Linking Form and Function
A geometric investigation of Multi-partite graph states

David Mack

Balliol College

Supervised by Bob Coecke

University of Oxford

A thesis submitted for the degree of

Master of Science

September 2010

Abstract

Quantum Computing has quickly established itself as a paradigm-shifting force, displaying properties that defy intuition. Its power has produced revolutionary algorithms, yet we have no clear understanding of else is possible; we are still stumbling through a jungle rather than mastering the field.

Bob Coecke *et al.* have produced a graphical calculus and algebraic model that intuitively captures quantum's essential features, allowing one to manipulate complex structures easily on paper. Major algorithms can be verified in just a couple of steps. However, combining the basic elements is still alchemy, no rules nor intuitions exist to predict the results.

This dissertation seeks to investigate those dark corners and catalogue its findings, presenting any rules it encounters on the way. This is prefaced by a thorough description of the advanced algebra and calculus used, displaying key results and insights. The final chapter presents interesting structures that warrant further investigation and possible components for a higher-level quantum tool-set.

Contents

Chapter 1

Introduction

1.1 A short history

Over the past forty years quantum computation theory has grown immensely. We now have built small scale quantum computers, have discovered many important algorithms and quantum key transfer is being deployed on consumer devices.

Timeline

Some of the major milestones in quantum computation's early development;

- **1932** von Neumann designed Hilbert space quantum mechanics, the formalism underpinning all of Quantum computation [vN32].
- **1969** Steven Wiesner suggested quantum information processing as a possible way to better accomplish cryptographic tasks [Wie83].
- **1976** Roman Ingarden showed that Shannon Information Theory cannot be generalised to the quantum case [Ing76].
- **1982** Richard Feynman first described the idea of a 'quantum computer'
- **1985** David Deutsch described the universal quantum computer [Deu85]
- **1991** Artur Ekert invented entanglement based secure communication

Within the 1990s Grover's database search was discovered, Quantum Teleportation was formalised and Shor's factoring algorithm was discovered also. These events proved to the world that quantum computation is a very important and exciting new field of information physics.

At the beginning of the 21st century we have seen Shor's algorithm and Deutsch's algorithm implemented, created qubytes, stored them and teleported them over 16km (see [phy]). The lifetimes of these experimental systems, their complexity and their physical scale have all seen marked improvements.

1.2 Difficulties

However, despite over forty years of work in the field, we have yet to realise quantum computers large enough to be useful. One hindrance is decoherence– qubits break down into incoherent states by interacting with the surrounding environment and forming entanglements. Quantum Error Correction has reduced this problem, enabling recent successes.

A greater problem is the current Quantum formalism. In the field of classical information many well-developed abstractions and tools exist, these have underpinned the colossal explosion of information technology. However, Quantum Computation is still taught and investigated in Dirac Notation – akin to the cumbersome Assembly language of decades ago.

$\|01\rangle + \|10\rangle$	$\|0\rangle + \|1\rangle$
Entanglement	**Superposition**

Figure 1.1: *Dirac Notation does not clearly differentiate between superposition and entanglement.*

The two key quantum resources – Entanglement and Superposition – have very different abilities, yet are depicted nearly identically in Dirac notation (see figure 1.1 above and figure 1.2 below). Once one creates moderately complex computations in Dirac notation the result is incredibly difficult to read, it has been argued that this is the reason that Quantum Teleportation was not discovered until almost seventy years after von Neuman's conception of the Quantum formalism [Coe05].

However, Quantum Computers have the potential to work completely outside the envelope of our current classical computers– for example they can decrypt industry standard secure communications. Therefore they are an essential part of our computational future and tools must be found to deal with the aforementioned problems. This dissertation explores the growing field of graphical representation.

1.3 A graphical approach

The difficulties in Dirac based reasoning have led some authors to pursue diagrammatic approaches to communicating quantum systems. Many have used

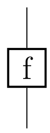
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\begin{aligned} |\psi\rangle \otimes \beta_{00} &= (\alpha|0\rangle + \beta|1\rangle)\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) \\ &= \frac{1}{\sqrt{2}}\left(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right) \end{aligned}$$

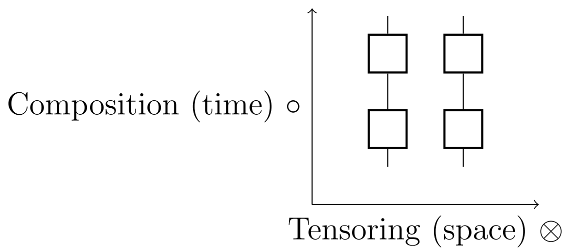
$$\begin{aligned} CNOT(1,2) \longrightarrow \quad & \frac{1}{\sqrt{2}}\left(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right) \\ H(1) \longrightarrow \quad & \frac{1}{\sqrt{2}}\left(\alpha\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right) \\ &= \frac{1}{2}\big(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) \\ &\quad + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\big) \\ &= \frac{1}{2}\sum_{b_1 b_2 = 0}^{1} |b_1 b_2\rangle (X^{b_2} Z^{b_1})|\psi\rangle \end{aligned}$$

Figure 1.2: *Quantum state teleportation is a primitive operation yet its description in Dirac notation is lengthy and unintuitive– an excerpt of a standard treatment is presented here as witness.*

the metaphors of qubit 'wires' that connect up gate 'boxes' to form a quantum circuit:



This displays the inherent two-dimensionality of the systems– qubits are tensored to form parallel wires, and gates are applied along those wires. These two operations, tensoring and composition, be seen as two separate axis of manipulation:



However most of these representations have been informal. They have not supported proof procedures, nor have they been free of ambiguity. The representation explored here has a precise formal meaning, making it a 'graphical calculus'. A statement is derivable in the graphical calculus[1] *if and only if* it is derivable from the axioms of the underlying quantum theory.

The calculus depicts Quantum algorithms much more intuitively. For example, its axioms (which will be later described) make the creation and measurement of multi-qubit states into simple diagrams such as the following:

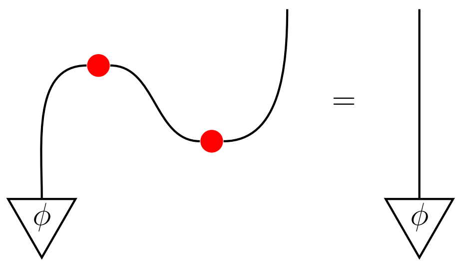


Figure 1.3: *A diagram in the graphical calculus, showing how a primative Teleportation protocol is equal to directly handing Alice's qubit ϕ to Bob*

[1] Multiple calculi are presented in this dissertation, not all of them have this property.

Chapter 2

Background

This dissertation builds upon the material presented in the Oxford University lecture courses on Category Theory [Doe09a] and Quantum Computation Science [Doe09b]. The initial chapters embed the Quantum Computation formalism into a host category and present a graphical calculus for it. The later chapters then explore the category that has been constructed.

This chapter outlines the prerequisite knowledge and provides references to the papers that underpin this dissertation.

2.1 Quantum Computation

The calculus presented is a Categorical treatment of the Quantum Computation formalism. A familiarity with the formalism is therefore helpful and a brief introduction is given here. For more information Andreas Doering's lecture notes [Doe09b] provide a concise guide to the whole subject.

Classical Computation works with systems of bits, the states of which are generally known at every point in time. In contrast, Quantum Computation's *qubits* are in a superposition of states; They are a probability distribution of different outcomes and remain so until a *measurement* is made. After measurement they collapse into a single state.

The second significant departure from the Classical world is the phenomenon of *quantum entanglement*: Measuring one qubit (and thus determining its state) can instantaneously affect other qubits, regardless of their physical locality. A composite system is no longer a simple sum of its parts, instead it becomes only describable as a whole.

Quantum systems are modelled as states of an algebraic space (some knowledge of vector spaces is assumed):

Definition 1. A *Hilbert Space* $\mathcal{H}$ is an n-dimensional vector space over the field

$\mathcal{F}$ with the following properties:

- It possesses an inner product $\langle - | - \rangle : \mathcal{H} \times \mathcal{H} \to \mathcal{F}$ that is
  - Linear in its second argument, i.e. $\forall \alpha, \beta \in \mathcal{F}, s, t, u \in \mathcal{H} \quad \langle s | \alpha t + \beta u \rangle = \alpha \langle s | t \rangle + \beta \langle s | u \rangle$
  - Conjugate-symmetric: $\forall s, t \in \mathcal{H} \quad \langle s | t \rangle = \overline{\langle t | s \rangle}$
  - Positive definite: $\forall s \in \mathcal{H} \quad \langle s | s \rangle \geq 0$ with $\langle s | s \rangle = 0 \iff x = 0$
- It has a norm operator $|s| = \sqrt{\langle s | s \rangle}$ that is complete[1].

Throughout this dissertation we will deal with Hilbert spaces, which will always be finite dimensional and over the field of complex numbers. A qubit is an element of the two dimensional Hilbert Space over the complex field known here as $\mathcal{Q}$.

A qubit has two primary states,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

As well as being in one of these states (known as the 'Computational Basis' for their likeness to bits), it can be in a superposition of both[2]:

$$|\theta\rangle = |0\rangle + |1\rangle$$

Here the qubit is equally likely to be in either state when measured. The later section on measurement describes this in greater detail.

Just like Classical systems, Quantum systems change over time. The change over any period of time can be described by a special type of linear map:

Definition 2. A *Unitary* operation is a linear map $U : \mathcal{H} \to \mathcal{H}$ such that its inverse equals its adjoint, i.e.

$$UU^\dagger = U^\dagger U = I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Where I is the identity matrix and $\dagger$ is the operation of transposing then conjugating the matrix.

Other aspects of Quantum Computation are introduced later as required.

[1] A definition of completeness is outside the scope of this chapter, please see lecture notes [Doe09b] for further details.

[2] Notice the vector has not been normalised to size 1– we are only interested in the relative probability of states. The (complex) size of a quantum state is known as its 'global phase' – it does not affect the probabistic outcome of the state and therefore equality between quantum states usually ignores the global phase. In this dissertation vectors will frequently be left unnormalised.

2.2 Category Theory

Category Theory is the framework within which this dissertation builds its formal algebra. Rather than being a large scale theory, Category Theory is more of a lexicon within which structures can be created and compared. The pre-requisite definitions are presented in this section.

Definition 3. A *Category* $\mathbf{C}$ consists of

- A collection of objects $\mathsf{A} \in Ob(\mathbf{C})$.
- A collection of arrows (also known as morphisms) $f : \mathsf{A} \to \mathsf{B} \in Arr(\mathbf{C})$ with functions $dom(f) = \mathsf{A}$ and $codom(f) = \mathsf{B}$ mapping arrows to a domain and co-domain object. Domain and co-domain act as a typing system mandating which arrows can be composed. $\mathsf{C}(\mathsf{A}, \mathsf{B})$ is the collection of all arrows from object A to B. Arrows are such that:
  - A binary composition operation $\circ$ exists.
  - For each pair of arrows $f : \mathsf{A} \to \mathsf{B}$ and $g : \mathsf{B} \to \mathsf{C}$ a *composite arrow* $g \circ f = h : \mathsf{A} \to \mathsf{C}$ exists.
  - Arrow composition is associative, i.e. $(h \circ g) \circ f = h \circ (g \circ f)$.
- Every object A has an identity arrow 1_{A} such that for all $f : \mathsf{A} \to \mathsf{B}$ $f \circ 1_{\mathsf{A}} = f$ and for all $g : \mathsf{B} \to \mathsf{A}$ $\quad 1_{\mathsf{A}} \circ g = g$.

Example 1. Every group $(\mathcal{G}, \diamond)$ gives rise to a category **Grp** with

- A single object $\star$.
- An arrow $g_i : \star \to \star$ for every $g_i \in \mathcal{G}$, where the arrow $1_\star$ corresponds to the group identity.
- Composition such that $g_i \circ g_j$ equals the object representing $g_i \diamond g_j$.
- An arrow ${g_i}^{-1}$ for each $g_i \in \mathcal{G}$ such that $g_i \circ g_i^{-1} = g_i^{-1} \circ g_i = 1_\star$.

Notice how this Category represents the group structure entirely with arrows, objects hold no information. This is typical of how Category theory is used, it recognises that the relationships between objects– rather than the objects themselves– are most important. Also notice that the group axioms of closure, associativity and identity operation all follow from the above definition without being explicitly defined– this is the power of Category Theory; One only needs to describe the essence of the structure and the rest naturally follows.

With Categories defined one final workhorse is required: Functors. These define a relationship between two Categories, expressed as a mapping of objects and arrows.

Definition 4. A *Functor* $F(-) : \mathbf{C} \to \mathbf{D}$ is such that:

- Every object $\mathsf{A} \in Ob(\mathbf{C})$ has an image $\mathsf{FA} \in Ob(\mathbf{D})$
- Every arrow $f : \mathsf{A} \to \mathsf{B} \in Arr(\mathbf{C})$ has an image $Ff : \mathsf{FA} \to \mathsf{FB} \in Arr(\mathbf{D})$

The functor respects the compositional structure of both Categories, i.e.

$$F(g \circ_{\mathbf{C}} f) = Fg \circ_{\mathbf{D}} Ff \quad \text{and} \quad F(1_{\mathsf{A}}) = 1_{\mathsf{FA}} \tag{2.1}$$

Further introduction to Category theory can be found in [BW95]. MacLane's imposing [Lan98a] provides an encyclopaedic treatment of the subject.

In this document **Categories** are displayed in bold, *Arrows* in italics and Objects in sans-serif.

2.3 Graphical Calculus

This dissertation will take the Quantum Formalism and rephrase it into Categorical terms. Not only will the category's objects and morphisms have a graphical depiction, every subsequent property we describe of the category will have a graphical interpretation. There is no prerequisite knowledge for the graphical calculus, but a brief historical background is presented here.

Graphical calculi have their roots in Penrose's work during the 1970's. They were later formalised by Yetter [PF89], Selinger and others (see Selinger's paper [Sel09] for a survey of this work).

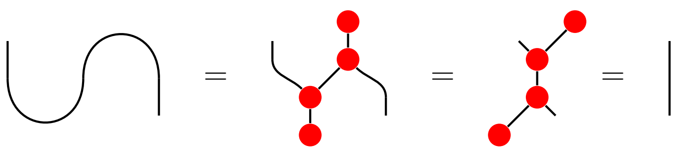
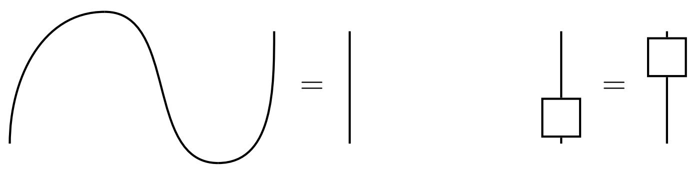


Figure 2.1: *An example equation from the graphical X/Z calculus.*

The calculus presented here builds heavily on Bob Coecke and Samson Abramsky's work on formalising quantum mechanics into diagrammatic categories. See [Coe04] for an early example of the work. The comprehensive tutorial 'Categories for the Practising Physicist' [Coe08] provides an enjoyable introduction. For the most recent work see [CK10] for a treatment of multi-partite entanglement (a focus of this dissertation). An earlier paper [CD09] presents the quite astonishing result that a very capable (yet simple) calculus is induced by every Hilbert basis.

The graphical calculus is both powerful and useful, it saves the user time whilst abstracting away unnecessary details. Not only is it a dramatic improvement upon the Dirac notation, statements that are non-trivially equal turn out to have identical diagrams. Furthermore intuitive visual metaphors such as 'yanking the wire straight' and 'sliding the box along the wire' express axioms that are terse when written as equations:



In the next chapters the quantum formalism will be expressed categorically and the diagrammatic calculus will be introduced.

Chapter 3

Bringing Quantum into the Categorical Realm

In this chapter we survey the Quantum formalism and incrementally build a category to represent it.

At its core the Quantum formalism allows us to take both qubits and groups of qubits and perform operations on them in parallel. Therefore the first piece of structure required is a basic process framework.

3.1 The Basics

Imagine we are trying to model a car production line with the category **CarFac**. The parts undergo various processes e.g. *SprayRed* and these shall be represented by arrows in **CarFac**. Next, the various stages in between processes will be represented by objects in **CarFac**. Therefore we could have $\mathsf{UnpaintedCar}$ as the domain of *SprayRed* and $\mathsf{PaintedCar}$ as the co-domain. We can then form a new arrow by composing processes *SprayRed* and *Wax* e.g.

$$\mathit{Wax} \circ \mathit{SprayRed} = \mathit{SprayAndWax} : \mathsf{UnpaintedCar} \to \mathsf{RedShinyCar}$$

Composition is such that the rightmost action is performed first, the $\circ$ symbol can be read as 'after'. Notice that the objects are not the particular cars, but rather their 'state'.

Similarly, we shall model quantum systems in the category **FdHilb**, the category of finite dimensional Hilbert spaces. We shall consider Hilbert spaces as the objects and linear maps as the arrows between them. Composing two arrows is simply matrix multiplication. We shall soon see **FdHilb** possesses many rich structures.

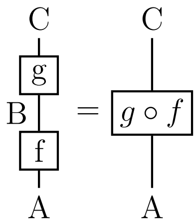


Figure 3.1: *Processes (arrows) are graphically depicted as boxes, with composition on the vertical axis. The diagram depicts $f : \mathsf{A} \to \mathsf{B}$, $g : \mathsf{B} \to \mathsf{C}$ and their composition. The diagram is read from the bottom up.*

3.1.1 A bit about Objects

We now introduce a special object I. This is not a Hilbert space, it is the space of complex scalars within which no qubits can exist.

Definition 5. An arrow from I to itself is a *scalar*. A scalar in a diagram is interpreted as a probabilistic weight. Composing two scalar arrows multiplies them. Once we have introduced monoidal structure into our category scalars will turn out to exhibit many familiar features: they experience commutative multiplication, form a multiplicative group and act globally.

Definition 6. A *point* is an arrow from I to another object (a Hilbert space). Points prepare quantum states. Points bijectively map to quantum states:

$$s : \mathsf{I} \to \mathsf{A} \Longleftrightarrow |s(0)\rangle$$

Definition 7. The object $\mathcal{Q}$ is the two-dimensional Hilbert space within which Qubits reside

Throughout this paper we will often use the same symbol for a point ψ and a ket $|\psi\rangle$ since in the category **FdHilb** (our primary focus) they are indeed the same thing.

