{E}'$ is a tensor product of 1_X's, 1_{X^*}, $\mu_X^\dagger$'s and $\mu_{X^*}^\dagger$. As $\mathcal{E}$ and $\mathcal{E}'$ are completely disconnected, then f_2 is a connected mixed network consisting of symmetries, δ's, $\delta^\dagger$'s and identities.

3. We now "push" the δ's after their adjoints in the composition. Again, using bifunctoriality of the tensor product we rewrite f_2 as f_2', a composite of terms of the form

   $$1_{\mathcal{X}^i} \circ s \circ 1_{\mathcal{X}^j}$$

   where $s \in \{\delta_X, \delta_X^\dagger, \delta_{X^*}, \delta_{X^*}^\dagger, \sigma_{X,X}, \sigma_{X^*,X}, \sigma_{X^*,X}^\dagger, \sigma_{X^*,X^*}\}$. In addition to the simple cases already treated in theorem 6.2.8 and the corresponding simple cases for those involving the comultiplication and multiplication of X^* as well as the extra symmetries, we might encounter new simple cases involving the dualiser. We will give only the cases with δ_X, those with δ_{X^*} should be obvious from them.

A. The cases



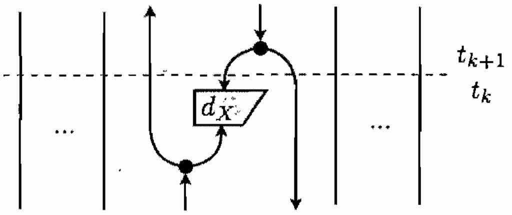
In either cases, we consider the composite of the dualiser and the comultiplication all at once and handle it as if it were a δ.

B. If the term we "push" forward has the form given in A. and another dualiser composes with the composite then there are two cases:

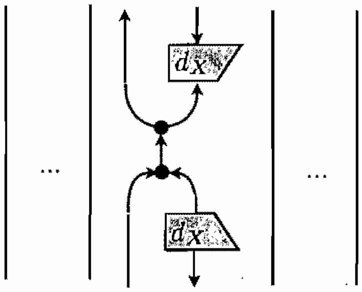
i. Either the dualiser composes with the dualiser already present in the composite. In such a case, the dualisers cancel out.

ii. The dualiser composes with δ but not with the dualiser already present. In that case, we then use the fact that d_X is a bijection to get $(d_X \otimes d_X) \circ \delta_X = \delta_{X^*} \circ d_X$.

C. The case

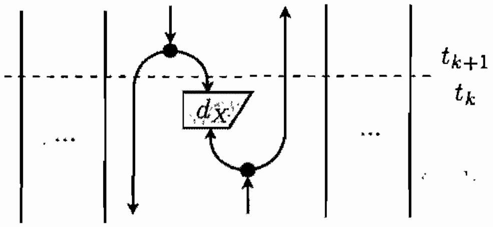


from where using the fact that d_X is a bijection and the Frobenius identity on X we obtain



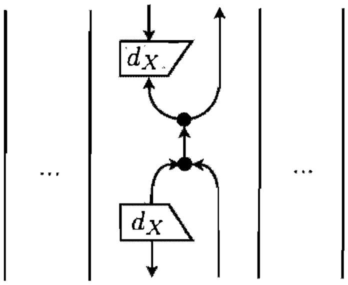
To this, we add the analogous case when the initial expression is dagger'ed (the final expression is self-adjoint).

D. The case



Mixed normal form

from where using the same fact and identity as in the previous case we obtain



and again, the analogous case when the initial expression in dagger'ed.

The generalisation of the non-simple case should be obvious from the simple cases we introduced; if d_X, $d_X^\dagger$ doesn't compose with δ_X or δ_{X^*} (depending on the case), we just ignore them. Dualisers will be dealt with in the next step.

Following this, we begin this step anew until all δ's come after the $\delta^\dagger$'s. Denote the final expression obtained from this step as f_3

4. Again, we obtain an expression which factors as

$$\mathcal{X}^n \to X^\circ \to \mathcal{X}^m;$$

However, the difference here when compared to theorem 6.2.8, the object X° is either X or X^*. From here, we use the fact that d_X and $d_X^\dagger$ are bijections, the naturality of the symmetry, and bifunctoriality of the tensor product in order to take

$$\mathcal{E} \circ f_3 \circ \mathcal{E}'$$

to the composite

$$\mathcal{E}'' \circ f_4 \circ \mathcal{E}'''.$$

From there, $\mathcal{E}''$ is then a tensor product of 1_X's, 1_{X^*}'s, d_X's, $d_X^\dagger$'s, μ_X's and μ_{X^*}, and $\mathcal{E}'''$ is a tensor product of 1_X's, 1_{X^*}, d_X, $d_X^\dagger$, $\mu_X^\dagger$'s and $\mu_{X^*}^\dagger$. What remains in f_4 are δ's and symmetries together with their adjoints but because of connectedness these symmetries and δ's are those coming from the $\dagger$-Frobenius structure on X°. So we may now apply proposition 6.2.6 and proposition 6.2.7 to reduce f_4 to normal form.

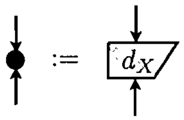
5. It just remains to cancel out the ϵ's and their adjoints against the δ's and their adjoints. Both are, by connectedness, from the $\dagger$-Frobenius structure on X°. Denote the resulting normal form excluding the d_X and $d_X^\dagger$ remaining on the extremities as f_5.

6. Finally, if $X^\circ = X$, we are done. Otherwise, if $X^\circ = X^*$ it suffices to take a $d_X^\dagger$ and as it is a bijection, we can take it from from one side of f_5 to the other side of f_5 thus changing the type of f_5 all along from which we obtain a normal form. If there are none available, we can use the identity $1_{X^*} = d_X \circ d_X^\dagger$ to produce one and take it from the right of f_5 to the left of f_5 so that we obtain a normal form.

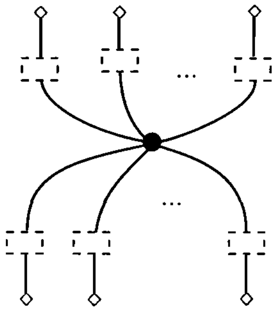
□

Let us introduce the following notation

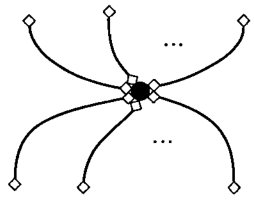
Mixed normal form



Since $d_X^\dagger = d_{X^*}$, we do not lose any information in doing so. Indeed, they can be identified by the direction of the arrows. Now, from the previous theorem, we can represent the obtained normal form as a "decorated" spider, *i.e.*:

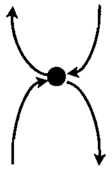


where in the dotted boxes there is either an identity or a dualiser while the small diamonds indicate the possible presence of an arrow depending on what is inside the dotted box on that wire. Now, using the dot notation for the dualiser and in the same spirit of "contracting the dots" as we had for the first spider form, we can unambiguously represent a mixed normal form as

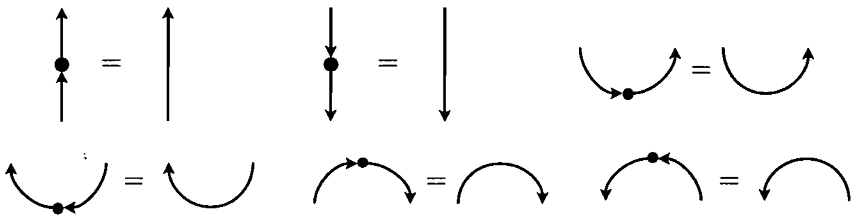


where again, in the small white diamonds are the corresponding arrows depending whether the wire has type X or X^*.

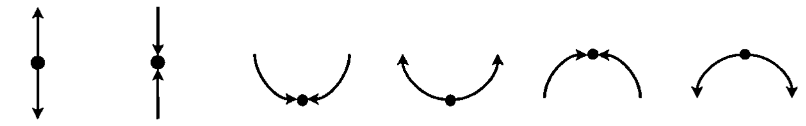
Example 6.4.2 The result of the case A of the step 3 of the theorem 6.4.1 is represented in spider form as



Now, using the mixed spider notation, we don't have to depict the dot in the following cases:



On the other hand, we must depict it in the following:

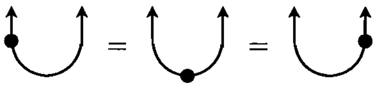


Finally, we have:

Lemma 6.4.3 For any object $X \in |\mathbf{C}_b|$, a category of basis structures, we have

$$(d_X^\dagger \otimes 1_X) \circ \epsilon_{X^*}^\dagger = \delta_X \circ \gamma_A^\dagger = (1_X \otimes d_X^\dagger) \circ \epsilon_X^\dagger$$

that is,



Proof: That the leftmost expression is equal to the rightmost one holds for any f in a category of quantum structures. That both expressions are equal to the one in the middle holds by definition of the dualisers.

□

6.5 Classical maps

We now introduce the notion of classical map. In **FdHilb**, such a map is a matrix with real positive entries. Such a notion of classicality makes sense as matrices with entries in $\mathbb{R}_+$ include, among others, basis vectors from the computational basis, bijections and stochastic vectors which are the outputs of measurements in quantum computing.

We first show that within our language, it is possible to characterise that a matrix in $\mathbf{FdHilb}_b$ contains only non-negative real entries. Indeed, let $f : \mathcal{H} \to \mathcal{H}'$ be a morphism in $\mathbf{FdHilb}_b$ where $\mathcal{H}$ and $\mathcal{H}'$ are equipped with basis structures $\langle \mathcal{H}, \delta_{\mathcal{H}}, \mu_{\mathcal{H}}, \epsilon_{\mathcal{H}} \rangle$ and $\langle \mathcal{H}', \delta_{\mathcal{H}'}, \mu_{\mathcal{H}'}, \epsilon_{\mathcal{H}'} \rangle$ respectively. Consider the composite map

$$(1_{\mathcal{H}} \otimes \delta_{\mathcal{H}'}^\dagger) \circ (1_{\mathcal{H}} \otimes f \otimes 1_{\mathcal{H}'}) \circ (\delta_{\mathcal{H}} \otimes 1_{\mathcal{H}'}).$$

It is an easy calculation to see that if $f = \sum_{\alpha_{ij}} |j\rangle\langle i|$ as a matrix relative to the basis induced by the basis structures, the morphism above is $\sum_{ij} \alpha_{ij} |ij\rangle\langle ij|$, and thus, a matrix of zeros except on the main diagonal which contains the columns of the original matrix f. In that sense, the operation *unfolds* f. Now, the unfolding of f is positive if f as a matrix had only non-negative entries in the beginning. Thus, we have used:

1. The basis structures via $\delta_{\mathcal{H}}$ and $\delta_{\mathcal{H}'}^\dagger$ and

2. The notion of positivity.

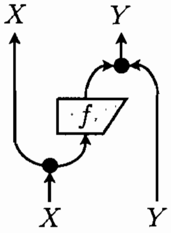
Remark 6.5.1 Above, when writing f as a matrix, we said "as a matrix relative to the basis induced by the basis structures". In the following, we won't specify that it is relative to such or such basis structure but it should be understood that it is implicit.

The concepts of basis structure and positivity are already formalised within our categorical language. Abstracting this we get

[Unfolding of a morphism] The *unfolding* of a morphism $f : X \to Y$ in $\mathbf{C}_b$ is given by

$$(1_X \otimes \delta_Y^\dagger) \circ (1_X \otimes f \otimes 1_Y) \circ (\delta_X \otimes 1_Y).$$

which is depicted as

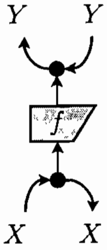


From which,

[Classical morphism] A morphism in $\mathbf{C}_b$ is a *classical morphism* if its unfolding is positive.

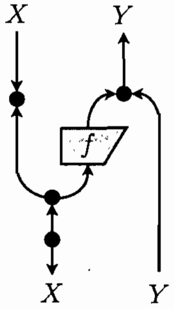
Following our discussion at the beginning of this section, this notion abstracts the notion of real-positive matrices in **FdHilb**. We have

Lemma 6.5.2 A morphism $f : X \to Y$ is classical if and only if

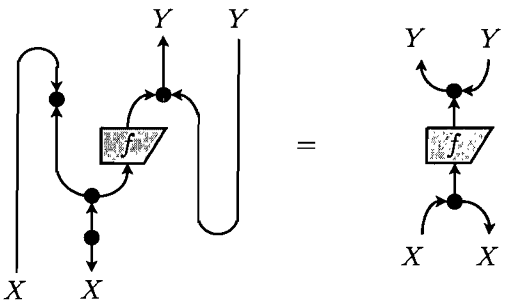


is completely positive.

Proof: The unfolding of f is positive if and only if



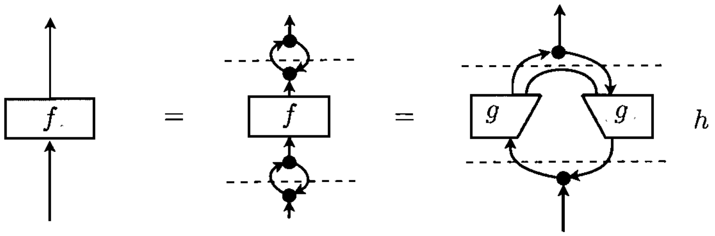
is positive. Indeed, if Unf(f) is positive then, by lemma 5.4.1-a, $(d_X \otimes 1_Y) \circ \mathrm{Unf}(f) \circ (d_X \otimes 1_Y)^\dagger$ is also positive. The converse is also true since $d_X \otimes 1_Y$ is unitary. From there, applying corollary 5.4.4, and the mixed normal form theorem,



is completely positive.

□

Remark 6.5.3 The previous result indicates that the classical morphisms are those $f : X \to Y$ of $\mathbf{C}_b$ such that



where h is completely positive.

Lemma 6.5.4 In $\mathbf{C}_b$,

i. For any $X \in |\mathbf{C}_b|$, 1_X is a classical map.

ii. The composite of classical maps is a classical map.

The proof is postponed to section 7.2

[**The category $\mathbf{C}_c$**] Given a category of basis structures $\mathbf{C}_b$, the category C_c *of classical maps* has for objects the same as $\mathbf{C}_b$ and for morphisms the classical maps in $\mathbf{C}_b$.

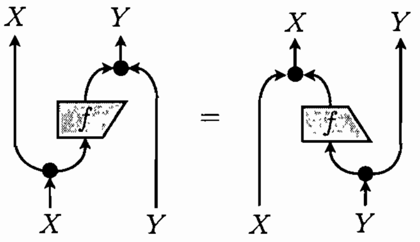
Theorem 6.5.5 The category $\mathbf{C}_c$ is again a category of basis structures. The †-monoidal structure and the basis structures in $\mathbf{C}_c$ are inherited from those of $\mathbf{C}_b$.

The proof of this theorem is also postponed to section 7.2.

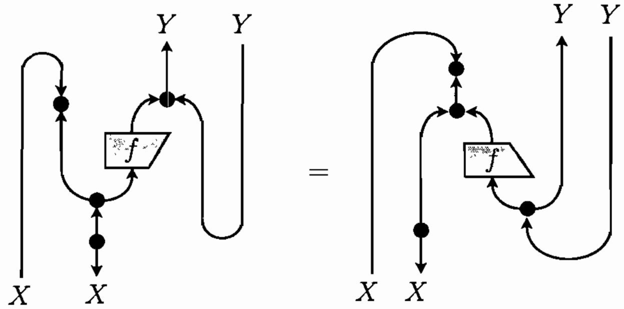
Continuing our analogy with **FdHilb**, classical morphisms therein matrix with real non-negative entries and hence, invariant under complex conjugation. It turns out that an abstract version of this fact is also true:

Proposition 6.5.6 If $f : X \to Y$ is in $\mathbf{C}_c$, then $f_\times = f$.

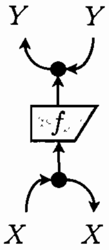
Proof: Suppose f is classical, then by definition $\mathrm{Unf}(f)$ is positive and thus, $\mathrm{Unf}(f) = \mathrm{Unf}(f)^\dagger$. Therefore,



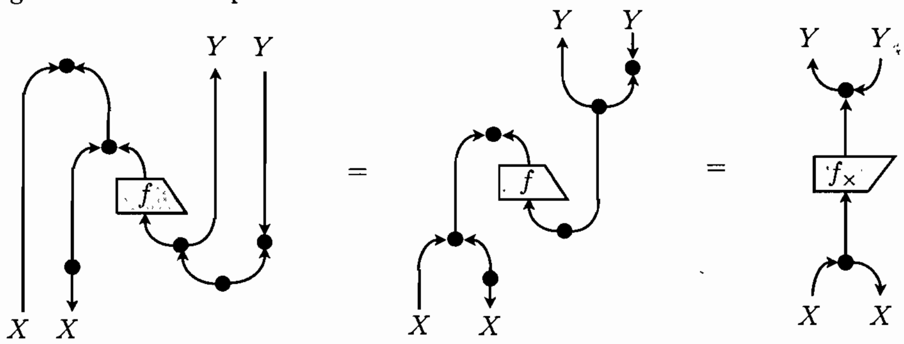
is positive if and only if



is completely positive—c.f. lemma 6.5.2. Now, the left-hand-side of the equality is equal to



while the right-hand side is equal to



with a simple application of the generalised normal form theorem and using the fact that arrows with top to bottom orientation carry a dualiser. Thus, we have

$$F(f_\times) = F(f) \qquad \text{where} \qquad F(-) := (1 \otimes d_X) \circ \delta_X \circ - \circ \delta_X^\dagger \circ (1 \otimes d_X^\dagger).$$

Now, F has a left inverse as $(1 \otimes d_X)$ is unitary and δ_X is an isometry. From this, F is injective so $f_\times = f$.

□

Section 7.3.1 of the next chapter will discuss the class of morphisms we find in $\mathbf{C}_c$ such as stochastic maps, partial maps and others.

7 Classical-quantum interfaces

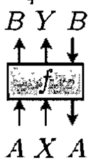
This chapter is the crux of this dissertation. We now take the classical and the quantum fragments of our theory, given respectively by the category of classical maps and the category of completely positive maps, and unify them into a single categorical framework. To do so, we will first define the notion of classical-quantum interfaces that encompass both classical and quantum maps. Then we will construct a category of interfaces that turns out to be a category of quantum structures. We will explain how the classical and the quantum fragment of the theory embed within this new category. Finally, we will provide a complete categorical semantics of all interfaces which contains, for instance, the various class of classical morphisms, states, unitary transformation, controlled-maps, measurements and POVMs.

The results presented here are new and are derived from [33] and [32] that the author wrote with B. Coecke and D. Pavlovic. In contrast to the first paper, we provide here a completely different construction for the category of classical-quantum interfaces which is direct, contrary to what has been done there. The second paper relies on higher-level category theory and, as mentioned in the introduction, we have put substantial efforts throughout this thesis to try to keep the discussion at a reasonable level of abstraction so that it remains (hopefully) intuitive. The major discrepancies between what's published in [32] and the presentation that follows reflect this.

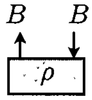
From now on, we assume that we have a fixed category of basis structures $\mathbf{C}_b$, a full subcategory of $\mathbf{C}_q$. When we refer to a basis object $X \in |\mathbf{C}_q|$, we mean an object equipped with a classical structure; such objects are denoted $X, Y, Z, W, \ldots.$ When we refer to a quantum object, we mean any object of $\mathbf{C}_q$ which we denote as $A, B, C, D, \ldots.$

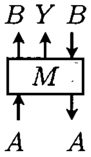
7.1 Classical-quantum interfaces

We will now define the notion of classical-quantum interfaces in $\mathbf{C}_q$. As the name indicates, these interfaces are morphisms of $\mathbf{C}_q$ which define the interactions between the classical and the quantum fragment of the theory. We will take the completely positive maps as the quantum fragment, while the classical fragment is given by classical maps. Following this, instances of classical-quantum interfaces consist of all classical maps, all quantum maps and all non-trivial interfaces such as, for instance, controlled-maps and measurements. The general type of a classical-quantum interface as a morphism of $\mathbf{C}_q$ is

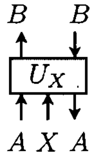


where X and Y are basis objects and A and B quantum objects. The wires labeled by X and Y are understood as carriers of classical data, that is in **FdHilb**, non-negative real data. On the other hand, the wires labeled by A and B are carriers of quantum data. As special instances of interface, a positive element, a measurement and a controlled set of unitaries have respective types

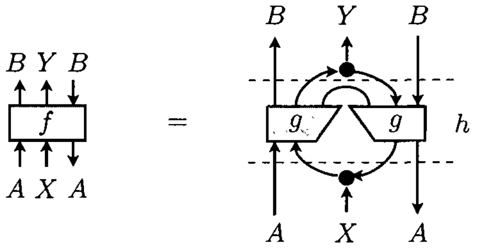




and

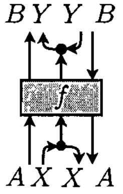


As we take quantum maps to be the morphisms of $\mathbf{CP}(\mathbf{C}_q)$ *i.e.*, completely positive maps in $\mathbf{C}_q$ and that morphisms of $\mathbf{C}_c$ admit a factorisation including a completely positive map (c.f. remark 6.5.3), it makes sense to think that interfaces will admit a representation which is closely related to the form of completely positive maps in $\mathbf{C}_q$. Taking in account the factorisation of classical maps including a completely positive map and the general form of completely positive maps, we expect that interfaces will factorise as



with h completely positive. In the light of the previous remark,

[Classical-quantum interface] Let $A, B \in \mathbf{C}_q$ be quantum objects, $X, Y \in |\mathbf{C}_q|$ be basis objects, $D_X := (1_X \otimes d_X) \circ \delta_X$ and $D_{A,X} := 1_A \otimes D_X \otimes 1_{A^*}$. A *(classical-quantum) interface* in $\mathbf{C}_q$ is a morphism $f : A \otimes X \otimes A^* \longrightarrow B \otimes Y \otimes B^*$ such that $D_{B,Y} \circ f \circ D_{A,X}$, which is depicted by



is completely positive.

