A Compositional Characterization of Multipartite Quantum States

Shibdas Roy

St. Cross College

University of Oxford

A thesis submitted for the degree of

Master of Science

September 2010

Abstract

The primary aim of this work is to study the compositional characterization of multipartite quantum states in an abstract setting of commutative Frobenius algebras expressed internal to symmetric monoidal categories. This work is based on the compositional structure of multipartite quantum entanglement established by Bob Coecke and Aleks Kissinger in [11]. The two SLOCC classes of tripartite entanglement, viz. GHZ and W states, were shown to correspond to the 'special' and 'anti-special' kinds of internal commutative Frobenius algebras (CFAs), respectively. A SCFA morphism is known to be just a *spider*, where as here we concretely lay down the nature of an ACFA morphism, explicitly spelling out the scalar involved.

The central result of this work, however, is to illustrate a normal form for interacting GHZ and W states. Based on the basic set of axioms of a GHZ/W pair, we study a class of scalars formed out of cups, caps and symmetries and/or identities. We develop some more relevant graphical identities, wherever required for the particular case of the SMC **FdHilb** of Hilbert spaces and linear maps. This, in turn, would equip us with tools to study the behaviour of a SCFA morphism or an ACFA morphism alongwith ticks, i.e. a CFA morphism with ticks and only white dots or only black dots. This naturally allows us to explore the values of the scalars expressed in this normal form for different cases. We also study the behaviour of certain class of mixed morphisms, hoping that this would assist in arriving at a normal form for any arbitrary morphism as part of future work.

Acknowledgements

I would like to first convey my gratitude to my supervisor, Dr. Bob Coecke, who has guided me with a lot of attention in my creation of this work. Ever since the beginning of my MSc degree here at Oxford University Computing Laboratory, I was keen to pursue my project in Quantum Computing and it has been a great privilege to have worked with Bob, who had also helped me choose the subjects for my coursework so as to suit my project. My special thanks to him for his allowing me to attend the lectures given by eminent researchers of Quantum Computing Community as part of the QICS Spring School 2010 at the Oxford University.

I would like to thank Aleks Kissinger for his valuable inputs. It was also a privilege to talk to and have attended lectures of Prof. Samson Abramsky. I also convey my thanks to Andreas Doering who took the course Quantum Computer Science, through which he gave me a deep insight into the subject. I thank him in particular to have covered the course from ground level to make his students get a solid grip over the subject. He has keenly devoted additional time even outside the lectures to explain vividly concepts that needed clarification. He had as well taught with utmost care the course Categories, Proofs and Processes, which has been highly useful in this work.

I also thank my academic supervisor Dr. David Parker and my senior mentor, Dr. Marina Jirotka for their valuable support. I would also like to thank Shoshannah Holdom, Leanne Carveth, Julie Sheppard, Wendy Adams and others to have made the MSc course so versatile and interesting.

Finally, I am grateful to my parents and others who have helped me to reach where I am today. If I have to dedicate this work to anyone, I would dedicate it to my parents.

Contents

Chapter 1

Introduction

"Anyone not shocked by quantum mechanics has not understood it." - Niels Bohr

Shocking it is... not only because one third of the world economy today involves products based on quantum mechanics... but mainly because the implications of quantum theory would take anyone into a world of wilderness, where our intuitive perception of the physical world around us is unanswerably challenged. On the one hand, quantum theory tells us that an observation of one object can instantaneously influence, through so-called *spooky interactions* (due to Einstein), the behaviour of another greatly distant object even if no physical force connects the two. On the other, it claims that observing an object to be someplace *causes* it to be there. If according to the theory, a (Schrödinger's) cat could be simultaneously dead and alive until our observation causes it to be either dead or alive, anyone cannot accept it with equanimity. For example, Stephen Hawking once remarked, *"When I hear about Schrödinger's cat, I reach for my gun"*.

However, despite this wilderness and/or weirdness, quantum mechanics is the most accurate and, unarguably, the most battle-tested theory in all of science. No prediction by the theory has ever been proven wrong. Had the Bell's inequality not been found to be violated as predicted, the history of science could have been written differently. As pointed out by John Preskill, *"Developing quantum theory was the crowning intellectual achievement of the last century"*.

Although quantum mechanics is around for over a hundred years now, we are still at Kinder-Garten with quantum computation and information. The quantum mechanical formalism can be considered 'low-level' in computer science terminology, since it does not support our intuition. It, therefore, took 50 years since the birth of quantum mechanical formalism to discover the quantum 'no-cloning' theorem and similarly 60 years to discover the conceptually intriguing and yet easily derivable physical phenomenon of 'quantum teleportation'. In [7], Bob Coecke thus introduced a diagrammatic 'high-level' alternative for the Hilbert space formalism, one which appeals to our intuition. This diagrammatic language built upon the mathematical foundation of monoidal categories allows for intuitive reasoning about interacting quantum systems and trivialises many otherwise tedious computations [6]. There has been considerable progress and ongoing extensive research in this new paradigm, that sits at the core of our work presented in this thesis.

In this chapter, we would present our motivation and then outline our objective(s) of this work. In chapter 2, we shall cover the background on categories, in particular certain types of monoidal categories. In chapter 3, we shall cover the background on Frobenius algebras, in particular expressing them internal to monoidal categories. In chapter 4, we shall talk about quantum entanglement in an abstract setting. In chapter 5, we would elucidate our main work and outline the core results. Finally, in chapter 6, we would make concluding remarks, summarising the results and mentioning future work in this context.

1.1 Motivation

What is a quantum computer? Why are we scratching our heads with quantum computing? What does it have to do with computer science? How is a quantum computer different from a classical computer? What is so exciting about Quantum Information Theory? What is entanglement and what is its role in quantum information? We address these questions in this section to give the reader a recipe of our motivation for our work in this thesis.

1.1.1 Quantum Computation

Quantum computers would exploit the strange rules of quantum mechanics to process information in ways that are impossible on a classical computer. Quantum computers are heralded for their potential to solve in minutes certain problems that would take a classical computer a billion years!

A quantum computer is proposed precisely based on the following three basic principles of quantum mechanics [24]:

- **Superposition principle:** An n-qubit quantum register that has $k = 2^n$ classical states has a quantum state that is a linear combination (superposition) of all classical states with complex coefficients. Therefore, the quantum state of this register (system) can be represented by a k-dimensional complex vector called the *state vector*, which is a unit vector in the system's *state space* (Hilbert space) and is represented as:

$$|\Psi\rangle = \sum_{i=0}^{i=k-1} \alpha_i |i\rangle$$

where α_i is the complex *amplitude* corresponding to classical state $|i\rangle$ which is a vector with only its i^{th} row equal to one and the rest zero.

The simplest quantum mechanical system is the *qubit* that has a two-dimensional state space, in which an arbitrary state vector is written as

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

where $|0\rangle$ and $|1\rangle$ form an orthonormal (computational) basis for the state space.

- **Measurement principle:** The quantum state of a quantum register or system is hidden to us. Upon measuring it in the computational basis, we will get classical state $|i\rangle$ with probability $|\alpha_i|^2$. The weird thing is that measurements following the first measurement will result in the same outcome that was obtained after the first measurement, which essentially causes a collapse of the system to one of the many states.

- **Unitary Evolution:** Every operation on the quantum state vector is a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2.

$$|\psi'\rangle = U|\psi\rangle$$

Intuitively, a unitary operator is a rotation or reflection of the Hilbert space.

Remark 1.1.1. [16] In continuous time, the evolution of a (closed) quantum system is described by the Schrödinger equation,

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where $\hbar$ is the Planck's constant and H is the Hamiltonian of the system.

1.1.2 Quantum Gates

Just like a classical computer is built from an electrical circuit containing wires and logic gates, a quantum computer is built from a *quantum circuit* containing wires and elementary *quantum gates* to carry around and manipulate the quantum information. Here, we mention some of the important gates for quantum circuits.

Single qubit gates

The quantum *NOT* gate or the X gate in matrix form is given by:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

The above gate takes a state $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|1\rangle + \beta|0\rangle$.

The Z gate given by:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

leaves $|0\rangle$ unchanged but flips the sign of $|1\rangle$ to give $-|1\rangle$.

The Y gate given by:

$$Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

takes $|0\rangle$ to $i|1\rangle$ and $|1\rangle$ to $-i|0\rangle$.

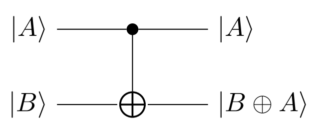
Another important quantum gate is the *Hadamard* gate given by:

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

which turns a $|0\rangle$ into $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ and turns a $|1\rangle$ into $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$. Note that $H^2 = I$ and, thus, applying H twice to a state leaves it unchanged.

Multiple qubit gates

The prototypical multiple-qubit quantum gate is the *controlled-NOT* or *CNOT* gate. This gate has two input qubits, known as the *control* qubit and the *target* qubit, respectively. The circuit representation for the *CNOT* gate is:



The matrix form for the $CNOT$ gate is given by:

$$U_{CN} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The action of the gate is given by $|A, B\rangle \rightarrow |A, B \oplus A\rangle$, where $\oplus$ is addition modulo 2. If the control qubit is set to 0, then the target qubit is left alone. If the control qubit is set to 1, then the target qubit is flipped. Thus,

$$|00\rangle \rightarrow |00\rangle; \quad |01\rangle \rightarrow |01\rangle; \quad |10\rangle \rightarrow |11\rangle; \quad |11\rangle \rightarrow |10\rangle.$$

Remark 1.1.2. [16] An arbitrary quantum computation on any number of qubits can be generated by a finite set of gates that is said to be *universal* for quantum computation. As an example, any multiple qubit logic gate may be composed from $CNOT$ and single qubit gates.

1.1.3 Quantum Parallelism

A small number of particles in superposition states can carry an enormous amount of information. For example, a mere 1000 particles can be in a superposition that represents every number from 1 to 2^{1000}. Thus, there are 2^{1000} possible outcomes (of measuring the particles), or about 10^{300} - more than there are atoms in the visible universe! Thus, we can store 10^{300} numbers on our 1000 particles simultaneously. Then, by performing various operations on the particles and on some auxiliary ones - perhaps hitting them with a sequence of laser pulses or radio waves - we can carry out an algorithm that transforms all 10^{300} numbers (each one a potential solution) at the same time. If after doing that we could read out the particles' final quantum state accurately, our computer would be able to check 10^{300} possible solutions to a problem and at the end we could quickly discern the right one.

However, the rules of quantum mechanics dictate that the measurement will pick out just one of the 10^{300} possibilities at random and that all the others will then disappear. So, to exploit quantum parallelism, a good quantum computer algorithm would ensure that computational paths leading to a wrong answer would cancel out when positive amplitudes combine with negative ones (destructive interference). It would also ensure that the paths leading to a correct answer would all have amplitudes with the same sign - which yields constructive interference and thereby boosts the probability of finding them when the particles are measured at the end [2].

1.1.4 P = NP?

A computational *complexity class* is a collection of computational problems, all of which share some common feature with respect to the computational resources needed to solve those problems. Problems in the class **P** are the ones that computers can solve efficiently in polynomial time. For example, given a road map showing n towns, can one get from any town to every other town? For a large value of n, the number of steps a computer needs to solve this problem increases in proportion to n^2, a polynomial. Because polynomials increase relatively slowly as n increases, computers can solve even very large **P** problems within a reasonable length of time. Problems in the class **NP**, on the other hand, are the ones whose solutions are easy to verify. For example, given an n-digit number, you want to find the prime factors of the number. If you are given the factors, you can verify that they are the answer in polynomial time by multiplying them. Every **P** problem is also an **NP** problem, so the class **NP** contains the class **P** within it. The factoring problem is in **NP** but conjectured to be outside of **P**, because no known algorithm for a standard computer can solve it in only a polynomial number of steps. Instead the number of steps increases exponentially as n gets bigger.

An **NP**-complete problem is one, for which an efficient solution would provide an efficient solution to all NP problems. For example, given a map, can you color it using only three colors so that no neighbouring countries are the same color? If you had an algorithm to solve this problem, you could adapt the algorithm to solve any other **NP** problem in about the same number of steps. In that sense, **NP**-complete problems are the hardest of the **NP** problems. No known algorithm can solve an **NP**-complete problem efficiently. An efficient algorithm for an **NP**-complete problem would mean that the class **P** would equal the class **NP**, i.e. **P** = **NP**. Does such an algorithm exist? This is literally a million dollar question - it carries a $1,000,000 reward from the Clay Math Institute in Cambridge, Massachusetts. This **NP** versus **P** question is one of the most fundamental questions in theoretical computer science and mathematics. The interested reader can further refer to [1].