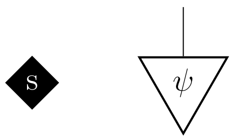


Figure 3.2: *The scalar space I is not depicted with wires since scalars are global and wires transport qubits. Therefore, scalars s are drawn as floating diamonds. Since points ψ (kets) are arrows from the scalar space I to a Hilbert space A, they are the beginning point for a wire. Points are conveyed by triangles in the graphical notation, imitating the kets $|\psi\rangle$ they represent.*

3.1.2 Arrows

For **FdHilb** to be a valid category it must fulfil two criteria:

- Every object must have an *identity arrow*. This is simply the identity matrix for each given Hilbert Space (and the scalar *1* for the object I).
- Arrows must compose associatively– which is true of linear maps and matrix multiplication.

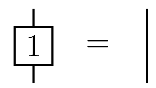
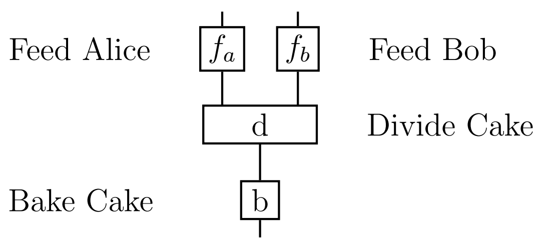


Figure 3.3: *Identity arrows are portrayed simply as blank wires*

3.1.3 Parallel Processes

We now have a simple process algebra– we can combine arrows to create simple 'production lines'. However, we cannot express parallel operations, an essential feature of any process algebra. We wish to express situations such as the following:



To do this we introduce the notion of 'tensoring':

Definition 8 (Monoidal Category)**.** A Monoidal Category **C** possesses a covariant bifunctor $\otimes(-,-) : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$ known as the tensor product. Its action is known as tensoring and forms a monoid structure within the host category.

- The $\otimes$ symbol is overloaded such that the image of objects $\otimes(\mathsf{A}, \mathsf{B})$ is $\mathsf{A} \otimes \mathsf{B}$ and the image of morphisms $\otimes(f : \mathsf{A} \to \mathsf{C}, g : \mathsf{B} \to \mathsf{D})$ is $f \otimes g : \mathsf{A} \otimes \mathsf{B} \to \mathsf{C} \otimes \mathsf{D}$.
- As $\otimes$ is a bifunctor it is a functor in two arguments i.e.

$$(\mathsf{A} \otimes \mathsf{B}) \circ (\mathsf{C} \otimes \mathsf{D}) = (\mathsf{A} \circ \mathsf{C}) \otimes (\mathsf{B} \circ \mathsf{D})$$

$$1_{\mathsf{A}\otimes\mathsf{B}} = 1_{\mathsf{A}} \otimes 1_{\mathsf{B}}$$

Equivalently $\otimes$ is a functor whose domain is the product category $\mathbf{C} \times \mathbf{C}$. Furthermore, for all $\mathsf{A}, \mathsf{B}, \mathsf{C} \in \mathbf{C}$:

1. The functor is associative; There exists a natural isomorphism

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

2. I acts as a identity for the monoid, i.e. there exist natural isomorphisms $\lambda_{\mathsf{A}} : \mathsf{I} \otimes \mathsf{A} \cong \mathsf{A}$ and $\rho_{\mathsf{A}} : \mathsf{A} \otimes \mathsf{I} \cong \mathsf{A}$.

3. Figures 3.4 and 3.5 commute (these are the 'coherence laws').

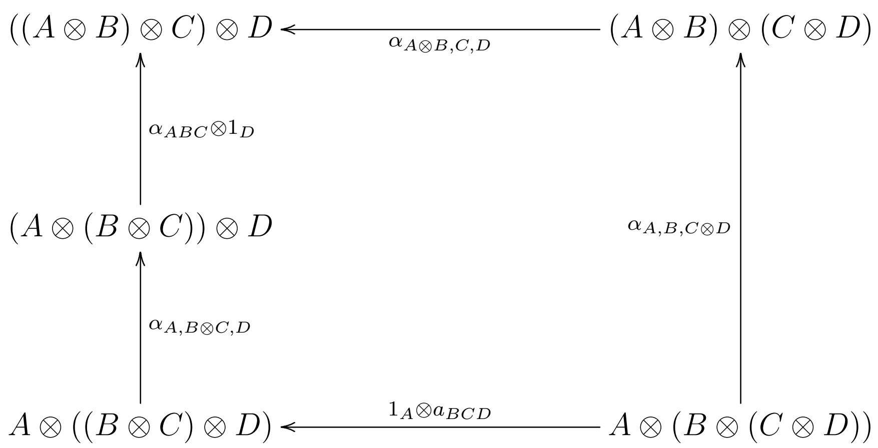


Figure 3.4: *Associativity Coherence Law*

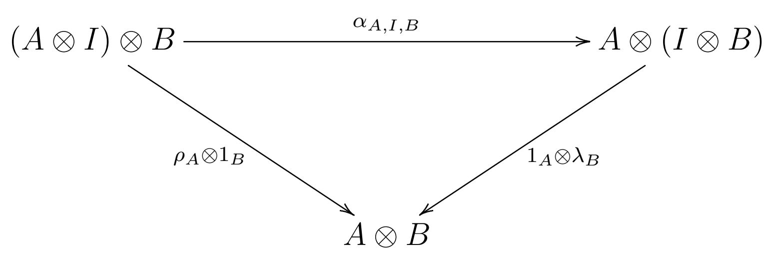


Figure 3.5: *Unit Coherence Law*

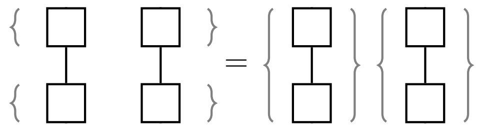
Now the earlier car example can be formalised as

$$\mathit{SprayRed} \circ \mathit{AttachWheels} \circ (\mathit{MakeChasis} \otimes \mathit{MakeWheels}) : \mathsf{I} \otimes \mathsf{I} \to \mathsf{PaintedCar}$$

where $\mathit{AttachWheels} : \mathsf{Chasis} \otimes \mathsf{Wheels} \to \mathsf{UnpaintedCar}$.

Notice that the tensored systems lie parallel along the horizontal axis, with the process stages taking place along the vertical axis. It is the projection of these two separate aspects onto one dimension that make Dirac notation so difficult to use.

The bifuntorality property is intuitively implicit in diagrams, it graphically depicts as:



Since brackets are not required in either of the above diagrams, bifuntorality is trivially true in the diagrammatic language.

Next we extend the Monoid Category to be Symmetric and Strict:

Definition 9 (Symmetry)**.** A monoidal category **C** is *symmetric* if for all $\mathsf{A}, \mathsf{B} \in$ **C** there exists a natural isomorphism $\sigma_{\mathsf{A},\mathsf{B}} : \mathsf{A} \otimes \mathsf{B} \cong \mathsf{B} \otimes \mathsf{A}$ such that $\sigma_{\mathsf{A},\mathsf{B}} \circ \sigma_{\mathsf{B},\mathsf{A}} = 1_{\mathsf{B},\mathsf{A}}$.

We also require that coherence diagrams 3.6, 3.7 and 3.8 commute.

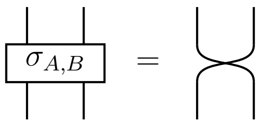


Figure 3.9: *The symmetric operator is depicted as the crossing of two wires*

By MacLane's Coherence Theorem (see [Lan98b]) any structure that obeys the previous five coherence conditions has a special property: Any diagram of its α, σ, λ and ρ arrows commutes.

The graphical language that we are introducing has various equalities built into it[1], such that the visual depiction of two categorically different statements could look identical. Strictness imports those equalities into the category, simplifying it by reducing the number of objects. This ensures there is a bijection between equal diagrams and equal categorical equations.

Definition 10 (Strictness)**.** A symmetric monoidal category (SMC) **C** is *strict* if

[1]More importantly (though obliquely) these equalities are built into the quantum physical processes themselves, see [Coe08]

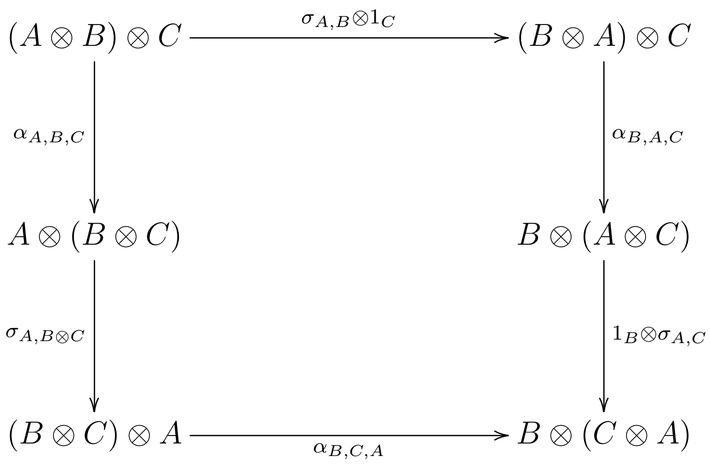


Figure 3.6: *Symmetric Associativity Coherence Law*

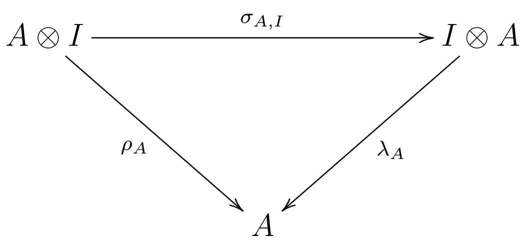


Figure 3.7: *Symmetric Unit Coherence Law*

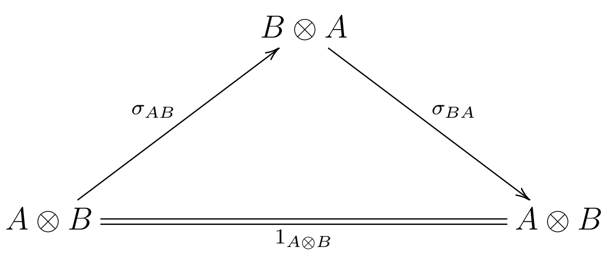


Figure 3.8: *Inverse Coherence Law*

- The natural isomorphisms λ_{A}, ρ_{A} and $\alpha_{\mathsf{A},\mathsf{B},\mathsf{C}}$ are all identities (i.e. the objects they are isomorphic between are in fact the same). We specifically do *not* require $\sigma_{\mathsf{A},\mathsf{B}} : \mathsf{A} \otimes \mathsf{B} \cong \mathsf{B} \otimes \mathsf{A}$ to be an identity as then when one applied $f \otimes g$ to $\mathsf{A} \otimes \mathsf{B}$ it would be unclear which object had which morphism applied.
- For all $\mathsf{A}, \mathsf{B} \in \mathbf{C}$ $\sigma^{-1}_{\mathsf{A},\mathsf{B}} = \sigma_{\mathsf{B},\mathsf{A}}$ holds
- The 'sliding' axioms in Figs. 3.10 and 3.11 hold.

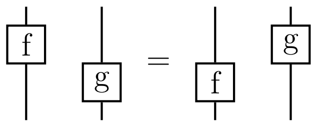


Figure 3.10: *The sliding axiom; for all* $f : \mathsf{A} \to \mathsf{B}$ *and* $g : \mathsf{C} \to \mathsf{D}$ *it is the case that* $(f \otimes 1_{\mathsf{D}}) \circ (1_{\mathsf{A}} \otimes g) = (1_{\mathsf{B}} \otimes g) \circ (f \otimes 1_{\mathsf{C}})$. *Interestingly, this holds as a result of bifunctorality.*

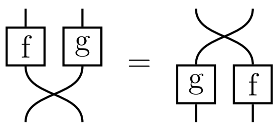


Figure 3.11: *The symmetric sliding axiom;* $(f \otimes g) \circ \sigma_{\mathsf{C},\mathsf{A}} = \sigma_{\mathsf{D},\mathsf{B}} \circ (g \otimes f)$

The Hilbert space tensor fulfils all the above properties making **FdHilb** a symmetric monoidal category (SMC). It is also Strict ([Lan98b] p.257).

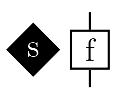
3.1.4 Scalar Multiplication

Now that linear maps have been formalised it is possible to define the multiplication of a map by a scalar.

Definition 11. *Scalar multiplication* is defined for scalar s and arrow $f : \mathsf{A} \to \mathsf{B}$ as

$$s \bullet f = \lambda_{\mathsf{B}} \circ (s \otimes f) \circ \lambda^{-1}_{\mathsf{A}}$$

Graphically,



Furthermore, by simple manipulation of the definition

$$(s \bullet f) \circ (t \bullet g) = (s \circ t) \bullet (f \circ g) \tag{3.1}$$

and

$$(s \bullet f) \otimes (t \bullet g) \cong (s \circ t) \bullet (f \otimes g) \tag{3.2}$$

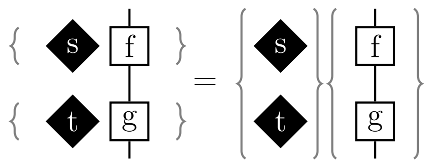


Figure 3.12: *Proof of* (3.1)

.

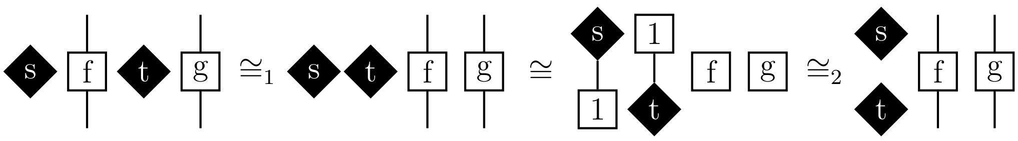


Figure 3.13: *Proof of* (3.2). *(1) holds by isomorphisms* λ, ρ, α *and* σ. *(2) holds by isomorphisms* λ *and* ρ. *Note that wires are included for some scalars to aid clarity.*

Equations (3.1) and (3.2) show that scalars act globally, they are not bound to any part of the quantum system. Scalars are not attached to wires in the graphical depiction, enabling them to move around the diagram.

As one would expect, scalars experience commutative multiplication. This is possible due to the λ_I and ρ_I coherence equations. The graphical proof:

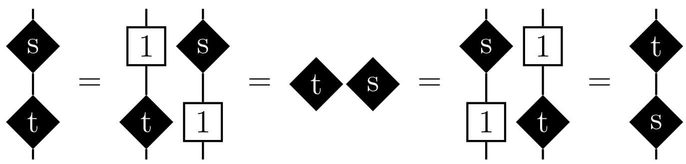


Figure 3.14: $s \circ t = (1 \otimes s) \circ (t \otimes 1) = t \otimes s = (s \otimes 1) \circ (1 \otimes t) = t \circ s$

Finally, since every object must have an identity, there must exist the unit scalar *1*.

Thanks to commutation a further piece of structure emerges:

Definition 12. The *zero scalar* is a scalar 0 such that for all scalars s

$$s \circ 0 = 0$$

Lemma 1. *The zero scalar is unique*

Proof. Consider zero scalars 0 and $\bar{0}$. Then

$$0 = \bar{0} \circ 0 = 0 \circ \bar{0} = \bar{0}$$

□

Therefore scalars form a multiplicative group $(\mathbf{FdHilb}(\mathsf{I}, \mathsf{I}), \circ, 0, 1)$

3.2 Capturing the Quantum Formalism

Here we attempt to build the Quantum Computation machinery within the symmetric monoidal category we have just constructed. In this section we will incrementally bolt on extra features to the category until it is sufficiently rich to represent what we require.

3.2.1 Unitary operations

The evolution of a quantum system is described by unitary operations, it is therefore necessary to understand their place within the category we have constructed. To achieve this we must introduce adjunction to the category **FdHilb**.

Definition 13. The *adjoint* $\dagger(-)$ (pronounced 'dagger') is an involutive identity-on-objects contravariant endofunctor. It preserves the monoid structure and therefore has the following properties:

- Objects A are mapped to themselves i.e. $\mathsf{A}^\dagger = \mathsf{A}$
- Arrows $f : \mathsf{A} \to \mathsf{B}$ are mapped to their contra-variant equivalent $f^\dagger : \mathsf{B} \to \mathsf{A}$ and identities to themselves $1_{\mathsf{A}}^\dagger = 1_{\mathsf{A}}$.
- Due to contravariance it is anti-homorphic i.e. $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$
- It preserves the tensor product i.e. $(\mathsf{A} \otimes \mathsf{B})^\dagger = \mathsf{A}^\dagger \otimes \mathsf{B}^\dagger$ and $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$
- Applying the dagger to itself results in the identity functor $\dagger(\dagger(-)) = 1(-)$ as it is involutive.

- As it is involutive, the functor (as a function between hom-sets) must be bijective– therefore the functor is fully faithful.

Equipping a symmetric monoidal category with this functor produces a †-SMC. In **FdHilb** the usual adjoint operation of taking a linear map's transpose and then conjugate performs the † role perfectly; fulfilling the required properties.

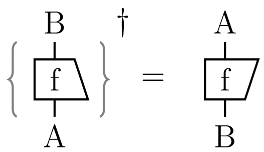
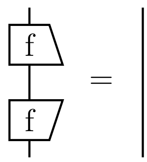


Figure 3.15: *The adjoint of* $f : \mathsf{A} \to \mathsf{B}$*. The adjoint flips the domain and co-domain and is therefore depicted as a vertical reflection. To make this clear the morphism boxes are given an asymmetric shape.*

With the adjoint added to the category, unitary operations can now be formulated in purely categorical terms:

Definition 14 (Unitary)**.** An arrow $f : \mathsf{A} \to \mathsf{B}$ is *unitary* if and only if $f \circ f^\dagger = 1_\mathsf{B}$ Graphically,



3.2.2 Hilbert structure

Hilbert spaces are characterised by having an inner product space. Introducing this structure completes our basic categorical treatment of Hilbert space.

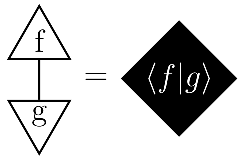
Definition 15. *Bras*, the complement to Kets in Bra-ket notation, are represented as the adjoint to their corresponding Kets i.e. for each point $f : \mathsf{I} \to \mathsf{A}$ (ket $|f\rangle$), $f^\dagger$ is the bra $\langle f|$.

Definition 16. The *inner product*

$$\langle\,\rangle\,(f, g) = \langle f|g\rangle = f^\dagger \circ g$$

maps pairs of points to scalars; it combines a bra with a ket. For the domain of $f^\dagger$ to match the co-domain of g both points must be from the same Hilbert space.

Graphically,



As expected in a Hilbert space, unitaries preserve inner products.