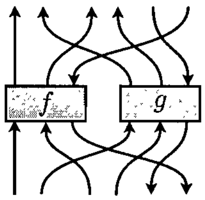
Lemma 7.1.1 In $\mathbf{C}_q$,

a. The identity $1_{A\otimes X\otimes A^*}$ is an interface.

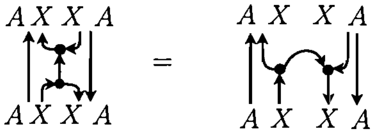
b. If $f : A \otimes X \otimes A^* \longrightarrow B \otimes Y \otimes B^*$ and $g : B \otimes Y \otimes B^* \longrightarrow C \otimes Z \otimes C^*$ are interfaces, then so is their composite $g \circ f : A \otimes X \otimes A^* \longrightarrow C \otimes Z \otimes C^*$.

c. If $f : A \otimes X \otimes A^* \longrightarrow B \otimes Y \otimes B^*$ and $g : C \otimes Z \otimes C^* \longrightarrow D \otimes W \otimes D^*$ are interfaces, then so is

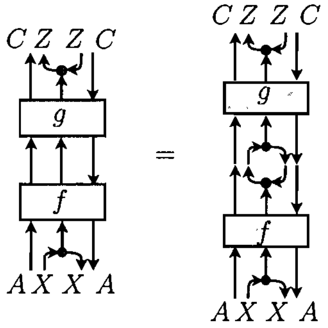
$f \boxtimes g :=$



Proof: For (a), we have

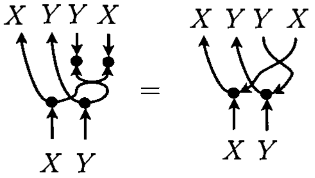


which is seen to be completely positive. For (b), consider

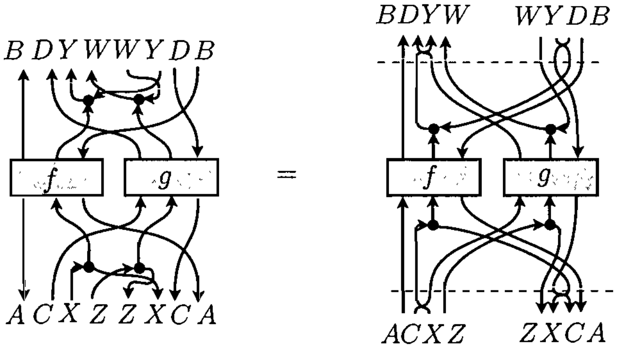


which is completely positive as the composition of completely positive maps is completely positive; therefore, interfaces are closed under composition. For (c), note first that by constraint on the dualisers in $\mathbf{C}_b$,

$D_{X\otimes Y} \;=$



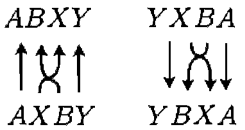
Using this, $D_{B\otimes D,Y\otimes W} \circ (f \boxtimes g) \circ D^{\dagger}_{A\otimes C,X\otimes Z}$ is



where the equality holds via an isomorphism of graph. Now, in the middle part, we have the $\mathbf{CP}(\mathbf{C}_q)$-tensor product of the completely positive maps

$$D_{B,Y} \circ f \circ D^{\dagger}_{A,X} \qquad \text{and} \qquad D_{D,W} \circ f \circ D^{\dagger}_{C,Z}$$

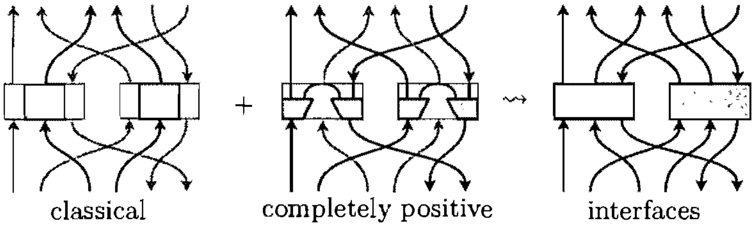
in $\mathbf{C}_q$, which is again completely positive. Finally, the morphisms at the extremities are both of the form



which is completely positive. As the composition of completely positive maps is completely positive, it follows that $D_{B\otimes D,Y\otimes W} \circ (f \boxtimes g) \circ D^{\dagger}_{A\otimes C,X\otimes Z}$ is completely positive as claimed.

□

Remark 7.1.2 The map $f \boxtimes g$ of the previous lemma can be thought of as a "mix" of the tensor product of classical and of completely positive maps. Indeed,



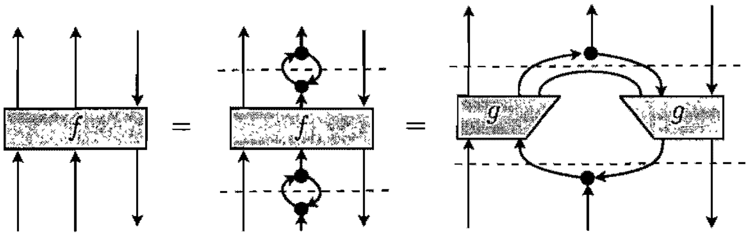
Example 7.1.3 Every completely positive map in $\mathbf{C}_q$ is an interface. Every classical map is an interface by lemma 6.5.2.

Using this, we give

Proof of lemma 6.5.4: The proof of (i) is analogous to the proof of (a) in the previous proposition when considering the identity $1_X : X \longrightarrow X$. For (ii), using lemma 6.5.2 we see that classical maps are interfaces; the proof then becomes the analogue of part (b) in the previous proposition when considering classical interfaces of type $X \longrightarrow Y$ and $Y \longrightarrow Z$.

□

Remark 7.1.4 Interfaces have the form we intended to target. Indeed,

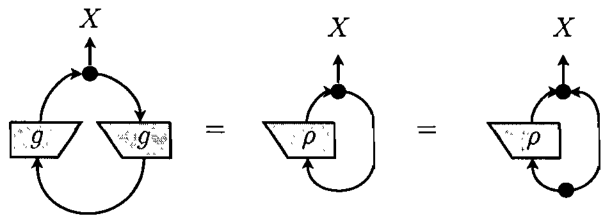


where the first equality follows from the mixed normal form theorem and the second from the notation for completely positive maps.

Now, one may wonder if such a definition is enough to ensure that wires typed with basis objects carry only classical data. We now argue that this is the case. For any positive map $\rho : I \longrightarrow X \otimes X^*$ in **FdHilb** with X is a basis object, we have that

$$D^{\dagger}_X \circ \rho : I \longrightarrow X$$

is a vector with only real positive entry. To see this, let us pass to the standard Dirac notation using



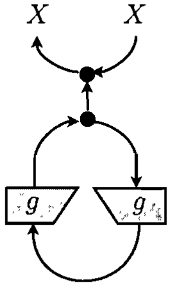
This is

$$\delta_X^\dagger \circ (\rho \otimes 1_X) \circ \nu_X = \sum_l |l\rangle\langle ll| \circ \left(\sum_{i,j} \alpha_{ij}|i\rangle\langle j| \otimes 1_X\right) \circ \sum_k |kk\rangle$$
$$= \sum_i \alpha_{ii}|i\rangle.$$

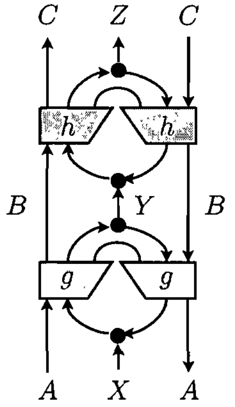
Conversely, if $p : I \to X$ is a column vector with real positive entries then

$$D_X \circ p : I \to X \otimes X^*$$

is a "diagonal" positive map or, correspondingly in the standard notation, a diagonal matrix of type $X \to X$ with all the entries of ρ on the diagonal. Finally, this entails that the composite $D_X \circ D_X^\dagger$ *i.e.*,



decoheres ρ. Thus, we see that if interfaces admit the form given above, then a composite of interfaces of the form



effectively only has classical data running along the vertical wires typed with basis objects.

7.2 The category $\mathbf{CQI}(\mathbf{C}_q)$ of interfaces

As we have seen in lemma 7.1.1, the identity is an interface and interfaces are closed under composition, so we can define

[The category $\mathbf{CQI}(\mathbf{C}_q)$ of interfaces] Given a category of quantum structures $\mathbf{C}_q$ and a full subcategory of basis structures $\mathbf{C}_b \hookrightarrow \mathbf{C}_q$, the *category* $\mathbf{CQI}(\mathbf{C}_q)$ *of Classical Quantum*

Interfaces has for objects pairs (A, X) where A is a quantum object and X a basis object of $\mathbf{C}_q$. A morphism $f : (A, X) \to (B, Y)$ in $\mathbf{CQI}(\mathbf{C}_q)$ is an interface $f : A \otimes X \otimes A^* \to B \otimes Y \otimes B^*$ in $\mathbf{C}_q$. Composition and identities are inherited from $\mathbf{C}_q$.

Theorem 7.2.1 The category $\mathbf{CQI}(\mathbf{C}_q)$ is a category of quantum structures. The symmetric monoidal product

$$\boxtimes : \mathbf{CQI}(\mathbf{C}_q) \times \mathbf{CQI}(\mathbf{C}_q) \to \mathbf{CQI}(\mathbf{C}_q)$$

with unit (I, I) is given on objects by $(A, X) \boxtimes (B, Y) = (A \otimes B, X \otimes Y)$ and on morphisms as in proposition 7.1.1-c. The natural transformation σ has components $\sigma_{(A,X),(B,Y)}$ given by $\sigma_{A,B} \otimes \sigma_{X,Y} \otimes (\sigma_{A,B})_*$ in $\mathbf{C}_q$. If $f : A \otimes X \otimes A^* \to B \otimes Y \otimes B^*$ is an interface in $\mathbf{C}_q$, then $f^\dagger$ in $\mathbf{CQI}(\mathbf{C}_q)$ is given by $f^\dagger : B \otimes Y \otimes B^* \to A \otimes X \otimes A^*$ in $\mathbf{C}_q$. Finally, any $(A, X) \in \mathbf{CQI}(\mathbf{C}_q)$ comes with a quantum structure

$$\langle (A, X), \epsilon_{(A,X)} : (A, X) \boxtimes (A, X)^* \to (I, I) \rangle$$

where $\epsilon_{(A,X)}$ is given by $\epsilon_A \otimes \epsilon_X \otimes (\epsilon_A)_*$ in $\mathbf{C}_q$.

Remark 7.2.2 Because of the expected form of the counit ϵ as an interface in $\mathbf{C}_q$, we will denote $(A, X)^*$ as (A^*, X^*) in what follows.

Proof: There are many equations to verify:

(i) $\mathbf{CQI}(\mathbf{C}_q)$ is symmetric monoidal:

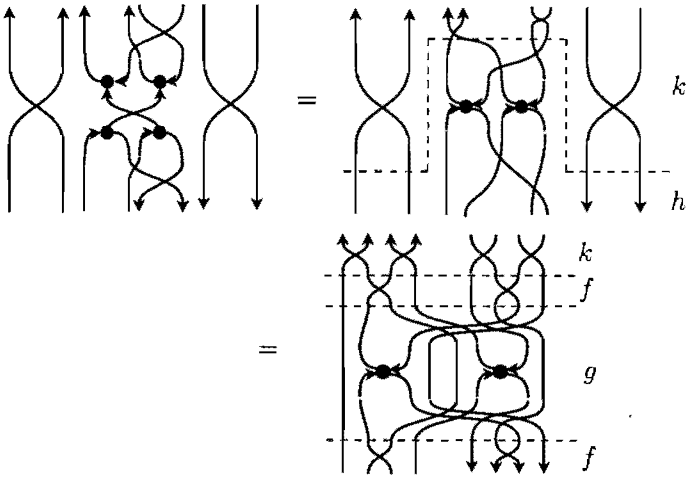
$\boxtimes$ *is a bifunctor.* First, note that the symmetry—say s—on top of $f \otimes g$ in proposition 7.1.1-c is inverse to the one on the bottom. Therefore, $(h \boxtimes k) \circ (f \boxtimes g)$ as an interface in $\mathbf{C}_q$ is

$$s \circ (h \otimes k) \circ s^{-1} \circ s \circ (f \otimes g) \circ s^{-1} {=} s \circ (h \otimes k) \circ (f \otimes g) \circ s^{-1} = s \circ (h \circ f) \otimes (k \circ g) \circ s^{-1}.$$

which is $(h \circ f) \boxtimes (k \circ g)$ in $\mathbf{CQI}(\mathbf{C}_q)$.

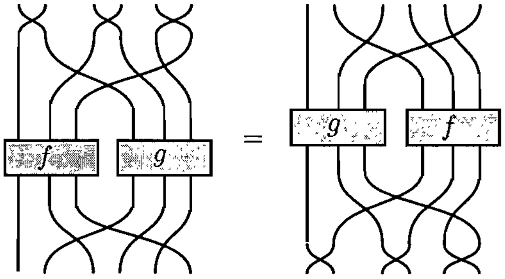
$\boxtimes$ *is a monoidal product with unit* (I, I). This follows directly from the definitions.

$\boxtimes$ *is symmetric.* For the symmetry, using the mixed normal form theorem and some isomorphisms of graph, we get



Now, g is the $\mathbf{CP}(\mathbf{C}_q)$-tensor product of completely positive maps in $\mathbf{C}_q$ hence completely positive. Moreover, since f and k are completely positive, it follows that the composite $k \circ h =$

$k \circ (f \circ g \circ f)$ is also completely positive, hence the symmetry is an interface. We now have to show that σ is a natural isomorphism. Manifestly, for any interfaces f and g, we have



Thus, σ is natural. The inverse of $\sigma_{(A,X),(B,Y)}$, $\sigma^{-1}_{(A,X),(B,Y)}$ is the interface

$$\sigma^{-1}_{A,B} \otimes \sigma^{-1}_{X,Y} \otimes \sigma^{-1}_{B^*,A^*}$$

in $\mathbf{C}_q$ and thus, σ is a natural isomorphism.

(ii) $\mathbf{CQI}(\mathbf{C}_q)$ is $\dagger$-symmetric monoidal:

The adjoint of an interface is an interface. Let $f : A \otimes X \otimes A^* \to B \otimes Y \otimes B^*$ be an interface in $\mathbf{C}_q$ *i.e.*, it is such that $D_{B,Y} \circ f \circ D^{\dagger}_{A,X}$ is completely positive. Consider,

$$D_{A,X} \circ f^{\dagger} \circ D^{\dagger}_{B,Y} = \left(D_{B,Y} \circ f \circ D^{\dagger}_{A,X}\right)^{\dagger},$$

as the adjoint of a completely positive map is a completely positive it follows that $f^{\dagger}$ is also an interface giving $f^{\dagger}$ in $\mathbf{CQI}(\mathbf{C}_q)$.

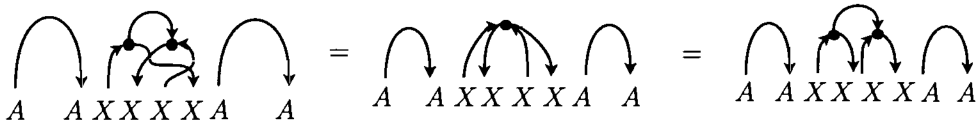
$\mathbf{CQI}(\mathbf{C}_q)$ *is* $\dagger$*-monoidal:* The dagger commutes with the monoidal product as $(f \boxtimes g)^{\dagger}$ is given in $\mathbf{C}_q$ as

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

which is $f^{\dagger} \boxtimes g^{\dagger}$ in $\mathbf{CQI}(\mathbf{C}_q)$. Moreover, we also have $\sigma^{\dagger}_{(A,X),(B,Y)} = \sigma^{-1}_{(A,X),(B,Y)}$ directly from the definitions. From which $\mathbf{CQI}(\mathbf{C}_q)$ is indeed $\dagger$-monoidal.

(iii) $\mathbf{CQI}(\mathbf{C}_q)$ is a category of quantum structures:

We first check that $\epsilon_A \otimes \epsilon_X \otimes (\epsilon_A)_*$ is an interface: via an application of the mixed normal form, we have



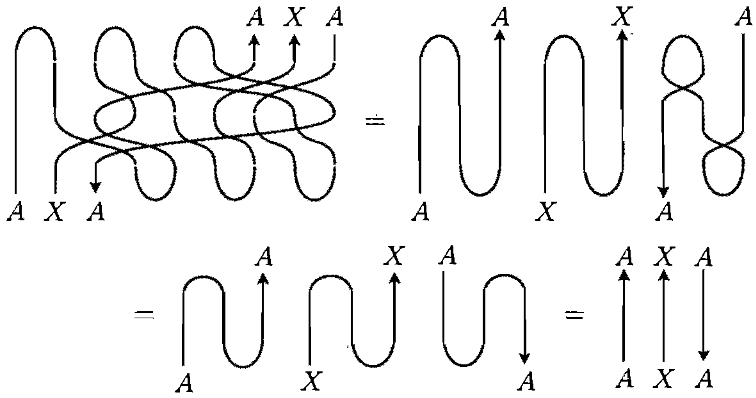
which is completely positive. Further, let

$$\eta_{(A,X)} : (I, I) \to (A^*, X^*) \boxtimes (A, X)$$

be $\eta_A \otimes \eta_X \otimes (\eta_A)_*$ in $\mathbf{C}_q$ where η_A and η_X the units of the quantum structures on A and X respectively. It is seen to be an interface using an analogue argument as the one given for the counit. The equation

$$(\epsilon_{(A,X)} \boxtimes 1_{(A,X)}) \circ (1_{(A,X)} \boxtimes \eta_{(A,X)}) = 1_{(A,X)}$$

is satisfied as the left-hand side is



as required. The dual equation is obtained in the same manner from which the objects of $\mathbf{CQI}(\mathbf{C}_q)$ are equipped with compact structures. To show that they are equipped with quantum structures, we must show that for any $(A, X) \in \mathbf{D}$,

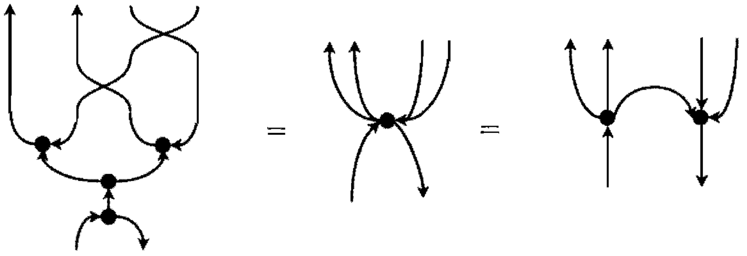
$$\begin{tikzcd}
(I,I) \arrow[r, "\epsilon^{\dagger}_{(A,X)}"] \arrow[dr, "\eta_{(A,X)}"'] & (A,X) \boxtimes (A^*,X^*) \arrow[d, "\sigma_{(A^*,X^*),(A,X)}"] \\
 & (A^*,X^*) \boxtimes (A,X)
\end{tikzcd}$$

commutes but this again follows directly from the definitions as well as $\epsilon_{(A^*,X^*)} = \epsilon_{(A,X)} \circ \sigma_{(A,X)}$. Hence, $\mathbf{CQI}(\mathbf{C}_q)$ is a category of quantum structures.