In 1994, Peter Shor found the first example of a quantum algorithm [21] that could dramatically speed-up the solution of a practical problem, known to be in **NP**, but not in **P**. Shor showed how a quantum computer could factor an n-digit number using a number of steps that increases only as about n^2, i.e. in polynomial time. The best algorithm known for classical computers uses a number of steps that increases exponentially. Note that factoring is not known to be **NP**-complete, otherwise we would already know how to efficiently solve all problems in **NP** using quantum computers. While this is disappointing, this does not rule out that some deeper structure exists in the problems in **NP** that will allow them all to be solved quickly using a quantum computer, thereby essentially rendering $\mathbf{P} = \mathbf{NP}$ [2].

The class of all computational problems which can be solved efficiently on a quantum computer is denoted as **BQP** (*B*ounded error, *Q*uantum, *P*olynomial time), where a bounded probability of error is allowed. The class **PSPACE** consists of those problems which can be solved using resources which are few in spatial size, but not necessarily in time. **PSPACE** is believed to be strictly larger than both **P** and **NP** although this has never been proved. Exactly where **BQP** fits with respect to **P**, **NP** and **PSPACE** is as yet unknown. What is known is that quantum computers can solve all problems in **P** efficiently and some **NP** problems, such as factoring and discrete logarithm problem, but that there are no problems outside of **PSPACE** which they can solve efficiently.

1.1.5 Quantum Information Theory

In quantum mechanics, *quantum information* is physical information that is held in the "state" of a quantum system. The ability to manipulate quantum information enables us to perform tasks that would be unachievable in a classical context, such as unconditionally secure transmission of information. The theory of quantum information is a result of the effort to generalize classical information theory to the quantum world.

Formally, the amount of classical information we gain, on average, when we learn the value of a random variable is represented by a quantity called the *Shannon entropy*, measured in bits. Since information is always embodied in the state of a physical system, we can also think of the Shannon entropy as quantifying the physical resources required to store classical information. Suppose Alice wishes to communicate some classical information to Bob over a classical communication channel. A relevant question concerns the extent to which the message can be compressed without loss of information, so that Bob can reconstruct the original message accurately from the compressed version. According to Shannon's *source coding theorem* or *noiseless coding theorem*, the minimal physical resource required to represent the message is given by the Shannon entropy of the source [5].

What happens if we use the quantum states of physical systems to store information, rather than classical states? It turns out that quantum information is radically different from classical information. For example, while classical information can be copied or cloned, the quantum 'no cloning' theorem asserts the impossibility of cloning an unknown quantum state. As we have seen, an arbitrarily large amount of classical information can be encoded in a qubit. This information can be processed and communicated but, because of the peculiarities of quantum measurement, at most one bit can be accessed! The quantum analogue of the Shannon's theorem is Schumacher's channel coding theorem, that quantifies the resources required to do quantum data compression, with the restriction that it is possible to recover the source with fidelity close to 1. According to a theorem by Holevo, the accessible information in a probability distribution over a set of alternative qubit states is limited by the *von Neumann entropy*, which is equal to the Shannon entropy only when the states are orthogonal in the space of quantum states, and is otherwise less than the Shannon entropy [5].

A challenge faced in quantum information theory is quantum distinguishability. Although classically it is possible to distinguish different items of information at least in principle, quantum mechanically it is not always possible to distinguish between arbitrary states. The indistinguishability of non-orthogonal quantum states is at the heart of quantum computation and quantum information. It is the essence of our assertion that a quantum state contains hidden information that is not accessible to measurement, and thus, plays a key role in quantum algorithms and quantum cryptography.

1.1.6 Entanglement as a resource

Entanglement is one of the properties of quantum mechanics that caused many physicists, including Albert Einstein, to dislike this formulation of quantum mechanical theory. Baffled with such *spooky interactions* between spatially separated physical systems (parts of a compound quantum system), Einstein reckoned that the quantum theory is essentially incomplete and in 1935, alongwith Podolsky and Rosen, formulated the *EPR paradox*. It was Schrödinger who coined the term 'entanglement' to describe this peculiar connection between quantum systems. However, contrary to his supposition of the spontaneous decay of entanglement as two entangled particles separate, Bell's investigation generated an ongoing debate involving confirmation that entanglement can persist over long distances.

It was in the 1980s that physicists, computer scientists, and cryptographers began to regard the non-local correlations of entangled quantum states as a new kind of non-classical resource that could be exploited. Entanglement can be measured, transformed, and purified. A pair of quantum systems in an entangled state can be used as a quantum information channel to perform computational and cryptographic tasks that are impossible for classical systems.

1.2 Objective

The objective of this thesis precisely is to study a compositional characterization of multipartite quantum entangled states.

Multipartite quantum states constitute a key resource for quantum computations and protocols. A recent novel approach for studying various quantum information protocols based on recasting the axiomatic presentation of quantum mechanics, due to von Neumann, at a more abstract level was laid down by Abramsky and Coecke in [3]. Entanglement plays a central role in the majority of these quantum protocols, such as quantum teleportation [17], quantum key distribution [13], logic-gate teleportation [14] and entanglement swapping [25]. However, obtaining a generic, structural understanding of entanglement in arbitrary N-qubit systems is a long-standing open problem in quantum computer science.

1.2.1 State of the Art: Compositional Structure of Entanglement

As a state of the art, it was shown in [11] that multipartite quantum entanglement admits a well-behaved compositional structure and hence is subject to modern computer science methods. In particular, a powerful *GHZ-W graphical calculus* was established, which is found to be expressive enough to generate and reason about representatives of arbitrary N-qubit quantum states. This calculus was also shown to have refined the graphical calculus of complementary observables [8], which was already previously shown to have many applications and admit automation. This result also induces a generalised graph-state paradigm for measurement-based quantum computing (MBQC) [4][12].

1.2.2 Contributions

A GHZ-W pair was shown in [11] to satisfy certain graphical identities in the abstract setting of Frobenius algebras expressed internal to monoidal categories. In this thesis, we further explore graphical equations satisfied by a GHZ-W pair, especially spelling out concretely, where necessary, in the particular case of the category of Hilbert spaces and linear maps. This provides us with a toolkit to reason about interacting GHZ and W states, in particular lending us a way to express a normal form for the same in the graphical paradigm. Based on this, we establish the behaviour of certain whole classes of scalars expressed in the normal form. We also illustrate the pattern for some non-trivial combinations of such graphs but arriving at a normal form for them is out of scope of this thesis, but these results would hopefully pave the way for the same as part of future work.

Chapter 2

Monoidal Categories

> *"I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space any more"* - John von Neumann

After the creator himself denounced the Hilbert space formalism [18], which in many ways is the most successful formalism physics has ever known, there have been attempts without much success to arrive at alternative formalisms, such as 'quantum logic'. In this chapter, we will delve into category theory, with particular focus on monoidal categories and the graphical calculus exhibited by them, that lends us with a 'high-level' abstract alternative to the counter-intuitive Hilbert space formalism.

First, we present the basics of categories and then introduce symmetric and †-symmetric monoidal categories and compact closed categories, also laying out the primitives of the diagrammatic calculus admitted by these categories. We would explicitly treat the category of Hilbert spaces and linear maps as one of prime interest to us and demonstrate its behaviour all along. The interested reader can refer to [9] for more elaborate survey of category theory, in particular monoidal categories, and [20] for a detailed account of the graphical languages for monoidal categories.

2.1 Categories

Categories were introduced and defined by Samuel Eilenberg and Saunders Mac Lane in 1945 as a framework intended to unify a variety of mathematical constructions within different areas of mathematics.

Definition 2.1.1. Category: A (concrete) **category C** consists of:

(i) A family of *objects* $|\mathbf{C}|$;

(ii) For any $A, B \in |\mathbf{C}|$, a set $\mathbf{C}(A, B)$ of *morphisms* called the *hom-set*;

(iii) For any $A, B, C \in |\mathbf{C}|$, and any $f \in \mathbf{C}(A, B) : A \to B$ and $g \in \mathbf{C}(B, C) : B \to C$, a composite $g \circ f \in \mathbf{C}(A, C)$, i.e. for all $A, B, C \in |\mathbf{C}|$ there is a *composition* operation

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

and this composition operation is associative and has units, i.e.

- for any $f \in \mathbf{C}(A, B)$, $g \in \mathbf{C}(B, C)$ and $h \in \mathbf{C}(C, D)$, we have

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

- for any $A \in |\mathbf{C}|$, there exists a morphism $1_A \in \mathbf{C}(A, A)$, called the *identity*, which is such that for any $f \in \mathbf{C}(A, B)$, we have

$$f = f \circ 1_A = 1_B \circ f$$

Example 2.1.2. **Set** is the concrete category with:

- all sets as *objects*
- all functions between sets as *morphisms*
- ordinary *composition of functions*, i.e. for $f : X \to Y$ and $g : Y \to Z$, we have $(g \circ f) := g(f(x))$ for $g \circ f : X \to Z$
- the obvious *identities*, i.e. $1_X(x) := x$.

Example 2.1.3. **Grp** is the concrete category with:

- all groups as *objects*
- all group homomorphisms between these groups as *morphisms*
- ordinary *function composition* (the composite of two group homomorphisms is again a group homomorphism)
- *identity functions*, which are group homomorphisms.

Example 2.1.4. $\mathbf{FdVect}_{\mathbb{K}}$ is the concrete category with:

- all finite dimensional vector spaces over $\mathbb{K}$ as *objects*
- all linear maps between these vector spaces as *morphisms*
- ordinary *composition* of the underlying functions (the composite of two linear maps is again a linear map)
- *identity functions*, which are linear maps.

Example 2.1.5. **Cat** is the concrete category with:

- all categories as *objects*
- all functors between these categories as *morphisms*
- *functor composition*
- *identity functors.*

Remark 2.1.6. The category which would be of prime interest to us in this thesis is the category **FdHilb** with finite dimensional Hilbert spaces as *objects* and with linear maps as *morphisms.* **FdHilb** is a variant of the concrete category $\mathbf{FdVect}_{\mathbb{K}}$ discussed above, since a Hilbert space is a vector space over $\mathbb{C}$ with an inner product

$$\langle -, - \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

Definition 2.1.7. Isomorphism: Two objects $A, B \in |\mathbf{C}|$ are *isomorphic* if there exist morphisms $f \in \mathbf{C}(A, B)$ and $g \in \mathbf{C}(B, A)$, such that $g \circ f = 1_A$ and $f \circ g = 1_B$. The morphism f is called an *isomorphism* and $f^{-1} := g$ is called the *inverse* to f.

Definition 2.1.8. Functor: Let $\mathbf{C}$ and $\mathbf{D}$ be two categories. A (*covariant*) functor $F : \mathbf{C} \to \mathbf{D}$ consists of

- a mapping
$$F : |\mathbf{C}| \to |\mathbf{D}| :: A \mapsto F(A) = FA$$
- for any $A, B \in |\mathbf{C}|$, a mapping
$$F : \mathbf{C}(A, B) \to \mathbf{D}(F(A), F(B)) :: f \mapsto F(f) = Ff$$

which preserves identities and composition, i.e.

– for any $f \in \mathbf{C}(A, B)$ and $g \in \mathbf{C}(B, C)$, we have

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

– for any $A \in |\mathbf{C}|$, we have

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

Remark 2.1.9. A *contravariant* functor $F : \mathbf{C} \to \mathbf{D}$, on the other hand, consists of the same data as a (covariant) functor, it also preserves identities, but 'reverses' composition, i.e.

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

Definition 2.1.10. Opposite Category: The *opposite* category $\mathbf{C^{op}}$ of a category $\mathbf{C}$ is the category with

- the same objects as $\mathbf{C}$,
- in which morphisms are 'reversed', i.e.

$$f \in \mathbf{C}(A, B) \Leftrightarrow f^{op} \in \mathbf{C^{op}}(B, A)$$

- identities in $\mathbf{C^{op}}$ are those of $\mathbf{C}$, and
- $f^{op} \circ g^{op} = (g \circ f)^{op}$

Remark 2.1.11. Contravariant functors of type $\mathbf{C} \to \mathbf{D}$ can now be defined as covariant functors of type $\mathbf{C^{op}} \to \mathbf{D}$.