Proof. For a unitary $f : \mathsf{A} \to \mathsf{B}$ and points $x : \mathsf{I} \to \mathsf{A}$ and $y : \mathsf{I} \to \mathsf{A}$,

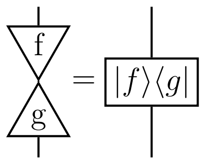
$$\begin{aligned} \langle x|y\rangle &= x^\dagger \circ y \\ &= x^\dagger \circ 1_\mathsf{A} \circ y \\ &= x^\dagger \circ f^\dagger \circ f \circ y \\ &= (f \circ x)^\dagger \circ (f \circ y) \\ &= \langle f \circ x| f \circ y\rangle \end{aligned}$$

□

Definition 17. Similarly by combining a bra and ket in the opposite order a *projection* is formed. Given points $f : \mathsf{I} \to \mathsf{A}$ and $g : \mathsf{I} \to \mathsf{B}$

$$|\rangle\, \langle|\, (f, g) = |f\rangle\langle g| = f \circ g^\dagger : \mathsf{B} \to \mathsf{A}$$

Graphically,



3.2.3 A first attempt at Measurement

Measurement occupies an uncomfortable place within the von Neuman formalism; all manipulations of the quantum state are both linear and unitary yet measurement is neither. The categorical approach given here only recently found a successful approach to putting measurement and unitaries on equal footing. However, this approach requires a lot more structure to be described and will be presented later. In this section an earlier, simpler treatment of measurement is given.

Measuring a quantum system requires an observable, a self-adjoint matrix with real eigenvalues. The eigenvectors of such a matrix form a spanning orthonormal basis for the state space it resides in. The measurement will result in the quantum system being projected onto one of these eigenvectors. An observable Ψ can therefore be thought of as a set $\{P_i\}$ of spanning projections for which

$$\forall P_i, P_j \in \Psi. \quad P_i \circ P_j = 0 \text{ if } i \neq j$$
$$= P_i \text{ otherwise}$$

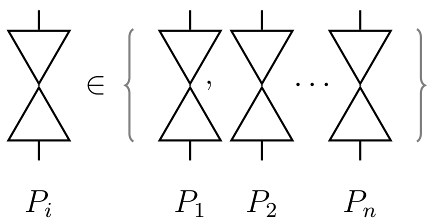
The outcome of each measurement is dictated by the Bonn Rule. The probability of a particular $P_i \in \Psi$ becoming the measurement result for quantum system ψ is calculated

$$\langle\psi|P_i|\psi\rangle$$

From this distribution one P_k is randomly chosen and the system is then projected onto that vector

$$|\bar{\psi}\rangle = P_k \circ |\psi\rangle$$

In our categorical formalisation, an observable Ψ for Hilbert space A is a set of projection arrows $\{P_i : \mathsf{A} \to \mathsf{A}\}$ and by relying on post-selection (i.e. we assume the measurement will be determined later and then the choice of projection index can be fixed) we simply label the measurement 'arrow' with P_i. Graphically,



This is known as the index method, the index is used to coordinate arrow selection across the graph. The classic example of this technique is to display quantum teleportation:

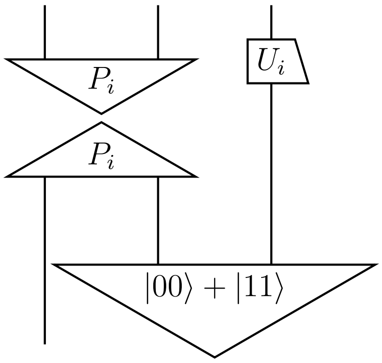


Figure 3.16: *Teleportation with indices. The circuit has a 'correction' unitary that relies on the measurement outcome.*

However this measurement formalism is unsatisfactory, it requires a meta level outside of the category. This will be solved in Chapter 4.

3.2.4 Transpose

Transposition (represented here by $(-)^*$) is an essential operation. It transforms linear maps in a fundamental way such that they operate on entirely different Hilbert spaces.

Before we can investigate transposition we need to include Dual spaces in the **FdHilb** category. As a vector space, every Hilbert space $\mathcal{H}$ has a dual space $\mathcal{H}^*$. $\mathcal{H}^*$ contains all continuous linear functionals into $\mathbb{C}$, that is arrows $g : \mathsf{H}^* \to \mathsf{I}$. These are the duals of the points contained within $\mathcal{H}$.

The Riesz representation theorem states that elements of Hilbert spaces bijectively map to elements of their dual. For any point $f : \mathsf{I} \to \mathsf{H}$ in $\mathcal{H}$ its mapping to f^* is defined:

$$f \mapsto \langle f, - \rangle(-)$$

In this dual space scalar multiplication and inner-products are conjugated, i.e.

$$s \bullet_{\mathcal{H}^*} f = \bar{s} \bullet_{\mathcal{H}} f \qquad \langle f|g\rangle_{\mathcal{H}^*} = \langle g|f\rangle_{\mathcal{H}}$$

Definition 18. A *category with duals* is such that every object A comes with a dual A^*.

The category **FdHilb** has duals, as described above. Note that I is self dual, i.e. $\mathsf{I} = \mathsf{I}^*$.

In the diagrammatic language wires operating in dual spaces have their direction reversed, such that their arrow-heads now point downwards. This makes it easy to see when a morphism acts in the dual space and will gain greater significance later on.

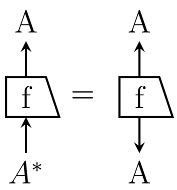


Figure 3.17: *Equivalent depictions of* $f : \mathsf{A}^* \to \mathsf{A}$

We can now define the transposition functor:

Definition 19. The *transpose* functor $(-)^*$ is a contravariant, anti-homomorphic involutive endofunctor with the following properties:

- Objects A are mapped to their duals A^*.
- Arrows $f : \mathsf{A} \to \mathsf{B}$ map to their duals, $f^* : \mathsf{B}^* \to \mathsf{A}^*$.
- Composition is reversed, $(f \circ g)^* = g^* \circ f^*$.
- The functor is involutive, a bijective mapping between hom-sets and fully faithful.

Definition 20. A functor $F(-)$ is *strictly monoidal* if it satisfies the equations

1. $F(\mathsf{A} \otimes \mathsf{B}) = F(\mathsf{A}) \otimes F(\mathsf{B})$
2. $F(\mathsf{I}) = \mathsf{I}$

The matrix transpose operator provides a strictly monoidal transpose functor for **FdHilb**. As the functor is involutive, a dual's dual is the original object i.e. $\mathsf{A}^{**} = \mathsf{A}$.

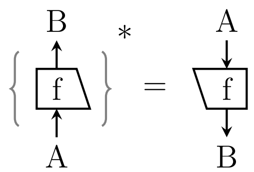


Figure 3.18: *Transposed arrows are graphically flipped on both axis*

3.2.5 Conjugation

The final basic matrix operation to be considered is complex conjugation $(-)_*$. Its operation is equal to the composition of transposition and adjunction

$$(-)_* = (-)^{*\dagger}$$

The effects of transposition and adjunction (see table 3.2.5) commute, therefore $(-)_* = (-)^{\dagger *}$.

Similar to before,

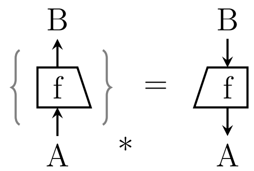
	Adjunction	**Transposition**	**Conjugation**
Object mapping	identity	dual	dual
Arrow mapping	anti-homomorphic	anti-homomorphic	homomorphic
Involutive?	Yes	Yes	Yes

Table 3.1: *Properties of the basic* **FdHilb** *functors*

Definition 21. The *conjugate* functor $(-)_*$ is a covariant, homomorphic involutive endofunctor with the following properties:

- Objects A are mapped to their duals A^*.
- Arrows $f : \mathsf{A} \to \mathsf{B}$ do not reverse domain and co-domain, but do now map to their domains' duals, $f_* : \mathsf{A}^* \to \mathsf{B}^*$
- It distributes over composition, $(f \circ g)_* = f_* \circ g_*$
- It is involutive, a bijective mapping between hom-sets and fully faithful.
- Its action is equal to the successive application of transposition then adjunction.

Graphically, conjugated arrows are horizontally reflected:



3.2.6 The interrelation between Transposition, Adjunction and Conjugation

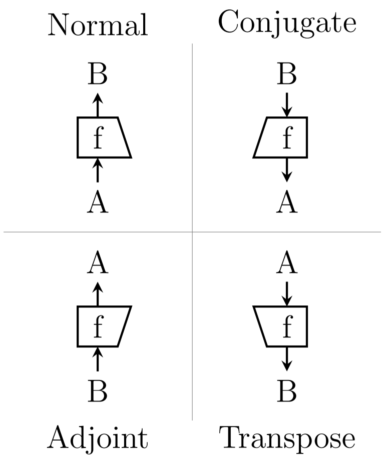
In the previous section it was shown how conjugation could be built from the other two functors. The functors display a rich compositional structure, forming a group:

Considered as a multiplicative group, every element is self-inverse and there exists an identity element[2]. Luckily for use as a graphical calculus, the group is also a symmetry group. Considering adjunction as vertical reflection and conjugation as horizontal, arrows admit an intuitive visual depiction of which functors they have experienced:

[2]Indeed, the group is isomorphic to the modulus-multiplicative group $\{1, 3, 5, 7\} \times \mod 8$

$\circ$	I	$\dagger$	T	C
I	I	$\dagger$	T	C
$\dagger$	$\dagger$	I	C	T
T	T	C	I	$\dagger$
C	C	T	$\dagger$	I

Key: I is the Identity functor, $\dagger$ the adjoint,
T the transpose and C the conjugate.



Notice how the morphism's box is reflected, but the direction of the arrowheads on the attached wires are not reflected: their direction depends only on whether they denote a dual space.

Also, the transpose is a 180° rotation as well as a reflection on both axis.

3.3 Entanglement

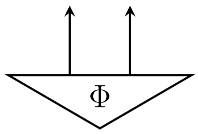
Entanglement is the major resource in quantum computation, it makes possible teleportation, superdense coding and quantum cryptography. Having caused controversy in the early 20^{th} century, Einstein famously derided it as 'spooky action at a distance'. Yet it is the non-local correlations provided by entanglement that truly distinguish Quantum from Classical systems and fuel the current interest in quantum computing.

Whereas in a classical system every bit can be manipulated independently from one another, in a quantum system modifying one qubit could have an effect on any other. This is expressed in the formalism as a system $\mathbf{S}_{AB}$ that cannot be split into two separate tensored parts, $\mathbf{S}_{AB} \neq \mathbf{S}_A \otimes \mathbf{S}_B$.

The most famous entangled quantum system is the *Bell state* Φ^+, an entanglement of two qubits such that they have identical values

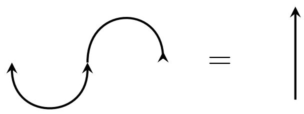
$$\Phi^+ = |00\rangle + |11\rangle$$

This can be graphically depicted as a point



However this hides the rich structure the entanglement possesses. For instance, since the state measured on the first qubit will be produced by the second qubit of the pair, the entangled pair act as an identity function. Therefore the Bell state could be represented as a cup:

Extending the representation to measurements in the Bell basis, quantum teleportation can then be loosely sketched as the equality:



This will be formalised in the next section.

3.3.1 Cups and Caps

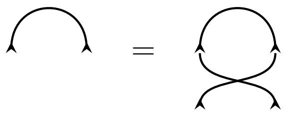
The 'yanking the wire' shown above, where a cup and cap became an identity arrow, is the essential property of the structure we now introduce.

Definition 22. Given an orthonormal basis[3] Θ for space A, a cap in **FdHilb** is an arrow $\kappa_\Theta : \mathsf{A} \otimes \mathsf{A} \to \mathsf{I}$ such that

$$\forall v_i \in \Theta \ . \ \kappa_\Theta \circ (v_i \otimes v_i) = \left(\frac{1}{|\Theta|}\right)_{\mathsf{I}} \qquad \text{or equivalently} \qquad \kappa_\Theta^\dagger = \sum_{v_i \in \Theta} |v_i\rangle \otimes |v_i\rangle$$

The cap is depicted as a u-turned wire and is invariant when its inputs are swapped i.e. $\kappa_\Theta = \kappa_\Theta \circ \sigma_{\mathsf{A},\mathsf{A}}$. Graphically:

[3] i.e. a set of points that obey the usual conditions of being orthogonal, normalised and spanning



The adjoint to a cap is a cup, and the defining condition for caps and cups (known as 'compactness'[4]) is

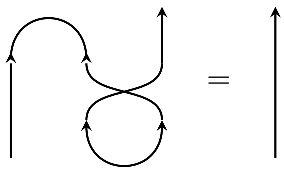


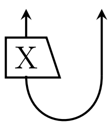
Figure 3.19: *The compactness property,* $(\kappa_{\Theta} \otimes 1_{\mathsf{A}}) \circ (1_{\mathsf{A}} \otimes \sigma_{\mathsf{A},\mathsf{A}}) \circ (1_{\mathsf{A}} \otimes \kappa_{\Theta}^{\dagger}) = 1_{\mathsf{A}}$

Now the Bell state Φ^+ can be understood as $\kappa_{\mathcal{C}}^{\dagger}$, a cup over the computational basis.

3.3.2 Other Bell Basis

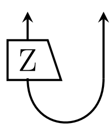
This understanding of the general Bell state can be extended to rest of the Bell basis. The basis can be thought of as functions between their two qubits, such that applying said function to the measured right qubit gives the state of the left qubit. From this perspective Φ^+ is the identity function.

- $\Psi^+ = |01\rangle + |10\rangle$ Considered as a function, Ψ^+ inverts the input qubit. Therefore appending a Pauli-X gate to Ψ^+ gives the desired result,



$$\Psi^+ = (X \otimes 1_{\mathcal{Q}}) \circ \kappa_{\mathcal{C}}^{\dagger}$$

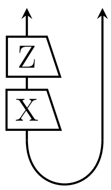
- $\Phi^- = |00\rangle - |11\rangle$ Similarly requires a Pauli-Z gate:



$$\Phi^- = (Z \otimes 1_{\mathcal{Q}}) \circ \kappa_{\mathcal{C}}^{\dagger}$$

[4] Eager readers will notice that this is not the normal condition for compactness– a proper compact closed category has a morphism $\eta_{\mathsf{A}} : \mathsf{A} \otimes \mathsf{A}^* \to \mathsf{I}$ and the definition of compactness necessarily involves the dual space (see [KL80]). True compactness is covered later in this document.

- $\Psi^- = |01\rangle - |10\rangle$ Requires both an X and Z gate:



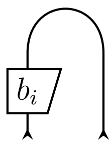
$$\Psi^- = ((Z \circ X) \otimes 1_{\mathcal{Q}}) \circ \kappa_{\mathcal{C}}^\dagger$$

3.3.3 A first attempt at full Teleportation

Now that the Bell basis has been incorporated into the calculus, the teleportation protocol can be graphically expressed.

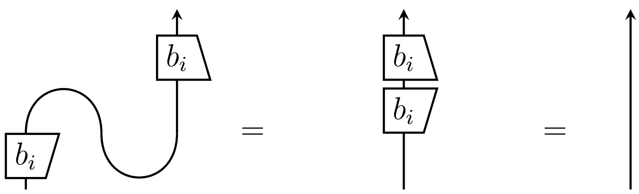
In the teleportation protocol a measurement is made in the Bell basis– its outcome could be any of $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\} = \mathcal{B}$. As in previous measurements we will use the post-selection indexing method of accounting for measurement results.

Every element of $\mathcal{B}$ can be factorised into Φ^+ with a different unitary on the left qubit, these are $\{I, Z, X, Z \circ X\} = \bar{\mathcal{B}}$ respective to $\mathcal{B}$. Therefore measurement can be seen as selecting an (adjointed) index of $\bar{\mathcal{B}}$ e.g.



The teleportation protocol requires a unitary correction after the aforementioned measurement. This is to remove the affect of the element $(b_i \in \bar{\mathcal{B}})^\dagger$ that was measured. Therefore the correcting unitary is simply b_i.

Putting this all together the teleportation protocol becomes:



This depiction of teleportation is much more intuitive, however it still suffers from a reliance on meta-level indices. The following Chapter exposes further structures within **FdHilb**. These structures will provide the machinery required to successfully express measurement.

Chapter 4

Delving Deeper

In the previous chapter the basic aspects of the Quantum formalism were translated into the category **FdHilb**. Although only simple structures were imported into **FdHilb**, it still exhibited rich algebraic structure – e.g. compactness, the interaction of scalars and tensors.

This chapter explores **FdHilb** further, adding new tools that will later help to dissect multi-partite entanglement.

4.1 Quantum Information

It is an apt time to explore the properties of Quantum information– the aspects that differentiate Quantum information from Classical information are fundamental to the structure of **FdHilb**.

4.1.1 Quantum Copying

Classical information can be infinitely copied, this property has led to computers' global ubiquity. In contrast to the Classical world, Quantum information cannot be copied. This has been famously termed the 'No-Cloning Theorem':

Theorem 1. *There exists no unitary* $\delta_{\mathsf{A}} : \mathsf{A} \to \mathsf{A} \otimes \mathsf{A}$ *such that for all points* $f : \mathsf{I} \to \mathsf{A}$

$$\delta_{\mathsf{A}}(f) = f \otimes f$$

This presents difficulties for standard classical practices such as Error Correction (which creates redundant copies) and multicasting. However this extreme restriction has resulted in protocols unique to the Quantum realm; one well known example is that of communication channels that are impossible to eavesdrop.

Unsurprisingly this property permeates the Quantum formalism. The tensor structure employed by †-SMCs is resource preserving[1], it stringently accounts for each qubit; all natural isomorphisms have been chosen to avoid information cloning. This explains some of the motivation for the I space of scalars– they provide a flexible substance from which qubits can be formed then later returned to. Scalars can be freely created $\lambda_{\mathsf{A}} : \mathsf{A} \cong \mathsf{I} \otimes \mathsf{A}$, later prepared into qubits by points $f : \mathsf{I} \to A$, then through the device of measurement $g : \mathsf{A} \to \mathsf{I}$ qubits return to scalar form to be $\lambda^{-1} : \mathsf{I} \otimes \mathsf{A} \to \mathsf{A}$ disposed of. These restrictions perfectly reflect the physical reality of quantum information.

Despite the No-Cloning theorem a limited form of copying is possible– orthonormal basis can be copied. The following simple matrix provides an example:

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

This reliably copies the computational basis $\{|0\rangle \mapsto |00\rangle, |1\rangle \mapsto |11\rangle\}$.

Lemma 2. *A system can be perfectly copied if its only states are those of an orthogonal basis (and not any superposition).*

Proof. Trivial. The system can therefore be measured with complete accuracy and replicated infinitely □

This produces a simple categorical definition of orthonormal basis:

Definition 23. A duplicator $\delta_\Phi : \mathsf{A} \to \mathsf{A} \otimes \mathsf{A}$ for space A is an arrow such that for every $(v_i : \mathsf{I} \to \mathsf{A}) \in \Phi$

$$\delta_\Phi(v_i) = v_i \otimes v_i$$

Theorem 2. *[CD09] A duplicator δ_Φ exists in* **FdHilb** *if and only if Φ is an orthonormal basis. That is, duplicators bijectively map to orthonormal basis.*

This definition does not rely upon the additive properties of vectors or definitions of vector-spanning, making it extremely convenient and efficient. The basis points a duplicator copies are known as its 'classical points' since they can be copied akin to classical information.