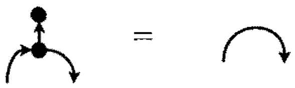
□

Using the proof of the previous theorem, we may now prove that $\mathbf{C}_c$ is a category of basis structures:

Proof of theorem 6.5.5: Using lemma 6.5.2, the first part of the proof has already been proved implicitly in theorem 7.2.1 by considering classical interfaces, *i.e.*, classical morphism $X \to Y$ in $\mathbf{C}_b$. It remains to show that the objects of $\mathbf{C}_c$ inherit their basis structure from $\mathbf{C}_b$. First, given any $X \in |\mathbf{C}_c|$, δ_X is also in $\mathbf{C}_c$ as using the generalised normal form theorem one sees that



is completely positive. For μ_X,



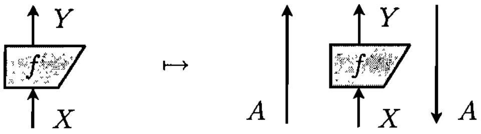
which is completely positive. Thus, for any X, both δ_X and μ_X are in $\mathbf{C}_c$. It remains to check that they satisfy the required equations, but this is the case since the composition, identities and tensor product are inherited from $\mathbf{C}_b$. The same applies for the dualisers, as the quantum structures are inherited from $\mathbf{C}_b$ and thus, so are the basis structures.

□

It remains to say how $\mathbf{CP}(\mathbf{C}_q)$ and $\mathbf{C}_c$ embed in $\mathbf{CQI}(\mathbf{C}_q)$. For $\mathbf{C}_c$, it is easy to see that for any $A \in |\mathbf{C}_q|$ there is a faithful canonical functor

$$C_A : \mathbf{C}_c \to \mathbf{CQI}(\mathbf{C}_q) :: X \mapsto (A, X).$$

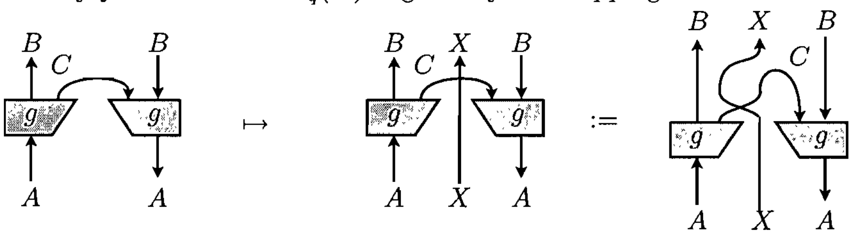
mapping any $f : X \to Y$ in $\mathbf{C}_c$ unto an $f' \in \mathbf{CQI}(\mathbf{C}_q)$ corresponding to the interface $1_A \otimes f \otimes 1_{A^*}$ in $\mathbf{C}_q$ that is:



For $\mathbf{CP}(\mathbf{C}_q)$, again for any $X \in |\mathbf{C}_b|$, there is a faithful canonical functor

$$Q_X : \mathbf{CP}(\mathbf{C}_q) \to \mathbf{CQI}(\mathbf{C}_q) :: A \mapsto (A, X)$$

whose action on any $f : A \to B$ in $\mathbf{CP}_q(\mathbf{C})$ is given by the mapping of interfaces



in $\mathbf{C}_q$. Thus, as we mentioned at the beginning of this section, the quantum and the classical fragment of our theory embed in the category of interfaces.

7.3 Categorical semantics of all data

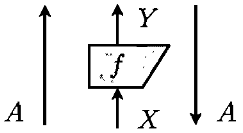
We now inspect the different types of interfaces. This will give us a complete semantics to describe quantum protocols as we will see in the next chapter. There are three major families of interfaces given by: classical maps, quantum maps and interaction maps.

7.3.1 Classical maps

The classical maps in $\mathbf{CQI}(\mathbf{C}_q)$ are those in the range of the functors

$$C_{\_} : \mathbf{C}_c \to \mathbf{CQI}(\mathbf{C}_q)$$

as defined in the preceding section. Thus, a general classical map in $\mathbf{CQI}(\mathbf{C}_q)$ is depicted as



To simplify the presentation, as maps $f : (I, X) \to (I, Y)$ are classical interfaces or morphisms of $\mathbf{C}_c$, we won't specify the particular type of such maps in $\mathbf{CQI}(\mathbf{C}_q)$ but we must keep in mind that this category embeds faithfully in $\mathbf{CQI}(\mathbf{C}_q)$.

We now classify classical interfaces in terms of their δ- and μ-preservation. Such a classification is summarised in

$$\begin{tikzcd}
 & \text{Classical maps} & \\
\text{Relations} \arrow[ur] & & \text{Stochastic maps } (\mu) \arrow[ul] \\
\text{Partial maps } (\delta) \arrow[u] & & \\
\text{Functions } (\delta,\mu) \arrow[u] \arrow[uurr] & & \text{Doubly stochastic maps } (\mu,\mu^\dagger) \arrow[uu] \\
 & \text{Permutations } (\delta,\mu,\delta^\dagger,\mu^\dagger) \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

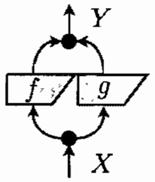
where the different types of classical maps are ordered by inclusion.

1. **Relations**

[Convolution] Let $X, Y \in |\mathbf{C}_c|$ and $f, g : X \to Y$. The *convolution* of f and g as

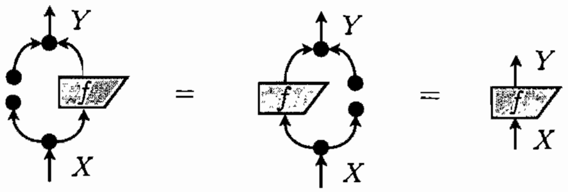
$$f * g = \delta_Y^\dagger \circ (f \otimes g) \circ \delta_X$$

which is depicted as



Lemma 7.3.1 **[Convolution monoid]** For any $X, Y \in \mathbf{C}_c$, the triple $\langle [X,Y], *, \iota_{X,Y} \rangle$ where $[X,Y] := \mathbf{C}_c(X,Y)$, $*$ is the convolution and $\iota_{X,Y} := \mu_Y \circ \mu_X$, is a commutative monoid called the *convolution monoid of X and Y*.

Proof: This is almost trivial. Indeed, it is immediate that $f * g \in [X,Y]$. To see that $\iota_{X,Y}$ is indeed a unit, consider $f : X \to Y$, then



Finally, associativity and commutativity of $*$ follows directly from the (co)commutativity and the (co)associativity of the (co)multiplication of the †-Frobenius structure on the objects of $\mathbf{C}_c$. □

Example 7.3.2 The convolution monoid $[I, I]$ is the monoid of scalars.

Example 7.3.3 In $\mathbf{FdHilb}_c$, since $\delta_X := \sum_i |ii\rangle\langle i|$ an easy calculation shows that the convolution of two matrices $f = \sum_{i,j} \alpha_{ij} |j\rangle\langle i|$ and $g = \sum_{i',j'} \beta_{i'j'} |j'\rangle\langle i'|$ is

$$f * g = \sum_{ij} \alpha_{ij}\beta_{ij}|j\rangle\langle i|.$$

This is nothing but the product of the entries of the two matrices. From this, it is easy to see that the identity $\iota_{X,Y}$ of a convolution monoid in **FdHilb** is a matrix of ones which indeed coincides with $\mu_Y^\dagger \circ \mu_X$.

[**Relation**] A map $R \in \mathbf{C}_c(X,Y)$ is a relation if it is idempotent under the convolution *i.e.*: $R = R * R$.

This definition makes sense taking the following two facts into account:

- The category **Rel**, since it admits a biproduct via the disjoint union, admits a matrix calculus (c.f. [35]); there, the matrices have entries in the boolean semiring $\mathbb{B}$ where both **0** and **1** are idempotent.
- Now, taking into account the example 7.3.3 and since the only two idempotent elements in $\mathbb{C}$ are 0 and 1, the previous definition indeed defines a relation in that perspective.

Manifestly, relations thus defined in a category of classical maps aren't closed under composition in general since they are not so in **FdHilb**. Indeed, consider

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix} \circ \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix} = \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}$$

the latter is not idempotent under convolution, so it is not a relation. However, we can overcome this problem by defining the suitable quotient category.

Lemma 7.3.4 Given any $X, Y \in \mathbf{FdHilb}_c$ and $f, g \in \mathbf{FdHilb}_c(X,Y)$, we say that $f \sim g$ if for all i and j, either

1. $(f)_{i,j} = (g)_{i,j} = 0$ or
2. both $(f)_{i,j}$ and $(g)_{i,j}$ are different from 0.

The binary relation $\sim$ is a congruence relation on **FdHilb** such that every class of equivalence contains exactly one relation as defined above.

Proof: Indeed, $\sim$ is reflexive symmetric and transitive so that it is an equivalence relation. We now need to show that if $f, f' : X \to Y$ are related in $\mathbf{FdHilb}_c(X,Y)$ and $g, g' : Y \to Z$ are related in $\mathbf{FdHilb}_c(Y,Z)$, then both $g \circ f$ and $g' \circ f'$ are related in $\mathbf{FdHilb}_c(X,Z)$. This is the case as these matrices have only non-negative real entries. Indeed,

$$(g \circ f)_{ij} = \sum_k (g)_{ik}(f)_{kj} = 0 \text{ if and only if for all } k \text{ , } (g)_{i,k} \text{ or } (f)_{k,j} = 0$$

and

$$(g' \circ f')_{ij} = \sum_k (g')_{ik}(f')_{kj} = 0 \text{ if and only if for all } k \text{ , } (g')_{i,k} \text{ or } (f')_{k,j} = 0.$$

Since $f \sim f'$ and $g \sim g'$, it follows that $(g \circ f)_{ij} = 0$ if and only if $(g' \circ f')_{ij} = 0$. In all the other cases, both $(g \circ f)_{kl}$ and $(g' \circ f')_{kl}$ are non-zero. Thus, $\sim$ is indeed a congruence relation on $\mathbf{FdHilb}_c$.

For the second claim, this is almost immediate; indeed, if $f \sim R$ where R is a relation, then they must have 0's in the same entries and where $(f)_{ij} \neq 0$, $(R)_{i,j} = 1$. Such an R is manifestly unique thus the result.

□

From this and using the definition of quotient category given in section 3.2,

[The category FdHilb$_R$] [4,6] The quotient category **FdHilb**$_R$ has

- The same objects as **FdHilb**$_c$ and
- As morphisms, equivalence classes of morphisms under $\sim$.

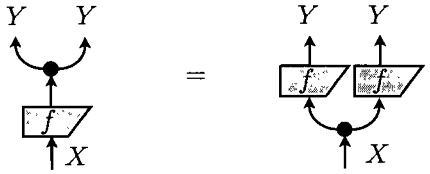
Remark 7.3.5 We gave this construction for the sake of completeness. When we speak of a relation below, we just mean a morphism which is idempotent under convolution and not an equivalence class of morphisms.

2. Partial maps

[Partial map] A *partial map* in $\mathbf{C}_c$ is a relation $f : X \to Y$ such that

$$\delta_Y \circ f = (f \otimes f) \circ \delta_X.$$

Graphically, this is



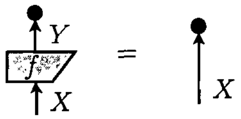
In **FdHilb**$_c$, such a morphism is a partial relation in the usual sense. Indeed, it is a matrix with at most one one in each column and zeros elsewhere.

3. Functions

[Function] A *function* in $\mathbf{C}_c$ is a partial map $f : X \to Y$ such that

$$\mu_Y \circ f = \mu_X.$$

This is depicted as



Again, in **FdHilb**$_c$, these are functions in the usual sense. That is, such an f has exactly one one in each column a zeros elsewhere.

4. Stochastic maps

[Stochastic map] A *stochastic map* in $\mathbf{C}_c$ is a morphism $f : X \to Y$ such that

$$\mu_Y \circ f = \mu_X.$$

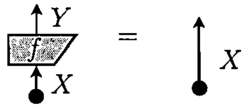
In **FdHilb**$_c$, these corresponds to stochastic matrices. Indeed, since $\mu_X = \sum_i \langle i|$, $\mu_Y \circ f = \mu_X$ entails that each column of non-negative real numbers of f have entries which sum to 1. Moreover, note that total maps are particular instances of stochastic maps.

5. Doubly stochastic maps.

[Doubly stochastic map] A *doubly stochastic map* in $\mathbf{C}_c$ is a stochastic map $f : X \to Y$ such that

$$f \circ \mu_X^\dagger = \mu_Y^\dagger.$$

That is,



In **FdHilb**, this means that both the columns and the rows of f sum to 1, thus, this is the usual notion of doubly stochastic matrix.

6. Bijection

[Bijection] A *bijection* $f : X \to Y$ in $\mathbf{C}_c$ is a function such that $f^\dagger$ is also a function. In other words, this entails that it preserves δ, μ and their adjoints.

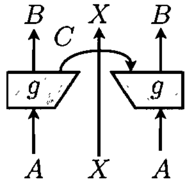
In **FdHilb**$_c$ these correspond to the usual notion of bijection that is a matrix with exactly one 1 in each row and each column and zeros elsewhere. Moreover, bijections are at once particular instances of functions and doubly stochastic maps.

7.3.2 Quantum maps

The quantum maps in **CQI**($\mathbf{C}_q$) are those in the range of the functors

$$Q_- : \mathbf{CP}(\mathbf{C}_q) \to \mathbf{CQI}(\mathbf{C}_q)$$

defined at the end of section 7.2. Such maps are depicted as:



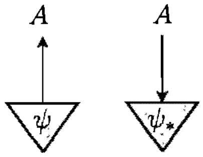
However, note that throughout this section, we will depict such maps as their images under Q_I so that we won't clutter the notation with central wires.

7. Pure states

[Pure state] A *pure state* in **CQI**($\mathbf{C}_q$) is a map $\psi : (I, I) \to (A, I)$ with

$$\psi = \phi \otimes \phi_* : I \otimes I^* \to A \otimes A^*$$

in $\mathbf{C}_q$. Such a map is depicted as



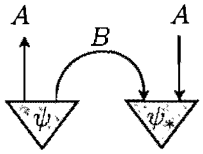
These exactly coincide with pure states in $\mathbf{CP}(\mathbf{C}_q)$.

8. Mixed states.

[Mixed state] A *mixed state* in $\mathbf{CQI}(\mathbf{C}_q)$ is a map of the form $\rho : (I, I) \to (A, I)$ with

$$\rho = (1_A \otimes \epsilon_B \otimes 1_{A^*}) \circ (\psi \otimes \psi_*) : I \otimes I^* \to A \otimes A^*$$

in $\mathbf{C}_q$. It depicts as



Again, these correspond to mixed states in $\mathbf{CP}(\mathbf{C}_q)$.

9. Unitary transformations

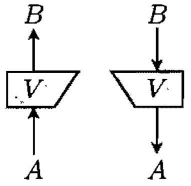
[Unitary transformation] A *unitary transformation* in $\mathbf{CQI}(\mathbf{C}_q)$ is a map of type $U : (A, I) \to (B, I)$ with

$$U = V \otimes V_* : A \otimes A^* \to B \otimes B^*$$

in $\mathbf{C}_q$ such that

$$U^\dagger \circ U = 1_{(A,I)} \quad \text{and} \quad U \circ U^\dagger = 1_{(B,I)}.$$

A unitary transformation is depicted as



Again, such a map corresponds to unitary transformations in $\mathbf{CP}(\mathbf{C}_q)$.

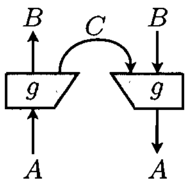
10. Quantum operations

Finally,

[Quantum operations] A (generic) *quantum operation* in $\mathbf{CQI}(\mathbf{C}_q)$ is a map of type $f : (A, I) \to (B, I)$ with

$$f = (1_B \otimes \epsilon_C \otimes 1_{B^*}) \circ (g \otimes g_*) \circ (1_A \otimes 1_{A^*}) : A \otimes A^* \to B \otimes B^*$$

that is



These are generic maps in $\mathbf{CP}(\mathbf{C}_q)$ *i.e.*, completely positive maps in $\mathbf{C}_q$.

7.3.3 Interaction maps

Interactions maps is the last family of transformations in our semantics. It consists of those maps of $\mathbf{CQI}(\mathbf{C}_q)$ where classical and quantum data interact as, for instance, in measurements or in controlled operations. In both cases, we will obtain families of maps indexed by a basis object X. By extension, we will often need to define some properties relative to X.

Controlled maps are those maps of $\mathbf{CQI}(\mathbf{C}_q)$ of type

$$f : (A, X) \to (B, I).$$

In order to justify the idea, consider the following result:

Lemma 7.3.6 In **FdHilb**, if

$$f : \mathcal{H} \otimes X \to \mathcal{H}'$$

where X admit a basis structure—and consequently a basis $\{|i\rangle\}_i$—and $\mathcal{H}, \mathcal{H}'$ a quantum structure. Then, f can be written as a row vector of operators

$$f = \sum_i F_i \otimes \langle i|$$

for some set of operators $\{F_i : \mathcal{H} \to \mathcal{H}'\}$.

Proof: We have

$$\begin{aligned} f &= f \circ 1_{\mathcal{H}\otimes X} \\ &= f \circ (1_{\mathcal{H}} \otimes \textstyle\sum_i |i\rangle\langle i|) \\ &= \textstyle\sum_i f \circ (1_{\mathcal{H}} \otimes |i\rangle\langle i|) \\ &= \textstyle\sum_i (f \circ (1_{\mathcal{H}} \otimes |i\rangle)) \otimes \langle i| \end{aligned}$$

Setting $F_i := f \circ (1_{\mathcal{H}} \otimes |i\rangle) : \mathcal{H} \to \mathcal{H}'$, the last expression can be re-written as

$$\sum_i F_i \otimes \langle i|$$

as required.

□

We can generalise this to a category of interfaces. Indeed, an instance of map of type $\mathcal{F} : (\mathcal{H}, X) \to (\mathcal{H}', \mathbb{C})$ in **CQI(FdHilb)** is given by an interface

$$(f \otimes f_*) \circ D_{\mathcal{H},X} \quad \text{with} \quad f : \mathcal{H} \otimes X \to \mathcal{H}',$$

in **FdHilb**. Using the previous lemma and the definition of $D_{\mathcal{H},X}$, we get

$$(f\otimes f_*)\circ D_{\mathcal{H},X} = \left(\left(\sum_i F_i\otimes\langle i|\right)\otimes\left(\sum_j\langle j|\otimes F_{j_*}\right)\right)\circ(1_{\mathcal{H}}\otimes 1_X\otimes d_X\otimes 1_{\mathcal{H}^*})\circ(1_{\mathcal{H}}\circ\delta_X\otimes 1_{\mathcal{H}^*}).$$

From this, as $\delta_X = \sum_k |kk\rangle\langle k|$, we see that if $1_{\mathcal{H}}\otimes|l\rangle\otimes 1_{\mathcal{H}'}$ is composed with the previous expression, we get

$$(F_l\otimes F_{l*})\circ(-).$$

Taking a positive map $\rho : \mathbb{C}\longrightarrow\mathcal{H}\otimes\mathcal{H}'$ as input in the previous expression and passing to standard notation, we get

$$F_l\circ\rho\circ F_l^\dagger.$$

Thus, indeed, classical data controls which operation in $\{F_i\otimes(F_i)_*\}_i$ is applied. Of course, this is just a generic map taken as an example but the following few cases are instances related to what we need in quantum computation.

11. Controlled unitaries.

We now introduce the notion of controlled-unitaries as was introduced in [36]. When taking a map $U : (A,X)\longrightarrow(B,I)$ as controlled unitary, the usual characterisation of unitary transformation, *i.e.*,

$$U^\dagger\circ U = U\circ U^\dagger = 1$$

is no longer valid as we have a type mismatch. However, we have the following result:

Proposition 7.3.7 [36] Let $X\in|\mathbf{FdHilb}|$ be a basis object with †-Frobenius structure

$$\langle X,\delta_X,\mu_X\rangle \quad\text{where}\quad \delta_X := \sum_i |ii\rangle\langle i| \;\text{ and }\; \mu_X := \sum_i\langle i|.$$

Then a map $U : \mathcal{H}\otimes X\longrightarrow\mathcal{H}$ satisfies

$$\begin{aligned}1_{\mathcal{H}\otimes X} &= (1_{\mathcal{H}}\otimes\delta_X^\dagger)\circ(U^\dagger\otimes 1_X)\circ(U\otimes 1_X)\circ(1_{\mathcal{H}}\otimes\delta_X)\\ &= (U\otimes 1_X)\circ(1_{\mathcal{H}}\otimes\delta_X)\circ(1_{\mathcal{H}}\otimes\delta_X^\dagger)\circ(U^\dagger\otimes 1_X)\end{aligned}\tag{7.1}$$

if and only if

$$U = \sum_i U_i\otimes\langle i|\tag{7.2}$$

where for all i, $U_i : \mathcal{H}\longrightarrow\mathcal{H}$ is unitary.