2.2 Symmetric Monoidal Categories

Definition 2.2.1. A **Symmetric Monoidal Category** (SMC) consists of:

(i) a *category* $\mathbf{C}$,

(ii) a *unit object* $\mathbf{I} \in |\mathbf{C}|$,

(iii) a *bifunctor* $- \otimes -$, called the tensor, that is an operation both on

- objects

$$- \otimes - : |\mathbf{C}| \times |\mathbf{C}| \to |\mathbf{C}| :: (A, B) \mapsto A \otimes B$$

  and

- morphisms

$$- \otimes - : \mathbf{C}(A, B) \times \mathbf{C}(C, D) \to \mathbf{C}(A \otimes C, B \otimes D) :: (f, g) \mapsto f \otimes g$$

The bifunctor also satisfies

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

and

$$1_A \otimes 1_B = 1_{A \otimes B}$$

for all $A, B \in |\mathbf{C}|$ and all morphisms f, g, h, k with appropriate matching types.

(iv) three *natural isomorphisms*:

- *Associativity*:

$$\alpha = \{A \otimes (B \otimes C) \xrightarrow{\alpha_{A,B,C}} (A \otimes B) \otimes C \mid A, B, C \in |\mathbf{C}|\}$$

- *Left Unit*:

$$\lambda = \{A \xrightarrow{\lambda_A} \mathbf{I} \otimes A \mid A \in |\mathbf{C}|\}$$

- *Right Unit*:

$$\rho = \{A \xrightarrow{\rho_A} A \otimes \mathbf{I} \mid A \in |\mathbf{C}|\}$$

such that $\lambda_{\mathbf{I}} = \rho_{\mathbf{I}}$ and the following diagrams commute

$$\begin{tikzcd}
A \otimes (B \otimes C) \arrow[r, "\alpha_{A,B,C}"] \arrow[d, "f \otimes (g \otimes h)"'] & (A \otimes B) \otimes C \arrow[d, "(f \otimes g) \otimes h"] \\
A' \otimes (B' \otimes C') \arrow[r, "\alpha_{A',B',C'}"] & (A' \otimes B') \otimes C'
\end{tikzcd} \tag{2.1}$$

$$
\begin{tikzcd}
A \arrow[r, "\lambda_A"] \arrow[d, "f"'] & \mathbf{I} \otimes A \arrow[d, "1_{\mathbf{I}} \otimes f"] \\
B \arrow[r, "\lambda_B"] & \mathbf{I} \otimes B
\end{tikzcd}
\tag{2.2}
$$

$$
\begin{tikzcd}
A \arrow[r, "\rho_A"] \arrow[d, "f"'] & A \otimes \mathbf{I} \arrow[d, "f \otimes 1_{\mathbf{I}}"] \\
B \arrow[r, "\rho_B"] & B \otimes \mathbf{I}
\end{tikzcd}
\tag{2.3}
$$

$$
\begin{tikzcd}
A \otimes B \arrow[r, "1_A \otimes \lambda_B"] \arrow[dr, "\rho_A \otimes 1_B"'] & A \otimes (\mathbf{I} \otimes B) \arrow[d, "\alpha_{A,\mathbf{I},B}"] \\
 & (A \otimes \mathbf{I}) \otimes B
\end{tikzcd}
\tag{2.4}
$$

(v) a fourth *natural isomorphism* called *Symmetry*:

$$\sigma = \{A \otimes B \xrightarrow{\sigma_{A,B}} B \otimes A \mid A, B \in |\mathbf{C}|\}$$

such that the following diagrams commute for all $A, B \in |\mathbf{C}|$:

$$
\begin{tikzcd}
A \otimes B \arrow[r, "\sigma_{A,B}"] \arrow[d, "f \otimes g"'] & B \otimes A \arrow[d, "g \otimes f"] \\
C \otimes D \arrow[r, "\sigma_{C,D}"] & D \otimes C
\end{tikzcd}
\tag{2.5}
$$

$$
\begin{tikzcd}
A \otimes B \arrow[r, "\sigma_{A,B}"] \arrow[dr, "1_{A \otimes B}"'] & B \otimes A \arrow[d, "\sigma_{B,A}"] \\
 & A \otimes B
\end{tikzcd}
\tag{2.6}
$$

$$
\begin{tikzcd}
A \arrow[r, "\lambda_A"] \arrow[dr, "\rho_A"'] & \mathbf{I} \otimes A \arrow[d, "\sigma_{\mathbf{I},A}"] \\
& A \otimes \mathbf{I}
\end{tikzcd}
\tag{2.7}
$$

(vi) Special morphisms $\psi : \mathbf{I} \to A$ called *elements*, $\phi : A \to \mathbf{I}$ called *co-elements* and $s : \mathbf{I} \to \mathbf{I}$ called *scalars*.

Remark 2.2.2. A symmetric monoidal category is called *strict* if the three natural isomorphisms, viz. associativity, left unit and right unit, are actually equalities.

2.3 †-Symmetric Monoidal Categories

Definition 2.3.1. A **†-Symmetric Monoidal Category C** is a symmetric monoidal category which is equipped with an identity-on-objects contravariant involutive functor

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

such that the functor preserves the tensor, i.e.

$$(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$$

and all unit, associativity and symmetry natural isomorphisms are *unitary*.

We refer to $f^\dagger : B \to A$ as the *adjoint* to $f : A \to B$. A morphism $U : A \to B$ in a †-monoidal category $\mathbf{C}$ is *unitary*, if its inverse and its adjoint coincide, i.e. $U^\dagger = U^{-1}$.

Remark 2.3.2. The category **FdHilb** admits two †-symmetric monoidal structures, respectively given by the tensor product $\otimes$, and by the direct sum $\oplus$. In both cases, the dagger functor

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

- is identity-on-object, i.e.

$$\dagger : |\mathbf{FdHilb^{op}}| \to |\mathbf{FdHilb}| :: \mathcal{H} \mapsto \mathcal{H}$$

- assigns morphisms to their adjoints, i.e.

$$\dagger : \mathbf{FdHilb}^{\mathbf{op}}(\mathcal{H}, \mathcal{K}) \to \mathbf{FdHilb}(\mathcal{K}, \mathcal{H}) :: f \mapsto f^{\dagger}$$

- is contravariant, since for $f \in \mathbf{FdHilb}(\mathcal{H}, \mathcal{K})$ and $g \in \mathbf{FdHilb}(\mathcal{K}, \mathcal{L})$,

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

- is involutive, since for all morphisms f,

$$f^{\dagger\dagger} = f$$

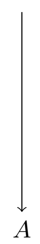
2.4 Graphical Calculus for SMCs

A remarkable feature of SMCs is the fact that they admit a purely diagrammatic calculus, which would be a central focus of this thesis. The corresponding axioms discussed above for SMCs or any other abstract categorical structure become very intuitive graphical manipulations. Thus, such a graphical language, as we will see further substantially in the rest of this thesis, drastically trivialises algebraic manipulations, which could, in general, be very complicated.

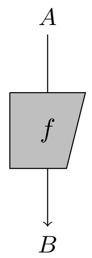
The graphical counterparts to the symmetric monoidal and the †-symmetric monoidal structures are outlined below:

(i) The *identity* $1_{\mathbf{I}}$ is the 'empty' picture.

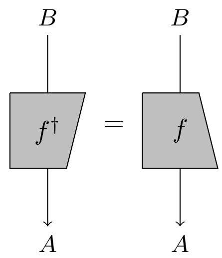
(ii) The *identity* 1_A for an object A different from $\mathbf{I}$ is depicted as



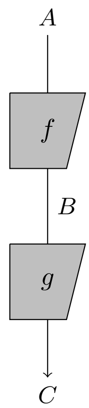
(iii) A *morphism* $f : A \to B$ is depicted as



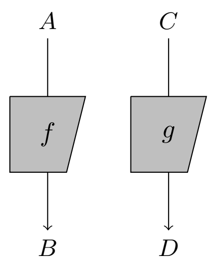
(iv) The *adjoint* $f^\dagger : B \to A$ is depicted as



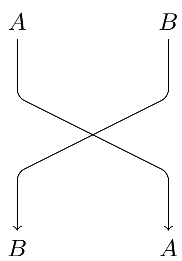
(v) The *composition* of morphisms $f : A \to B$ and $g : B \to C$ is depicted as



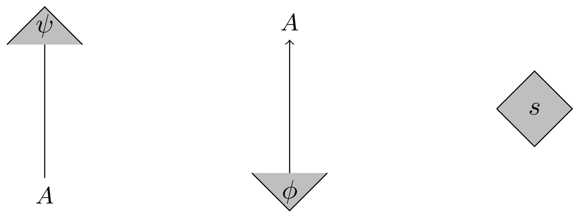
(vi) The *tensor* of morphisms $f : A \to B$ and $g : C \to D$ is depicted as



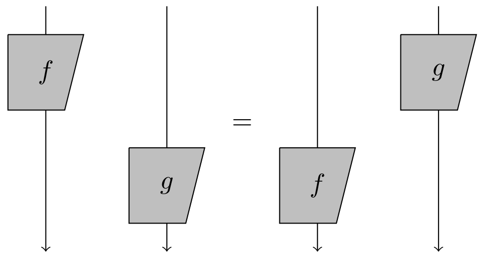
(vii) The *symmetry* $\sigma_{A,B} : A \otimes B \to B \otimes A$ is depicted as



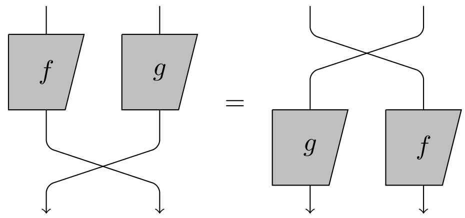
(viii) The *elements* $\psi : \mathbf{I} \to A$, *co-elements* $\phi : A \to \mathbf{I}$ and *scalars* $s : \mathbf{I} \to \mathbf{I}$ are respectively depicted as:



Remark 2.4.1. We can express the bifunctoriality of $\otimes$ as follows:



and the naturality of σ as follows:



Theorem 2.4.2. *(Coherence for symmetric monoidal categories). A well-formed equation between morphisms in the language of symmetric monoidal categories follows from the axioms of symmetric monoidal categories if and only if it holds, up to isomorphism of diagrams, in the graphical language.*

2.5 Compact Closed Categories

Definition 2.5.1. A **compact closed category C** is a symmetric monoidal category in which every object $A \in |\mathbf{C}|$ comes with

(i) another object A^*, the dual of A,

(ii) a pair of morphisms

$$\mathbf{I} \xrightarrow{d_A} A^* \otimes A \;\; and \;\; A \otimes A^* \xrightarrow{e_A} \mathbf{I}$$

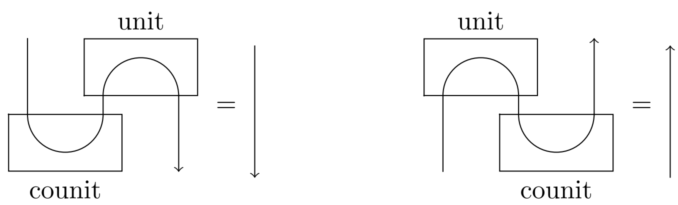
respectively called *unit* and *counit*, which are such that the following two diagrams commute:

$$
\begin{tikzcd}
A \arrow[r, "\rho_A"] \arrow[d, "1_A"'] & A \otimes I \arrow[r, "1_A \otimes d_A"] & A \otimes (A^* \otimes A) \arrow[d, "\alpha_{A,A^*,A}"] \\
A & I \otimes A \arrow[l, "\lambda_A^{-1}"] & (A \otimes A^*) \otimes A \arrow[l, "e_A \otimes 1_A"]
\end{tikzcd}
\tag{2.8}
$$

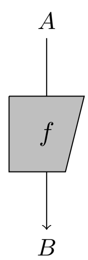
$$
\begin{tikzcd}
A^* \arrow[r, "\lambda_{A^*}"] \arrow[d, "1_{A^*}"'] & I \otimes A^* \arrow[r, "d_A \otimes 1_{A^*}"] & (A^* \otimes A) \otimes A^* \arrow[d, "\alpha^{-1}_{A^*,A,A^*}"] \\
A^* & A^* \otimes I \arrow[l, "\rho^{-1}_{A^*}"] & A^* \otimes (A \otimes A^*) \arrow[l, "1_{A^*} \otimes e_A"]
\end{tikzcd}
\tag{2.9}
$$

Diagrammatically, the unit d_A and counit e_A are respectively depicted as:

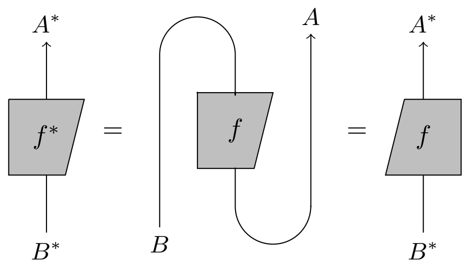
The commutation diagrams now boil down to:



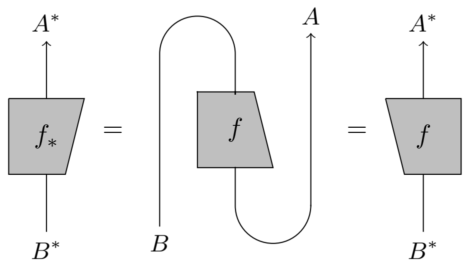
Also, for a morphism $f : A \to B$,



the *transpose* $f^* : B^* \to A^*$ is depicted as:



Remark 2.5.2. We can construct the transpose of the adjoint, or equivalently, the adjoint of the transpose given by $f_* : B^* \to A^*$, called the *conjugate* map, depicted as:



Theorem 2.5.3. *(Coherence for compact closed categories). A well-formed equation between morphisms in the language of compact closed categories follows from the axioms of compact closed categories if and only if it holds, up to isomorphism of diagrams, in the graphical language.*

Definition 2.5.4. A **†-compact closed category C** is both a compact closed category and a †-symmetric monoidal category, such that for all $A \in |\mathbf{C}|$, $e_A = d_A^\dagger \circ \sigma_{A,A^*}$.