As will shortly be made apparent, duplicators provide an elegant and ubiquitous calculus for many of the quantum systems we wish to express. They are therefore depicted as simple dots, the colour of which specifies which basis is in use:

[1]This interpretation is very similar to Lafont's interpretation of linear logic. Indeed, linear logic has been incorporated into studies of Quantum physics and used as the basis of Quantum Type Systems.

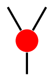


Figure 4.1: *The duplicator* $\delta : \mathsf{A} \to \mathsf{A} \otimes \mathsf{A}$ *. For clarity arrows and basis have been dropped in this section when there is no ambiguity*

When horizontally reflected the node remains visually unchanged, this reflects the symmetry

$$\delta = \sigma \circ \delta$$

Furthermore the node has the same appearance when rotated by 180° as when vertically reflected– this is because the duplicator's adjoint and transpose correspond, i.e.

$$\delta^\dagger = \delta^*$$

One final property of duplicators relates to their composition and will prove to be very useful later:

Theorem 3. *[CD09] Duplicators in* **FdHilb** *are* special *and obey the* Frobenius law*. That is,*

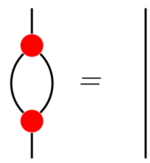


Figure 4.2: *The special property;* $\delta^\dagger \circ \delta = 1_A$

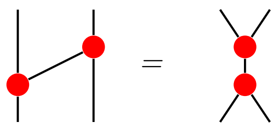
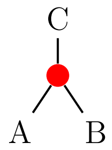


Figure 4.3: *The Frobenius law;* $(1_A \otimes \delta^\dagger) \circ (\delta \otimes 1_A) = \delta \circ \delta^\dagger$

4.1.2 δ as a monoid

An interesting structure that arises from duplicators is that of a monoid. By considering the upside-down duplicator $\delta^\dagger$ as a binary multiplier, the dot of the graphical depiction becomes the operator $A \cdot B = C$



This multiplication is associative. i.e.

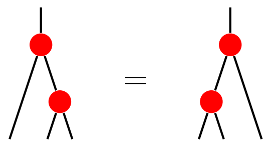


Figure 4.4: $\delta^\dagger \circ (1 \otimes \delta^\dagger) = \delta^\dagger \circ (\delta^\dagger \otimes 1)$

And also commutative

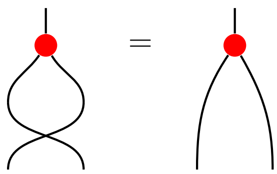


Figure 4.5: $\delta^\dagger \circ \sigma_{A,A} = \delta^\dagger$

And therefore forms a commutative monoid. The structure can be further embellished:

Definition 24. A *unit* $\epsilon_\Phi : \mathsf{A} \to \mathsf{I}$ for duplicator δ_Φ is an arrow such that

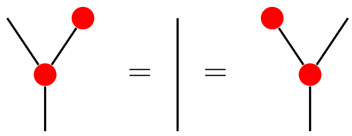


Figure 4.6: $(1_\mathsf{A} \otimes \epsilon_\Phi) \circ \delta_\Phi = 1_\mathsf{A} = (\epsilon_\Phi \otimes 1_\mathsf{A}) \circ \delta_\Phi$

With the addition of the unit $(\delta_\Phi^\dagger, \epsilon_\Phi^\dagger)$ now forms a multiplicative group.

Theorem 4. *[CD09] Units in* **FdHilb** *have the form*

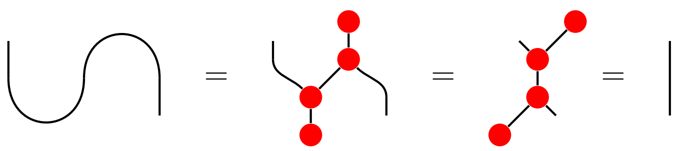
$$\forall v_i \in \Phi \;\; . \;\; \epsilon_\Phi(v_i) = 1_\mathsf{I}$$

Units are known as 'deleting points' because they uniformly map[2] their associated basis to *1*. Furthermore measuring the point $\epsilon_\Phi^\dagger$ in basis Φ is equally likely to return any $v_i \in \Phi$. In this sense units are 'unbiased' and contain no information.

The combination of duplicator and unit,

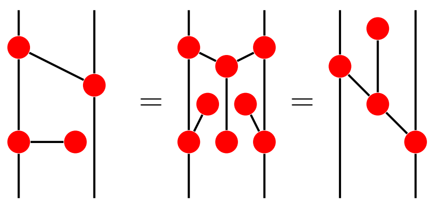
$$\delta_\Phi \circ \epsilon_\Phi : \mathsf{I} \to \mathsf{A} \otimes \mathsf{A} = \sum_{v_i \in \Phi} |v_i\rangle \otimes |v_i\rangle$$

forms a cup as defined earlier. Its adjoint is a cap. By the Frobenius Law and the definition of the unit, it experiences compactness as expected:



Definition 25. The triple $(\mathsf{A}, \delta_\Phi, \epsilon_\Phi)$, where A is the space inhabited by base Φ, is known as an *Observable structure*. Specifically, an observable structure is an internal special Frobenius cocommutative comonoid[3], also known as a †-Frobenius structure.

Observable structures have the surprising property that every diagram of duplicators and units is equal to every other with the same number of incoming and outgoing legs. For example,



This is known as the *Spider Theorem*,

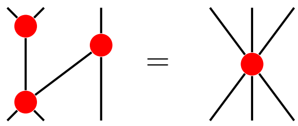
Theorem 5 (Spider Theorem)**.** *[Lac04] For any observable structure* $(\mathsf{A}, \delta, \epsilon)$ *in a strict †-SMC, every combination of duplicators and units* $f : \mathsf{A}^{\otimes n} \to \mathsf{A}^{\otimes m}$ *is equal to* $\delta_m \circ \delta_n^\dagger$ *where* δ_n *is recursively defined*

$$\delta_0 = \epsilon\ , \qquad \delta_n = \delta \circ (1_\mathsf{A} \otimes \delta_{n-1})$$

[2]Waiving the normalising factor

[3] A quick glossary: Internal refers to the fact it is relative to a particular object, cocommutative as it is commutative ('co' refers to it being the dual of the normal understanding of commutative) and comonoid as the arrows form a (dual) monoid structure, as described earlier.

Thanks to the spider theorem all dots can be fused together:



This is yet another instance of the graphical calculus's strength: these systems are non-trivially equal, yet their graphical depictions are intuitively the same.

4.2 True Compactness

In the earlier treatment of Entanglement cups and caps were presented, which when combined 'compacted' into an identity arrow. These were simplifications of the †-compact structure presented in this section– caps $\kappa : \mathsf{A} \otimes \mathsf{A} \to \mathsf{I}$ are refined to become u-turn arrows $\eta : \mathsf{A} \otimes \mathsf{A}^* \to \mathsf{I}$, depicted

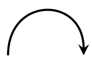


Figure 4.7: $\eta \circ (|v_i\rangle \otimes |\bar{v_j}\rangle) = \langle v_i|v_j\rangle$

η arrows bridge between objects A and their duals A^* and highlight another area of structure latent in **FdHilb**.

Definition 26. A †-*compact category* is a †-SMC where every object A comes with a †-*compact structure*. A †-compact structure is a pair $(\mathsf{A}, \eta_\mathsf{A} : \mathsf{A} \otimes \mathsf{A}^* \to \mathsf{I})$ where η has the compact property:

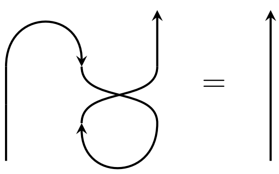


Figure 4.8: *The compactness property* $(\eta_\mathsf{A} \otimes 1_\mathsf{A}) \circ (1_\mathsf{A} \otimes \sigma_{\mathsf{A},\mathsf{A}^*}) \circ (1_\mathsf{A} \otimes \eta_\mathsf{A}^\dagger) = 1_\mathsf{A}$

Furthermore the η arrows of an object and its dual must be connected by

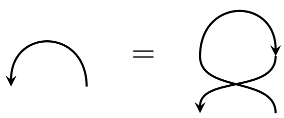


Figure 4.9: $\eta_{\mathsf{A}^*} = \eta_\mathsf{A} \circ \sigma_{\mathsf{A}^*,\mathsf{A}}$

Definition 27. A †-compact category is *strict* if $(\mathsf{A} \otimes \mathsf{B})^* = \mathsf{B}^* \otimes \mathsf{A}^*$ and

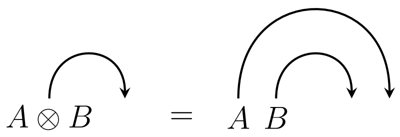


Figure 4.10: $\eta_{\mathsf{A}\otimes\mathsf{B}} = \eta_{\mathsf{A}} \circ (1_{\mathsf{A}} \otimes \eta_{\mathsf{B}} \otimes 1_{\mathsf{A}^*})$

Compact structures are deeply integrated into the category we have already built. The transposition functor can now have its action on arrows equivalently redefined:

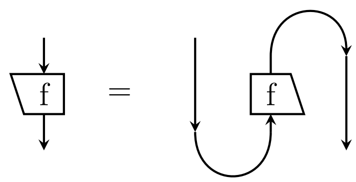
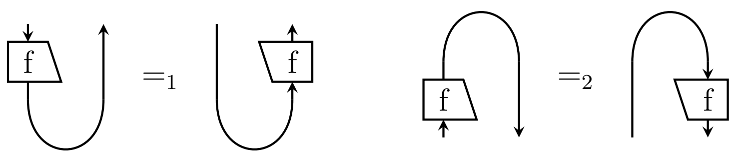


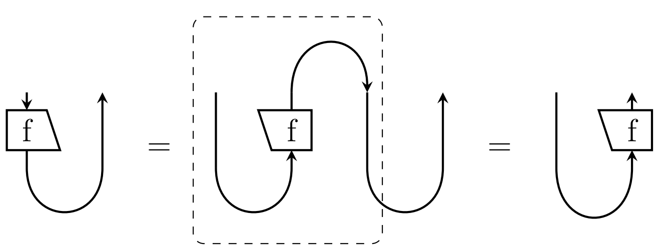
Figure 4.11: $(f : \mathsf{A} \to \mathsf{B})^* = (1_{\mathsf{A}^*} \otimes \eta_{\mathsf{B}}) \circ (1_{\mathsf{A}^*} \otimes f \otimes 1_{\mathsf{B}^*}) \circ (\eta_{\mathsf{A}}^\dagger \otimes 1_{\mathsf{B}^*})$

This accounts for why an arrow's transpose is rotated by 180° degrees, it is simply 'pulling the wire taut' in the above diagram.

Similar to the sliding axioms introduced earlier, we now introduce sliding axioms for cups and caps. With these in place morphism boxes can freely slide along all wires– until blocked by another box.



The proof of (1) is as follows:



using the above defn. of f_*

The proof of (2) is similar.

4.3 Compact Cups

We have now introduced two very similar devices- caps κ and compact structures η. This prompts the question of whether they are interrelated. Furthermore, since κ can be built from the duplicators δ and units ϵ of observable structures, a link between κ and η would interrelate compactness and Spider theorem – providing an extremely versatile calculus.

4.3.1 Self-duality

One approach to this problem is to simply require that every †-compact structure's object A equals its dual. As a result wires no longer have arrowheads and $\kappa = \eta$ as required. This is a quick solution and has proven successful ([CD09]).

However, this poses significant problems. As discussed in the Strictness definition for †-SMC, it is vital that $\sigma_{\mathsf{A},\mathsf{B}} : \mathsf{A} \otimes \mathsf{B} \cong \mathsf{B} \otimes \mathsf{A}$ does not become an equality as otherwise arrows' domain restrictions fail. However, if objects are made self dual then

$$\mathsf{A} \otimes \mathsf{B} = (\mathsf{A} \otimes \mathsf{B})^*$$

and by the strictness property for †-compactness

$$(\mathsf{A} \otimes \mathsf{B})^* = \mathsf{B}^* \otimes \mathsf{A}^*$$

and therefore

$$\mathsf{A} \otimes \mathsf{B} = \mathsf{B} \otimes \mathsf{A}$$

the very situation we took pains to avoid in the earlier definition of σ's strictness! If we desire **FdHilb** to be strict and have a meaningful set of objects, self-duality is unfeasible.

4.3.2 Explicit duality

As originally described in [CPP08], a much neater solution exists – one which breaks η down into its fundamental parts. For this we introduce a new morphism:

Definition 28. A *dualiser* is a unitary arrow $d_{\mathsf{A}} : \mathsf{A} \to \mathsf{A}^*$. Many possible dualisers exist for each object. The dualiser is depicted as

Now the the definitions of η, δ and ϵ can be interwoven:

Definition 29. A †-*dual Frobenius structure* in a †-SMC is the tuple

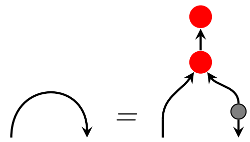
$$(\mathsf{A}, \delta_\Phi : \mathsf{A} \to \mathsf{A} \otimes \mathsf{A}, \epsilon_\Phi : \mathsf{A} \to \mathsf{I}, d_\mathsf{A} : \mathsf{A} \to \mathsf{A}^*)$$

where $(\mathsf{A}, \delta_\Phi, \epsilon_\Phi)$ is a †-Frobenius structure.

Theorem 6. *[CPP08] A †-compact structure arises from every †-dual Frobenius structure*

$$\eta_\mathsf{A} = \epsilon_\Phi \circ \delta_\Phi^\dagger \circ (1_\mathsf{A} \otimes d_\mathsf{A}^\dagger)$$

Graphically,



Since $\kappa_\Phi = \epsilon_\Phi \circ \delta_\Phi^\dagger$ all five operators can all be drawn together. A dualiser factorises η in the following way:

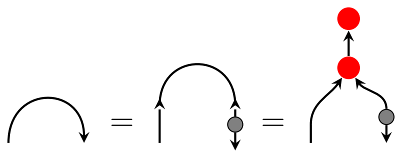


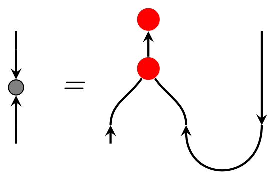
Figure 4.12: $\eta_\mathsf{A} = \kappa_\Phi \circ (1_\mathsf{A} \otimes d_\mathsf{A}^\dagger) = \epsilon_\Phi \circ \delta_\Phi^\dagger \circ (1_\mathsf{A} \otimes d_\mathsf{A}^\dagger)$

One may have noticed that δ and ϵ are specified relative to bases, but the dualiser d and compact structure η are specified relative to objects. This is because η's definition is base agnostic; η can be factorised by any observable structure– the dualiser acts as a 'correcting unitary' (this property of bipartite entanglement will be formally established later). In this fashion the dualiser can be defined in terms of the Frobenius and Compact structures you wish it to factorise:

Theorem 7. *[CPP08] A dualiser can be defined by combining a †-compact structure with an observable structure;*

$$d_\mathsf{A} = (\epsilon_\Phi^\dagger \otimes 1_{\mathsf{A}^*}) \circ (\delta_\mathsf{A}^\dagger \otimes 1_{\mathsf{A}^*}) \circ (1_\mathsf{A} \otimes \epsilon_\mathsf{A}^\dagger)$$

which is



Definition 30. A †-*compact category with bases* is a †-SMC where every object A comes with a †-dual Frobenius structure and the dualiser d_A has the following properties:

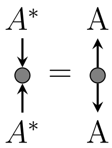


Figure 4.13: $d_{A^*} = d_A^\dagger$

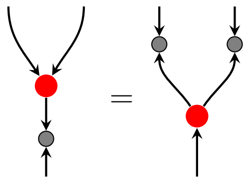


Figure 4.14: $\delta_{A^*} \circ d_A = (d_A \otimes d_A) \circ \delta_A$

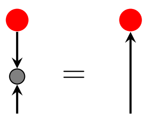


Figure 4.15: $\epsilon_{A^*} \circ d_{A^*} = \epsilon_A$

Definition 31 (Strictness)**.** A †-compact category with basis is *strict* when the following equalities hold:

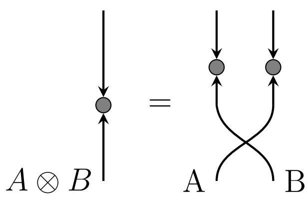


Figure 4.16: $d_{A\otimes B} = (d_B \otimes d_A) \circ \sigma_{A,B}$

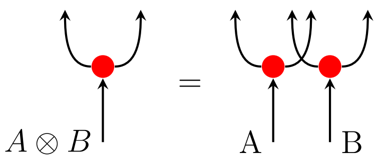


Figure 4.17: $\delta_{A\otimes B} = (1_A \otimes \sigma_{A,B} \otimes 1_B) \circ (\delta_A \otimes \delta_B)$

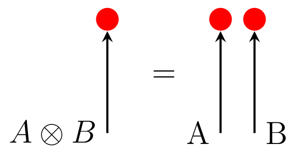
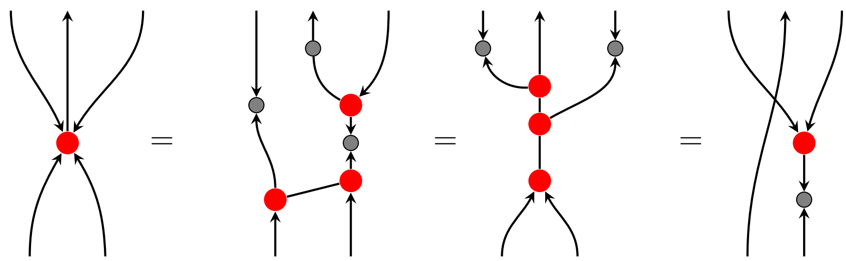


Figure 4.18: $\epsilon_{\mathsf{A}\otimes\mathsf{B}} = \epsilon_{\mathsf{A}} \otimes \epsilon_{\mathsf{B}}$

Now it is possible to re-introduce the spider theorem, completing what we set out to achieve:

Theorem 8 (Orientated Spider). *[CPP08] In a †-compact category with bases, any connected diagram composed entirely of elements from a single †-dual Frobenius structure can be simplified down to a spider as long as the number of incoming and outgoing legs and their directions are preserved.*

Example 2. The following are equal:



Thanks to this result a †-compact category with bases $(\mathsf{A}, \delta_\Phi : \mathsf{A} \to \mathsf{A}\otimes\mathsf{A}, \epsilon_\Phi : \mathsf{A} \to \mathsf{I}, d_{\mathsf{A}} : \mathsf{A} \to \mathsf{A}^*)$ has a simpler depiction: dualisers, duplicators and units can all be drawn as the same familiar coloured nodes. Additionally, these nodes can have any number of legs, in any direction.