The result was not proven in the cited paper, so we provide a proof here:

Proof: Suppose that U satisfies (7.1). Since we have a †-Frobenius structure on $\mathcal{H}$ and these are in bijection with orthonormal bases, we can write U as a vector of matrices A_j *i.e.*,

$$U = \sum_j\langle j|\otimes A_j.$$

Using this, the first equality of (7.1) becomes

$$\begin{aligned}
1_{\mathcal{H}\otimes X} &= (1_{\mathcal{H}}\otimes\delta_X^{\dagger})\circ\left(\sum_{j,j'}(A_{j'}^{\dagger}\circ A_j)\otimes|j'\rangle\langle j|\right)\circ(1_{\mathcal{H}}\otimes\delta_{\mathcal{H}})\\
&= (1_{\mathcal{H}}\otimes\sum_l|l\rangle\langle ll|)\circ\left(\sum_{j,j'}(A_{j'}^{\dagger}\circ A_j)\otimes|j'\rangle\langle j|\right)\circ(1_{\mathcal{H}}\otimes\sum_{l'}|l'l'\rangle\langle l'|)\\
&= \left(\sum_{ll'}(A_l\circ A_{l'}^{\dagger})\otimes|l\rangle\langle l'|\right)\langle l|l'\rangle\\
&= \sum_l(A_l\circ A_l^{\dagger})\otimes|l\rangle\langle l|
\end{aligned}$$

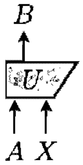
Hence, we must have $A_{j'}\circ A_j^{\dagger}=1_{\mathcal{H}}$ since the whole expression is equal to $1_{\mathcal{H}}\otimes 1_X$ showing that for all j, A_j is an isometry. Using the second equation gives that for all j, A_j is unitary.

The right to left implication follows directly by calculation.

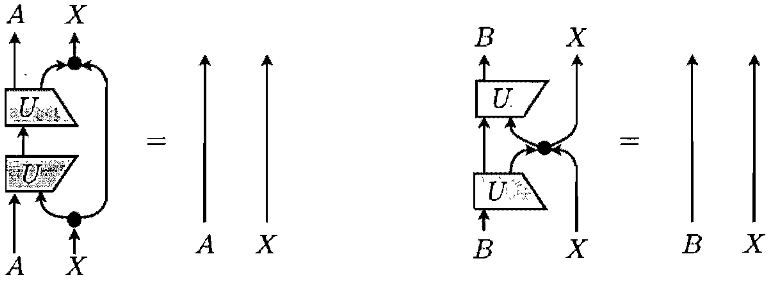
□

In other words, we have a bijection between tuples of unitaries and the maps satisfying (7.1). Translating this to a quantum structures $\mathbf{C}_q$, one gets

[X-**unitary morphism**] [36] An X-*unitary* is a morphism $U : A\otimes X\rightarrow B$ which is depicted as



where X is equipped with a basis structure and both A and B with a quantum structure and such that



Lifting the notion to $\mathbf{CQI}(\mathbf{C}_q)$ yields

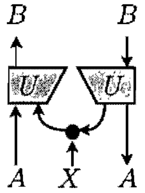
[**Controlled-unitary**] A *controlled-unitary* in $\mathbf{CQI}(\mathbf{C}_q)$ is a morphism

$$\mathcal{U} : \langle A, X\rangle \rightarrow \langle B, I\rangle$$

with

$$\mathcal{U} = (U\otimes U_*)\circ D_{A,X}$$

in $\mathbf{C}_q$ and where U is an X-unitary. Such a morphism is depicted as

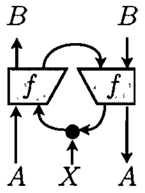


12. Controlled quantum maps

These are the most general controlled maps *i.e.*, controlled completely positive operations $\mathcal{F} : (A, X) \longrightarrow (B, I)$ with

$$\mathcal{F} = (1_B \otimes \epsilon_C \otimes 1_{B^*}) \circ (f \otimes f_*) \circ D_{A,X}$$

in $\mathbf{C}_q$. These are depicted as



13. Projective measurements

At the beginning of chapter 8, we have said that the type of quantum measurement is

Initial quantum state $\mapsto$ Final quantum state $\otimes$ Classical output.

We now inspect what this means in details. Manifestly, the above is translated within our construction as a morphism

$$A \longrightarrow A \otimes X$$

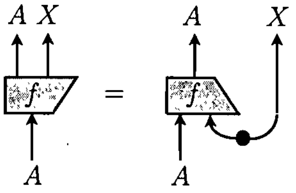
in $\mathbf{C}_q$ where A is a quantum object and X is a basis object. However, just having the right type is manifestly not enough. Indeed, we have seen in chapter 2 that a projective measurement is defined by a set of projectors $\{P_i\}_i$ which are self-adjoint, idempotent and mutually orthogonal. Moreover, such a projective measurement is *complete* if $\sum_i P_i = 1$. Our plan is now to find an analogue of these notion in $\mathbf{C}_q$. Again, the basis of the presentation is taken from [36].

First, we handle the notion of

[Self-adjointness relative to a basis object] [36] Let $X \in |\mathbf{C}_q|$ be a basis object. A morphism $f : A \longrightarrow A \otimes X$ is *self-adjoint relative to* X, or X *self-adjoint*, if

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "1_A\otimes\nu_X"'] & A \otimes X \\
& A \otimes X \otimes X \arrow[u, "f^\dagger\otimes 1_X"']
\end{tikzcd}$$

commute. This is depicted as

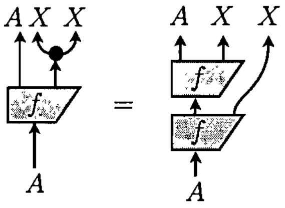


Now, for

[Idempotence relative to a basis object] [36] A morphism $f : A \longrightarrow A \otimes X$ is *idempotent relative to* X, or X*-idempotent* if

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "f"'] & A \otimes X \arrow[d, "f\otimes 1_X"] \\
A \otimes X \arrow[r, "1_A\otimes\delta_X"'] & A \otimes X \otimes X
\end{tikzcd}$$

commute. This is



From there, we can define

[**X-Projector**] [36] An *X-projector* is a morphism $P : A \to A \otimes X$ which is X-self-adjoint and X-idempotent.

Proposition 7.3.8 In **FdHilb**, a $\mathbb{C}^n$-projector $P : \mathcal{H} \to \mathcal{H} \otimes \mathbb{C}^k$ where $\mathcal{H} \simeq \mathbb{C}^n$ exactly corresponds to a family of k mutually orthogonal projectors $\{P_i\}_{i=1}^k$, hence we have $\sum_{i=1}^k P_i \leq 1_{\mathcal{H}}$.

Proof: See [36].

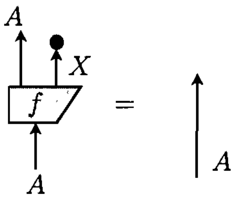
□

It just remains to handle the notion of completeness which, unsurprisingly, relates to μ_X.

[**Completeness relative to a basis object**] A morphism $f : A \to A \otimes X$ is *complete relative to a basis object X*, or *X-complete* if

$$(\mu_X \otimes 1_A) \circ f = 1_A$$

which is depicted as



Finally,

[**Projector-valued spectrum**] [36] A morphism $P : A \to A \otimes X$ is a *projector-valued spectrum* if it is an X-complete X-projector.

From which

Theorem 7.3.9 [36] Projector-valued spectra in **FdHilb** exactly correspond to complete families of mutually orthogonal projectors $\{P_i\}_i$ *i.e.*, $\sum_i P_i = 1_{\mathcal{H}}$.

Proof: See [36].

□

With this, in **FdHilb**, given a state $\psi : \mathbb{C} \to \mathcal{H}$ and a projector-valued spectrum $P : \mathcal{H} \to \mathcal{H} \otimes X$ where $X := \mathbb{C}^n$, then

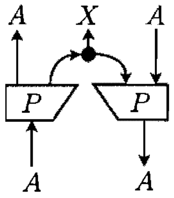
$$P \circ \psi = \sum_i \langle i|\psi\rangle(|i\rangle \otimes |i\rangle)$$

As already mentioned, the outcome is still in coherent superposition. We can lift the notion to $\mathbf{CQI(C}_q\mathbf{)}$ so that

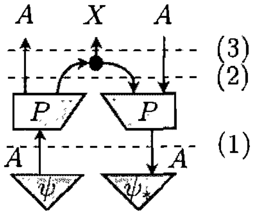
[Projective measurement] A *projective measurement* is a morphism $\mathcal{P} : (A, I) \to (A, X)$ with

$$\mathcal{P} = (1_A \otimes \delta_X \otimes 1_{A^*}) \circ (1_A \otimes 1_X \otimes d_X^\dagger) \circ (P \otimes P_*)$$

in $\mathbf{C}_q$ and where $P : A \to A \otimes X$ is an X-projector. A projective measurement is *complete* if, in addition, P is a projector valued spectrum. Such a morphism depicts as



Now, this is exactly what we want. Indeed, separating the various steps in



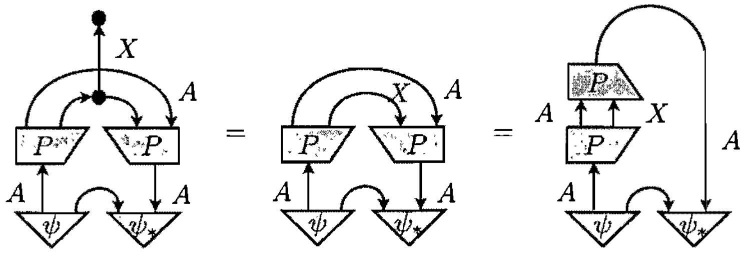
and again taking $X := \mathbb{C}^n$, and $|\psi\rangle := \sum_i \langle i|\psi\rangle|i\rangle$ and $\alpha_i := \langle i|\psi\rangle$, we get

$$\begin{aligned} \textstyle\sum_{i,j} \alpha_i\overline{\alpha_j}\; |i\rangle_{\mathcal{H}} \otimes |j\rangle_{\mathcal{H}^*} &\mapsto \textstyle\sum_{i,j} \alpha_i\overline{\alpha_j}\; |i\rangle_{\mathcal{H}} \otimes |i\rangle_X \otimes |j\rangle_{X^*} \otimes |j\rangle_{\mathcal{H}^*} \\ &\mapsto \textstyle\sum_{i,j} \alpha_i\overline{\alpha_j}\; |i\rangle_{\mathcal{H}} \otimes \delta_{i,j}\; |i\rangle_X \otimes |j\rangle_{\mathcal{H}^*} \\ &= \textstyle\sum_i \alpha_i\overline{\alpha_i}\; |i\rangle_{\mathcal{H}} \otimes |i\rangle_X \otimes |i\rangle_{\mathcal{H}^*} \end{aligned}$$

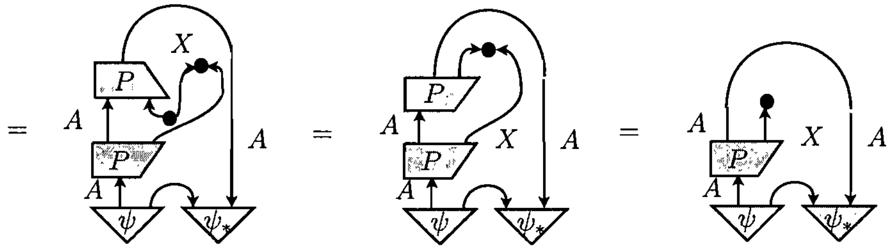
thus, the output is no longer in coherent superposition and the classical output $|i\rangle_X$ is correctly correlated with the quantum output. The previous calculation manifestly extends to mixed states.

Proposition 7.3.10 Given an normalised mixed state $\rho : (I, I) \to (A, I)$ and a projective measurement $\mathcal{P} : (A, I) \to (A, X)$, then $tr_A \circ (\mathcal{P} \circ \rho)$ is a stochastic map $s : (I, I) \to (I, X)$.

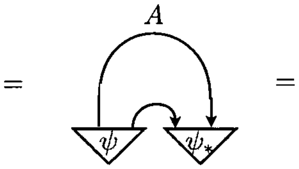
Proof: The map s is stochastic if $(1_I \otimes \mu_X \otimes 1_{I^*}) \circ s = 1_I$ in $\mathbf{C}_q$. The left-hand-side of the previous equality depicts as



The first equality holds by the generalised normal form theorem. The second one by a graph isomorphism.



The first equality uses the compactness of the †-Frobenius structure. The second uses the fact that P is X-self-adjoint. The third equality that it is X-idempotent and the normal form theorem.



The first equality uses the fact that P is X-complete. The second equality is obtained by isomorphism of graph. The last equality uses the assumption that ρ is normalised. This shows that, indeed, s is a stochastic vector as claimed.

□

14. Positive operator-valued measurements

In this section we study the notion of positive operator-valued measurements (POVMs). We will do so by defining the notion in $\mathbf{CQI}(\mathbf{C}_q)$ and prove an abstract version of Naimark's theorem. The result presented here are new and are published in [31] which the author wrote with B. Coecke. Note that since the pictures we need to prove such a theorem are quite big, we will depict them horizontally, thus one should read them from left to right.

In **FdHilb**, POVMs are defined as a set of positive operators

$$\{F_i : \mathcal{H} \to \mathcal{H}\}_i, \ F_i = f_i^\dagger \circ f_i \tag{7.3}$$

such that $\sum_i F_i = 1_{\mathcal{H}}$. Given a state $\rho : \mathcal{H} \to \mathcal{H}$, a POVM assign for each i an outcome probability $\mathrm{Tr}(F_i \rho)$ which, by positivity of F_i and cyclicity of the trace can be re-written as

$$\mathrm{Tr}(f_i \rho f_i^\dagger). \tag{7.4}$$

Even if quantum operations take in account the quantum residue of such an operation, we will be concerned here only with probabilities so that the type of a POVM f is

$$f : A \otimes A^* \to X \tag{7.5}$$

where A is a quantum object and X is a basis object. In other words, it takes as input a quantum state and outputs a classical state which means, in the case of **FdHilb**, a stochastic vector if the quantum state is normalised, *i.e.*:

$$f : \rho \mapsto \sum_i \mathrm{Tr}(f_i \rho f_i^\dagger)|i\rangle. \tag{7.6}$$

Before carrying on and abstracting the notion in **CQ(C)**, we need to introduce some notions.

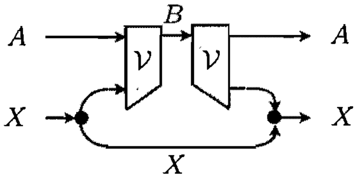
[**X-isometry**] An X-*isometry* is a morphism $\mathcal{V} : A \otimes X \to B$ for which

$$\mathcal{V}_\delta := (\mathcal{V} \otimes 1_X) \circ (1_A \otimes \delta_X) : X \otimes A \to X \otimes B$$

is an isometry *i.e.*,

$$\mathcal{V}_\delta^\dagger \circ \mathcal{V}_\delta = 1_{X \otimes A}.$$

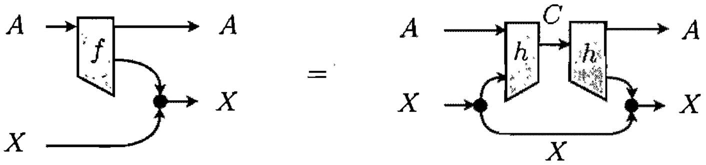
The later condition is depicted as



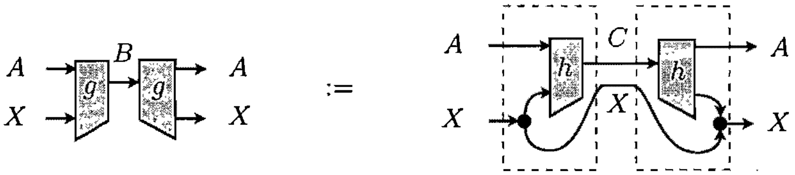
[**X-positivity**] A morphism $f : A \to A \otimes X$ is X-*positive* if there exists a morphism $h : C \to A \otimes X$ such that

$$(1_A \otimes \delta_X^\dagger) \circ (f \otimes 1_X) = (1_A \otimes \delta_X^\dagger) \circ h \circ h^\dagger \circ (1_A \otimes \delta_X). \qquad (7.7)$$

This is depicted as



Remark 7.3.11 In what follows, it will be notationally convenient to set



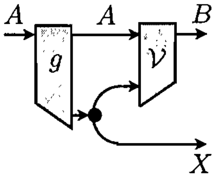
where $B := C \otimes X$, $g := (1_A \otimes \delta_X) \circ (h \otimes 1_X)$ which entails that the right-hand-side of equation (7.7) re-write as $g \circ g^\dagger$ for this g.

The *polar decomposition* of a linear operator M is defined as the composite $V \circ H = M$ where V is an isometry and H is positive. Abstracting such a notion yields the following:

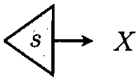
[**X-Polar decomposability**] A morphism $f : A \to X \otimes B$ is *polar decomposable relative to* X if there exists a morphism $g : A \to X \otimes A$ positive relative to X and a controlled isometry $\mathcal{V} : X \otimes A \to B$ such that

$$f = g \circ (\delta_X \otimes 1_A) \circ (1_X \otimes \mathcal{V}) \qquad (7.8)$$

that is



[X-**scalar**] An *X-scalar* is an element $s : I \longrightarrow X$ of the convolution monoid $[I, X]$ which is depicted as



Moreover, we say that the X-scalar $t : I \longrightarrow X$ is an *X-inverse* of s if

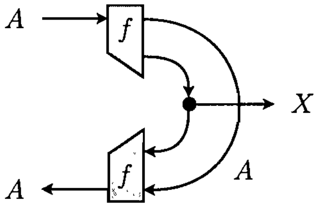
$$s * t = \mu_X^\dagger$$

Finally,

[**POVM**] A *POVM* in **CQI**($\mathbf{C}_q$) is a morphism $\mathcal{F} : (A, I) \longrightarrow (I, X)$ where

$$\mathcal{F} := Tr_A \circ D_{A,X} \circ (f \otimes f_*)$$

which is depicted as



where $f \in \mathbf{C}_q(A, A \otimes X)$ is X-polar-decomposable and such that $f^\dagger \circ f = 1_A$.

Remark 7.3.12 The author doesn't know how restrictive the assumption of X-polar-decomposability is in the previous definition. We postpone the discussion of this to future work.

Theorem 7.3.13 In **CQI(FdHilb)**, POVMs as defined in the previous definition exactly coincide with the assignments $\rho \mapsto \sum_i \mathrm{Tr}(g_i \rho g_i^\dagger)|i\rangle$ corresponding to POVMs defined in the usual manner.

Proof: Consider a POVM $\mathcal{F} : (A, I) \longrightarrow (I, X)$ where

$$\mathcal{F} := Tr_A \circ D_{A,X} \circ (f \otimes f_*).$$

In **FdHilb**, the $\dagger$-Frobenius structure of the basis object X induces a canonical basis vectors $\{|i\rangle\}_i$. Using lemma 7.3.6,

$$f = \sum_i (f_i \otimes |i\rangle).$$

Using this, we can rewrite $\mathcal{F}$ as

$$
\begin{aligned}
&Tr_A \circ (1_A \otimes D_X \otimes 1_{A_*}) \circ \left[(\textstyle\sum_i f_i \otimes |i\rangle) \otimes \left(\textstyle\sum_j |j\rangle_* \otimes (f_j)_*\right)\right] \circ - \\
&\quad = Tr_A \circ \left[(1_A \otimes D_X \otimes 1_{A^*}) \circ \left(\textstyle\sum_{i,j} f_i \otimes |i\rangle \otimes |j\rangle_* \otimes (f_j)_*\right)\right] \circ - \\
&\quad = Tr_A \circ (\textstyle\sum_i f_i \otimes |i\rangle \otimes (f_i)_*) \circ -.
\end{aligned}
$$

Passing from the notation of **CQI(FdHilb)** to standard Dirac notation that is $(f_i \otimes |i\rangle \otimes (f_i)_*) \circ -$ to $f(-)f^\dagger \otimes |i\rangle$ we obtain

$$\sum_i Tr_A(f_i(-)f_i^\dagger)|i\rangle.$$

Using the polar decomposition of f_i and cyclicity of the trace, we get

$$
\begin{aligned}
\textstyle\sum_i Tr_A(f_i(-)f_i^\dagger)|i\rangle &= Tr_A(U_i g_i(-)g_i^\dagger U_i^\dagger)|i\rangle \\
&= \textstyle\sum_i Tr_A(g_i(-)g_i^\dagger)|i\rangle
\end{aligned}
$$

which is the intended result. Finally, by hypothesis we have $f^\dagger \circ f = 1_A$ from which it follows that $g^\dagger \circ g = 1_A$. The converse direction constitutes a straightforward translation into the graphical language.