Remark 2.5.5. The category **FdHilb** is †-compact closed. Moreover, objects in **FdHilb** are *self-dual*.

Chapter 3

Frobenius Algebras

"There is no royal road to mathematics." - Ferdinand G. Frobenius

In this chapter, we introduce, with due credits to [10], a particularly well-behaved kind of finite dimensional associative algebra called Frobenius algebra that began to be studied in the 1930s by Richard Brauer and Cecil Nesbitt and was named after Ferdinand Frobenius.

Frobenius algebras possess a special kind of *bilinear form* that allows them to exhibit nice duality properties. Frobenius algebras have been shown to have an abstract presentation internal to monoidal categories, that makes our treatment and use of the same in this thesis particularly interesting, owing to the rich graphical language admitted by symmetric monoidal categories.

3.1 Concrete Frobenius Algebras

Definition 3.1.1. For some field k, a *unital associative k-algebra* (A, μ, η) is a k-vector space A with a map $\mu : A \otimes A \to A$ called the *multiplication* and a map $\eta : k \to A$ called the *unit*, such that $\mu \circ (1_A \otimes \mu) = \mu \circ (\mu \otimes 1_A)$ and $\mu \circ (1_A \otimes \eta) = \mu \circ (\eta \otimes 1_A) = 1_A$.

Definition 3.1.2. For some field k, a *counital coassociative k-coalgebra* (B, δ, ϵ) is a k-vector space B with a map $\delta : B \to B \otimes B$ called the *comultiplication* and a map $\epsilon : B \to k$ called the *counit*, such that $(1_B \otimes \delta) \circ \delta = (\delta \otimes 1_B) \circ \delta$ and $(\epsilon \otimes 1_B) \circ \delta = (1_B \otimes \epsilon) \circ \delta = 1_B$.

Let $\sigma_{A,B}$ be the *swap* map: $\sigma_{A,B} : A \otimes B \to B \otimes A$

Then, a k-algebra (resp. k-coalgebra) is *commutative* (resp. *cocommutative*) if and only if $\mu = \mu \circ \sigma_{A,A}$ (resp. $\delta = \sigma_{A,A} \circ \delta$).

Definition 3.1.3. A *Frobenius k-algebra* $(F, \mu, \eta, \delta, \epsilon)$ is a vector space F such that

- (F, μ, η) is a unital associative k-algebra,
- (F, δ, ϵ) is a counital coassociative k-coalgebra, and
- $(\mu \otimes 1_F) \circ (1_F \otimes \delta) = (1_F \otimes \mu) \circ (\delta \otimes 1_F) = \delta \circ \mu$

Example 3.1.4. Let M be the vector space of $n \times n$ matrices. Take μ to be matrix multiplication, which is associative and bilinear. Let η be the $n \times n$ identity matrix, and let $\epsilon : M \to k$ be the trace functional. This data induces a unique map δ such that $(M, \mu, \eta, \delta, \epsilon)$ is a Frobenius k-algebra.

Remark 3.1.5. A Frobenius k-algebra $(F, \mu, \eta, \delta, \epsilon)$ is called a *commutative Frobenius algebra* (CFA), if moreover, (F, μ, η) is commutative and (F, δ, ϵ) is cocommutative.

3.2 Internal Frobenius Algebras

Frobenius algebras can also be formulated in a much more general setting where they are defined *internal* to a category $\mathbf{C}$.

Definition 3.2.1. Internal Monoid: A monoid internal to a monoidal category $(\mathbf{C}, \otimes, \mathbf{I})$, is an object A and a pair of maps $\mu : A \otimes A \to A$ called multiplication and $\eta : \mathbf{I} \to A$ called the unit.

Multiplication is associative, so this diagram commutes:

$$\begin{tikzcd}
(A \otimes A) \otimes A \arrow[r, "\mu \otimes 1_A"] \arrow[d, "\alpha_{A,A,A}"] & A \otimes A \arrow[dr, "\mu"] & \\
 & & A \\
A \otimes (A \otimes A) \arrow[r, "1_A \otimes \mu"] & A \otimes A \arrow[ur, "\mu"'] &
\end{tikzcd} \tag{3.1}$$

Multiplication is left and right unital, so this diagram also commutes:

$$\begin{tikzcd}
I \otimes A \arrow[d, "\eta \otimes 1_A"'] & A \arrow[l, "\lambda"'] \arrow[r, "\rho"] & A \otimes I \arrow[d, "1_A \otimes \eta"] \\
A \otimes A \arrow[ur, "\mu"] & & A \otimes A \arrow[ul, "\mu"']
\end{tikzcd} \tag{3.2}$$

Definition 3.2.2. Internal Comonoid: A comonoid internal to a monoidal category $(\mathbf{C}, \otimes, \mathbf{I})$, is an object A and a pair of maps $\delta : A \to A \otimes A$ called comultiplication and $\epsilon : A \to \mathbf{I}$ called the counit.

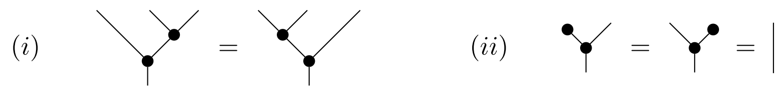
Coassociativity:

$$\begin{tikzcd} & A \otimes A \arrow[r, "\delta \otimes 1_A"] & (A \otimes A) \otimes A \arrow[d, "\alpha_{A,A,A}"] \\ A \arrow[ur, "\delta"] \arrow[dr, "\delta"'] & & \\ & A \otimes A \arrow[r, "1_A \otimes \delta"] & A \otimes (A \otimes A) \end{tikzcd} \tag{3.3}$$

Counit:

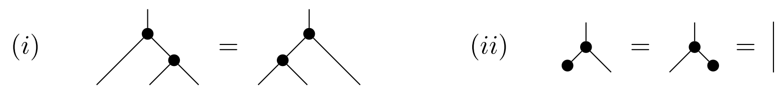
$$\begin{tikzcd} I \otimes A & A \arrow[l, "\lambda"'] \arrow[r, "\rho"] \arrow[dl, "\delta"] \arrow[dr, "\delta"'] & A \otimes I \\ A \otimes A \arrow[u, "\epsilon \otimes 1_A"] & & A \otimes A \arrow[u, "1_A \otimes \epsilon"'] \end{tikzcd} \tag{3.4}$$

Graphically, by depicting μ and η as and , respectively, the axioms of a monoid $(A, ,)$ can be expressed as follows:



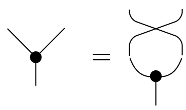
(3.5)

By depicting δ and ϵ as and , respectively, the axioms of a comonoid $(A, ,)$ are just the previous ones, upside-down:

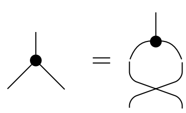


(3.6)

Moreover, if the monoid is commutative, i.e. $\mu = \mu \circ \sigma_{A,A}$, then graphically, we have:



Similarly, if the comonoid is cocommutative, i.e. $\delta = \sigma_{A,A} \circ \delta$, then graphically, we have:

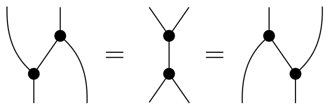


Since the notion of internal monoid and comonoid gives us an abstract way to define k-algebras and k-coalgebras, we also have an abstract way to define Frobenius algebras:

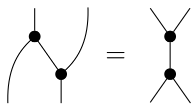
Definition 3.2.3. Internal Frobenius Algebra: A Frobenius algebra *internal* to a monoidal category $\mathbf{C}$ is an object A and four maps $\mu, \eta, \delta, \epsilon$, such that

- (A, μ, η) is an internal monoid,
- (A, δ, ϵ) is an internal comonoid, and
- $(\mu \otimes 1_A) \circ (1_A \otimes \delta) = \delta \circ \mu = (1_A \otimes \mu) \circ (\delta \otimes 1_A)$

Graphically, the third condition (*Frobenius law*) becomes:



Remark 3.2.4. A Frobenius algebra internal to a symmetric monoidal category (SMC) $\mathbf{C}$ is moreover a *commutative Frobenius algebra* (CFA), since the internal monoid (A, μ, η) is commutative and the internal comonoid (A, δ, ϵ) is cocommutative. The *Frobenius law* then simplifies to:



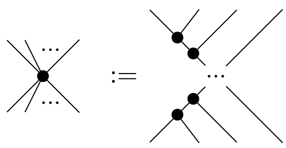
3.3 Spider Notation

Definition 3.3.1. [11] For a CFA $A = (A, \mu, \eta, \delta, \epsilon)$, an *A-graph* is a morphism obtained from the following maps: 1_A, $\sigma_{A,A}$, $\alpha_{A,A,A}$, μ, η, δ, and ϵ, combined with composition and the tensor product. An A-graph is said to be *connected* precisely when its graphical representation is connected.

Theorem 3.3.2. *Any connected A-graph is uniquely and completely determined by its number of inputs, number of outputs and number of loops.*

This makes CFAs highly topological, in that A-graphs are invariant under deformations that respect the number of loops. It follows easily from this fact that any A-graph has a normal form.

In the special case where there are 0 loops, the following notational simplification, called the *spider* notation was made in [11]:

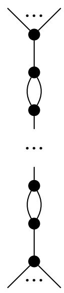
$S_m^n =$ 

Note that $S_m^0 := S_m^1 \circ$ and $S_0^n := \circ S_1^n$.

Thus, it follows that any connected A-graph for a CFA A admits the *normal form*:

$$S_n^1 \circ (\mu \circ \delta) \circ (\mu \circ \delta) \circ \ldots \circ (\mu \circ \delta) \circ S_1^m$$

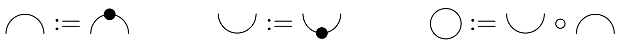
i.e. any connected CFA-morphism can be graphically written like this:



(3.7)

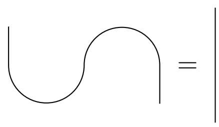
In particular, the following maps, called *cap* and *cup*, respectively, can be constructed:

For caps and cups, the dots are usually omitted when there is no ambiguity:



For CFAs it is also assumed that circles admit an inverse [1], i.e. $= 1_I$.

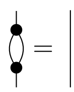
Corollary 3.3.3. *Any object admitting a commutative Frobenius algebra admits a* ***self-dual compact*** *structure, i.e.*



3.4 Special and anti-special CFAs

Let $\mathbf{C}$ be a symmetric monoidal category.

Definition 3.4.1. A *special* commutative Frobenius algebra (SCFA) on $\mathbf{C}$ is a CFA $(A, \mu, \eta, \delta, \epsilon)$, such that $\mu \circ \delta = 1$. Graphically,



(3.8)

Definition 3.4.2. An *anti-special* commutative Frobenius algebra (ACFA) on $\mathbf{C}$ is a CFA $(A, \mu, \eta, \delta, \epsilon)$, such that the following diagram commutes:

[1] In **FdHilb**, $= D$, the dimension of the underlying Hilbert space and so, $= \frac{1}{D}$.

$$
\begin{tikzcd}
A \otimes A \arrow[r, "\delta \otimes \delta"] & (A \otimes A) \otimes (A \otimes A) \arrow[r, "\mu \otimes \mu"] & A \otimes A \arrow[d, "\epsilon \otimes 1_A"] \\
A \cong I \otimes A \arrow[u, "\eta \otimes 1_A"] & & A \cong I \otimes A \arrow[d] \\
A \arrow[u] \arrow[d, "\delta"] & & A \\
A \otimes A \arrow[d, "\mu"] & & A \otimes A \arrow[u, "\mu"'] \\
A \arrow[r, "\epsilon"] & I \arrow[r, "\eta"] & A \arrow[u, "\delta"']
\end{tikzcd}
$$

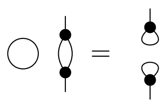
We denote $\qquad \widehat{\eta} = \mu\delta\eta, \qquad \widehat{\epsilon} = \epsilon\mu\delta$

and refer to these respectively, as the *anti-unit* and *anti-counit*.