4.4 Interactions between different obervables

In the previous section †-dual Frobenius structures were introduced, bringing the concepts from many earlier sections together into a single flexible calculus. The orientated spider theorem allows for quick intuitive manipulation of these structures, regardless of their complexity.

However when multiple Frobenius structures occur in the same diagram the preceding theory provides no answer as to how they interact.

In this section that question is explored.

4.4.1 X and Z observables

We will focus on two observable structures in particular, those of the X and Z Pauli matrices. These provide a rich calculus that can encode real-world protocols– some of which will be featured in later examples.

One can construct Frobenius structures from these Pauli matrices by taking their eigenvectors ('classical points') and using them as the bases for duplicators. The two Frobenius structures are described in the following table:

	Matrix	**Classical Points**	**Unbiased points**	**Frobenius structure**
Pauli-X 	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\|+\rangle, \|-\rangle$	$\|0\rangle, \|1\rangle$, $\|\alpha_X\rangle = \cos(\frac{\alpha}{2})\|0\rangle + \sin(\frac{\alpha}{2})\|1\rangle$	$\delta_X : \begin{Bmatrix} \|+\rangle \mapsto \|++\rangle \\ \|-\rangle \mapsto \|--\rangle \end{Bmatrix}$ $\epsilon_X : \|0\rangle \mapsto 1$
Pauli-Z 	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\|0\rangle, \|1\rangle$	$\|+\rangle, \|-\rangle$, $\|\alpha_Z\rangle = \|0\rangle + e^{i\alpha}\|1\rangle$	$\delta_Z : \begin{Bmatrix} \|0\rangle \mapsto \|00\rangle \\ \|1\rangle \mapsto \|11\rangle \end{Bmatrix}$ $\epsilon_Z : \|+\rangle \mapsto 1$

To differentiate the two observable structures their dots will be drawn in different colours; The Pauli-X structure in red and the Pauli-Z in green.

Definition 32. *Complementary* observables are a pair of observable structures with the property that each structure's classical points are unbiased for the other.

The X and Z matrices were chosen because they are complementary and their compact structures coincide:

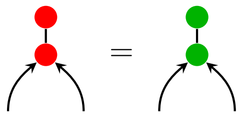


Figure 4.19: $\epsilon_X \circ \delta_X^\dagger = \epsilon_Z \circ \delta_Z^\dagger$

Another consequence of their compact structures coinciding is that they share the same dualiser d_A to form η_A:

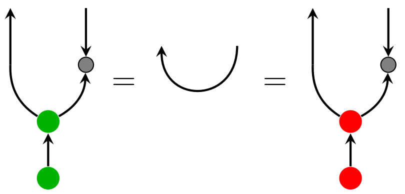
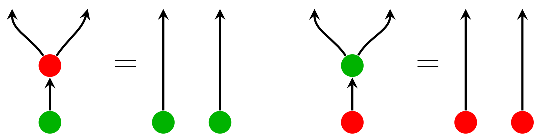


Figure 4.20: $(1_\mathsf{A} \otimes d_\mathsf{A}) \circ \delta_Z \circ \epsilon_Z^\dagger = \eta_A^\dagger = (1_\mathsf{A} \otimes d_\mathsf{A}) \circ \delta_X \circ \epsilon_X^\dagger$

The first consequence of being complementary is that each structure can copy the others unit:



Furthermore, as each's classical points are unbiased for the other structure, connecting a red duplicator to a green duplicator results in no information being transmitted i.e. a disconnected graph:

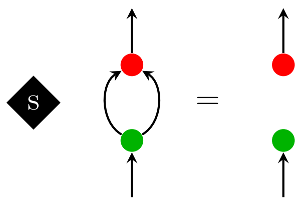


Figure 4.21: *The* scaled Hopf law with trivial antipode

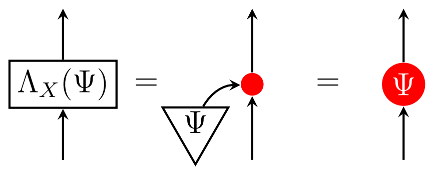
This result holds for complementary observable structures whose compact structures coincide and at least one of which was formed from a vector basis.

4.4.2 Point Multiplication

For the calculus of complementary structures to be of practical use it needs to include arbitrary rotation gates. This section demonstrates how points can be used to create these rotations and afterwards presents some applications.

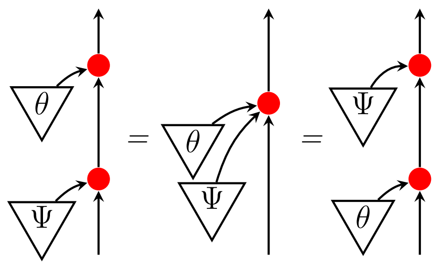
The first new tool is an functor mapping points $f : \mathsf{I} \to \mathsf{A}$ to endomorphisms of A:

Definition 33. For an observable structure $(\mathsf{A}, \delta_X, \epsilon_X)$ let $\Lambda_X(\Psi) = \delta_X^\dagger \circ (\Psi \otimes 1_\mathsf{A})$



Proposition 1. *Arrows* $\Lambda_X(\alpha) : \mathsf{A} \to \mathsf{A}$ *are*

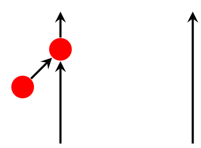
1. *Commutative*



2. *Associative*

   Proof. This follows naturally from morphism composition. □

3. *The identity when* $\alpha = \epsilon^\dagger$

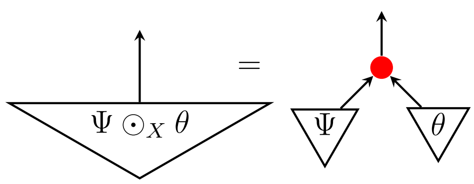


Next we define point multiplication:

Definition 34. For an observable structure $(\mathsf{A}, \delta_X, \epsilon_X)$ and points $\mathit{\Psi} : \mathsf{I} \to \mathsf{A}$ and $\theta : \mathsf{I} \to \mathsf{A}$, their *multiplication* is

$$\Psi \odot_X \theta = \delta_X^\dagger \circ (\Psi \otimes \theta)$$

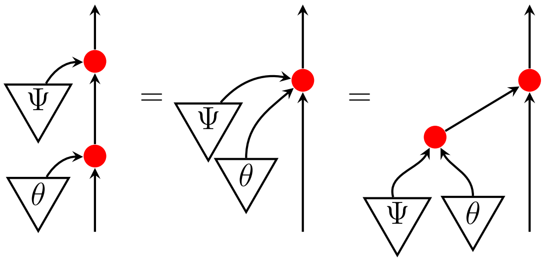
Graphically,



Proposition 2. *Composition of $\Lambda_X(-)$ terms is equivalent to point multiplication i.e.*

$$\Lambda_X(\Psi) \circ \Lambda_X(\theta) = \Lambda_X(\Psi \odot_X \theta)$$

Proof. Graphical.



□

Therefore point multiplication is commutative, associative and has a unit– it is forms the commutative monoid. $(\mathbf{C}(\mathsf{I}, \mathsf{A}), \odot, \epsilon^\dagger)$

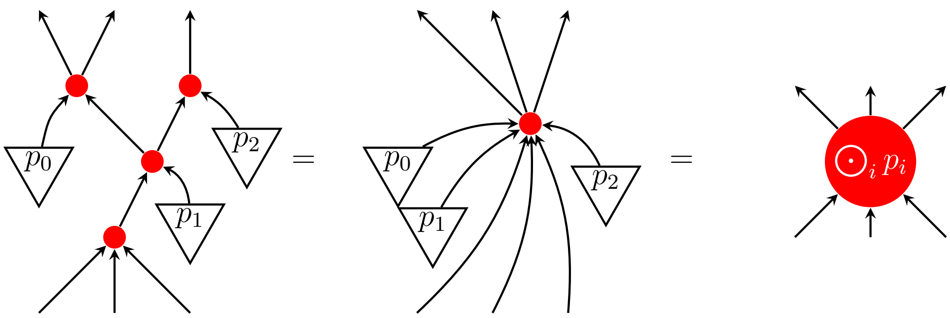
This supports a natural extension of the previous spider theorem:

Theorem 9 (Decorated spider)**.** *Any connected graph entirely composed of elements from a †-dual Frobenius structure $(\mathsf{A}, \delta_X, \epsilon_X, d_\mathsf{A})$ and points $\{p_i\}$ admits a spider normal form,*

$$\left(\bigotimes_m d_\mathsf{A} \;\; or \;\; 1_\mathsf{A}\right) \circ \delta_m \circ \Lambda_X \left(\bigodot_i p_i\right) \circ \delta_n^\dagger \circ \left(\bigotimes_n d_\mathsf{A} \;\; or \;\; 1_\mathsf{A}\right)$$

purely dependant on the number n of incoming and number m of outgoing legs, their direction and the points present. All points are multiplied together.

Proof. Using the orientated spider theorem points can be moved into the multiplying arrangement, forming an orientated spider with an $\Lambda_X(-)$ arrow in the centre. Graphically:



□

4.4.3 Phase Shifts

Now a reflection operator can be defined:

Definition 35. For any point $f : \mathsf{I} \to \mathsf{A}$ in a †-dual Frobenius structure $(\mathsf{A}, \delta_X, \epsilon_X, d_A)$ its reflection f_{R_X} is defined

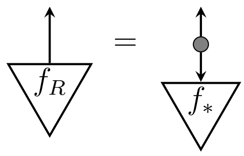


Figure 4.22: $f_{R_X} = d_A \circ f_*$

This operator is such that

$$\Lambda(-\alpha) \circ \epsilon^\dagger = (\Lambda(\alpha) \circ \epsilon^\dagger)_{R_X}$$

and

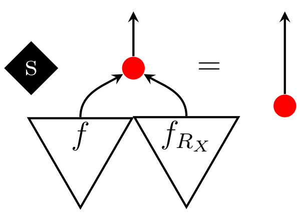
$$(\epsilon_Z^\dagger)_{R_X} = \epsilon_Z^\dagger$$

Now the multiplication operator provides an elegant definition for unbiased points:

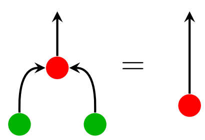
Definition 36. *Unbiased points* $f : \mathsf{I} \to \mathsf{A}$ in a †-dual Frobenius structure $(\mathsf{A}, \delta_X, \epsilon_X, d_A)$ are such that for some scalar $s : \mathsf{I} \to \mathsf{I}$

$$s \bullet (f \odot f_{R_X}) = \epsilon_X^\dagger$$

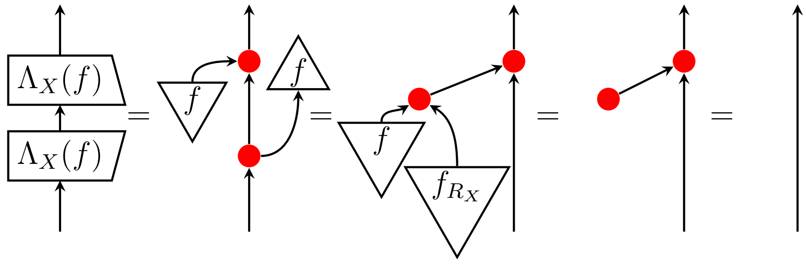
i.e.



Since we are dealing with complementary observables, taking one structure's classical points and passing them into the other's duplicator forms a unit. By the above definition these are classed as unbiased points:



Consider the points $f : \mathsf{I} \to \mathsf{A}$ for which $\Lambda_X(f)$ is unitary: These points are necessarily unbiased and normalised,

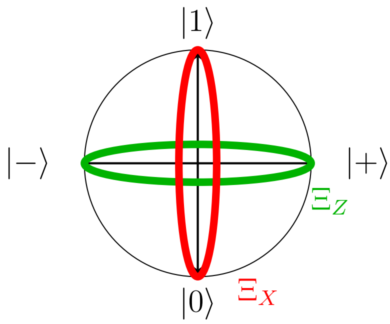


Let those unbiased normalised points be the set Ξ_X. If we restrict the point multiplication monoid to only act on these points then the reflection operator performs an inversion operation and we have formed the abelian group

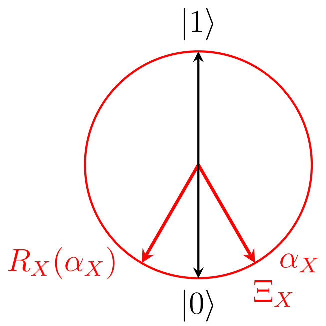
$$(\Xi_X, \odot, \epsilon^\dagger, (-)_{R_X})$$

This is known as the *Phase group* for the †-dual Frobenius structure $(\mathsf{A}, \delta_X, \epsilon_X, d_X)$. The following example makes the term's origin clear:

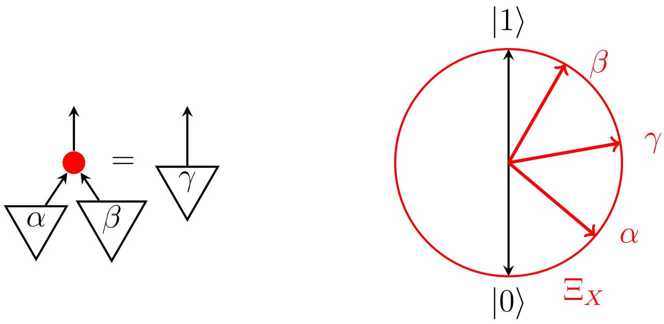
Example 3 (Z and X phase shifts)**.** The *Bloch Sphere* is a visualisation of the Qubit such that every unique pure state (i.e. a state that is not a super-position) of magnitude 1 maps to a point on the sphere. Some reference points are drawn on the sphere for orientation. The sets Ξ_X and Ξ_Z are both great circles of the Bloch sphere:



Therefore the sets also form additive rotational (modulo 2π) groups with $\epsilon_X^\dagger$ and $\epsilon_Z^\dagger$ as their respective zero points. For this reason the points $x \in \Xi_X$ (Ξ_Z) are respectively referred to as θ_X (θ_Z) for $\theta \in [0 \dots 2\pi]$. The reflection operator reflects across the line of $0°$ and therefore negates angles (where $0°_X = \epsilon_X^\dagger = |0\rangle$), e.g.



Finally, δ acts as an averaging function of the two angles given to it, returning $0°$ ($\epsilon_X^\dagger$) for reflective pairs – as per the definition of unbiased.



Using the phase groups Ξ_X and Ξ_Z general rotations can be constructed:

Example 4. Any 1 bit unitary can be formed via

$$\Lambda(\psi, \phi, \varphi) = \Lambda_X(\psi) \circ \Lambda_Z(\phi) \circ \Lambda_X(\varphi)$$

since a unitary is simply a general rotation.

Proof. The above series of rotations is equivalent to a general rotation by Euler's rotation theorem: Rotating in the Ξ_X plane then the Ξ_Z plane orientates the '$|0\rangle$ pole' to an arbitrary axis. The final $\Lambda_X(\psi)$ rotation, about that axis, is therefore sufficient to define a general rotation. □

Example 5 (CNOT)**.** Within the X-Z calculus it is possible to build a CNOT gate and to demonstrate its action.

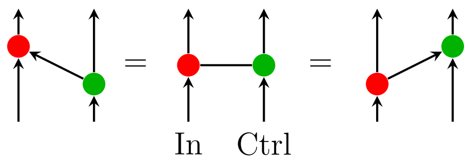


Figure 4.23: *The CNOT gate*

The gate can be tested by 'plugging'– just as a linear function can be mapped by applying it to each basis vector, a unitary graph can be understood by attaching each possible orthogonal input. First $|0\rangle = 0_X = \epsilon_X^\dagger$ is plugged into the control wire, then $|1\rangle = \pi_X$. See Figure 4.24 for an illustration of the process.

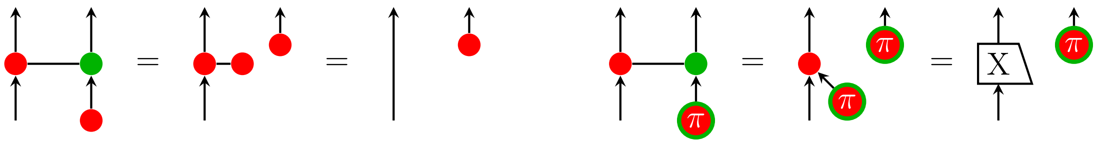
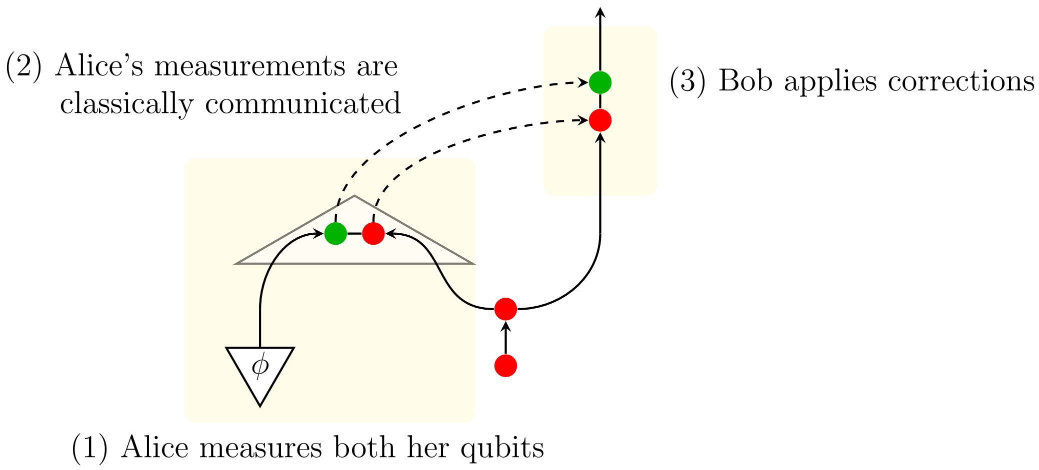


Figure 4.24: *As $|1\rangle$ is equivalent to $\epsilon_X^\dagger$ rotated by $\Lambda_X(\pi)$ it is labelled as 'π'. The red center denotes its origin as an unbiased point of δ_X and the green rim signifies that it is classical for δ_Z.*

Each case produces a rotation on the input gate, where $\Lambda_X(0)$ is the identity and $\Lambda_X(\pi) = X$, i.e. the inversion gate, as expected.