□

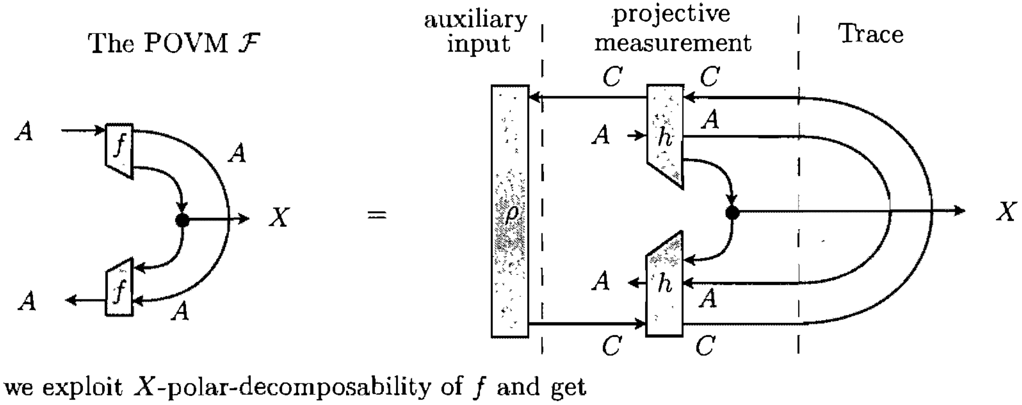
Theorem 7.3.14 [**Naimark's theorem**] Let $\mathcal{F} : (A, I) \to (I, X)$ be a POVM in $\mathbf{CQI(C}_q\mathbf{)}$ with

$$\mathcal{F} = Tr_A \circ (1_A \otimes D_X \otimes 1_{A^*}) \circ (f \otimes f_*)$$

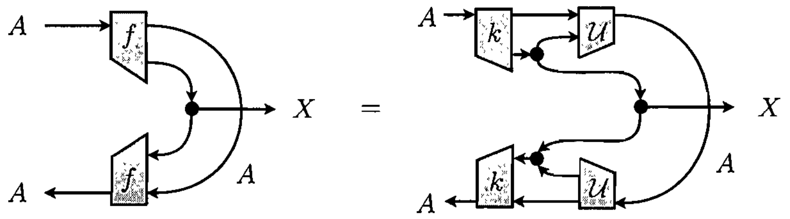
in $\mathbf{C}_q$, where $f = k \circ (\delta_X \otimes 1_A) \circ (1_X \otimes \mathcal{V})$ by X-polar-decomposition. If $s := Tr_A(k) : I \to X$ admits an X-inverse $t : I \to X$ under convolution, then there exists a projective measurement on an extended system which realises $\mathcal{F}$. Conversely, each projective measurement on an extended system yields a POVM.

Remark 7.3.15 The condition that s admits an X-inverse is not very restrictive. Indeed, in **CQI(FdHilb)** we can think of s as a family of scalars s_{ii} where each s_i is the trace of some f_i. As each of the latter are positive, that s admits an X-inverse just means that none of the f_i is equal to 0. In any case, 0 is never observed anyway so it would be silly to add such a map to the X-family given by f.

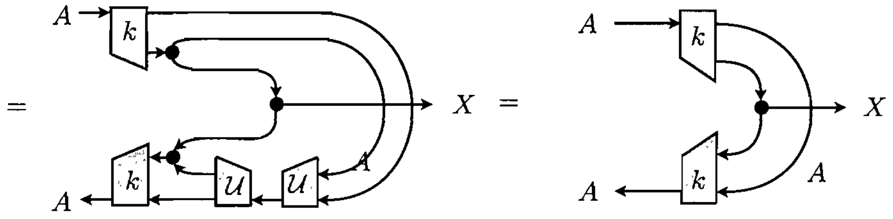
Proof: We need to show that there exists an X-projector $h : C \otimes A \to C \otimes A \otimes X$ in $\mathbf{C}_q$ together with an auxiliary input $\rho : (I, I) \to (C, I)$ in $\mathbf{CQI(C}_q\mathbf{)}$ such that



First, we exploit X-polar-decomposability of f and get

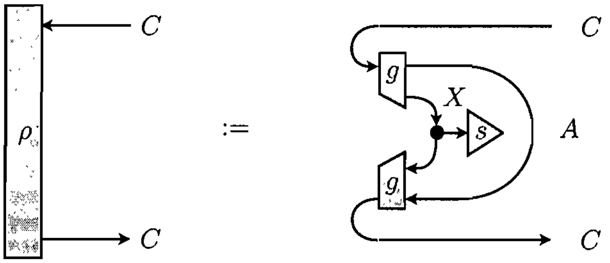


Using graph isomorphism the right-hand-side of the previous equality is equal to

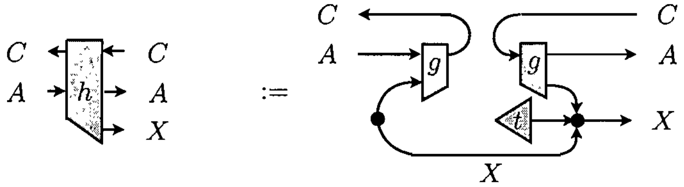


where the last equality proceeds from the fact that $\mathcal{U}$ is an X-isometry and an application of the generalised normal form theorem using the spider notation.

Let



and



where $k = g^{\dagger} \circ g$ by X-positivity of k and remark 7.3.11.

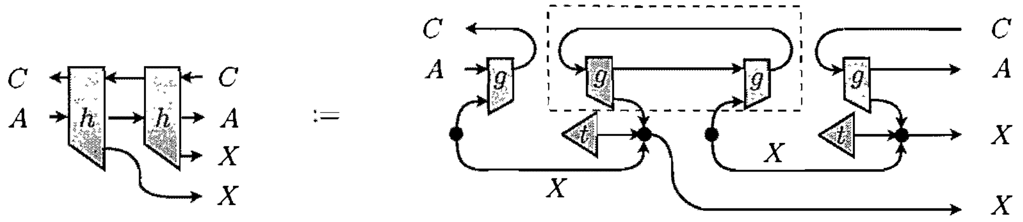
In order to show that h is an X-projector, we need to show that it is X-idempotent and X-self-adjoint.

For X-self-adjointness. First, observe that since k is X-positive, then $s := Tr_A(k)$ is in $\mathbf{C}_c$ so that $s_\times = s$. Moreover, since μ_X, δ_X and s are all invariant under $(-)_\times$,

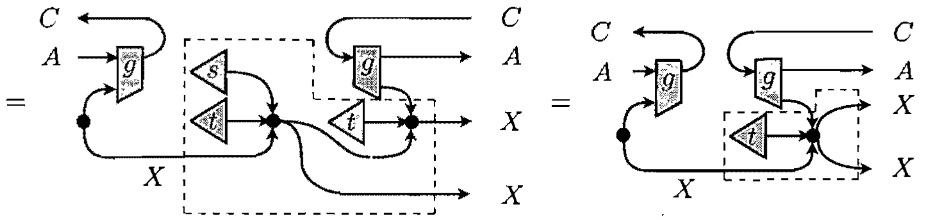
$$\begin{aligned}
\mu_X &= (\mu_X)_\times \\
&= (\delta_X^{\dagger} \circ (s \otimes t))_\times \\
&= (\delta_X^{\dagger})_\times \circ (s_\times \otimes t_\times) \\
&= \delta_X^{\dagger} \circ (s \otimes t_\times),
\end{aligned}$$

we must also have $t_\times = t$ by uniqueness of inverses. This entails that $t^\times = t^\dagger$. Thus, X-self-adjointness proceeds by the preceding fact and a simple application of the generalised form theorem.

Now, for X-idempotence, we have

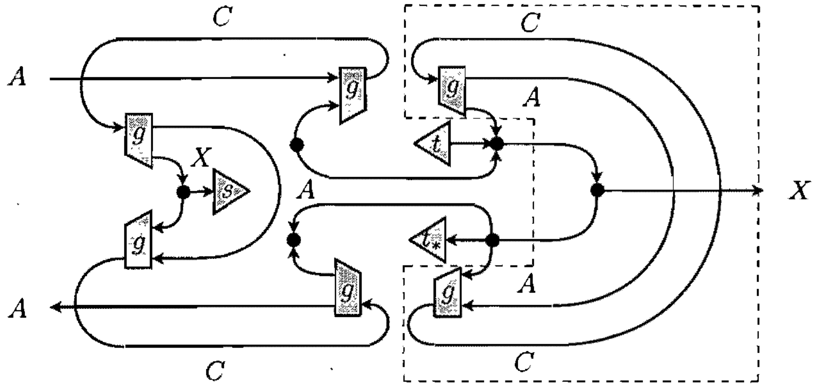


By X-positivity, the dotted rectangle in the previous picture reduces to $\delta_X \circ s$ where $s := Tr_A(k)$ which is X-inverse to t under convolution, that is $\delta_X \circ (s \otimes t) = \mu_X$. Thus, factoring out s and t and cancelling them out via convolution, we obtain the following equality between the dotted squares below

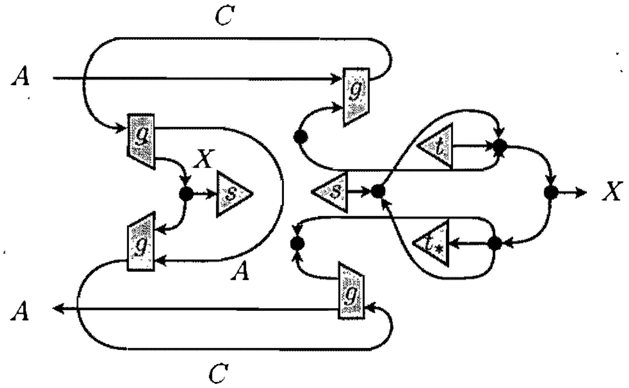


So indeed, h is X-idempotent and X-self-adjoint and thus X-projector which defines a projective measurement by adjoining the morphism D_X.

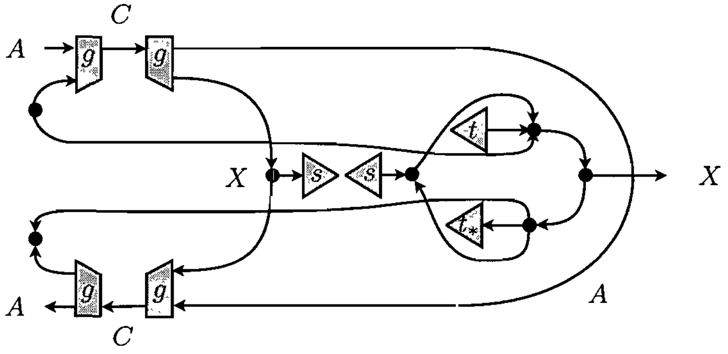
We now show that the state ρ defined as above when composed with the projective measurement defined by h and when tracing out $C^* \otimes A$ realises the POVM $\mathcal{F}$ that is, we have to show that the following picture is equal to $\mathcal{F}$.



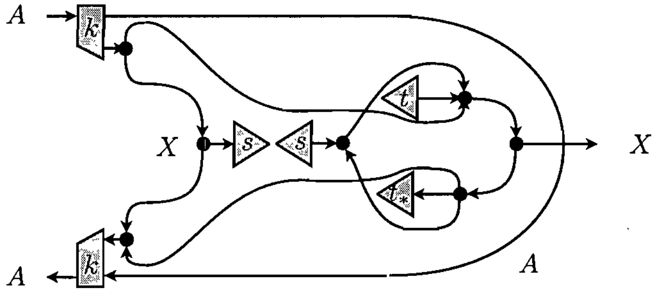
The dotted square reduces to $\delta_X \circ s$ by X-positivity of f so we obtain



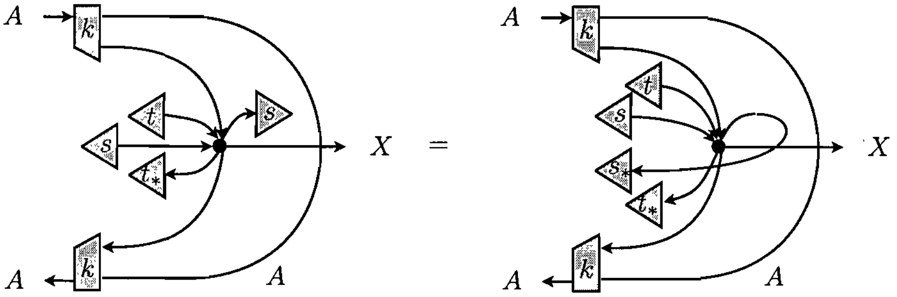
Now, using an obvious graph isomorphism, we obtain



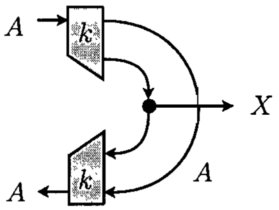
Again, using X-positivity of k, the previous reduces to



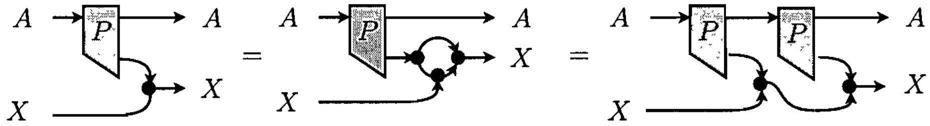
From there, we use the generalised normal form theorem to get

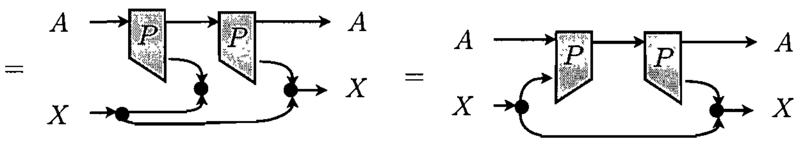


From there, we use again the normal form theorem to cancel the loop and the symmetries and then use convolution to cancel s against t and s_* against t_* so we obtain



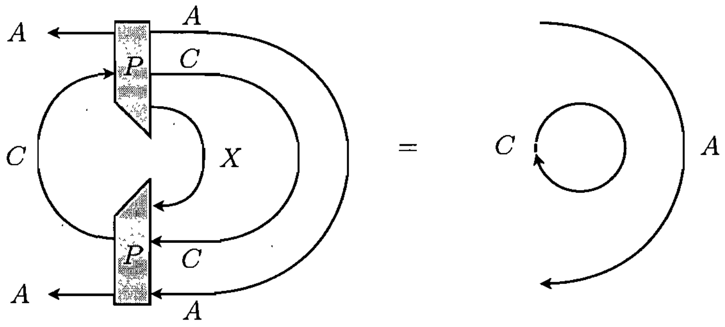
The converse is almost immediate. First, given any projector-valued spectrum P, its X-idempotence and X-self-adjointness entail its X-positivity. Indeed,



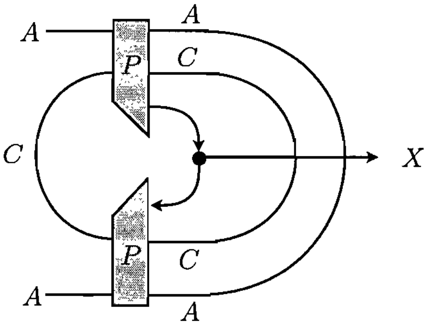


There, the first equality is an application of the normal form theorem. The second equality uses X-idempotence of P. The third equality is again an application of the normal form theorem. The last equality is obtained using X-self-adjointness.

Now, again for any projector-valued spectrum $P : A \to A \otimes X$, we have $P^\dagger \circ P = 1_A$ as was already implicitly proved in proposition 7.3.10. Using this, given a projector-valued spectrum $P : A \otimes C \to A \otimes C \otimes X$ with the auxiliary input given by the unnormalised completely mixed state, we have



which is normalised up to a C-dependent scalar—note that this is normal since the auxiliary state is not normalised. Thus, the induced POVM is



This completes the proof.

□

We also have an analogue of proposition 7.3.10 for POVMs:

Proposition 7.3.16 Given an normalised mixed state $\rho : (I, I) \to (A, I)$ and a POVM $\mathcal{F}(A, I) \to (I, X)$, then $\mathcal{F} \circ \rho$ is a stochastic state $s : (I, I) \to (I, X)$.

Proof: Immediate because of the normalisation condition of the POVM $\mathcal{F}$.

□

8 Protocols

"The end justifies the means"
- Niccolo Machiavelli

The purpose of this chapter is to recast some quantum protocols in $\mathbf{CQI}(\mathbf{C}_q)$ using the semantics presented in the previous chapter. To do so, we will first introduce a graphical calculus for $\mathbf{CQI}(\mathbf{C}_q)$ that will greatly lighten the graphical notation of interfaces. Next, we will discuss two subtle issues involving scalars namely: inverses and square roots. We will need both to work out protocols; indeed, as a matter of example, we will need inverses of square roots to normalise our analogue of the Bell state. For the protocols, we will introduce and prove correctness of the quantum teleportation protocol and of superdense coding. We will show that these two protocols are essentially equivalent up to a reversal of the operations. We will introduce and prove correctness of the protocol of mixed state generation, and discuss the protocol of TelePOVM. Finally, we will derive the protocol BBM92 from BB84 and *vice versa*. The material presented in section 8.1 is new while the results presented in section 8.3 and above first appeared in [33] and some of them are presented again in [32] which the author wrote with B. Coecke and D. Pavlovic. Moreover, some protocols presented in these papers are not presented here such as coherent dense coding and coherent teleportation [48]. A different presentation of the teleportation protocol and entanglement swapping involving biproducts can be found in [5].

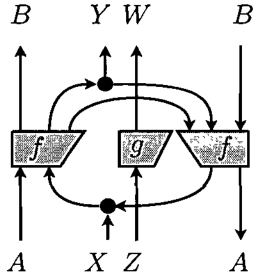
This chapter marks our departure from **FdHilb**. Indeed, while we have motivated our semantics with this category as our primary example, we won't rely on it to motivate our protocols here. Of course, the protocols we present here were originally developed in that category so they indeed work there. However, we believe it is suitable to work in the general case to stress that the semantics presented in the previous chapter is self-sufficient.

8.1 A graphical notation for interfaces

To depict protocols in $\mathbf{CQI}(\mathbf{C}_q)$ it will be convenient to simplify the pictures. We will do so using the fact that when depicting an interface, the quantum part of a picture is always symmetric with respect to the classical part which lies along some vertical axis; using this idea, we will introduce a notation that allows us to "fold" the picture thus simplifying the notation. The notation we will introduce can be seen as the formalisation of the "ground" notation for the decoherence that has been in circulation for some time together with some elements of the notation introduced in [24] where a black triangle was used to represent the environment. In contrast with these, the graphical notation we present here fully accommodates interfaces and is richer than the previous notations at many levels: namely, it clearly distinguishes the notion of central and non-central symbols (see below) and it accommodates the issue of dimension of X as a central symbol (see remark 8.1.9 and usage in the teleportation protocol below).

Folding of central symbols

We start by discussing the notation for central symbols that is, wires and morphisms carrying classical data. Consider the following (very) general interface:



There, we have the morphism f on the left-hand-side which is reflected on the right-hand-side along some axis running parallel to the vertical wires labeled by X, Y, Z and W. On the other hand, the morphism f is not duplicated and the set of wires labeled by X are connected by the morphism D_X while those controlled by Y are connected by the morphism $D_Y^\dagger$. In other words, the controlling wire splits in two while the outputs merge in a single wire. Thus, when folding a picture, we must find a way to distinguish the classical wires and morphisms that are doubled or reflected from those that are not. For the remainder of the discussion, we will say that a symbol—wire or morphism—is *central* if it not doubled or reflected when depicted as an interface. We will distinguish central from non-central wires—and by extension such morphisms—by adding a circle around the usual black dots *i.e.*:

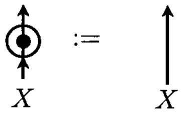
⦿

Notation. A wire that connects to the black dot is central. A wire that connects to (or stop at the circumference of) the outer circle gets duplicated and one of the two resulting wires is dualised when unfolding the picture. Finally, we will call the previous symbol a *big circle.*

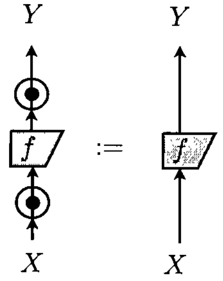
Remark 8.1.1 Of course, this doesn't mean we will add circles around all the black dots. We will do so only in the presence of central symbols. Indeed, nothing in the semantics of $\mathbf{CQI(C_q)}$ prevents us to have non-central structural morphisms from the †-Frobenius structure since a basis object is also a quantum object.