Graphically, these are:

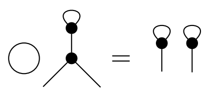
So, the commutativity boils down to the equation $\epsilon\mu\delta\eta \otimes \mu\delta = \widehat{\eta}\widehat{\epsilon}$.

Graphically, this condition is:



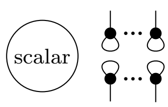
(3.9)

Remark 3.4.3. The difference between a SCFA and an ACFA is, thus, essentially topological, in terms of 'connected vs. disconnected'.

Lemma 3.4.4. *[11] (Loop copy). For any ACFA, we have:* 

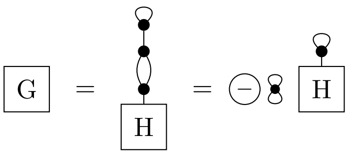
We now state a theorem below about the nature of any CFA morphism for SCFAs and ACFAs, the proof for which can be found in [11]. However, here we reproduce the proof again but spelling out explicitly the scalar involved.

Theorem 3.4.5. *Let* **C** *be any SMC. For a SCFA on* **C**, *any connected CFA-morphism is equal to a spider, for an ACFA, any connected CFA-morphism is either equal to a spider or of the following form:*

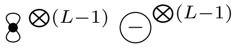


Proof. (SCFA) Substituting Eq (3.8) in Eq (3.7) removes all loops, yielding a spider.

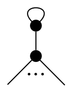
(ACFA) If Eq (3.7) has no loops, then it is a spider. If it has two or more loops, it can be reduced to a product of a graph with one loop and copies of . Suppose some graph G has $L \geq 2$ loops. Then, we can find an equivalent graph with one fewer loop.



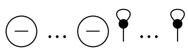
By induction, we can always rewrite a connected graph G to  or another graph with at most one loop.

If the graph has zero inputs and zero outputs, then the above result suffices to find a normal form. Moreover, the scalar would be , where L is the number of loops.

Now, suppose the graph has zero inputs, at least one output, and exactly one loop. Then, it must be of the form:

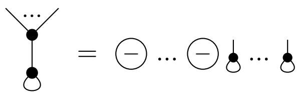


By Lemma (3.4.4), this can be written as:



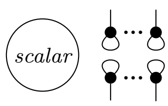
The number of copies of  above would be equal to $O - 1$, where O is the number of outputs.

The case of at least one input, zero outputs, and one loop is treated similarly:

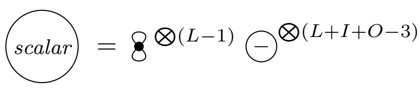


and the number of copies of  would be equal to $I - 1$, where I is the number of inputs.

Thus, it follows that in the general case, where the $ACFA$-morphism has I inputs, O outputs and L loops, it is of the form:



where the scalar is given by:



□

Chapter 4

Quantum Entanglement

"God does not play dice." - Albert Einstein

Entanglement is a key resource in quantum computation and is at the root of the most surprising quantum phenomena. Spatially separated compound quantum systems exhibit correlations under measurement, which cannot be explained by classical physics. For reasons which nobody fully understands, entanglement plays a crucial role in the usage of quantum systems to process information in tasks such as cryptographic key distribution, quantum teleportation, quantum communication and superdense coding.

For Hilbert spaces $\mathcal{H}_i$, $i = 1, ..., n$, let $|\Psi\rangle \in \bigotimes \mathcal{H}_i$ be a state. If there exist states $|\psi_i\rangle \in \mathcal{H}_i$ such that $|\Psi\rangle = \bigotimes |\psi_i\rangle$, $|\Psi\rangle$ is said to be *separable*. If no such states exist, $|\Psi\rangle$ is said to be *entangled*.

Consider the two qubit state

$$|Bell\rangle = |00\rangle + |11\rangle$$

Since there are no single qubit states $|a\rangle$ and $|b\rangle$ such that $|\Psi\rangle = |a\rangle \otimes |b\rangle$, we say that $|\Psi\rangle$ is a (bi-partite) entangled state. On the other hand, the states $|00\rangle$ and $|11\rangle$ individually are separable.

4.1 Degeneracy

Let us take the state $|\Psi\rangle \in \bigotimes \mathcal{H}_i$ considered above. We say that $|\Psi\rangle$ is a *degenerate* n-partite entangled state if there exist non-trivial states $|\Phi_1\rangle$, $|\Phi_2\rangle$ such that $|\Psi\rangle = |\Phi_1\rangle \otimes |\Phi_2\rangle$. If there are no such states, $|\Psi\rangle$ is said to be a *genuine* or *non-degenerate* n-partite entangled state.

In $\mathbb{C}^2 \otimes \mathbb{C}^2$, two examples of genuine bipartite entangled states are the *Bell* state $|Bell\rangle =$

$|00\rangle + |11\rangle$ and the EPR state $|EPR\rangle = |10\rangle + |01\rangle$. On the other hand, the tripartite state

$$|\psi\rangle = |100\rangle + |111\rangle$$

is degenerate, since $|\psi\rangle$ can be expressed as

$$|\psi\rangle = |1\rangle \otimes (|00\rangle + |11\rangle)$$

4.2 Example: Quantum Teleportation

In this section we discuss an example protocol (from [16]) where entanglement is used as a resource.

Quantum teleportation is the technique for sending a quantum state from one party to another distant party even in the absence of a quantum communications channel between the sender and the recipient.

The two distant parties, Alice and Bob, share a Bell state and each of them possesses one qubit of the entangled state. Alice now needs to send an unknown qubit $|\psi\rangle$ to Bob and can only send classical information to Bob. The laws of quantum mechanics prevent her from determining the state when she only has a single copy of $|\psi\rangle$ in her possession. Even if she did know $|\psi\rangle$, it would take forever for her to describe the state to Bob, since $|\psi\rangle$ takes values in a continuous space and so describing it would precisely take an infinite amount of classical information. The quantum teleportation protocol, however, allows Alice to utilize the entangled Bell state in order to send $|\psi\rangle$ to Bob, with only a small overhead of classical communication.

Let the state to be teleported be $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are unknown amplitudes. Alice interacts the qubit $|\psi\rangle$ with her half of the shared Bell state, thus obtaining

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\Big]$$

Alice's second qubit and Bob's qubit start out in the Bell state.

Alice sends her qubits through a $CNOT$ gate, obtaining

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\Big]$$

She then sends the first qubit through a Hadamard gate, obtaining

$$|\psi_2\rangle = \frac{1}{2}\Big[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|00\rangle + |11\rangle)\Big]$$

$$= \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big]$$

If Alice now performs a measurement, Bob's qubit will end up in one of the following four possible states, depending on Alice's measurement outcome:

$$00 \mapsto \big[\alpha|0\rangle + \beta|1\rangle\big]$$

$$01 \mapsto \big[\alpha|1\rangle + \beta|0\rangle\big]$$

$$10 \mapsto \big[\alpha|0\rangle - \beta|1\rangle\big]$$

$$11 \mapsto \big[\alpha|1\rangle - \beta|0\rangle\big]$$

Alice then classically communicates her measurement outcome (2 bits) to Bob, who can recover $|\psi\rangle$ by applying the appropriate quantum gate. If the measurement is 00, then Bob's system will be in the state $|\psi\rangle$ and he needs to do nothing. If the measurement is 01, then Bob can recover $|\psi\rangle$ by applying the X-gate to his qubit. If the measurement is 10, he can recover $|\psi\rangle$ by applying the Z-gate to his qubit. If the measurement is 11, then he can recover $|\psi\rangle$ by applying first an X and then a Z-gate to his qubit.

4.3 Equivalence Classes

It is of special interest in quantum information theory (QIT) to classify multipartite states into equivalence classes, such that states in the same equivalence class are suited to implement the same tasks. Such equivalent states are then said to have the same kind of entanglement. A multipartite state is the entangled state of a composite system shared between multiple parties that are spatially separated from each other. Here we discuss two types of equivalence relations defined in the set of entangled states that have been of interest in quantum information theory.

4.3.1 LOCC Equivalence

When the parties sharing an entangled state are allowed to only perform physical operations locally to their subsystems and typically allowed to communicate only through a classical channel, it is still possible for the parties to modify the entanglement properties of the composite system and, in particular, to convert one entangled state into another.

Definition 4.3.1. If two states can be deterministically inter-converted with only local (one-qubit) physical operations and classical communication, they are said to be *LOCC-equivalent.*

In other words, any two states are identified as LOCC-equivalent if they can be obtained from each other with certainty by means of local operations and classical communication (LOCC). No quantum communication between the parties is allowed. The parties can use two LOCC-equivalent states indistinctively for *exactly* the same tasks of quantum information theory [23].

The following theorem holds when the classification concerns the entanglement properties of a single copy of the state.

Theorem 4.3.2. *Two states $|\psi\rangle$ and $|\phi\rangle$ are* ***LOCC-equivalent*** *if and only if there exist local unitary maps U_i such that $|\psi\rangle = (U_1 \otimes U_2 \otimes ... \otimes U_n)|\phi\rangle$.*

For example, $|Bell\rangle = |00\rangle + |11\rangle$ and $|EPR\rangle = |01\rangle + |10\rangle$ are LOCC-equivalent, but they are not LOCC-equivalent to $\frac{1}{3}|00\rangle + \frac{2}{3}|11\rangle$.

4.3.2 SLOCC Equivalence

As discussed earlier, for single copies, two pure states $|\psi\rangle$ and $|\phi\rangle$ can be obtained from each other by means of LOCC iff they are related by local unitaries. However, even in the simplest bipartite systems, $|\psi\rangle$ and $|\phi\rangle$ are typically not related by local unitaries, and continuous parameters are needed to label all equivalence classes, i.e. one has to deal with infinitely many kinds of entanglement.

An alternative classification is possible if we just demand that the conversion of the states is through stochastic local operations and classical communication (SLOCC), i.e. through LOCC but without imposing that it has to be achieved with certainty.

Definition 4.3.3. If two states can be inter-converted with only local (one-qubit) physical operations and classical communication, but only with some non-zero probability, they are said to be *SLOCC-equivalent.*

In other words, two states $|\psi\rangle$ and $|\phi\rangle$ are SLOCC-equivalent if the parties have a non-vanishing probability of success when trying to convert $|\psi\rangle$ into $|\phi\rangle$ and also $|\phi\rangle$ into $|\psi\rangle$. Both these states can also be used to implement the same tasks of quantum information theory, but this time the probability of a successful performance of the task may differ from $|\phi\rangle$ to $|\psi\rangle$ [23].

Theorem 4.3.4. *[22] Two states $|\psi\rangle$ and $|\phi\rangle$ are* ***SLOCC-equivalent*** *if and only if there exist local invertible maps L_i such that $|\psi\rangle = (L_1 \otimes L_2 \otimes ... \otimes L_n)|\phi\rangle$.*

For example, although $|Bell\rangle$ and $|EPR\rangle$ are not LOCC-equivalent to $\frac{1}{3}|00\rangle + \frac{2}{3}|11\rangle$, all three are SLOCC-equivalent. Thus, for bipartite entanglement, there is exactly one SLOCC equivalence class, viz. $|Bell\rangle = |00\rangle + |11\rangle$.

4.4 GHZ and W states

It was shown in [23] that for pure states of three qubits, there are exactly two SLOCC equivalence classes of genuine tripartite entanglement. The first is witnessed by a 3-qubit generalisation of the Bell state, called the *Greenberger-Horne-Zeilinger (GHZ)* state:

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

and the second is witnessed by the W state:

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

Both of these states are symmetric tripartite maximally entangled states. However, with the $|GHZ\rangle$ state, when one of the qubits is traced out, then the remaining two are completely unentangled. This means, in particular, that if one of the three parties sharing the system decides not to co-operate with the other two, then they cannot use at all the entanglement resources of the state. The same happens if for some reason the information about one of the qubits is lost. Thus, the entanglement properties of the $|GHZ\rangle$ state are very fragile under particle losses [23].