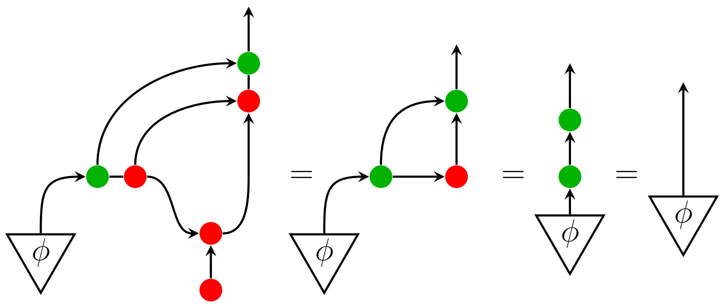
As the calculus contains one bit unitaries and CNOT gates, any possible quantum state can be built. The X/Z calculus is therefore universal, it can express every possible quantum state and unitary gate [CD09].

Example 6 (Teleportation)**.** It is now possible to depict the teleportation protocol without indexing.



Alice's measurement is equivalent to measuring each of the communication lines in the computational basis. Transferring these two (classical) bits to Bob allows him to correct his entangled qubit and retrieve ϕ. This example demonstrates how duplicator nodes successfully model classical communication, showing the versatility of the X/Z calculus.

Proof. Verification of the protocol's correctness now becomes a trivial application of the spider theorem[4].



□

This section has explored the interaction of two particular observable structures. Whilst this work can be generalised to other observables, the X/Z calculus has bore the most fruit. The tools presented here will be used again later as we analyse Entanglement in the next chapter.

[4]Recall that a red or green node with only two legs is an identity function.

Chapter 5

A tale of Entanglement

Entanglement is fundamental in distinguishing Quantum mechanics from Newtonian; The ability to instantaneously affect a particle's state regardless of distance is truly extraordinary. Furthermore, in the previous chapters' investigations of **FdHilb**'s structure, entanglement has played a central algebraic role– consider both Frobenius and Compact structures. However we have focused on one single expression of entanglement– the Bell basis. In this chapter we investigate other forms of Entanglement and look at the Multi-partite case, ultimately exploring the tripartite *GHZ/W calculus*. The calculus itself has only recently been introduced ([CK10], *Feb. 2010*) and little is currently known about it. This chapter provides new insights, rules and tools for the calculus.

5.1 Distinguishing between entanglements

The aim of this section is to form distinct classifications of Entanglement. The simplest division is the number of Qubits employed in the entangled state; so far the focus has always been on two qubit cases. However this granularity is too coarse, it doesn't unearth any deeper structure. To gain finer discrimination an equivalence relation will be employed, dividing each N-qubit case into equivalence classes.

Ideally the equivalence class will not divide the entanglements too finely, rather expose some fundamental structure. Also it should be robust to minor changes; For example, the Bell Basis are trivial to generate from Φ^+ and all operate similarly– therefore they should all be in the same class.

A first attempt at an equivalence relation is to group together quantum states that can be made equal by applying unitaries to each qubit, These local operations do not interfere with the *non-local* properties of the entanglement which we are trying to categorise. The resulting equivalence classes are known as *local operations and classical communication (LOCC)* classes.

Definition 37 (LOCC)**.** For points $f, g : \mathsf{I} \to \mathcal{Q}^{\otimes n}$ and unitaries $\{u_i : \mathcal{Q} \to \mathcal{Q}\}_0^n$, *LOCC equivalence* is

$$f \sim g \iff \left(\bigotimes_{i=0}^{n} u_i \right) \circ f = g$$

However this classification is too restricted and forms too many classes. Instead a stochastic variant is used (*SLOCC*) in which states are equivalent if with non-zero probability they can be converted into one-another, using only local operations and classical communication. The realisation of this definition is the use of invertible linear maps rather than unitaries:

Definition 38. For points $f, g : \mathsf{I} \to \mathcal{Q}^{\otimes n}$ and invertible matrices $\{s_i : \mathcal{Q} \to \mathcal{Q}\}_0^n \subseteq \mathbf{SL}(2, \mathbb{C})$ *stochastic LOCC equivalence (SLOCC)* is

$$f \sim g \iff \left(\bigotimes_{i=0}^{n} s_i \right) \circ f = g$$

SLOCC equivalence has been well studied ([CSZB06]) and its application to small numbers of entangled qubits is widely known. The major results are displayed here:

Qubits	Classes	Class description
1	1	No entanglement is possible therefore all qubits are in the same class.
2	1	All entangled qubits are equivalent to the Bell state.
3	2	Each is equivalent to either the **W** state or the **GHZ** state.
$N \geq 4$	∞	The number of classes is infinite and specified by a set of parameters that grows exponentially with N.

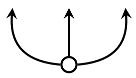
The equivalence of all entangled pairs of qubits to the Bell state is very useful; Any bipartite entanglement can be easily constructed from Φ^+ and correcting unitaries, and therefore from the X/Z calculus with the requisite points. Furthermore it proves that every cap κ can, with an appropriate dualiser d, factorise a compact structure η.

For graph states of four or more qubits SLOCC equivalence broke down, providing an infinite number of classes. This is because the pure state is formed with N qubits and therefore has $O(2^N)$ parameters, but the equivalence relation's 'grouping power', achieved through its use of local operations, scales linearly $O(N)$. Higher level equivalences have been designed that output parameterised classes, however the tripartite result is sufficient for the current investigation.

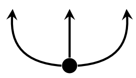
5.2 The three qubit case

Perhaps surprisingly, all three-qubit entanglements fall into one of two classes. Furthermore, the classes are distinguished by a simple structural property. In this section the graph states will be introduced and their calculus explored.

The two classes are:

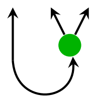


GHZ state
$|\text{GHZ}\rangle = |000\rangle + |111\rangle$



W state
$|\text{W}\rangle = |001\rangle + |010\rangle + |100\rangle$

The GHZ state is equal to δ_Z considered as a point:



$$= |000\rangle + |111\rangle$$

Accordingly the GHZ state induces a special commutative Frobenius algebra identical to the Z calculus presented earlier. The W state has no equivalent node in the X/Z calculus, but can be created through a combination of X, Z nodes and phase shifts. However for the purpose of studying entanglement, the GHZ/W is our calculus of choice.

Note that at this time a completeness result does not exist for the GHZ/W calculus.

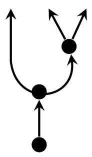
5.2.1 Exploring the W state

The W state induces an algebra different from those studied earlier. The first difference apparent is its cup structure:

Proposition 3. $\kappa_W \neq \kappa_{GHZ}$

Proof. Suppose $\kappa_W^\dagger = \kappa_{\text{GHZ}}^\dagger = |00\rangle + |11\rangle$. Since

$$(1_A \otimes \delta_W) \circ \kappa_W^\dagger \quad =$$



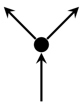
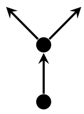
$$= \quad |100\rangle + |010\rangle + |001\rangle$$

then $\delta_W = |00\rangle\langle 1| + |01\rangle\langle 0| + |10\rangle\langle 0|$, and therefore for any $\epsilon_W^\dagger = \alpha|0\rangle + \beta|1\rangle$

$$\kappa_W = \delta_W \circ \epsilon_W^\dagger = \alpha \bullet (|01\rangle + |10\rangle) + \beta \bullet |00\rangle \neq \kappa_{\text{GHZ}}^\dagger$$

contradicting the initial assumption. □

Taking $\kappa_W^\dagger$ to equal $|01\rangle + |10\rangle$, the W state induces the following commutative Frobenius algebra:

 $= \delta_W = |01\rangle\langle 1| + |00\rangle\langle 0| + |10\rangle\langle 1|$  $=$  $= \kappa_W^\dagger = |01\rangle + |10\rangle$

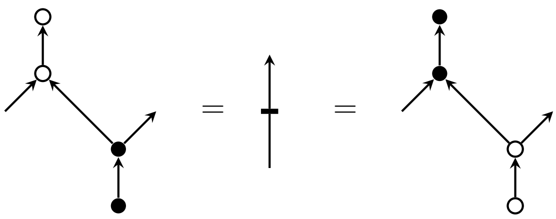
 $= \epsilon_W^\dagger = |1\rangle$  $= X \circ \epsilon_W^\dagger = |0\rangle$  $= X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

In this calculus nodes change their qubit value when flipped upside down– this is due to the cap structure.

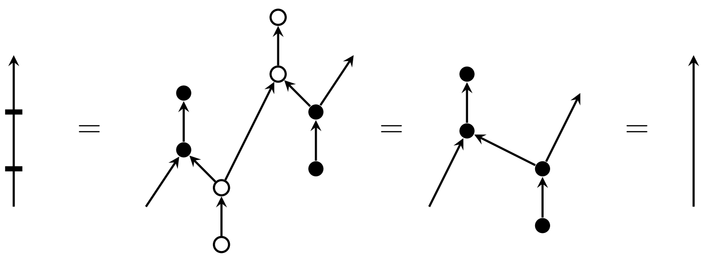
'Stops'  $\langle 0|$  $|1\rangle$

'Flowers'  $\langle 1|$  $|0\rangle$

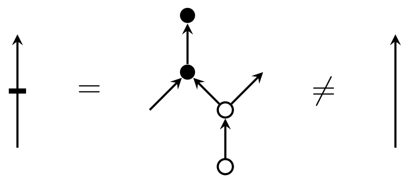
Combining the GHZ and W graphical calculi forms a *tick* $X : \mathcal{Q} \to \mathcal{Q}$:



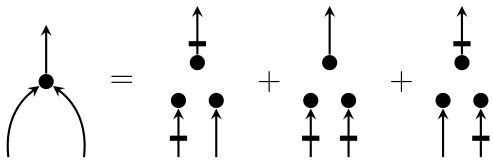
The tick operator is exactly the Pauli X gate, and is therefore self-adjoint, unitary and involutive. These properties are readily proven graphically, for example:

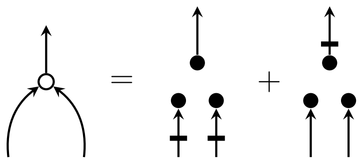
Involutive 

As explained earlier, cups (caps) can be thought of as unitary operations between their qubit outputs (inputs). κ_W and κ_{GHZ} perform unrelated operations – therefore they do not compact when connected together. Equivalently, the tick X does not equal the identity $1_{\mathcal{Q}}$:



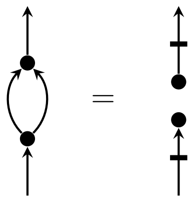
Now both states can be expressed as graphical superpositions:





Speciality

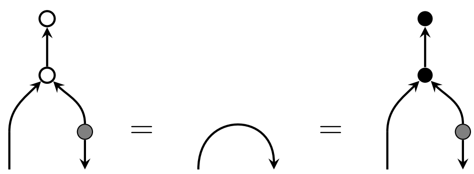
The W calculus is *anti-special*:



Speciality is the distinguishing feature between the W and GHZ induced algebras; More fundamentally, speciality distinguishes the two Entanglement classes they represent. The spider theorem, which holds for the GHZ-algebra, does not hold for the W-algebra because of anti-speciality. This is because anti-speciality causes connected graphs to become disconnected. However, with careful handling, anti-speciality enables unique and useful applications– as will be shown later.

Factorisation of η

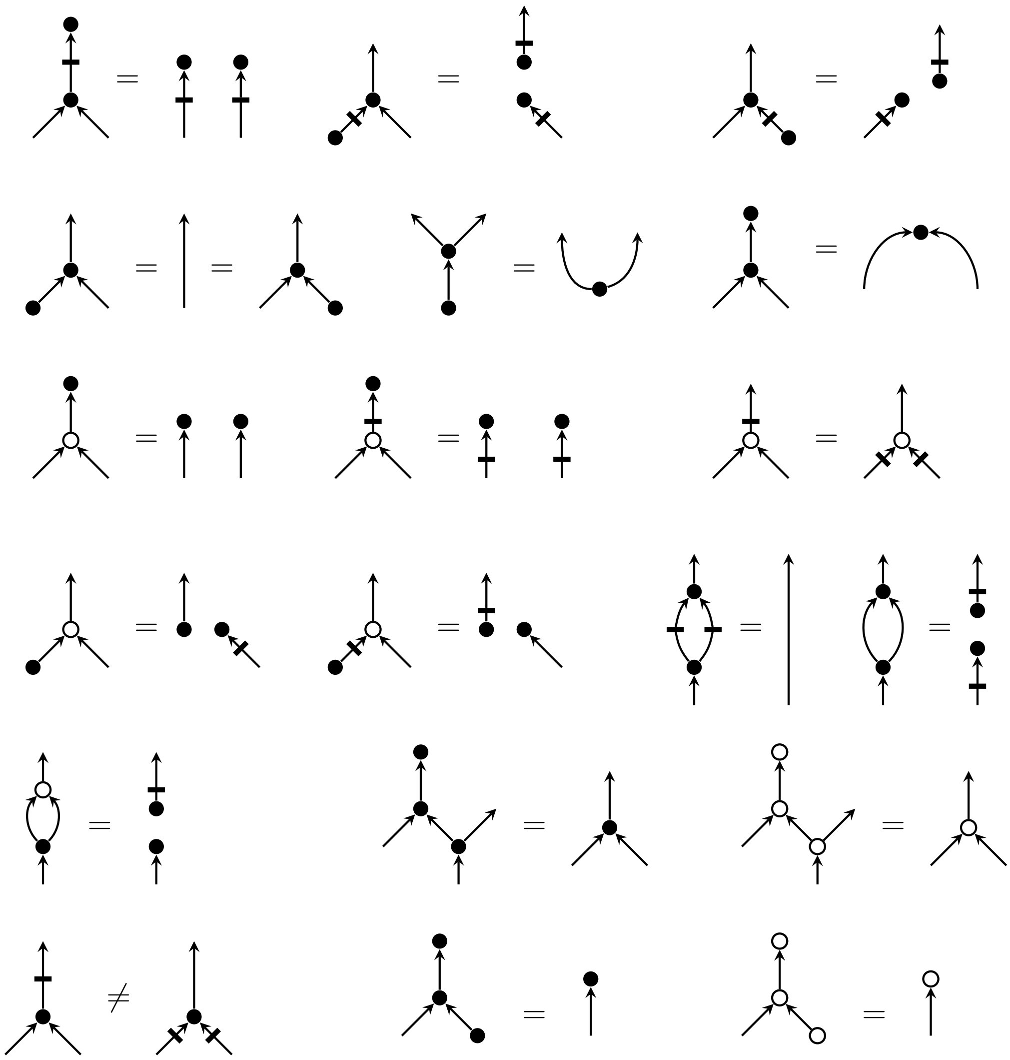
Both GHZ and W nodes factorise $\eta_{\mathcal{Q}} : \mathcal{Q} \otimes \mathcal{Q}^* \to \mathsf{I} = |00\rangle + |11\rangle$. This is possible through the use of dualisers.



The dualiser used with the GHZ node simply maps arrows to their duals, i.e. $d_{\text{GHZ}}(-) = (-)^*$ whereas the W node's dualiser performs the mapping $d_w(-) = (X \circ -)^*$. This similarity in factorisation shows that despite the fundamental differences in W and GHZ entanglement, they still share low-level structure.

5.2.2 Basic Axioms

By plugging the basic nodes together a wide range of axioms can be formed. These provide simplifications for larger graphs. The axioms are given in the graphical equations below[1]:



[1]Notice that both the GHZ and W nodes have horizontal symmetry, therefore any axiom can be reflected to gain another

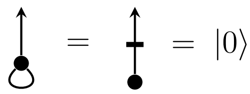
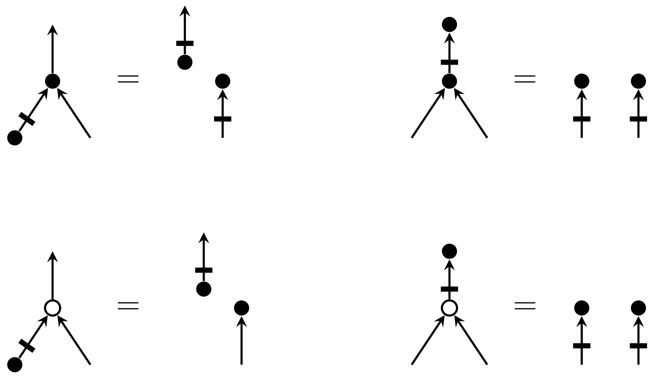
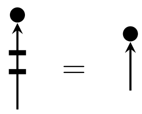


Figure 5.1: *Flowers can equivalently be drawn as 'Loops'*

An important aspect of the GHZ/W calculus is the propagation of flowers. If a flower is attached to any leg of a GHZ or W node it will always propagate to another leg, often both:



This can be seen as a difficulty since flowers can rampantly spread through carefully constructed graphs. Furthermore units (which are by definition benign inputs to duplicator nodes) are inter-converted to flowers by ticks:



Therefore graph design in the GHZ/W calculus requires greater diligence than in the X/Z. However graph primitives resilient to flowers exist – these will be shown later.

5.2.3 Normal Forms

One great strength of the X/Z calculus is its support of the spider theorem– this enables graphs to be quickly and intuitively manipulated. The GHZ node is identical to the Z node studied earlier, therefore GHZ graphs support the (orientated and decorated) spider theorem. The W calculus does not support the spider theorem but it does obey a weaker version:

Proposition 4. *Any acyclic graph built from elements* $(\delta_W, \epsilon_W, d_W)$ *obeys the orientated spider theorem.*

Proof. The requirement of acyclicity ensures that the graph never exhibits specialness and its associate disconnection; Cycles form flowers which rapidly duplicate through the graph. As a result, the graphs' calculus can be considered a †-dual 'special' Frobenius structure on both $\mathcal{Q}$ and $\mathcal{Q}^*$. Therefore the orientated spider theorem is supported. □

Tick-free cycles of W nodes exhibit the following equality:

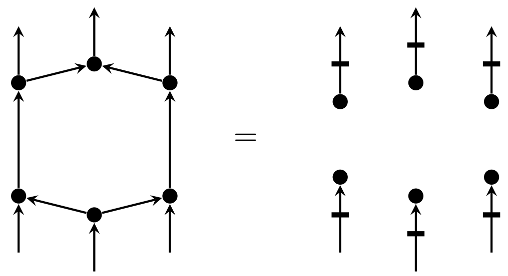


Figure 5.2: *W node cycles always explode into flowers*

Proposition 5 (Cycle theorem for W graphs)**.** *For any tick-free cycle of W nodes* $(\delta_{W,1} \cdots \delta_{W,n})$ *forming the function* $f : \mathcal{Q}^{\otimes p} \to \mathcal{Q}^{\otimes q}$ *where* $p + q = n$*,*

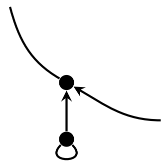
$$f = (X \circ \epsilon_W^\dagger)^{\otimes q} \circ (\epsilon_W \circ X)^{\otimes p}$$

Proof. If the cycle simplifies to flowers as described above one cannot plug a in flower node; this would produce a zero scalar (a sign the graph cannot be constructed), e.g.