All this is better illustrated by some examples. There, the symbol appearing in the folded graphical representation is on the left while the regular graphical representation of interfaces is on the right.

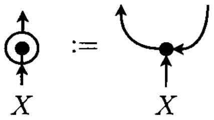
1. Identity over the controlling data:



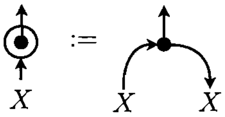
By extension, a central morphism is depicted as



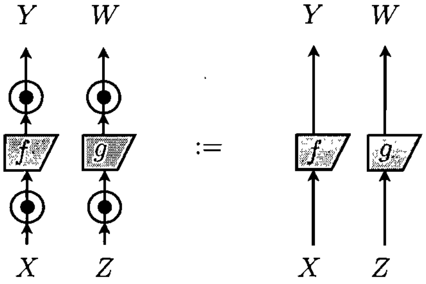
2. The morphism D_X:



3. The morphism $D_X^\dagger$:

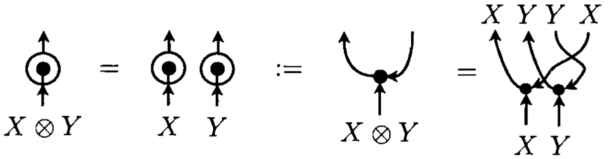


4. Tensor product of classical maps: If $f : X \to Y$ and $g : Z \to W$ are classical maps, their folded representation depict as



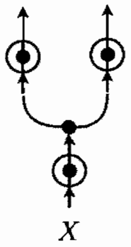
All this, of course, with possible reorientation of the wires.

Remark 8.1.2 One must be careful when passing from the folded to the unfolded notation with D_Z's where Z is a compound object *i.e.*: an object of the form $X \otimes Y$. Indeed, we have



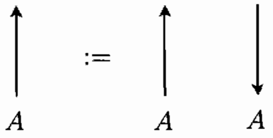
by constraints on the structural morphisms of the basis structures in $\mathbf{C}_b$. In particular, we must not forget these symmetries when unfolding D_Z and factoring the tensor product of morphisms. Of course, the same remark applies for $D_Z^\dagger$ with $Z := X \otimes Y$.

Remark 8.1.3 One must not confound δ's and D's or their adjoints. If a δ (or its adjoint) is central, then it gets depicted as a central morphism *i.e.*, for instance, δ_X gets depicted as

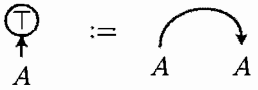


Folding of quantum symbols

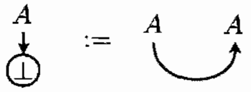
1. Identities:



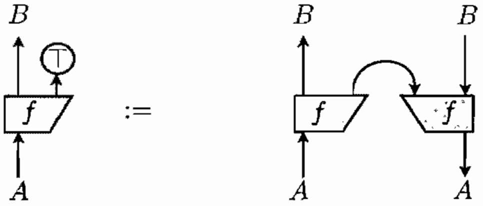
2. Traces:



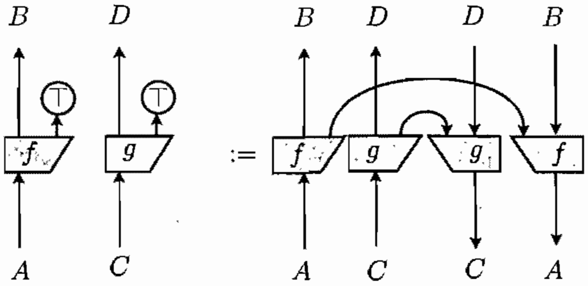
3. Cotraces (unnormalised maximally mixed states):



4. Quantum maps:

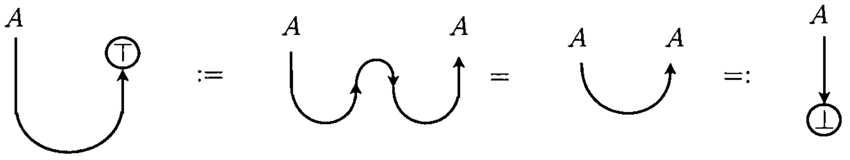


5. Tensor product of quantum maps:



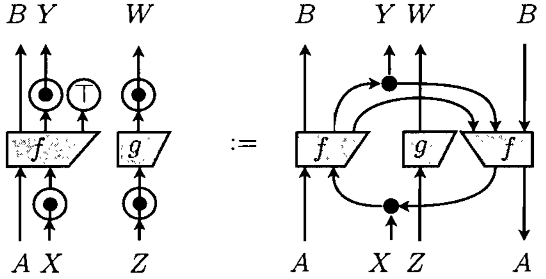
and again, with possible reorientation of the wires.

Example 8.1.4 We have:

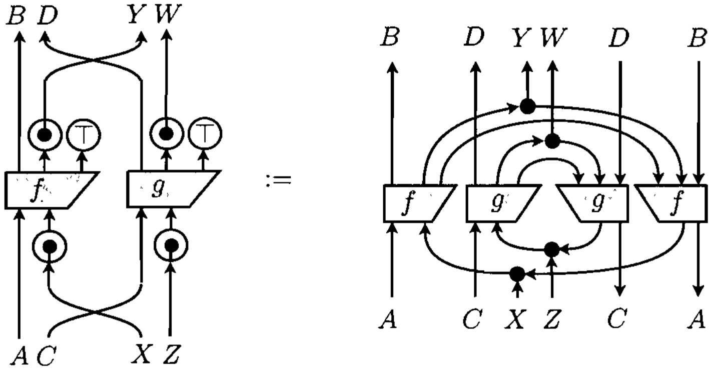


General folding

Using this notation, the general interface depicted above can be denoted as

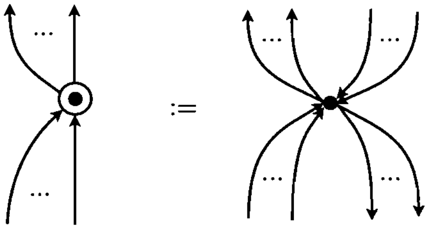


While the simplification in the notation might not be obvious with this, consider the folding of the tensor product of two morphisms in **CQI**($\mathbf{C}_q$) as interfaces, this is:

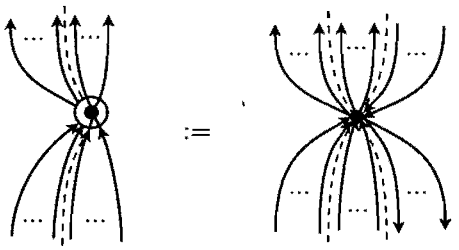


Our notation reduces the number of symmetries in the depiction from six to two. In most cases, such symmetries are meaningless from an operational standpoint and getting rid of these is a major achievement of this notation. That it indeed simplifies the notation will become even clearer when we depict protocols below.

Now, while this notation is sufficient to depict the morphisms of **CQI**($\mathbf{C}_q$) as interfaces, we might need to use the mixed normal form theorem with the big circles in our proofs. Thus, we can generalise the preceding notation to spiders as follows: when there are no central wires we get

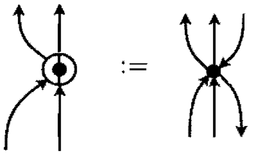


When there are central wires—separated from their counterparts by dotted lines in the following picture—, we use

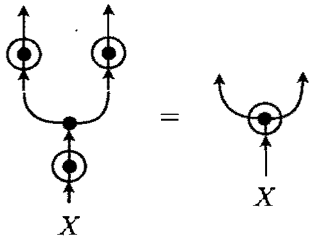


which is the obvious generalisation of the preceding notation.

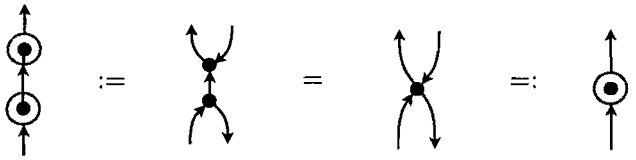
Example 8.1.5 Using the previous notation, one gets:



Example 8.1.6 Again, using this notation, a central δ becomes

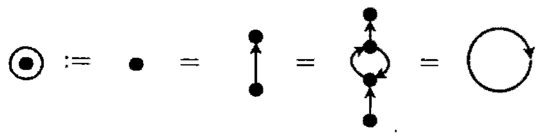


Example 8.1.7 An application of the generalised normal form theorem with spider notation adapted to this graphical notation is



Remark 8.1.8 In general, one may "fuse" two big circles together as long as he keeps central wires connected to the black dot in the resulting big circle and the non-central ones connected to the outer circle of the resulting big circle. That is, in the same way as we did in the previous two examples. Clearly, non-ambiguity of the big circle notation together with the mixed normal form theorem allow such an operation.

Remark 8.1.9 Just a big circle without wires makes sense. Indeed, switching over to the regular notation for interfaces, one gets



which is the dimension of the basis object labelling the wire as $\mu \circ \mu^\dagger = \sum_i \langle i|i\rangle$. Importantly, it must be stressed that such a symbol remains central.

In conclusion, note that while this notation is convenient for clarity, it is sometimes useful to work with the standard notation for proofs c.f. the proof of Naimark's theorem where we sometimes used asymmetrical arguments. However, as we won't need to do this for protocols, the folded notation will enable us to present some less cluttered and more readable pictures.

8.2 Inverses and square roots of scalars

In this section, we discuss the notions of inverses and square-roots of scalars in $\mathbf{CQI}(\mathbf{C}_q)$. Such notions will be crucial when working out protocols.

8.2.1 Square-roots of scalars

The following was also remarked by B. Coecke and D. Pavlovic in [36].

Proposition 8.2.1 The positive scalars in the scalar monoid $\mathbf{C}_q(I, I)$ have self-adjoint square-roots when embedded in $\mathbf{CP}_q(\mathbf{C})$ via $s \mapsto s \otimes s_*$.

Proof: Let $s : I \longrightarrow I$ be a positive scalar with $s = \psi \circ \psi$ where $\psi : I \longrightarrow A$. The morphism $\epsilon_A \circ (\psi \otimes \psi_*)$ is in $\mathbf{CP}_q(\mathbf{C})(I, I)$ and we have $t \circ t = s \otimes s_*$. Self-adjointness of t follows from the fact that

$$t = \epsilon_A \circ (\psi \otimes \psi_*) = (\psi^\dagger \otimes \psi^*) \circ \eta_{A^*} = t^\dagger$$

by properties ϵ and η.

□

8.2.2 Universal localisation of a †-compact category

In general, the commutative monoid of scalar $\mathbf{C}(I, I)$ of a category of quantum structures does not admit multiplicative inverses. However, it was remarked by B. Coecke and D. Pavlovic in [37] that for any category of quantum structures $\mathbf{C}_q$, it is possible to construct an essentially unique category $L\mathbf{C}_q$ where every positive scalar has an inverse. Such a construction shares many analogies with the construction of the field of quotients of an integral domain (see [62] pp. 210 for instance). We now give a brief outline of the results of [37] which themselves rely on the calculus of fraction presented in [47]:

[Positive scalar] Let $\mathbf{C}_q$ be a category of quantum structures. A scalar $s \in \mathbf{C}_q(I, I)$ is *positive* if there exists a morphism $\psi : I \longrightarrow A$ such that $s = \psi^\dagger \circ \psi$.

[Zero and divisors of zero] A scalar s is a *zero* if for all scalars t, $s \circ t = s$. Moreover, a scalar s is a *divisor of zero* if there exists a scalar t such that $s \circ t$ is equal to zero.

It is easy to see that if $\mathbf{C}_q(I, I)$ has a zero, it is unique. If it exists, we will denote zero as o.

[Locality] [37] A category of quantum structures is *local* if all its positive scalars are either divisors of zero or are invertible.

Note that the scalars $s : (I, I) \longrightarrow (I, I)$ in $\mathbf{CQI}(\mathbf{C}_q)$ are positive, hence if $\mathbf{CQI}(\mathbf{C}_q)$ is local, this is enough for our purposes but still, this might not be the case in general. However, the following holds:

Theorem 8.2.2 [37] Every category of quantum structures $\mathbf{C}_q$ has a universal localisation $L\mathbf{C}_q$ equipped with a functor $\mathbf{C}_q \to L\mathbf{C}_q$ preserving the quantum structures, which is initial for all local categories of quantum structures with functor preserving the quantum structures from $\mathbf{C}_q$. In particular, the objects of $L\mathbf{C}_q$ are those of $\mathbf{C}_q$, and a morphism in $L\mathbf{C}_q(A, B)$ is of the form f/s, where

$$s \in \Sigma := \{s \in \mathbf{C}(I, I) \mid \text{for all } t \in \mathbf{C}(I, I),\ \ s \circ t \neq o\},$$

and these fractions are taken modulo the congruence

$$\frac{f}{s} = \frac{g}{t} \text{ if and only if } \text{ there exists } u, v \in \Sigma \text{ such that } u \circ s = v \circ t \text{ and } u \cdot f = v \cdot g.$$

Proof: See [37].

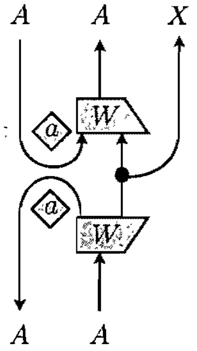
□

Remark 8.2.3 One should be careful with the preceding result. Indeed, the construction may be applied without problems provided the functor turns out to be faithful. This seems to be the case, for instance, in the category of modules over a ring R since the choice of Σ excludes all divisors of zero. It is not known to the author whether or not this functor is faithful in general. Nonetheless, we will assume in what follows that the category in which we work is local.

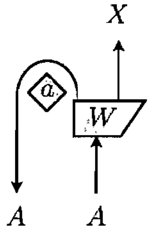
8.3 Teleportation-enabling measurements

In [76], R. F. Werner establishes the one-to-one correspondence between quantum teleportation schemes, dense coding schemes and certain orthonormal bases of maximally entangled vectors. We now abstract his results in terms of X-unitaries and X-states.

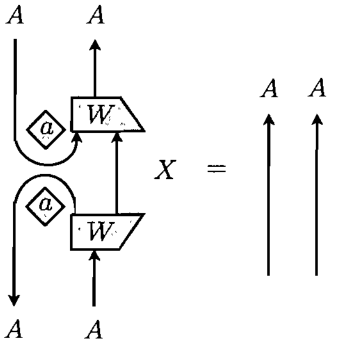
[Teleportation-enabling measurement] A *teleportation-enabling measurement* is a morphism $W : A \otimes A \to A \otimes A \otimes X$



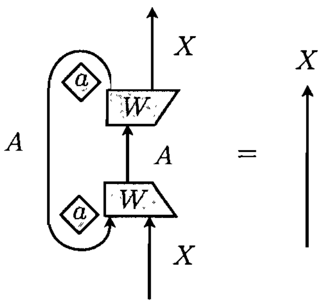
where $W : A \otimes X \to A$ is an X-unitary, $a : I \to I$ is $\mathrm{Dim}(A)^{-1/2}$ and



is such that

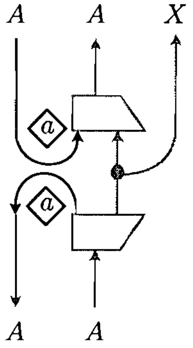


and



which are the abstractions of $\mathrm{Dim}(X) \geq \mathrm{Dim}(A)^2$ and $Tr(U_j^\dagger \circ U_i) = \delta_{i,j}$ respectively.

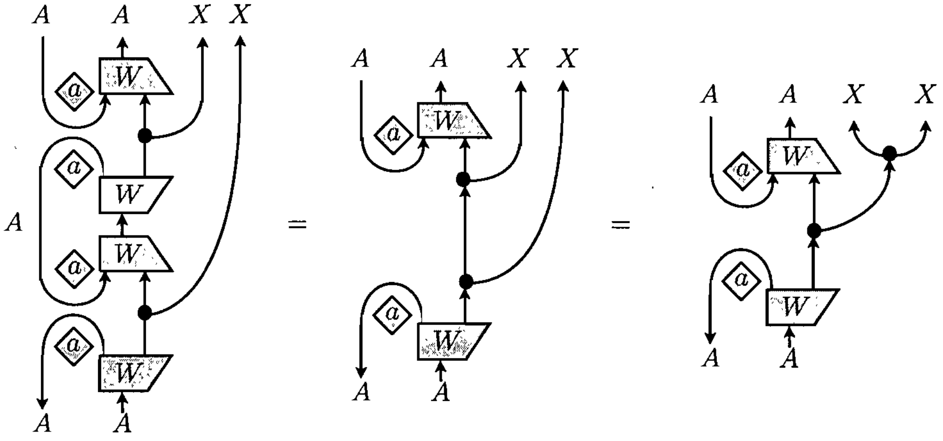
Now, note that in



the non-grey part is a bipartite projector defined by the composition of a normalised abstract Bell state with its adjoint. Using the fact that $W : A \otimes X \to A$ is an X-unitary indeed gives the following

Proposition 8.3.1 A teleportation-enabling measurement is a projector-valued spectrum.

Proof: We have to verify that W is X-self-adjoint, X-idempotent and X-complete. It is manifestly X-self adjoint and X-complete by construction, so it remains to check that it is X-idempotent:



as required.

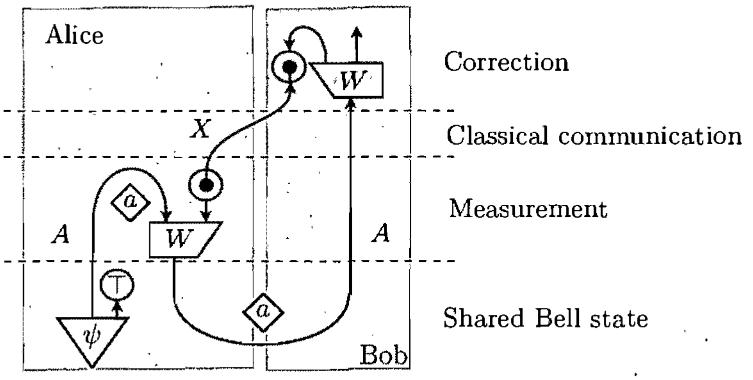
□

8.4 Teleportation

The teleportation protocol [13] is a means by which two parties, Alice and Bob, exchange the information contained quantum state using quantum entanglement and classical communication. The protocol is described as follows:

- Alice and Bob share a Bell state $\eta_A : I \to A^* \otimes A$ *i.e.*, Alice has one half and Bob the other.
- Alice performs a teleportation-enabling measurement on the compound system consisting of the state she wishes to exchange with Bob and her share of the Bell state. By doing so, she collapses the state of the compound system so the information that was contained in the state she wishes to transfer is no longer accessible to her[11].
- Alice sends the result of her measurement to Bob via a classical channel.
- Using the classical information he received from Alice, Bob applies a correction via the underlying X-unitary transformation W of the teleportation-enabling measurement on his share of the Bell state and recovers the initial state.

Using the folded notation and a teleportation-enabling measurement as described in the previous section, we can depict this protocol as:

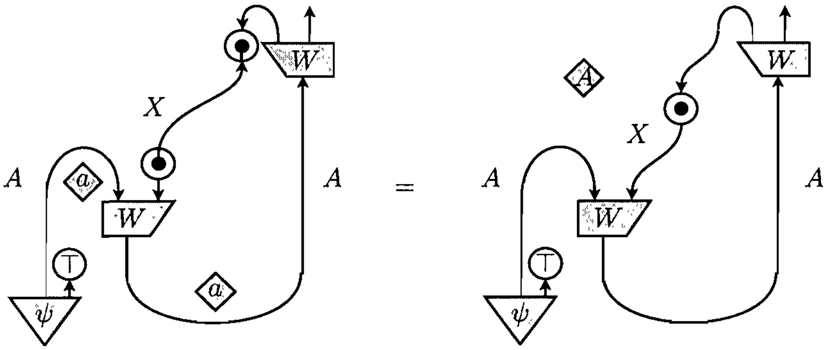


There, the scalars $a : I \to I$ are equal to $\mathrm{Dim}(A)^{1/2}$ and are added to normalise the Bell state and its adjoint.