On the other hand, the entanglement of the $|W\rangle$ state is maximally robust under disposal of any of the three qubits, i.e. the remaining reduced density matrices [1] ρ_{AB}, ρ_{BC} and ρ_{AC} retain the greatest possible amount of entanglement, compared to any other state of three qubits, either pure or mixed. This means, in particular, that if one of the three parties, say Alice, decides not to co-operate with the other two, Bob and Claire, and Alice tries to destroy the entanglement between Bob and Claire, this would not be possible, since any local action on qubit A (owned by Alice)

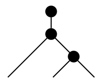
[1] The reduced density matrix ρ_{AB} of a pure tripartite state $|\psi\rangle$ is defined as $\rho_{AB} \equiv tr_C(|\psi\rangle\langle\psi|)$

cannot prevent Bob and Claire from sharing, at least, the entanglement between qubits B and C (owned by Bob and Claire respectively) contained in ρ_{BC} [23].

Thus, intuitively, all of the entanglement present in $|W\rangle$ is due to pairwise correlations between each of the three qubits, unlike in the case of $|GHZ\rangle$, for which the entanglement is solely due to a true tripartite correlation.

4.4.1 GHZ and W states as Commutative Frobenius Algebras

Let us consider the below graph:

$S_3^0 =$ $:=$  (4.1)

Let $(\mathbb{C}^2, , , ,)$ be a CFA in **FdHilb**, where **FdHilb** is the symmetric monoidal category of finite-dimensional Hilbert spaces, linear maps, the tensor product and with $\mathbb{C}$ as the tensor unit. Since is a map from $\mathbb{C}^2$ to $\mathbb{C}^2 \otimes \mathbb{C}^2$ and is a map from the tensor unit $\mathbb{C}$ to $\mathbb{C}^2$, Eq. (4.1) is a map $\Psi : \mathbb{C} \to \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. We can interpret this map as a ket, simply taking $\Psi(1) = |\Psi\rangle$. The point is every Frobenius algebra can be canonically associated with a state [10].

Special CFAs are GHZ states

Theorem 4.4.1. *[11] Each SCFA $\mathcal{G}$ on $\mathbb{C}^2$ in* **FdHilb** *canonically induces a symmetric state in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ which is SLOCC-equivalent to $|GHZ\rangle$. Conversely, any symmetric state that is SLOCC-equivalent to $|GHZ\rangle$ arises from a unique SCFA $\mathcal{G}$ on $\mathbb{C}^2$ in* **FdHilb**.

Anti-special CFAs are W states

Theorem 4.4.2. *[11] Each ACFA $\mathcal{W}$ on $\mathbb{C}^2$ in* **FdHilb** *canonically induces a symmetric state in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ which is SLOCC-equivalent to $|W\rangle$. Conversely, any symmetric state that is SLOCC-equivalent to $|W\rangle$ arises from a unique ACFA $\mathcal{W}$ on $\mathbb{C}^2$ in* **FdHilb**.

Induced CFAs in FdHilb for GHZ and W states

For the GHZ-state the induced SCFA is:

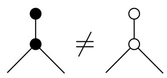
$$\begin{aligned} &= |0\rangle\langle 00| + |1\rangle\langle 11| & &= |+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= |00\rangle\langle 0| + |11\rangle\langle 1| & &= \langle +| := \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|) \end{aligned} \tag{4.2}$$

and for the W-state the induced ACFA is:

 $= |1\rangle\langle 11| + |0\rangle\langle 01| + |0\rangle\langle 10|$ $= |1\rangle$

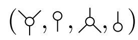
 $= |00\rangle\langle 0| + |01\rangle\langle 1| + |10\rangle\langle 1|$ $= \langle 0|$ (4.3)

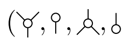
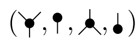
Remark 4.4.3. The cups and caps induced by each CFA in general do not coincide, e.g.

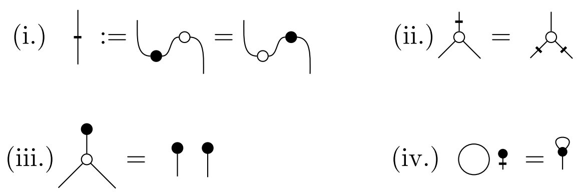
$|10\rangle + |01\rangle =$  $= |00\rangle + |11\rangle$

Therefore explicit dots were introduced in order to distinguish them.

4.4.2 General multipartite states

The structure of either an SCFA or ACFA alone generates only the non-degenerate multipartite states canonically analogous to GHZ and W states, respectively. However, combining these two gives rise to a wealth of states as shown in [11]. For the specific cases of the GHZ-SCFA and the W-ACFA as in Eqs (4.2) and (4.3), there are many equations which connect  and . What is of interest to us here is a small subset of these that helped to show that representatives of all known multipartite SLOCC-classes arise from the interaction of a SCFA with an ACFA.

Definition 4.4.4. [11] A *GHZ/W-pair* consists of a SCFA  and an ACFA  which satisfy the following four equations.



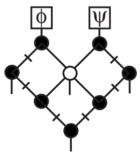
In **FdHilb** these conditions have a clear interpretation. By compactness of cups and caps, the first condition implies that a 'tick' on a wire is self-inverse which together with the second condition implies that it is a permutation of the copiable points of the SCFA. The third condition asserts that  is a copiable point. The fourth condition implies that  is also a (scaled) copiable point since it is the result of applying a permutation to a scalar multiple of .

The following are two examples of arbitrary N-partite states clearly arising out of interaction of SCFAs with ACFAs:

It was shown in [23] that there are essentially infinite SLOCC classes for 4 qubits or more. To be able to finitely classify multipartite states for $N \geq 4$, SLOCC *super-classes* were introduced representing families of SLOCC classes parameterised by one or more continuous variables. The heavy-handed inductive classification scheme established in [19] can be realised by the more intuitive graphical language of GHZ/W-pairs. Below we state a result illustrated in [11] that would give the reader an idea how all genuine new kinds of entanglement arise from the GHZ/W-calculus only.

Proposition 4.4.5. *[11] Given a representative of a SLOCC-class we can reproduce the whole SLOCC-class when we augment the GHZ/W-calculus with 'variables', i.e. single-qubit states. In other words, if we adjoin variables to the graphical language of GHZ/W-pairs, then any N-qubit entangled state can be written in this graphical language.*

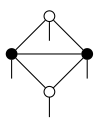
For example, the following graph



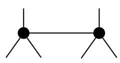
represents the parameterised SLOCC-superclass

$$|0\rangle(\underbrace{(|00\rangle + |1\psi\rangle)}_{\overset{\text{SLOCC}}{\simeq}|Bell\rangle}|\phi\rangle) + |1\rangle|0\rangle|Bell\rangle$$

Let us now witness here the construction of the following much simpler representative of a SLOCC-superclass for 4 qubits.



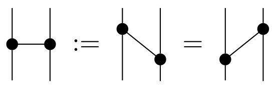
We start by constructing the following graph



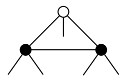
which can be easily verified to be

$$(|01\rangle|01\rangle + |10\rangle|01\rangle + |01\rangle|10\rangle + |10\rangle|10\rangle + |00\rangle|00\rangle)\langle 0|\langle 0| + (|00\rangle|00\rangle)\langle 1|\langle 1|$$

where:



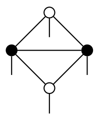
Next we include  $= |0\rangle|00\rangle + |1\rangle|11\rangle$ into the graph to obtain:



which clearly is

$$|0\rangle(|01\rangle|01\rangle + |10\rangle|01\rangle + |01\rangle|10\rangle + |10\rangle|10\rangle + |00\rangle|00\rangle) + |1\rangle(|00\rangle|00\rangle)$$

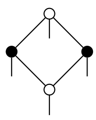
Finally, upon plugging $= |0\rangle\langle 00| + |1\rangle\langle 11|$ at the bottom of the graph, we obtain the desired graph:



which clearly can now be computed to be the SLOCC-superclass:

$$|0\rangle \underbrace{(|000\rangle + |101\rangle + |010\rangle)}_{\overset{\text{SLOCC}}{\simeq}|W\rangle} + |1\rangle|000\rangle$$

On the other hand, the following graph:

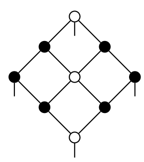


represents the SLOCC-superclass [11]:

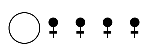
$$|0\rangle \underbrace{(|000\rangle + |111\rangle)}_{\overset{\text{SLOCC}}{\simeq}|GHZ\rangle} + |1\rangle|010\rangle$$

Thus, we saw how *composing* simpler graphical elements of GHZ/W pair can help build up representatives of SLOCC-superclasses corresponding to arbitrary multipartite states.

Let us now consider the following graph:



One can easily construct and verify that this graph represents the state $2|0000\rangle$, which is completely unentangled. Graphically, this is equivalent to:



However, the axioms of GHZ/W pair appear to be fairly weak and by no means help us to reduce the original graph to the above graphically. Thus, these conditions need to be extended with other ones that will suffice to identify when two graphs represent the same state.

Chapter 5

Normal Form Theorems

"The challenge is to discover the necessary additional pieces of structure that allow us to predict genuine quantum phenomena." - Bob Coecke

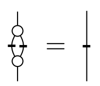
In this chapter we would first enlist here some preliminary results of relevance to us further in this chapter. In particular, we introduce additional graphical lemmas that essentially follow from the axioms satisfied by a GHZ/W pair as outlined in Def. 4.4.4 and help us to enrich the graphical language of *GHZ/W calculus*, particularly for the case of **FdHilb**. We also introduce an alternative normal form for a CFA morphism before laying down normal form for morphisms with ticks and then more theorems and their proofs.

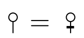
5.1 Preliminary Work

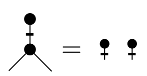
5.1.1 More graphical lemmas

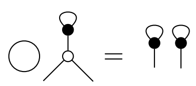
For General SMCs

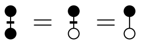
Lemma 5.1.1. *[11] For a GHZ/W pair, we have:*

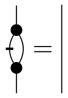
(i) 

(ii) 

(iii) 

(iv) 

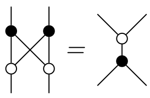
(v)  $= 1_I$

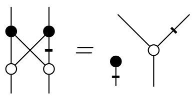
(vi) 

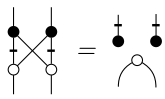
For FdHilb in particular

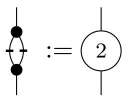
Here we develop more graphical lemmas, that hold in the particular case of the symmetric monoidal category **FdHilb** of Hilbert spaces and linear maps.

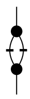
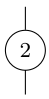
Lemma 5.1.2. *[15]* ***Bialgebra rules:***

(i) 

(ii) 

(iii) 

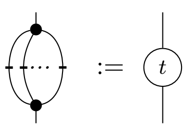
Lemma 5.1.3. 

Proof. We denote the map  in **FdHilb** as , which is precisely $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, since if we input $|0\rangle$ and $|1\rangle$ to the map, we get as follows:

$$|0\rangle \mapsto |00\rangle \mapsto |11\rangle \mapsto |1\rangle \qquad \textit{and} \qquad |1\rangle \mapsto (|01\rangle + |10\rangle) \mapsto (|10\rangle + |01\rangle) \mapsto 2|0\rangle$$

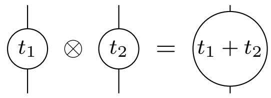
□

Corollary 5.1.4. *In general, we denote*

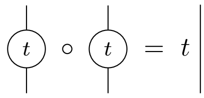


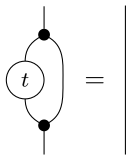
where t is the number of ticks.

Remark 5.1.5. It follows from the above that the tensor product of two such maps admits a straightforward representation as follows:



However, when composing two such maps, we do not get well-behaved result, except in the particular case where the number of ticks in the two maps are the same, in which case:



Lemma 5.1.6. 

Proof. This follows by applying lemma (5.1.1.(vi)) iteratively to one tick at a time. □

Lemma 5.1.7.  := *zero map*

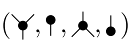
Proof. This is so because if we input $|0\rangle$ and $|1\rangle$ to the map, we get as follows:

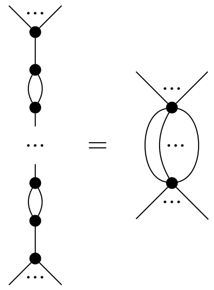
$$|0\rangle \mapsto |00\rangle \mapsto |10\rangle \mapsto 0 \qquad \textit{and} \qquad |1\rangle \mapsto |11\rangle \mapsto |01\rangle \mapsto 0$$

□

5.1.2 Alternative Representation of Normal Form

We have previously witnessed the graphical representation of the normal form for any connected CFA morphism in Eq. (3.7). Here we extend the treatment of the normal form by laying down an alternative graphical representation of the normal form that would assist us in our results discussed in later sections.