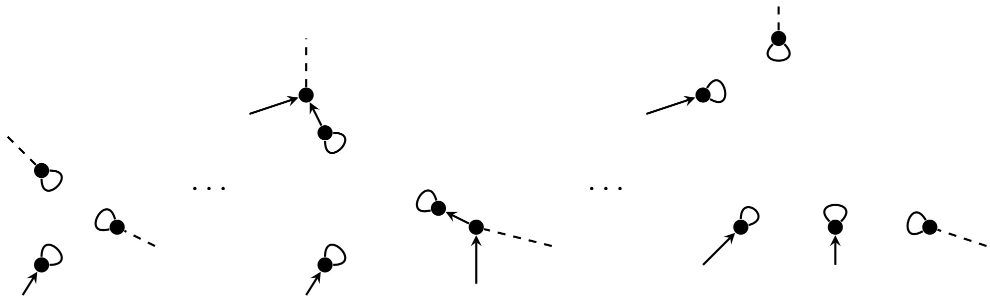
$$(\epsilon_W \circ X) \circ (X \circ \epsilon_W^\dagger) = \langle 1|0\rangle = 0$$

indicating that such a structure has zero probability of occurring.

However, suppose a duplicator did not simplify to a loop, it must then simplify to a stop, or a superposition of stop and loop. In this case one could validly plug in a loop



However, by the above axioms, the loop would propagate:



and eventually two loops would meet. This results in the zero scalar, a flag that the structure is not buildable– and therefore the assumption is incorrect and all duplicators simplify to loops. □

The above normal forms are for tick free graphs of a single type of node (GHZ or W). These can be used within larger graphs to simplify sub-graphs. However, the requirements of being tick free and of a single type of node are restrictive. In the following section we explore what results exist outside of these bounds.

5.2.4 Cycle normal forms

Acyclic graphs in the GHZ/W calculus simplify easily– both GHZ and W nodes support the spider theorem. However, as seen in the earlier discussion of speciality, graph cycles have differing treatments depending on node class. This section presents a method of analysing mixed node cycles that include ticks.

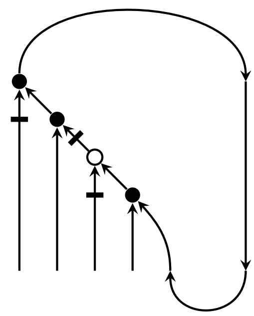
Definition 39. *Tree cycle form* for a cycle of nodes $[s_1, \cdots s_n]$ where each s_i is either a GHZ or W node, with each leg potentially ticked, i.e. $s_i \in \{\delta_W, \delta_{\mathrm{GHZ}}, X \circ \delta_W, \delta_W \circ (X \otimes 1_{\mathcal{Q}}), X \circ \delta_W \circ (X \otimes 1_{\mathcal{Q}}) \dots\}$ is defined

$$\eta_{\mathcal{Q}} \circ (\Delta_1 \otimes 1^*{}_{\mathcal{Q}}) \circ (1_{\mathcal{Q}}^{\otimes n-1} \otimes \eta_{\mathcal{Q}}^\dagger)$$

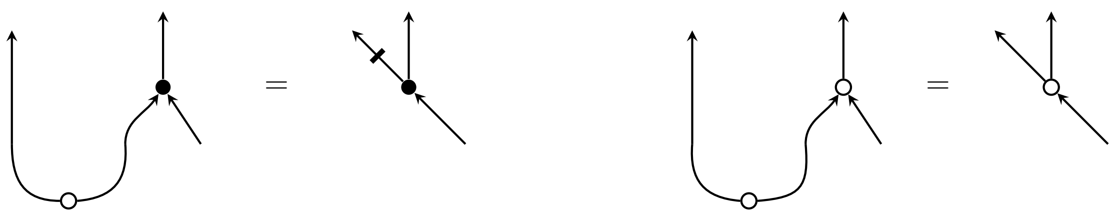
where

$$\Delta_i = s_i^\dagger \circ (1_{\mathcal{Q}} \otimes \Delta_{i+1})$$
$$\Delta_n = s_n^\dagger$$

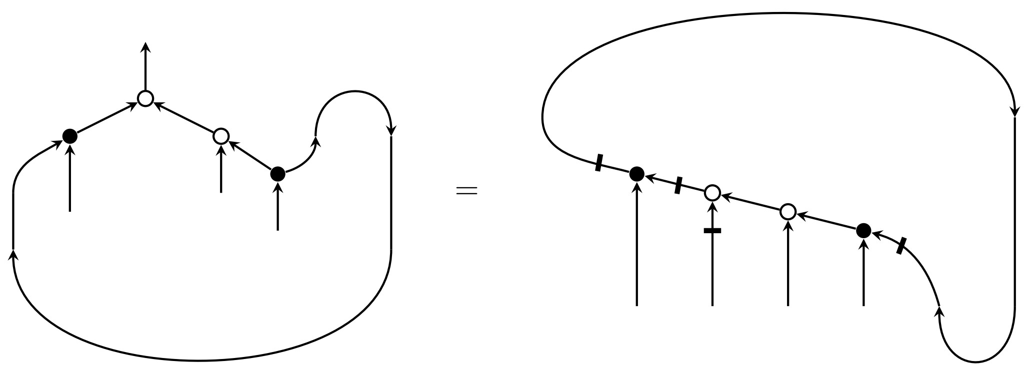
A graphical example:



Example 7. Any cycle can be converted into tree cycle form. We wish to convert nodes into a state where their legs are all correctly orientated, yet not change the graph state. For W nodes this requires adding a tick to any legs that switch between upward and downward orientation. By the spider law GHZ nodes can have their legs reoriented without further changes.



Therefore the following cycle converts as shown:

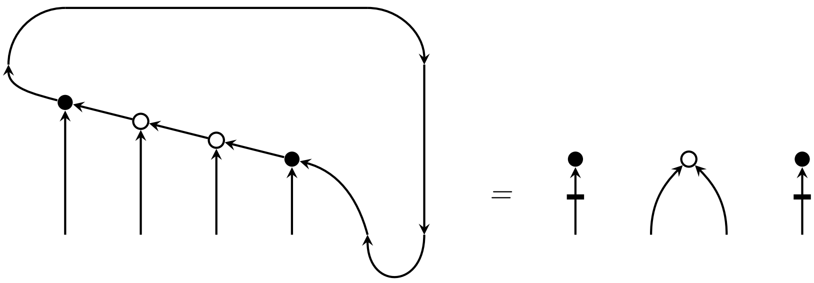


Once in this form further analysis and simplification is possible. Note that ticks on the unconnected legs do not affect the simplification, they only change how the outside graph 'views' this sub-graph. However, ticks between nodes do affect which simplifications are possible.

Proposition 6. *When no ticks occur between nodes tree cycle form experiences the following simplification:*

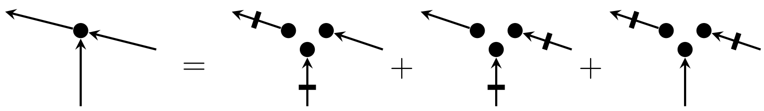
- *All GHZ nodes merge into a spider and disconnect from all W nodes*
- *All W nodes disconnect, leaving flowers*

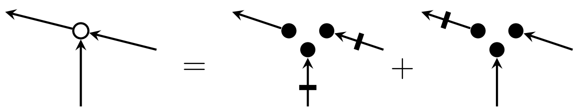
A graphical example:



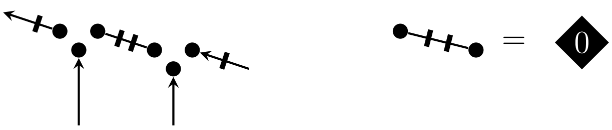
This result is the combination of the spider theorem for GHZ graphs and the cycle theorem for W graphs. When the cycle is entirely GHZ or W nodes the above result reduces into those theorems.

Proof. Here we look at nodes $[\delta_0, \cdots \delta_n]$ in tree cycle form, with no ticks between nodes. Consider the GHZ and W nodes displayed as superpositions of qubit states:

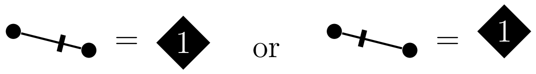




Only particular states fit together. For example, when two W nodes are connected they cannot display a unit on their spare wires as the zero scalar would emerge (from the joining of two flowers):



Instead states must interlock in one of two ways:

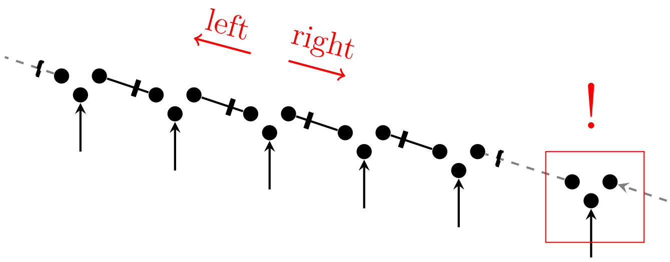


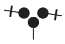
Omitting from the W state superposition  only two cases emerge for the tree cycle:

- All are in 'left' orientation. All GHZ nodes display a unit and all W nodes display a flower.

- All are in 'right' orientation. All GHZ nodes display a flower and all W nodes display a flower.

The W state  results in a 'left' and a 'right' section coexisting. This eventually leads to a node that is met by flowers on either side, which therefore must display units on both its linked legs (in red box, below):



Since neither W nor GHZ nodes contain a state which displays units on both linked legs, a complete cycle with both left and right sections is impossible. Thus the W state  cannot occur.

Therefore

- All W nodes output a flower.
- All GHZ nodes have the same output, either a flower or a unit. This is equivalent to them being fused into one single spider node.

□

We have now examined cyclic and acyclic graphs of a single type of node and the interaction between both GHZ and W nodes. However, this has all been under the proviso that the graph is tick free.

As touched upon earlier, ticks convert benign units into flowers, which duplicate rapidly through the graph. Therefore it is very difficult to provide general rules in the presence of ticks and none have yet been discovered. However, there do exist connectivity results as presented here.

The following table lists the significant results experienced by Tree Normal forms with various characteristics:

The results above are elaborated further:

- **W Nodes / Odd No. of ticks**: This graph is a superposition of many states, each of which always produces an odd number of units on its unconnected wires. The other wires display flowers. As a corollary of this observation, all the nodes must remain connected for the number of displayed units to always have an odd total.

	GHZ nodes only	**W nodes only**	**Mixed GHZ and W nodes**
Zero ticks	Spider Theorem	W Cycle Theorem	Tree Cycle Normal Form
Odd No. of ticks	Equals *Zero* scalar	Connected. Displays odd No. of units.	Connected.
Even No. of ticks	Ticked Spider	Connected. Displays even No. of units.	Connected.

Note that only inter-nodal ticks are counted– those on the free legs do not affect this analysis and are not included in the tick counts.

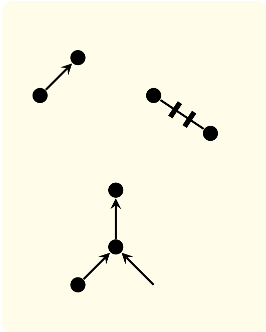
- **W Nodes / Even No. of ticks**: Exactly the even counterpart of the above.
- **GHZ Nodes / Even No. of ticks**: A 'ticked spider' is a standard orientated spider node with ticks on some of its free legs. By the GHZ node's tick axiom, ticks can be moved from between nodes to the free legs. Since an even number of ticks exist, all inter-nodal ticks can eventually be made to cancel out one-another.
- **GHZ and W nodes / Odd or Even No. of ticks**: In this circumstance the strongest result is simply connectedness. The state superposition of such graphs is complex and has yet to admit simplification.

These properties can be verified in exactly the same manner as used to verify Tree Cycle Normal Form. They are not particularly difficult to prove although the proofs are wordy and due to limited space are not included here.

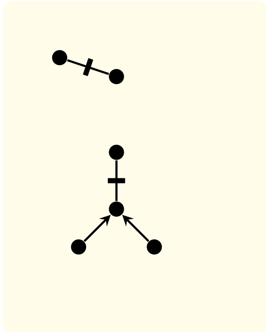
5.2.5 Zeros

If a state produces a zero scalar, it is not a valid state of the system; The zero scalar means 'zero probability of this state occurring'. Equivalently, the appearance of a zero scalar is an important sign that the graph cannot be constructed. Unlike when working with the X/Z calculus, in GHZ/W graphs frequently result in zero and it is therefore important to work out when the condition occurs.

Example 8. Depicted below are various graphs that either equal the zero scalar or the one scalar



Equal to Zero



Equal to One

The rules from the previous section give rise to a fast method of detecting whether a graph precipitates a zero scalar:

Definition 40. A *closed* graph has no input nor output wires

Theorem 10 (Quick zero check)**.** *Any connected and closed graph* **G** *composed of elements* $(\delta_W, \epsilon_W, d_W)$ *with* n *flower nodes and* m *cycles produces a zero scalar* iff $n + m \neq 1$*. It produces a non-zero scalar otherwise.*

Proof.

1. *Case* $n + m = 0$: Therefore the graph is acyclic. Therefore it obeys the orientated spider theorem. As the graph is closed it reduces down to •–• which equals zero.

Case $n + m \geq 2$: Since every cycle reduces down to flower nodes, the graph necessarily has multiple flower nodes. Since flower nodes are always copied and the graph is connected, the case •⧺• $= 0$ must eventually occur. □

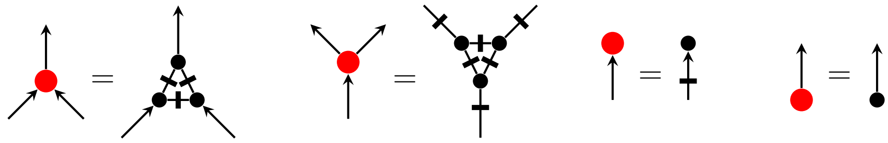
As cycle detection operates in linear time this method can quickly detect zero-scalar graphs.

5.3 Applications of the GHZ/W calculus

The previous sections have presented many tools for working with the calculus as well as an understanding of its character. In exploring the calculus we aim to learn more about the logic of quantum information, as well as to develop further quantum algorithms. In this section various building-blocks for future applications are presented.

5.3.1 Universality

Earlier it was shown that the X/Z calculus is universal, every possible point and unitary transformation can be built within the calculus. It was also stated that the W node can be formed through a combination of X and Z nodes and phase shifts. Similarly, the X node can be constructed out of W nodes and ticks:



Therefore the entire X/Z calculus can be embedded in the GHZ/W calculus and is therefore subsumed. The universality property is thus inherited once one includes the definition of phase shifts from earlier:

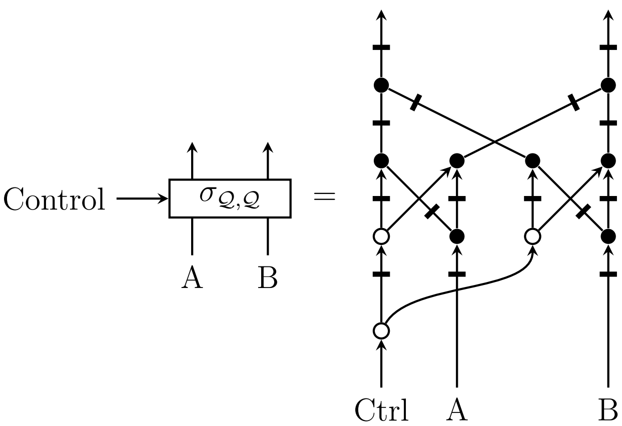
Proposition 7. *The GHZ/W calculus with phase shifts is universal. Therefore the GHZ/W calculus can encode every quantum system.*

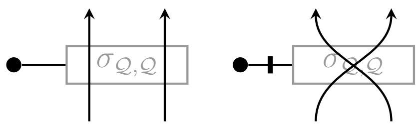
The above construction of the X node is quite interesting: The X node has the Special property, yet it has been built entirely from anti-Special W nodes and the tick operator (the Pauli-X gate). This shows the two entanglement classes are not separated by an algebraic gulf, instead they are very closely related.

5.3.2 Q-Swap gate

Earlier particular attention was given to the viral nature of flower nodes– they are duplicated by every node they encounter. A quick mental induction suggests that they may therefore defeat any attempt to build intelligent graph structures. However, careful use of ticks can prevent this behaviour entirely.

Much as logic gates were built to harness the potential of transistors, the Q-Swap gate leverages the anti-speciality (disconnection) of the W node.



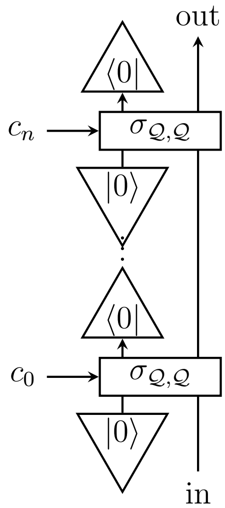


Plugging in $|1\rangle$ and $|0\rangle$

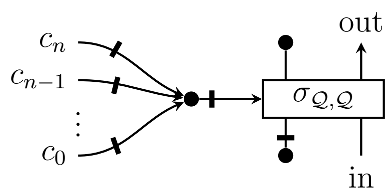
The Q-Swap is a refinement of the Q-Mux recently presented in [CK10]. Connecting a unit to its control input causes the gate act as two identity arrows and connecting a flower to the control causes it to act as a swap gate $\sigma_{Q,Q}$. Furthermore, connecting a GHZ unit (which is a superposition of the W unit and loop) to the control places it into a superposition of identity and swap behaviour. It therefore provides a simple and well-defined function, one under which loops and units have an equal footing as its operation is symmetric between them.

Using the gate one can quickly build many forms of quantum logic, examples of which are given here.