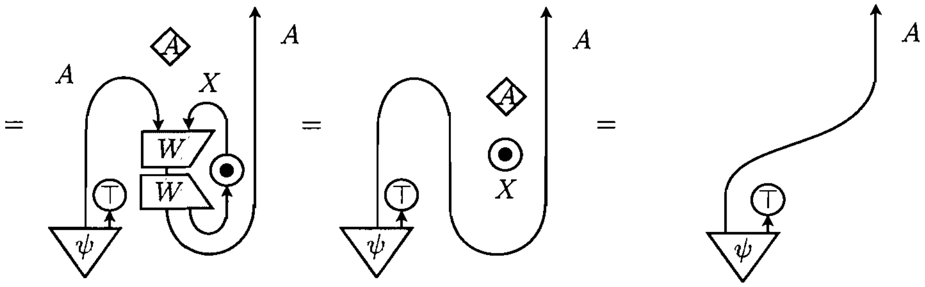
Remark 8.4.1 To be perfectly aligned with the standard notation, the big circles and the classical wires should pass to the right of the rightmost quantum wire. However, the symmetry induced by such a graph isomorphisms are irrelevant when taking in account the description of the protocol therefore, we can omit them. This fact provides further motivation for the notation.

We can also prove correctness of the protocol as

[11] From which teleportation is not a cloning operation but really a transfer of information.



where $A = a \bullet a = \text{Dim}(A)^{-1}$ (where the first "A" is a scalar) and fused the two big circles together. Now, using a graph isomorphism, we obtain:



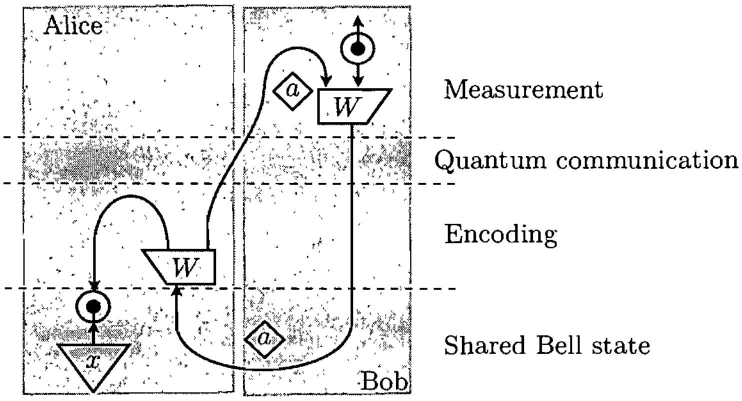
The first equality proceeds using X-unitarity of W while the second is obtained by the fact that the big circle is central but not the scalar A. Hence, in the regular graphical representation of $\mathbf{CQI}(\mathbf{C}_q)$—which is implicit here—, we have two such scalars and we obtain $A \bullet A \bullet \text{Dim}(X) = 1_I$ since $\text{Dim}(X) = \text{Dim}(A)^2$. Hence, teleportation reduces to the identity channel between Alice and Bob.

8.5 Superdense coding

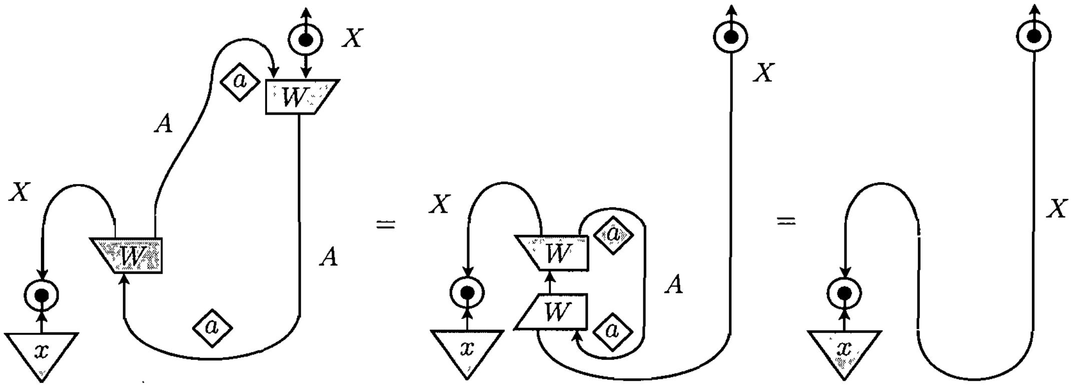
The protocol of superdense coding [14] is way in which two parties sharing a maximally entangled state exchange classical information using qubits instead of bits. Without entanglement, the maximum number of bits per qubit is one. However, in the case of superdense coding, since Alice and Bob share a maximally entangled state, they can achieve a ratio of two bits per qubit hence the term *superdense*. Superdense coding is described as follows:

- Alice and Bob share a Bell state $\eta_A : I \longrightarrow A^* \otimes A$.
- To transmit a classical message x, Alice applies a unitary transformation depending on x on her share of η_A using the X-unitary transformation W from the teleportation-enabling measurement.
- Alice sends her encoded qubit to Bob.
- Bob measures the joint system via a teleportation-enabling measurement and recovers the message.

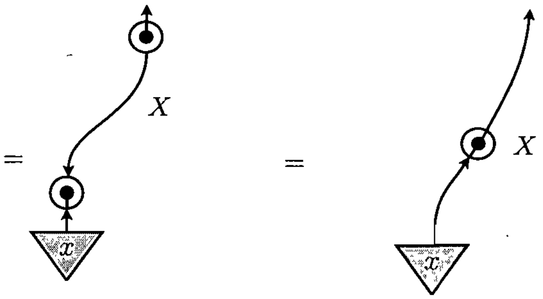
This protocol can be depicted as



We can also prove correctness of the protocol as



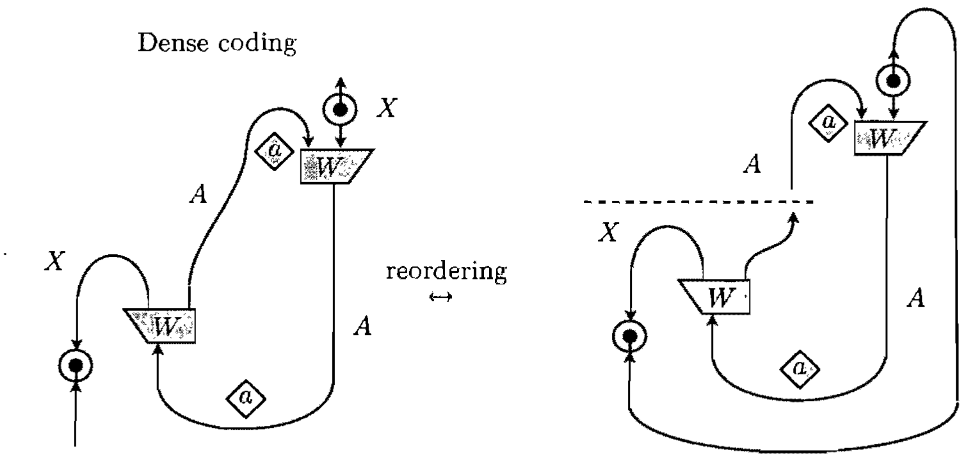
The first equality is obtained from a graph isomorphism *i.e.*, to slide W along the wire labeled by A in order to bring it aside W^*. The second equality is obtained from the condition on the X-states in the definition of a teleportation-enabling measurement.



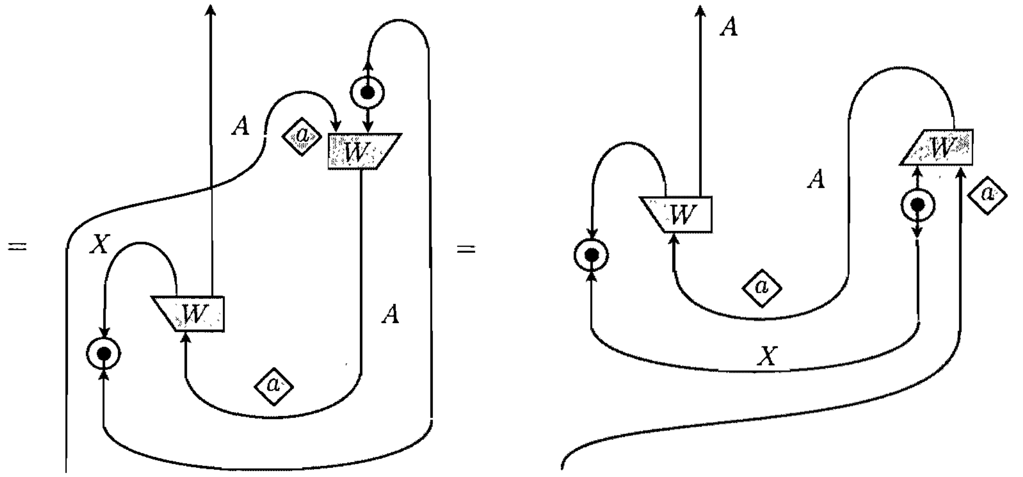
The first equality is obtained by yanking the wire labeled by X and the second by fusing together the two big circles. Hence, the superdense coding indeed reduces to an identity over a classical channel.

8.6 Teleportation ↔ Superdense coding

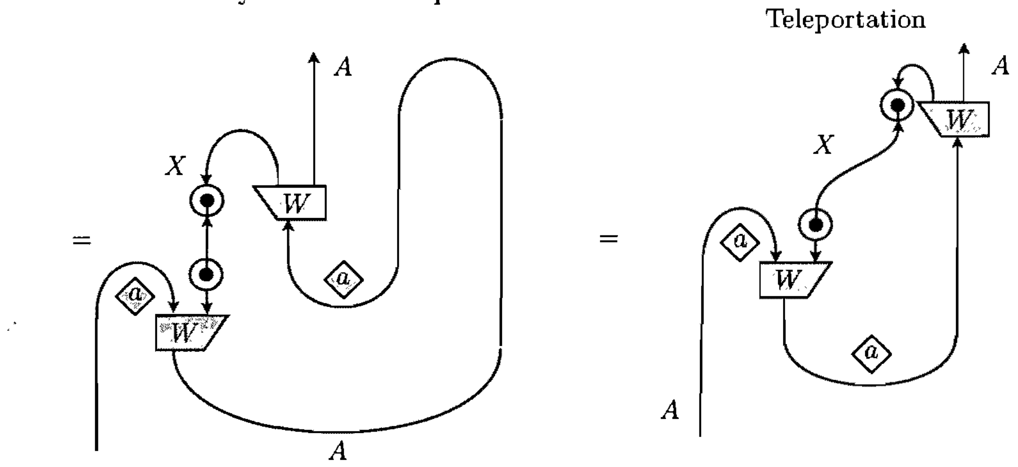
We now show that superdense coding is equivalent to quantum teleportation up to a reordering of the operations. Starting from superdense coding, swapping of the encoding ↔ correction and the measurement is done as



The right-hand-side picture can be read as follows: the input is now *after* the dotted line, while the output is *before* the dotted line. Also, we connected the wires labeled by X as the measurement now comes before the correction. Such a "temporal" ordering of the picture is counterintuitive but we will just use isomorphism of graphs to recover teleportation. In order to have input and outputs of the protocol at the right place, we stretch the wires to the boundary of the picture to obtain:



The equality is obtained by sliding the W along the wire labeled by X and using yanking on the leftmost wire labeled by A on the first picture.



The first equality is obtained by yet another sliding of the W along the wire labeled by X and the second equality is obtained by yanking the "zig-zagging" wire labeled by A—we can do so as this zig-zag is just an artefact of the reorganisation of the operations. We indeed recover the teleportation protocol.

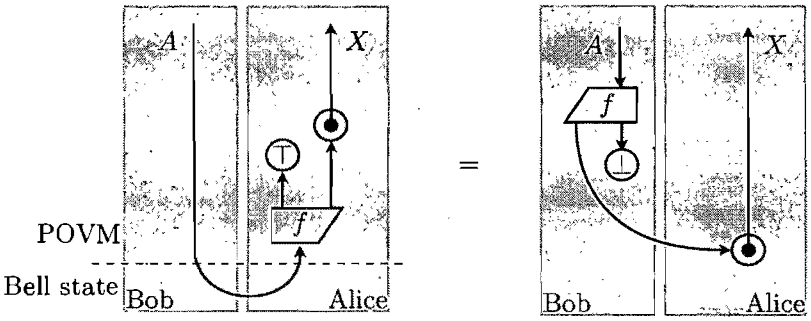
Remark 8.6.1 Such a result is unsurprising. Indeed, teleportation and superdense coding share the same structural resources.

8.7 Mixed state generation

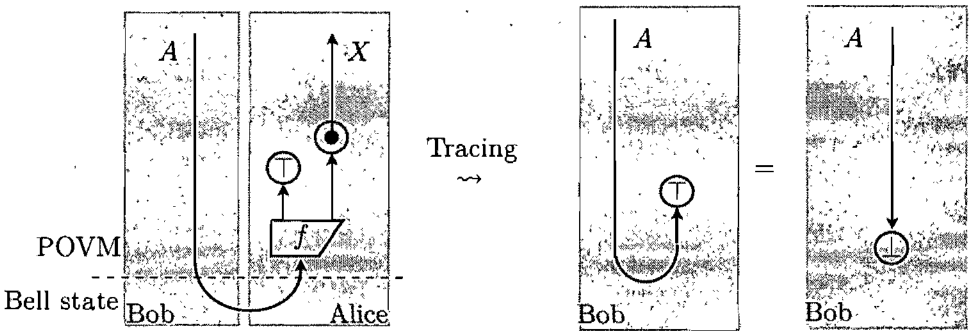
Mixed state generation [16] is a simple protocol that can be described as follows:

- Alice and Bob share a Bell state $\eta_A : I \to A^* \otimes A$.
- Alice measures her part of the Bell state using a POVM.
- Now Bob has the completely mixed state and Alice has additional information concerning his state given by the outcome of the measurement.

Such a protocol is depicted from the perspective of Alice as:



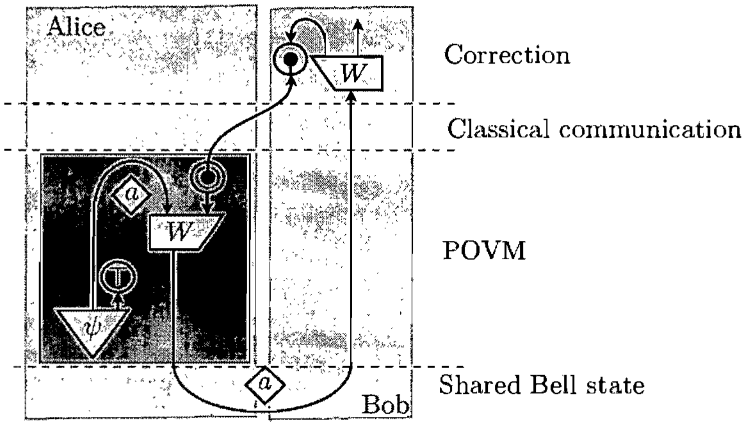
To see that Bob indeed holds the completely mixed state, note that if trace out Alice's part, we obtain:



8.8 telePOVM

We now use the idea behind mixed state generation and extend it to a generalised teleportation protocol called TelePOVM [16]. From Naimark's theorem which we proved in chapter 7, we know that each projective measurement on an extended system yields a POVM. Thus, we may use the state to teleport as an ancilla and a teleportation enabling-measurement to construct a POVM. Alice can then measure her share of the Bell state using this POVM and send the outcome to

Bob who can apply a correction in order the recover the initial state. TelePOVM is depicted as follows:



We can also prove correctness of this protocol, but this is essentially the same as for the quantum teleportation protocol.

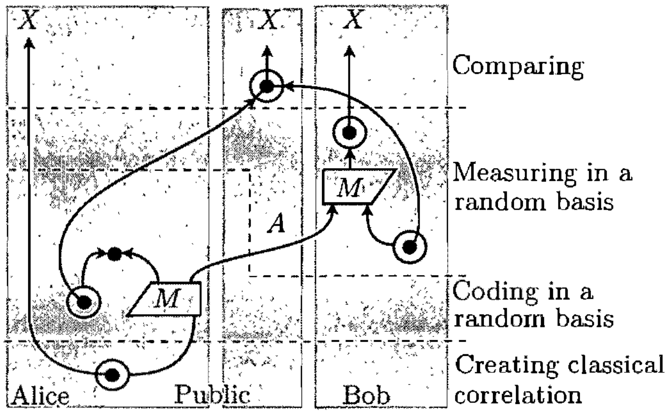
8.9 BBM92 ↔ BB84

We now show that BBM92 [12] is topologically (or graphically) equivalent to BB84 [11], a protocol akin to Ekert91 ??. This result is more surprising than the equivalence that we described between teleportation and superdense coding, since these two protocols do not share the same structural resources.

BBM84 is a cryptographic protocol that describes how two parties sharing entangled states can generate a key to communicate securely. It is described as follows:

- Alice first chooses random classical data.
- Alice chooses a random basis in which she encodes the classical data from the previous step.
- Alice then transmits the encoded data through a quantum channel to Bob.
- Bob measures the data he receive in a random basis (but from the same set of bases as Alice). If he measures in the same basis as Alice encoded her data, then he receives the information that Alice intended to send; otherwise, the outcome of his measurement is random data.
- Alice and Bob then compare the bases in which they encoded/measured, and keep the data if both agree and add it to the key. Otherwise, they discard it.

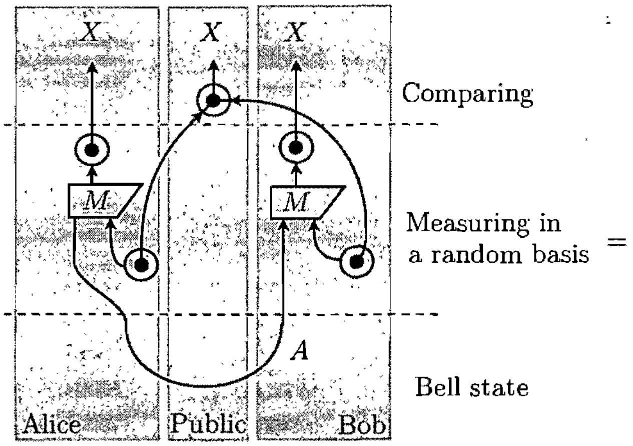
This protocol is depicted as follows:



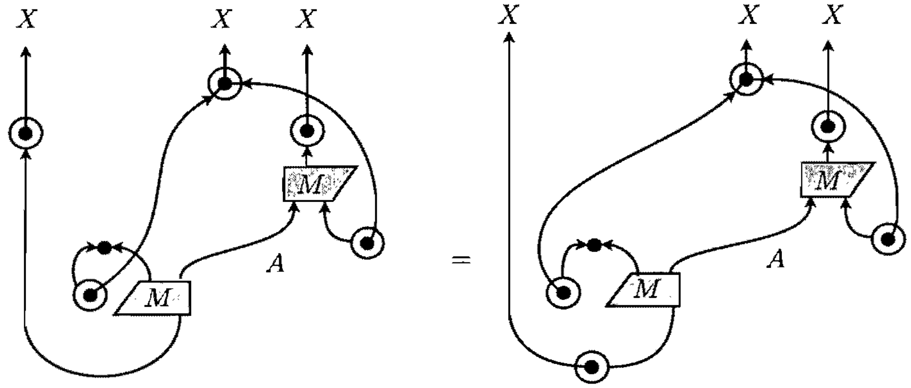
BBM92 is yet another cryptographic protocol used to generate a secure key between two parties. It is described as follows:

- Alice and Bob share a Bell state $\eta_A : I \to A^* \otimes A$.
- Both Alice and Bob choose a random basis in which they measure their share of the Bell state. If they both measured in the same basis, they must have the same result since η_A is entangled. If not, then the outcome is discarded.
- Alice and Bob compare their result on a public channel. By the remark of the previous point, if they measured in the same basis, then the outcome is kept and becomes a part of the key to communicate securely.
- The process is repeated as needed to construct a key of appropriate length.

BBM92 is depicted as follows:



We can now derive BB84 from BBM92 by first sliding the leftmost M along A, that is



and the second equality is obtained by sliding the big circle at the bottom of the Bell state.

Although BB84 and BBM92 do not share the same structural resources, the previous result is akin to the so-called purification of BB84 found in a security proof of BB84 [72]. The exact nature of the correspondence of this security proof—of the purification of BB84—and the topological equivalence between BB84 and BBM92 that we showed in our formalism remains to be determined.

9 Conclusion

In this dissertation, we provided a categorical semantics for quantum computation with classical control. In contrast to the previous works on this subject, namely [5] and [68], we did so without relying on a biproduct structure, thus remaining in the language of †-monoidal categories. It is worth noting that such a construction relies on relatively few structures, namely, to have a category **C** with

- A symmetric monoidal structure for the tensor,
- A dagger structure *i.e.*, the symmetric monoidal structure comes together with an involutive identity-on-object contravariant functor coherent with the symmetric monoidal structure. Such a structure provides us with a formal framework to handle the notion of adjoints,
- Quantum structures as compact structures coherent with the dagger structure which provides the categorical analogue of bipartite maximally entangled states and
- Base structures as special †-Frobenius objects which provide us with an axiomatisation of bases in the monoidal language.