Abiding by Theorem (3.3.2), we extend our previous argument by stating that any connected morphism constructed from a commutative Frobenius algebra () admits the normal forms:



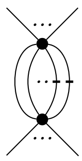
(5.1)

respecting the number of inputs, number of outputs and number of loops in both cases.

5.1.3 Normal Forms with ticks

Here we articulate a normal form for a CFA morphism formed out of either a SCFA (, , ,) or an ACFA (, , ,), but also with ticks, i.e. for a CFA morphism with only white dots or only black dots and with ticks.

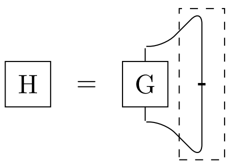
Theorem 5.1.8. *Let* **C** *be an SMC. Any general connected CFA morphism on* **C** *with ticks and with only white dots or only black dots admits the normal form given by:*



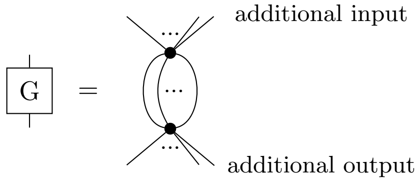
Proof. Let us denote a given CFA morphism with ticks and only white dots or black dots as H.

If H has no ticks, then it admits the normal form as given in section 5.1.2.

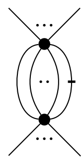
If it has one tick, the tick can be removed from the rest of the graph, which is then without any ticks at all.



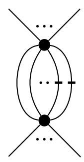
The remaining graph G has, therefore, an additional input and an additional output but no ticks anymore and, thus, admits a normal form as given in section 5.1.2. Note that the graph G could be left disconnected upon removing the tick if there were no loops in H.



Now, including the tick back into the normalised graph G, we get the graph that is normalised and equivalent to the original graph H. In case G was rendered disconnected upon removing the tick, including the tick back into G leaves H unchanged since it is already in the desired normalised form.



By induction, we can always rewrite a connected CFA morphism with ticks to the normal form:



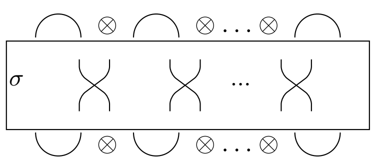
$\square$

5.2 Theorems

5.2.1 Scalars in FdHilb

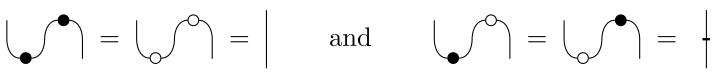
In this section we shall explore various scalars constructed from interacting GHZ and W states in the symmetric monoidal category **FdHilb**.

Theorem 5.2.1. *Any scalar formed out of a SCFA (, , ,) and an ACFA (, , ,) on $\mathbb{C}^2$ in* **FdHilb***, using only cups, caps and σ and/or identities as below is either equal to the dimension or zero.*



where the box contains symmetries and/or identities.

Proof. We know that



Let a be the number of black dots and s be the number of white dots. Note that $(s + a)$ should always be even. Then, we can have the following two cases:

(i) When both s and a are even: Considering $s > a$, the a number of black dots and white dots give rise to an even number of ticks, thereby cancelling out each other. The remaining $(s - a)$ number (even) of white dots just give rise to identities, unless $s = a$ and, in either case, the scalar boils down to a circle , i.e. dimension in **FdHilb**. Likewise for $a > s$.

(ii) When both s and a are odd: Considering $s > a$, the a number of black dots and white dots give rise to an odd number of ticks that cancel out each other leaving only one tick. This remaining tick inverts one white dot out of remaining $(s - a)$ white dots into a black dot, leaving $(s - a - 1)$ white dots out of which $(s - a - 2)$ white dots give rise to identities. So, the scalar would boil down to  which is zero. Likewise for $a > s$. When $s = a$, $a - 1$ number of black dots and white dots give rise to an even number of ticks, thereby cancelling each other and leaving one white dot and one black dot. The scalar then again boils down to  which is zero.

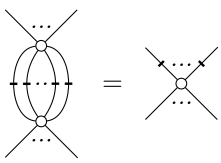
□

5.2.2 White dots with ticks

Theorem 5.2.2. *Let* **C** *be an SMC. Every connected SCFA morphism with ticks on* **C** *is uniquely determined by its number of inputs, number of outputs, number of loops* (l) *and/or the number of ticks* (t)*, such that*

(i) When $t = 0$*, then the morphism is just a spider.*

(ii) When $t = l + 1$*, then the morphism is a spider with all its input legs ticked:*



(iii) When $0 < t < l + 1$*, then the morphism is just a* ***zero map*** *in* **FdHilb**.

Proof. When $t = 0$, the result just follows from theorem (3.4.5).

When $t = l + 1$, the result is a direct consequence of lemma (5.1.1.(i)).

Finally, when $0 < t < l + 1$, the result follows from lemma (5.1.7). $\square$

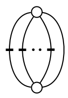
Theorem 5.2.3. *Any scalar formed out of a SCFA (, , ,) and ticks in the normal form of Theorem (5.1.8) is either equal to zero or the dimension in* **FdHilb** *according to the following rules, where l is the number of loops and t is the number of ticks:*

(i) When $0 < t \leq l$, it equals zero.

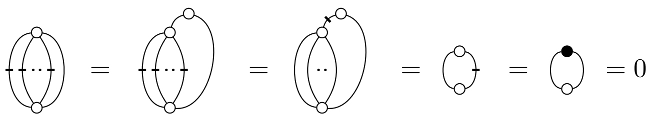
(ii) When $t = 0$ or $t = l + 1$, it equals dimension.

Proof. When $t = 0$, applying Eq. (3.8) iteratively, the scalar gets reduced to one with only one loop, yielding $\bigcirc$, i.e. dimension in **FdHilb**.

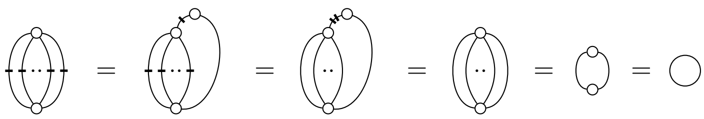
When $0 < t \leq l$, applying Eq. (3.8) iteratively, the scalar gets reduced to the following form (with $t = l$):



which upon applying lemma (5.1.1.(i)) and Eq. (3.8) again reduces to zero as follows:



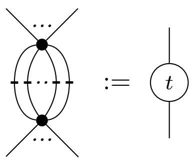
Finally, when $t = l + 1$, the scalar reduces to $\bigcirc$, i.e. dimension in **FdHilb** as follows:



$\square$

5.2.3 Black dots with ticks

Theorem 5.2.4. *Let* **C** *be an SMC. Every connected ACFA morphism with ticks on* **C** *is uniquely determined by its number of inputs, number of outputs and the number of loops (l) less the number of ticks (t), with the following exception: When $t = l + 1$, then the morphism is of the form*



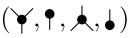
where t is the map $\begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix}$ in **FdHilb**.

Proof. When $t = 0$, then the morphism just admits the normal form as in section 5.1.2.

When $t < l$, we apply lemma (5.1.1.(vi)) iteratively to get rid of all the ticks and are left with the same number of inputs, same number of outputs and $l - t$ loops.

When $t = l$, we are, thus, left with $l - t = 0$ loops, yielding a spider.

Finally, when $t = l + 1$, then the result is a direct consequence of corollary (5.1.4). □

Theorem 5.2.5. *Any scalar formed out of an ACFA (*  *) and ticks in the normal form of Theorem (5.1.8) is either equal to zero or the dimension or t in* **FdHilb***, where t is the number of ticks and l is the number of loops, according to the following rules:*

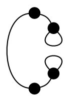
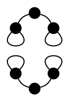
(i) When $t = 0$, the scalar is zero except in the case $l = 1$, when it equals the dimension.

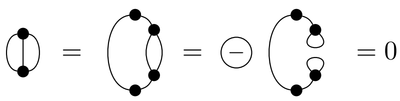
(ii) When $t = l$, the scalar equals zero.

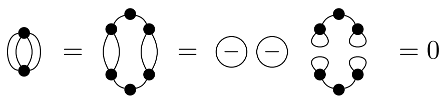
(iii) When $t = l - 1$, the scalar equals the dimension.

(iv) When $t = l + 1$, the scalar is equal to t.

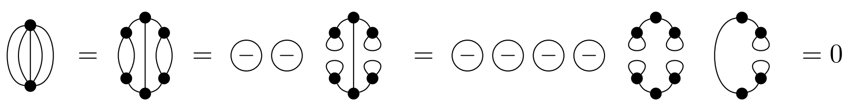
(v) When $0 < t < l - 1$, the scalar equals zero.

Proof. When $t = 0$, the scalar is simply the dimension when $l = 1$, i.e. there is only one loop, but is zero otherwise since the scalar would be a product of either or both of the primitives (which are zeroes)  and  where

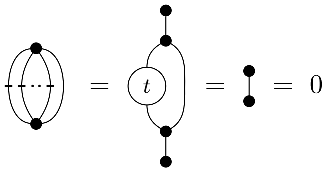




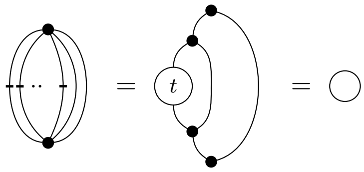
For example, using anti-specialness and lemma (3.4.4),



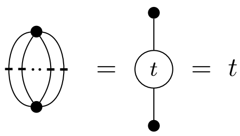
When $t = l$, the scalar equals zero since applying lemma (5.1.6), we get:



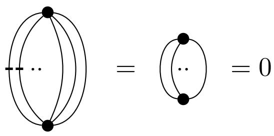
When $t = l - 1$, the scalar boils down to the dimension as follows:



When $t = l + 1$, the scalar reduces to t as follows:



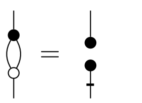
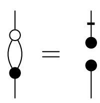
Finally, when $0 < t < l - 1$, the scalar equals zero, since $l \geq 3$ and:



□

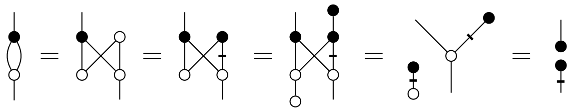
5.2.4 Mixed Cases

We now develop in this section some graphical lemmas for mixed cases and would then use them to study the behaviour of certain class of mixed morphisms.

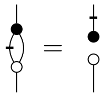
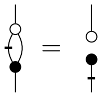
Lemma 5.2.6.  *and* 

Proof. We shall only prove the first here, and the second naturally follows by *dualising* the first.

Applying lemma (5.1.2.(ii)), we get

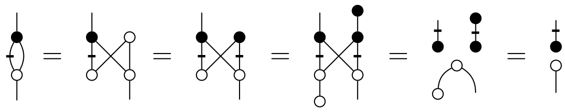


□

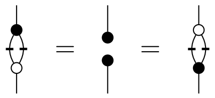
Lemma 5.2.7.  *and* 

Proof. We shall only prove the first here, and the second naturally follows by *dualising* the first.

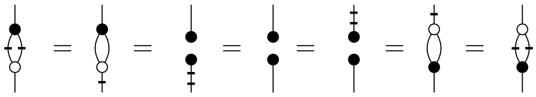
Applying lemma (5.1.2.(iii)), we get



□

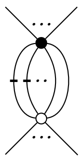
Lemma 5.2.8. 

Proof. The proof is simple as shown below:



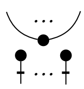
□

Theorem 5.2.9. *A (mixed) morphism of the following form:*

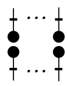


reduces to simple disconnected graphs or zero morphisms in **FdHilb** *according to the following rules (where t is the number of ticks and l is the number of loops):*

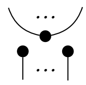
(i) When $t = 0$, then the morphism always equals the following irrespective of the number of loops:



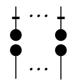
(ii) When $t = 1, t < l$, then the morphism always equals the following irrespective of the number of loops:



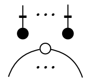
(iii) When $t = l + 1$, then the morphism always equals the following irrespective of the number of loops:



(iv) When $t = l, l > 1$, then the morphism always equals the following irrespective of the number of loops:



(v) When $t = l = 1$, then the morphism is just the following:

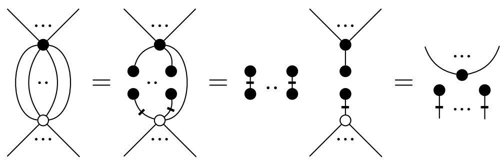


(vi) When $1 < t < l$, then the morphism always equals zero morphism irrespective of the number of loops.