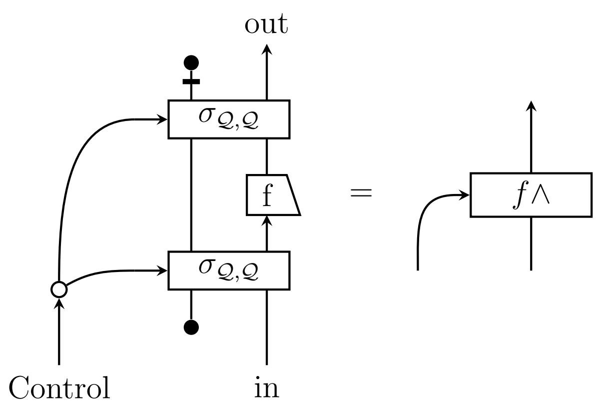
Example 9. Quantum AND Gate: By daisy chaining Q-Swap gates an AND function is created. Control bits $c_0 \cdot c_n$ are ANDed together, passing *in* through to *out* when all c_i are units, and outputting $|0\rangle$ otherwise:



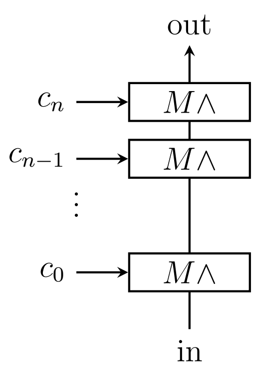
Example 10. Quantum OR Gate: By ORing the control bits $c_0 \cdot c_n$ with a W node, the following OR gate is formed. If any of the control bits are units it will pass the input to output, otherwise it outputs $|0\rangle$:



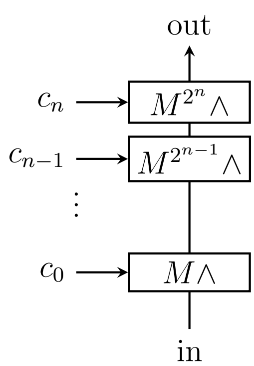
Example 11. Controlled-Gate: Using two Q-Swaps together a gate can easily be made switchable:



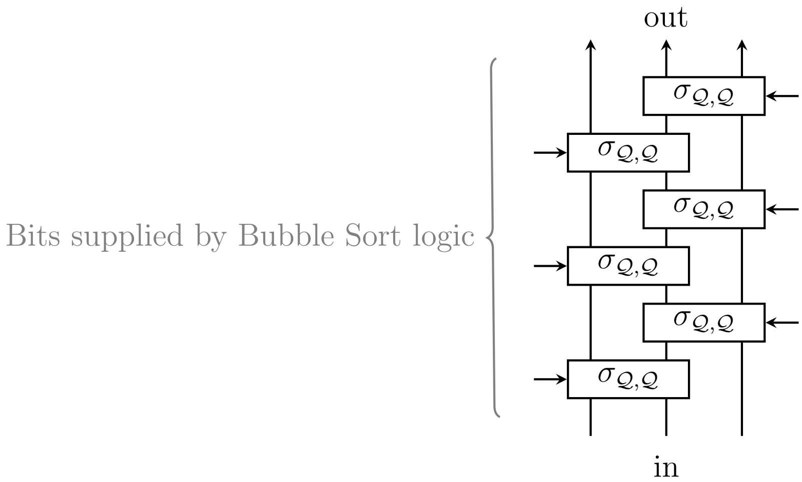
Example 12. Quantum POW Gate: Using a chain of controlled gates the control bits can govern matrix exponentiation, raising M to the power n where n is the number of control bits equal to the unit:



Example 13. Quantum POW2 Gate: By pre-exponentiating the controlled gates, the input string can be interpreted as a binary number, to which power M is raised:



Example 14. Quantum Interconnect: A flexible interchange between n wires can be formed with order $O(n^2)$ Q-Swap gates. The input bits to those $O(n^2)$ gates are determined by the logic of the Bubble Sort.



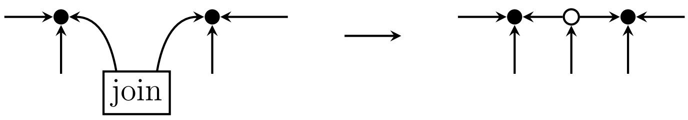
The above examples demonstrate that the Q-Swap is a practical and versatile building block.

5.3.3 Measurement Chains

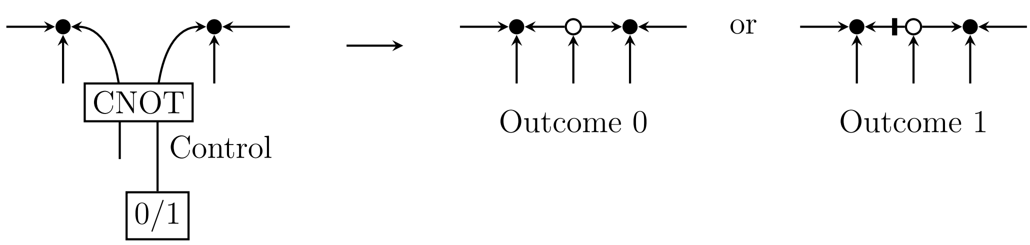
Finally, a demonstration that W nodes elegantly form universal measurement based computers. The protocol presented here is a significant extension of an unpublished idea suggested by Alexs Kissinger of the Oxford University Comlab, and was originally motivated by [BR05]. The protocol aims to provide a practical and implementable way to transform a source of W states into a flexible computer. The only aparatus required are W states, CNOT gates and measurements.

The basic protocol

The core premise is a linking operation that stochastically joins two W nodes via a GHZ node. By repeating the operation a chain can be formed:

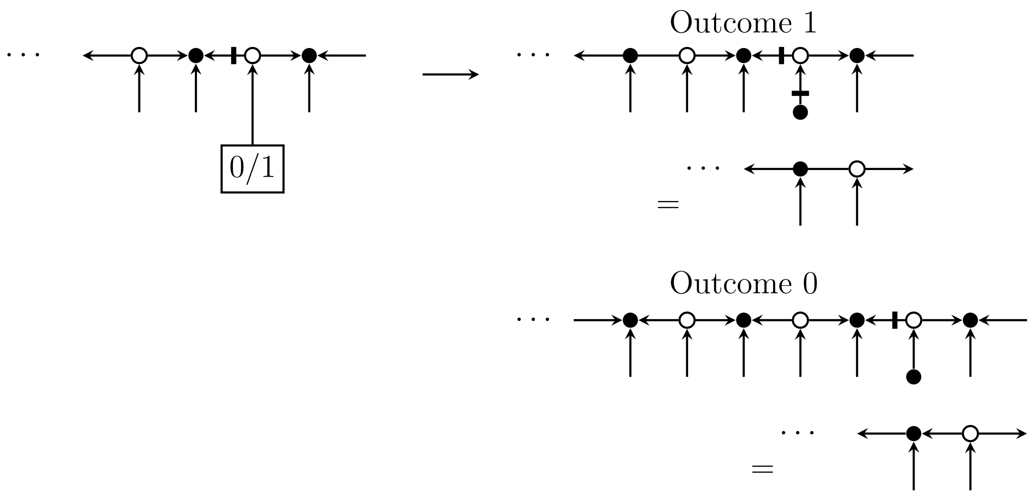


The linking operation is performed in two stages. First a qubit of each W state is passed through a CNOT gate. Then the output of the CNOT control line is measured in the computational basis. A measurement of zero declares that the nodes have been successfully linked, a measurement of one indicates that a rogue tick has been formed:

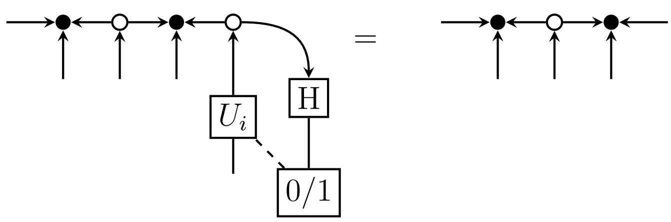


Therefore 50% of the time the chain is successfully extended. In the other case a protocol exists to undo the operation:

One measures the GHZ qubit in the computational basis. Depending on the outcome of the measurement this causes the chain to 'roll-back' a number of links. The resulting chain ends on a GHZ node:



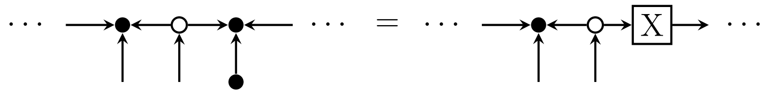
And then finally a measurement (in the Hadamard basis) and correction remove the excess GHZ node:



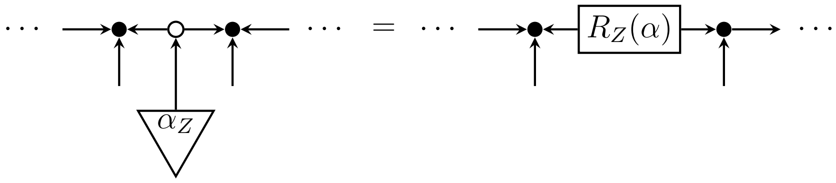
Chain Preparations

The W-GHZ chain can now be set up to perform calculations. By measuring the chain's free qubits a number of gates can be constructed.

Example 15. Measuring a zero on a W state is equivalent to the following situation in which an X gate is produced:



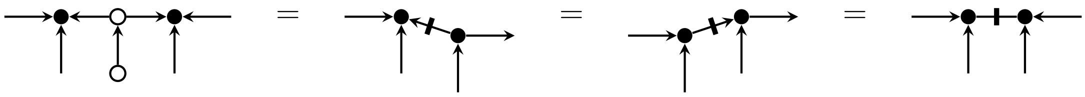
Example 16. Since GHZ nodes are exactly Z nodes, a phase shift can be constructed using a point of form $|\alpha_Z\rangle$:



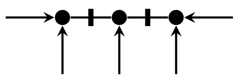
However the previous example only brings rotation in one plane– for general calculations we require rotation in two different planes. This was previously achieved using X and Z node phase shifts. This practice can be employed here, however X nodes must be constructed.

Constructing X nodes

It is surprisingly easy to create an X node using the processes described above. This relies on an important equality[2]:

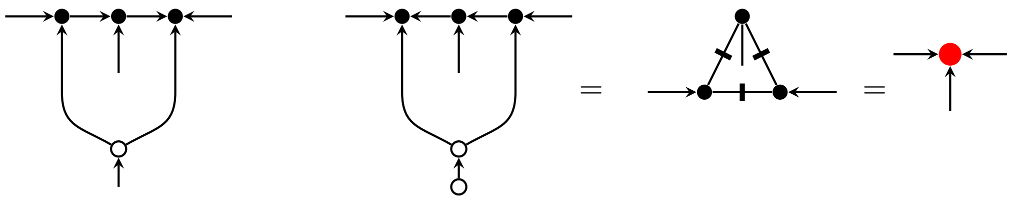


Therefore by measuring two GHZ nodes the following situation is reached:



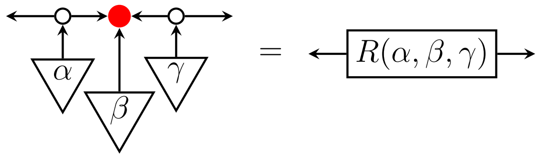
And by performing a lateral link operation an X node is formed:

(1) Link (2) Convert into a tick

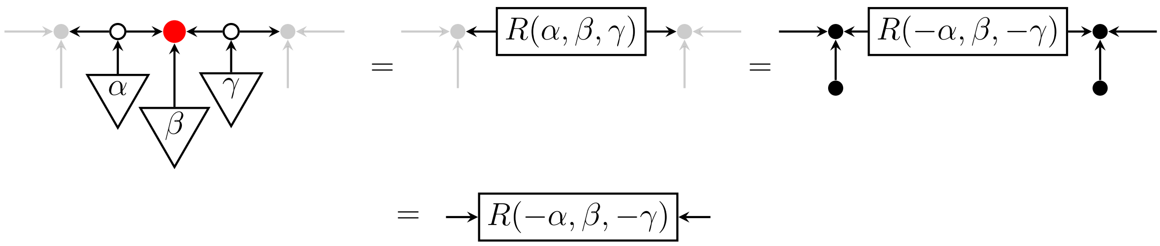


Taking the X node and the two surrounding Z (GHZ) nodes, a general rotation and therefore any one bit unitary can be produced:

[2]The flat, un-arrowed line between the final pair of W nodes represents the fact that the direction is not important

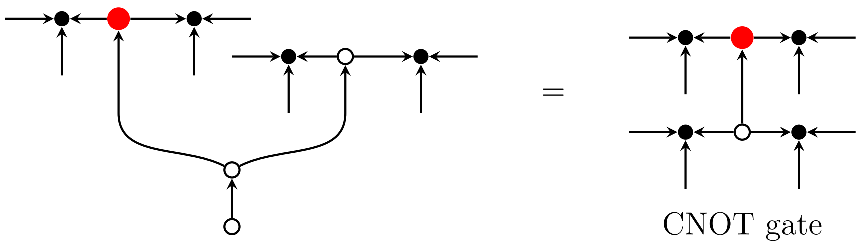


Also, remembering that the above GHZ-X-GHZ configuration is usually surrounded by W nodes, a handy trick exists: For any matrix M the product $X \circ M \circ X$ (where X is the Pauli gate here) is simply a permutation, therefore surrounding W nodes can be incorporated without loss of generality:



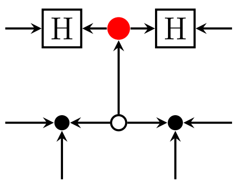
Forming multi-qubit gates

The linking operation can be used between separate chains. By taking an X node of one chain and a GHZ node of another and linking them, a CNOT (or 'controlled X') gate is formed between the chains:



CNOT gate

Also, since general unitaries are available, the controlled Z gate can also be formed with the aid of Hadamard gates:



With the addition of these two operations the W/GHZ chains provide a computationally universal set of multi-qubit gates (see [CD09]). Therefore a simple source of W states has been transformed into an efficient substrate for all measurement based computing.

Chapter 6

Conclusion

This dissertation has surveyed a wealth of literature on Categorical Quantum Mechanics[1], bringing together the work of many papers into a single coherent presentation. The theories from these papers have been incorporated together and extended to cover new ground.

The final chapter presented recently published work and embellished it with further theories, observations, examples and proofs. New protocols, both novel and practical, have been invented and described.

Many Categorical treatments of Quantum Mechanics have presented their algebras in a terse and unmotivated manner. This dissertation has attempted to make the subject more accessible to a student of Quantum Mechanics, structuring itself around pre-existing knowledge and including better designed proofs, descriptions and examples.

Whilst the field of Categorical Quantum Mechanics is still relatively new, it has quickly made significant advances. It is hoped this work both promotes and furthers the field.

6.1 The work ahead

Being a new field, there are many fruitful areas to be explored. A greater emphasis on the implementable, reigning focus away from algebraic concerns, could revolutionise future Quantum architectures. At the same time, deeper abstract probing into entanglement of greater degrees could have the same effect. Tripartite entanglement divides by Speciality; Looking at higher degree entanglements, do distinct algebraic properties provide meaningful classes?

More immediately, small graph states stand to be catalogued and analysed to find further geometric insights. Measurement based computing has proved

[1][Coe08], [CD09], [BR05], [CK10], [CSZB06] and [CPP08] in particular.

to be an important paradigm and the GHZ/W calculus is only beginning to be analysed from this angle.

Much has been learned and much remains to be explored. The field of Categorical Quantum Mechanics remains an exciting one to work within.

6.2 Acknowledgements

This dissertation would not have been possible without the guidance, support and belief of my supervisor Bob Coecke. Bob has been a tireless source of insight and I am deeply grateful. Balliol College, through the work of Doug Dupree, has provided a Graduate Bursary to keep me safe and warm– Floreat Domus! Finally, thank you to the great many people whose background work has made this whole year at Oxford possible.

Bibliography

[BR05] Daniel E. Browne and Terry Rudolph. Resource-efficient linear optical quantum computation. Feb 2005. Available from: http://arxiv.org/abs/quant-ph/0405157, arXiv:quant-ph/0405157.

[BW95] Michael Barr and Charles Wells, editors. *Category theory for computing science, 2nd ed.* Prentice Hall International (UK) Ltd., Hertfordshire, UK, UK, 1995.

[CD09] Bob Coecke and Ross Duncan. Interacting quantum observables: Categorical algebra and diagrammatics. Jun 2009. Available from: http://arxiv.org/abs/0906.4725, arXiv:0906.4725.

[CK10] Bob Coecke and Aleks Kissinger. The compositional structure of multipartite quantum entanglement. Feb 2010. Available from: http://arxiv.org/abs/1002.2540, arXiv:1002.2540.

[Coe04] Bob Coecke. The logic of entanglement, March 2004. Available from: http://arxiv.org/abs/quant-ph/0402014, arXiv:quant-ph/0402014.

[Coe05] Bob Coecke. Kindergarten quantum mechanics. Oct 2005. Available from: http://arxiv.org/abs/quant-ph/0510032, arXiv:quant-ph/0510032.

[Coe08] Bob Coecke. Introducing categories to the practicing physicist. Aug 2008. Available from: http://arxiv.org/abs/0808.1032, arXiv:0808.1032.

[CPP08] Bob Coecke, Eric O. Paquette, and Simon Perdrix. Bases in diagrammatic quantum protocols. Aug 2008. Available from: http://arxiv.org/abs/0808.1029, arXiv:0808.1029.

[CSZB06] G. Casati, D. L. Shepelyansky, P. Zoller, and G. Benenti. *Quantum Computer, Algorithms and Chaos: Volume 162 International School of Physics Enrico Fermi.* IOS Press, Inc., 2006.

[Deu85] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 400(1818):97–117, 1985. Available from: `http://dx.doi.org/10.2307/2397601`, `doi:10.2307/2397601`.

[Doe09a] Andreas Doering. Categories, proofs and processes, 2009. Available from: `http://web.comlab.ox.ac.uk/teaching/courses/2009-2010/catsproofsprocs/`.

[Doe09b] Andreas Doering. Quantum computer science, 2009. Available from: `http://web.comlab.ox.ac.uk/teaching/courses/2009-2010/quantum/`.

[Ing76] Roman Ingarden. Quantum information theory. *Rep. Math. Phys.*, 10:43–72, 1976.

[KL80] Max Kelly and M. L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[Lac04] Stephen Lack. Composing props. *Theory and Applications of Categories*, pages 147–163, 2004.

[Lan98a] Saunders M. Lane. *Categories for the Working Mathematician (Graduate Texts in Mathematics)*. Springer, 2nd edition, September 1998. Available from: `http://www.worldcat.org/isbn/0387984038`.

[Lan98b] Saunders M. Lane. *Categories for the Working Mathematician (Graduate Texts in Mathematics)*. Springer, 2nd edition, September 1998. Available from: `http://www.worldcat.org/isbn/0387984038`.

[PF89] D. Yetter P. Freyd. *Braided compact closed categories with applications to low-dimensional topology.*, volume 77. 1989.

[phy] Quantum teleportation achieved over 16 km. *PhysOrg.com.* Available from: `http://www.physorg.com/news193551675.html`.

[Sel09] Peter Selinger. A survey of graphical languages for monoidal categories. Aug 2009. Available from: `http://arxiv.org/abs/0908.3347`, `arXiv:0908.3347`.

[vN32] J. von Neumann. Mathematische grund lagen der quantenmechanik. 1932.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. Available from: http://dx.doi.org/10.1145/1008908.1008920, doi:10.1145/1008908.1008920.