Assuming these structures and using standard techniques, we constructed a comprehensive categorical semantics for quantum computation with classical control.

Something that hasn't been discussed elsewhere is that there has been another proposal for classical types given by P. Selinger in [69]. Classical types therein are obtained by splitting of self-adjoints idempotents on quantum types; in the words of the author "this means that classical data can be described as quantum data with additional properties (for example, the property of being a standard basis vector)." From this, it may seem obvious that there are strong affinities between the notion of classical types presented there and the one we presented in this dissertation. However, the exact nature of this correspondence isn't known either to me or to the author of the cited paper. In contrast to splitting idempotents, the construction we presented here enables us to define various species of classical maps such as (bi)stochastic maps and bijections which are valuable assets from an operational standpoint.

We now propose a few avenues of research and concluding remarks:

Internal traces

First, a point that was briefly mentioned in chapter 5 was the notion of *internal traces.* Still succinctly but in more details than there, the notion of internal traces in a symmetric monoidal category **C**—as initially proposed by Y. Delbecque—can be formalised as a family of morphisms $\{\mathrm{Tr}_A : A \to I \mid A \in |\mathbf{C}|\}$ where each components of the family behaves coherently with the monoidal structure *i.e.*: $tr_I = 1_I$,

$$\begin{tikzcd}
I \otimes A \arrow[r, "\mathrm{Tr}_{I\otimes A}"] \arrow[d, "\lambda_A"'] & I \\
A \arrow[ur, "\mathrm{Tr}_A"'] &
\end{tikzcd}
,
\begin{tikzcd}
A \otimes I \arrow[r, "\mathrm{Tr}_{A\otimes I}"] \arrow[d, "\rho_A"'] & I \\
A \arrow[ur, "\mathrm{Tr}_A"'] &
\end{tikzcd}
,
\begin{tikzcd}
A \otimes B \arrow[r, "\mathrm{Tr}_{A\otimes B}"] \arrow[d, "\sigma_{A,B}"'] & I \\
B \otimes A \arrow[ur, "\mathrm{Tr}_{B\otimes A}"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
A \otimes (B \otimes C) \arrow[r, "\mathrm{Tr}_{A\otimes(B\otimes C)}"] \arrow[d, "\alpha_{A,B,C}"'] & I \\
(A \otimes B) \otimes C \arrow[ur, "\mathrm{Tr}_{(A\otimes B)\otimes C}"'] &
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
A \otimes B \arrow[r, "\mathrm{Tr}_A \otimes \mathrm{Tr}_B"] \arrow[dr, "\mathrm{Tr}_{A\otimes B}"'] & I \otimes I \arrow[d, "\simeq"] \\
& I
\end{tikzcd}$$

With respect to this, most of the axioms of the usual trace as presented in section 4.4 carry over in the context of internal traces. However, the dinaturality axiom of traces finds no counterparts in the context of internal traces. Last year, we remarked that this yields some incongruities *e.g.* $\sum_i \langle i|$ is an internal trace in **FdHilb** which seems to indicate that something is missing to this axiomatisation. Consequentially, the author conjectured that we must require invariance of the internal trace under some isomorphisms. For instance, invariance over unitaries would accommodate the notion of internal trace in the category of trace non-increasing completely positive maps, a subcategory of **CP(FdHilb)** which is not monoidal traced. Invariance under permutations is probably sufficient for the category **SRel**; however, the details still need to be checked and it is not clear whether requiring such an invariance is the right way to proceed to correctly axiomatise this concept.

Topological quantum computing

One of the main problems faced in the implementation of a quantum computer is that of quantum decoherence. Basically, this problem reduces to the fact that it is not possible to isolate a quantum system from its environment, thus causing a rapid corruption of the data. In response to this, Kitaev, Freedman, Larsen and Wang proposed in [45] and [46] the concept of topological quantum computation, that is, to encode quantum data into global (*i.e.*, topological) degrees of freedom instead of local ones as it is usually done. Such a topological quantum computation uses anyons—quasi-particles with fractional statistics—to encode information. A full exposition of the physics and the mathematics describing these particles involves a mix of experimental phenomena (the fractional quantum Hall effect), topology (braids), algebra (Temperley-Lieb algebra, braid group and category theory) and quantum field theory. In particular, it is because of their topological nature that it is believed that they can provide a robust realisation of a quantum computer, *i.e.*, one less subject to decoherence.

Closer to the subject at stake here, the formalism of topological quantum computation relies heavily on category theory—see [51], a survey paper that the author wrote with P. Panangaden.

In fact, the algebra of anyons are described in terms of semisimple modular categories, a particular instance of monoidal categories. However, it is usually taken that the hom-sets of these categories are enriched over finite-dimensional Hilbert spaces thus enabling the passage from the algebra of anyons to the usual context of quantum computation. Now, as categories of quantum structures are a suitable framework to discuss quantum computation the natural question here is how to give a categorical semantics for topological quantum computation that fits the semantics given in this thesis.

Graphical protocol design

In the introduction, we mentioned that the graphical calculus may be, to some extent, a suitable alternative to quantum circuits as a representation of quantum computations. Such an assertion however, is perhaps a bit to wide to be taken as it stands.

Even if it is clear that any quantum circuit can be translated within our graphical language, the strength of the graphical language is that it is a proof technique allowing one to show, for instance, the equivalence or correctness of protocols. From this, graphical manipulations and transformations require a good identification of the various properties of the different morphisms that are used, or else, we end up with a (static) representation of formulas and we lose the main interest of the graphical calculus. Manifestly, the semantics presented in the previous chapters enables us to define many remarkable properties for morphisms but to what extent? This question is probably still too broad to have a precise answer. Let us say that in the quantum circuit model, one can define a *basis* for quantum circuits; these are defined by a set of gates which can simulate any quantum gates. Using such a notion, one can indeed show that any quantum circuit can be written with the elements of such a basis. However, in the context of Hilbert space, one can rely on the notion of distance between operators derived from the norm which is always a real non-negative value. In contrast, in a general categorical context, there is no order whatsoever between the elements (perhaps of some subset) of the scalar monoid $\mathbf{C}_q(I, I)$, such as one has in **FdHilb**, from which the regular notion of "universal set of gates" probably makes no sense in such a context.

Thus, if axiomatising the classical control with respect to the monoidal structure is an important step towards a comprehensive categorical presentation of quantum computation, and since it is not possible to speak of universality in this context, I believe that the next step is to reason about states and operations. An important step forward in that direction has been taken in [29] where B. Coecke and R. Duncan discuss complementary observables in terms of the abstract notion of scaled bialgebras and derive many known identities about quantum gates, circuits and algorithms (see section 6 of the cited paper).

In conclusion, it is my belief that the graphical calculus is much more intuitive and "human readable" than $2^n \times 2^n$ matrices. In that sense, I see good chances that in a near future, new protocols and algorithms will be invented using such a calculus. However, the work contained in this thesis was—perhaps unfortunately—just a stepping stone towards this goal.

Bibliography

[1] S. Abramsky, *Abstract scalars, loops, free traced and strongly compact closed categories*, in Proceedings of CALCO 2005, pp. 1–31, Springer Lecture Notes in Computer Science **3629**, 2005.

[2] S. Abramsky, *A Structural Approach To Reversible Computation*, Theoretical Computer Science vol. 347(3), pp. 441–464, 2005.

[3] S. Abramsky, R. Blute and P. Panangaden, *Nuclear trace ideals in tensored $*$-categories.* Journal of Pure and Applied Algebra, **45**, pp. 3–47, 1999.

[4] S. Abramsky and B. Coecke, *Physical Traces: Quantum vs. Classical Information Processing*, in Electronic notes in Theoretical computer science (ENTCS) (special issue: Proceedings of Category Theory in Computer Science 2002), **69**, 2003.`arXiv:cs/0207057`

[5] 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'04), IEEE Computer Science Press, pp. 415–425, 2004. An extended & improved version is available at `arXiv:quant-ph/0402130`

[6] S. Abramsky and B. Coecke, *Abstract physical traces*, in Theory and Application of Categories **14**, pp. 111–124, 2005. `http://www.tac.mta.ca/tac/volumes/14/6/14-06abs.html`

[7] S. Abramsky and B. Coecke, *Categorical quantum mechanics*, in the Handbook of Quantum Logic and Quantum Structures vol II, Elsevier, 2008.

[8] S. Abramsky and R. Duncan, *A Categorical Quantum Logic*, in Proceedings of the 2nd Worskhop on Quantum Programming Languages (QPL), pp. 3–20, P. Selinger, Ed., TUCS General Publication, 2005.

[9] T. Altenkirch and J. Grattage, *A functional quantum programming language.* Proceedings of the 20th Annual IEEE Symposium, pp. 249–258, 2005.

[10] D. Bouwmeester, A. Ekert and A. Zeilinger, eds. *The Physics of Quantum Information.* Springer-Verlag, 2001.

[11] C. H. Bennett and G. Brassard, *Quantum cryptography: public key distribution and coin tossing*, Proceedings of IEEE international conference on computer systems and signal processing, Bangalore India, pp. 175-179, 1984.

[12] C. H. Bennett, G. Brassard and N. D. Mermin, *Quantum cryptography without Bell's theorem.* Phys. Rev. Lett. **68**, 557, 1992.

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

[14] C. Bennett and S. J. Wiesner, *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states.* Phys. Rev. Lett., **69**:2881, 1992.

[15] G. Brassard, A. Broadbent, A. Tapp, *Quantum pseudo-telepathy*, Foundations of physics, **35**:11, pp. 1877–1907, 2005.

[16] G. Brassard, P. Horodecki and T. Mor. *Telepovm – a generalized quantum teleportation scheme.* IBM Journal of Research and Development, 2004.

[17] J. Baez, *Quantum quandaries: A category-theoretic perspective*, in S. French et al. (Eds.) Structural Foundations of Quantum Gravity, Oxford University Press, 2004. `arXiv:quant-ph/0404040`

[18] B. Bakalov and A. Kirilov Jr., *Lectures on tensor categories and modular functor.* In *University Lectures Series* vol. 21, American Mathematical Society, 2001.

[19] M. Barr, **-Autonomous Categories*, in Lecture Notes in Mathematics **752**, Springer-Verlag, 1979.

[20] S. Bell, *On the Einstein Podolsky Rosen paradox.* Physics **1**, 195, 1964.

[21] M. Choi, *Completely positive linear maps on complex matrices*, Linear Algebra and Its Applications, pp. 285–290, 1975.

[22] B. Coecke, *The logic of entanglement. An Invitation*, in Oxford University Computing Laboratory Research Report nr. PRG-RRR-03-12, 2004. Eight page short version (recommended) available at `arXiv:quant-ph/042014`. Full version at `web.comlab.ox.ac.uk/oucl/public` `03-12.html`

[23] B. Coecke, *Quantum information-flow, concretely, and axiomatically*, in Proceedings of the 2nd Workshop on Quantum Programming Languages (QPL), P. Selinger Ed., TUCS General Publication, pp. 57–74, 2005.

[24] B. Coecke, *Axiomatic description of mixed states from Selinger's CPM construction.*in Proceedings of the 4th Workshop on Quantum Programming Languages (QPL), P. Selinger Ed., Electronic Notes in Theoretical Computer Science (ENTCS), pp. 57–74, 2006.
`http://www.mathstat.dal.ca/ selinger/qpl2006/proceedings.html`

[25] B. Coecke, *Quantum information-flow, concretely, and axiomatically*, in Proceedings of Quantum Informatics 2004, pp. 15–29, Y. I. Ozhigov Ed., Proceedings of SPIE **5833**, 2005. `arXiv:quant-ph/050613`

[26] B. Coecke, *De-linearizing linearity: Projective quantum axiomatics from strong compact closure*, in Electronic Notes in Theoretical Computer Science (special issue: Proceeding of the 3rd International Workshop on Quantum Programming Languages), 2005. `arXiv:quant-ph/0506134`

[27] B. Coecke, *Kindergarten Quantum Mechanics*, Invited talk at Quantum Information, Computation and Logic: Exploring New Connections, Perimeter Institute, Waterloo, Canada, July 1722, 2005. `arXiv:quant-ph/0510032v1`.

[28] B. Coecke, *Introducing Categories to The Practising Physicist – Lecture notes*, 2005.
`http://web.comlab.ox.ac.uk/oucl/work/bob.coecke/Cats.pdf`

[29] B. Coecke and R. Duncan, *Interacting quantum observables* in Proceedings of Automata, Languages and Programming 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008.

[30] B. Coecke and B. Edwards, *Toy quantum categories.* in Proceedings of Quantum Physics and Logic 2008, Electronic Notes in Theoretical Computer Science, to appear.

[31] B. Coecke and É. O. Paquette, *POVMs and Nairmarks theorem without sums*, to appear in Proceedings of the 4th International Workshop on Quantum Programming Languages, Electronic Notes in Theoretical Computer Science. `arXiv:quant-ph/0608072v2`

[32] B. Coecke, É. O. Paquette and D. Pavlovic, Classical and quantum structuralism. To appear in: *Semantic techniques in Quantum Computation.* S. Gay and I. Mackie, Eds. Cambridge University Press.

[33] B. Coecke, É. O. Paquette and D. Pavlovic, *Classical and quantum structures.* Oxford University Computing Laboratory Research Report PRG-RR-08-02. Available at `http://web2.comlab.ox.ac.uk/oucl/publications/tr/rr-08-02.html`

[34] B. Coecke, É. O. Paquette and S. Perdrix, *Bases in diagrammatic quantum protocols.* Proceedings of the 24th Conference on the Mathematical Foundation of Programming Semantics (MFPS XXIV). Electronic Notes in Theoretical Computer Science. To appear.

[35] B. Coecke, É. O. Paquette, Categories for the Practising Physicist. To appear in: *New structures in physics.* B. Coecke Ed. Springer Lecture Notes in Physics.

[36] B. Coecke and D. Pavlovic, *Quantum measurements without sums*, invited paper to appear in The Mathematics of Quantum Computation and Technology; Chen, Kauffman and Lomonaco Eds., Taylor and Francis, 2006.

[37] B. Coecke and D. Pavlovic, *Scalar inverses in quantum structuralism.* Oxford University Computing Laboratory Research Report PRG-RR-08-03. `http://web2.comlab.ox.ac.uk/oucl/publications/tr/rr-08-03.html`

[38] 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.

[39] Y. Delbecque, *Game semantics for quantum data.* Proceedings of the wokshop on Quantum workshop on physics and logic (QPLV), 2008.

[40] Y. Delbecque and P. Panangaden, *Game semantics for quantum stores.* Proceedings of the 24th Conference on the Mathematical Foundation of Programming Semantics (MFPS XXIV). Electronic Notes in Theoretical Computer Science. To appear.

[41] Y. Delbecque, *A quantum game semantics for the measurement calculus.* Proceedings of the 4th International Workshop on Quantum Programming language (QPL'06), 2006.

[42] R. Duncan, *Types for quantum computing.* D.Phil. Thesis, Oxford University, 2006.

[43] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Let., **6**, pp. 661-663, 1991.

[44] A. Einstein, B. Podolsky and N. Rosen. *Can quantum-mechanical description of physical reality can be considered complete?* Physical review **47**, 777, 1935.

[45] M. Freedman, A. Kitaev and Z. Wang, *Simulation of Toplogical Field Theories by Quantum Computers*, Comm. Math. Phys., **227**(3), pp. 587–603, 2002.

[46] M. Freedman, M. Larsen and Z. Wang, *A modular functor which is universal for quantum computation.* Springer-Verlag in Comm. Math. Phys, **227**(4), pp. 605–622, 2001.

[47] P. Gabriel and M. Zisman, *Calculus of Fractions and Homotopy Theory.* Springer-Verlag, 1967.

[48] A. Harrow. *Coherent communication of classical messages.* Phys. Rev. Let., **92**:097902, 2004.

[49] D. Knuth. *The Art of Computer Programming, Volume 3: Sorting and Searching*, Third Edition. Addison-Wesley, 1997.

[50] É. O. Paquette, *A categorical semantics for topological quantum computation*, M. Sc. thesis, University of Ottawa, 2004.

[51] É. O. Paquette and P. Panangaden, *A categorical presentation of quantum computation with anyons.* To appear in: *New structures in physics.* B. Coecke Ed. Springer Lecture Notes in Physics.

[52] A. Joyal and R. Street, *The geometry of tensor calculus I.* Advances in Mathematics, **88**, pp. 55–112.

[53] A. Joyal and R. Street, *Braided tensor categories.* Advances in Mathemathics, **102**, pp. 20–78, 1993.

[54] A. Joyal, R. Street and D. Verity, *Traced monoidal categories*, London Mathematical Society Lecture Note Series **64**, Cambridge University Press, 1982.

[55] A. Y. Kitaev, A. H. Shen and M. N. Vyalyi, *Classical and quantum computation.* In Graduate studies in Mathematics, Vol. 47. American Mathematical Society, 2002.

[56] J. Kock, *Frobenius Algebras and 2D Topological Quantum Field Theories*, London Mathematical Society, in Student Texts **59**, 2004.

[57] G. M. Kelly and M. L. Laplaza, *Coherence for compact closed categories*, Journal of Pure and Applied Algebra, **88**, pp. 193–213, 1980.

[58] S. Mac Lane, *Categories for the Working Mathematician*, in Graduate texts in mathematics vol. 5, Springer, second edition, 2000.

[59] J. Lambek and P. J. Scott, *Introduction to higher order categorical logic*, Cambridge University Press, Cambridge, 1986.

[60] A. K. Lenstra and H. W. Lenstra, Jr. (eds.). *The development of the number field sieve.* Lecture Notes in Math. (1993) 1554. Springer-Verlag.

[61] S. Lipschutz, *Algèbre Linéaire, cours et problèmes*, Série Schaum, 1977.

[62] W. K. Nicholson, *Introduction to Abstract Algebra.* John Wiley & Sons, Inc. 1999.

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

[64] A. K. Pati and S. L. Braunstein, *Quantum no-deleting principle and some of its implications.* Nature, **404**, 164, 2000.

[65] R. Penrose and W. Rindler, *Spinors and Spacetime*, Cambridge University Press, 1984.

[66] P. Selinger, *Towards a quantum programming language*, in Mathematical Structure in Computer Science, **14**(4), pp. 527–586, 2004. `http://www.mscs.dal.ca/ selinger/papers/qpl.pdf`

[67] P. Selinger, *A brief survey of quantum programming languages.* Proceedings of the 7th International Symposium on Functional and Logic Programming, Nara, Japan. Springer LNCS 2998, pp 1–6.

[68] P. Selinger, *Dagger compact closed categories and completely positive maps*, in Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL), ENTCS **170** pp. 139–163, 2007. `http://www.mscs.dal.ca/ selinger/papers/dagger.pdf`

[69] P. Selinger, *Idempotents in dagger categories*, to appear in Proceedings of the 4th International Workshop on Quantum Programming Languages.
`http://www.mscs.dal.ca/ selinger/papers/idem.pdf`

[70] P. Selinger and B. Valiron, *On a fully abstract model for a quantum linear functional language.* Proceedings of the 4th International Workshop on Quantum Programming language (QPL'06), 2006.

[71] P. Selinger and B. Valiron, *A lambda calculus for quantum computation with classical control.* Mathematical structures in computer science, **16**(3), pp. 527–552, 2006.

[72] P. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol.* Phys. Rev. Lett., **85**, pp. 441–444, 2000. `arXiv:quant-ph/0003004`

[73] B. Valiron, *A functional programming language for quantum computation with classical control.* M. Sc. Thesis, University of Ottawa, 2004.

[74] A. van Tonder, *A lambda calculus for quantum computation*, SIAM J. of Comput. **33**, pp. 1109–1135, 2004.

[75] V. G. Tuarev, *Axioms for topological quantum field theories*, in Annales de la faculté des sciences de Toulouse 6^e série **3**(1), pp. 135 – 152, 1994.

[76] R. F. Wener, *All teleportation and dense coding schemes.* J. Phys. A: Math. Gen. 34 7081-7094 J. Phys. A: Math. Gen. **34** 7081-7094. `arXiv:quant-ph/0003070v1`

[77] W. K. Wooters and W. H. Zurek. *A single quantum cannot be cloned.* Nature, 299(5886), pp. 802–803.

[78] W. H. Zurek, *Decoherence and the transition from quantum to classical – Revisited*, arXiv:quant-ph/0306072, 2003.

Index