Proof. We prove the different cases one by one by induction below.

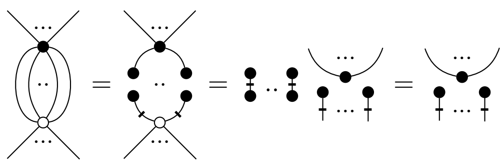
(i) For $l = 1$, it follows directly from lemma (5.2.6).

For $l = L > 1, L = \mathit{even}$, applying lemma (5.2.6) to $\frac{L}{2}$ loops the morphism reduces to



The number of copies of  above is equal to $\frac{L}{2} - 1$ and they disappear upon applying lemma (5.1.1.(v)). The last step uses the fact that a black dot is copied by a white dot.

Now, for $l = L + 1$, l is odd, such that the morphism reduces as follows

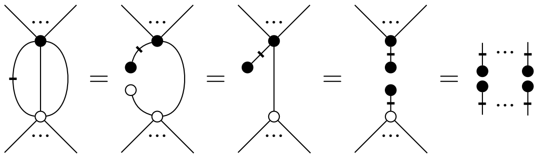


The number of copies of  above is equal to $\frac{L}{2}$.

It can be easily verified that when $L = \mathit{odd}$ the reduction is just vice-versa for $l = L$ and $l = L + 1$ as compared to the case $L = \mathit{even}$.

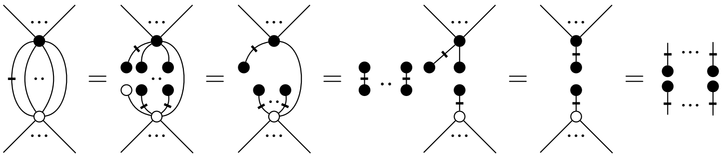
(ii) For $t = 1, t < l$, the starting point for induction is $l = 2$.

For $l = 2$, applying lemma (5.2.7) we get



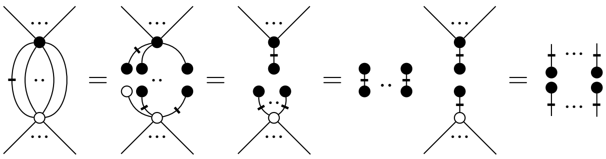
The last step uses lemma (5.1.1.(iii)) and the fact that a black dot is copied by a white dot.

For $l = L > 2, L = even$, applying lemma (5.2.7) to the leftmost loop and lemma (5.2.6) to the next $\frac{L}{2} - 1$ loops, the morphism reduces to



The number of copies of  above is equal to $\frac{L}{2} - 1$.

Now, for $l = L + 1$, l is odd, such that the morphism reduces as follows

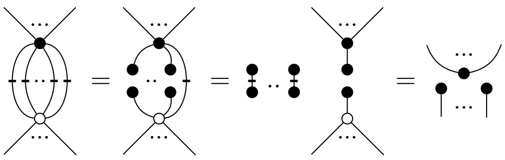


The number of copies of  above is equal to $\frac{L}{2}$.

It can be easily verified that when $L = odd$ the reduction is just vice-versa for $l = L$ and $l = L + 1$ as compared to the case $L = even$.

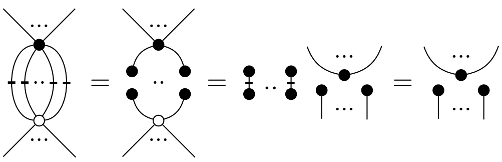
(iii) For $l = 1$, it follows directly from lemma (5.2.8).

For $l = L > 1, L = even$ applying lemma (5.2.8) to $\frac{L}{2}$ loops the morphism reduces to



The number of copies of  above is equal to $\frac{L}{2} - 1$.

Now, for $l = L + 1$, l is odd, such that the morphism reduces as follows

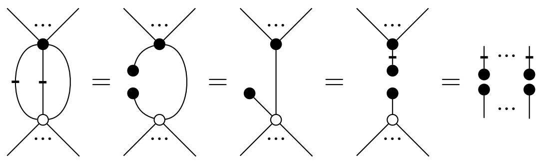


The number of copies of above is equal to $\frac{L}{2}$.

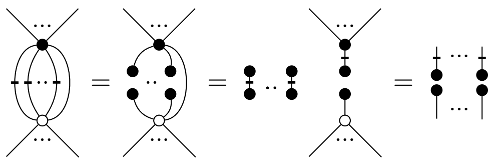
It can be easily verified that when $L = odd$ the reduction is just vice-versa for $l = L$ and $l = L + 1$ as compared to the case $L = even$.

(iv) For $t = l, l > 1$, the starting point for induction in this case is $l = 2$.

For $l = 2$, applying lemma (5.2.8) to the left loop we get

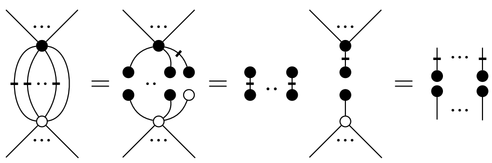


For $l = L > 2, L = even$, applying lemma (5.2.8) to the leftmost $\frac{L}{2}$ loops, the morphism reduces to



The number of copies of above is equal to $\frac{L}{2} - 1$.

Now, for $l = L + 1$, l is odd, applying lemma (5.2.8) to the left $\frac{L}{2}$ loops and lemma (5.2.7) to the rightmost loop, the morphism reduces as follows



The number of copies of above is equal to $\frac{L}{2}$.

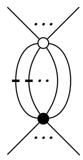
It can be easily verified that when $L = odd$ the reduction is just vice-versa for $l = L$ and $l = L + 1$ as compared to the case $L = even$.

(v) This follows directly from lemma (5.2.7).

(vi) It can be easily verified that in this case, the morphism can always be reduced to an arbitrary disconnected graph multiplied by copies of , which is zero in **FdHilb**, thereby reducing the morphism to a zero morphism.

□

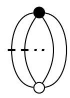
Corollary 5.2.10. *The reduced forms for various cases for a (mixed) morphism of the following form:*



are just upside-down of those in Theorem (5.2.9), since the morphism is obtained by just ***dualising*** *the one treated in the above theorem.*

Remark 5.2.11. Note that although we treated the mixed morphism(s) above and observed the nature of such a morphism, we do not claim that either of these forms is a *normal form* for any arbitrary morphism of interacting GHZ and W states. To be precise, we do not know if any arbitrary morphism of interacting GHZ and W states admit a normal form at all. However, the above result definitely gives a good insight into particular kinds of mixed morphisms.

Theorem 5.2.12. *Any (mixed) scalar of the form:*



is either equal to zero, 1_I or dimension in **FdHilb** *according to the following rules (where t is the number of ticks and l is the number of loops):*

(i) When $t = 0$ or $t = l + 1$, the scalar equals zero.

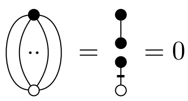
(ii) When $t = l = 1$, the scalar equals dimension.

(iii) When $l > 1$ and either $t = 1$ or $t = l$, the scalar equals 1_I.

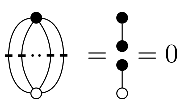
(iv) When $1 < t < l$, the scalar equals zero.

Proof. The proofs follow directly from Theorem (5.2.9) as follows:

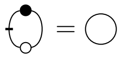
(i) When $t = 0$, the scalar reduces to



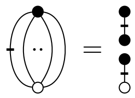
When $t = l + 1$, the scalar reduces to



(ii) When $t = l = 1$, the scalar reduces to

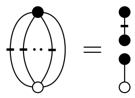


(iii) When $t = 1, l > 1$, the scalar reduces to



$= 1_I$

When $t = l, l > 1$, the scalar reduces to

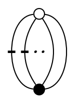


$= 1_I$

(iv) When $1 < t < l$, it follows directly from the last condition of Theorem (5.2.9) that the scalar always equals zero.

□

Corollary 5.2.13. *It can be easily verified that any (mixed) scalar of the form:*



is either equal to zero, 1_I *or dimension in* **FdHilb** *according to the same rules as Theorem (5.2.12).*

Chapter 6

Conclusion

"Nobody understands quantum mechanics." - Richard Feynman

In this final chapter, we first summarize our results and then sketch possible future work in this context.

6.1 Summary of Results

We know that there are exactly two SLOCC classes of genuine tripartite entangled states called the GHZ and W states. It was also previously known that 'special' and 'anti-special' commutative Frobenius algebras (CFAs) represent these GHZ and W states, respectively. We have seen the graphical counterparts of these, when the CFAs are presented internal to symmetric monoidal categories. Having noted the normal form admitted by a CFA morhpism, we already knew that any SCFA morphism is just a spider whereas we spelled out concretely the nature of any ACFA morphism, particularly stating explicitly the scalar involved.

We have as well witnessed the previously laid down basic axioms satisfied by a GHZ/W pair, that help to generate and reason about arbitrary multipartite states. However, the behaviour of such interacting GHZ and W states needed to be further studied to identify which graphical properties lead to what states.

We developed more graphical identities satisfied by a GHZ/W pair, particularly in the SMC **FdHilb** of Hilbert spaces and linear maps. We studied the well-behaved nature of a class of scalars, formed out of cups, caps and symmetries and/or identities and identified when such a scalar equals zero and when it equals dimension in **FdHilb**.

Based on an alternative normal form for any CFA morphism, respecting the number of inputs, number of outputs and the number of loops, we derived the normal form admitted by any CFA morphism (either SCFA or ACFA morphism) alongwith ticks (self-inverses). In particular, we identified the nature of a general SCFA morphism with ticks and a general ACFA morphism with ticks. We also observed what scalars in this normal form having ticks and only white dots or black dots equal to, in different cases.

Finally, we derived more graphical lemmas for the mixed cases based on bialgebra rules. Based on this, we studied the nature of a general class of certain kinds of mixed morphisms and the values of scalars expressed in this mixed form.

6.2 Future Work

In this work, we have mainly established a normal form for interacting GHZ and W states. However, we have laid down such a normal form for only morphisms where the black dots and white dots interact with each other to give rise to ticks, leaving only black or white dots in the remaining graph. Note that wherever necessary we have considered the specific case of the SMC **FdHilb** to arrive at the result(s). Arriving at a normal form for cases where we are left with both black and white dots even after reducing all interacting contrasting dots into ticks appears to be highly non-trivial and we have kept this out of the scope of this thesis.

We have, however, explored and further identified here the behaviour of certain non-trivial mixed morphisms in the graphical language. Thus, what follows naturally as future work to this is to possibly arrive at a normal form for morphisms with ticks and both black and white dots, that would provide us with an exhaustive toolkit alongwith our results to completely qualify all known multipartite states in our graphical language. Moreover, generalizing our results to general SMCs from the specific case of **FdHilb** (wherever such assumption has been made) as future work would further enrich the graphical language.

Bibliography

[1] Scott Aaronson. NP-complete Problems and Physical Reality. *ACM SIGACT News, March 2005*, Feb 2005.

[2] Scott Aaronson. The Limits of Quantum Computers. *Scientific American (2008)*, Mar 2008.

[3] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. *Proceedings of the 19th IEEE conference on Logic in Computer Science (LiCS'04). IEEE Computer Science Press (2004)*, quant-ph, Mar 2007.

[4] R. Raussendorf, D.E. Browne and H.J. Briegel. Measurement-based quantum computation with cluster states. *Phys. Rev. A 68, 022312 (2003)*, Jan 2003.

[5] Jeffrey Bub. Quantum entanglement and information. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Summer 2009 edition, 2009.

[6] Bob Coecke. Kindergarten Quantum Mechanics. *arXiv*, quant-ph, Oct 2005.

[7] Bob Coecke. Quantum Picturalism. *Contemporary Physics 51, 59-83, 2010*, quant-ph, Aug 2009.

[8] Bob Coecke and Ross Duncan. Interacting Quantum Observables: Categorical Algebra and Diagrammatics. *ICALP 2008*, quant-ph, Jun 2009.

[9] Bob Coecke and Éric Oliver Paquette. Categories for the practicing physicist. *arXiv*, quant-ph, Oct 2009.

[10] Bob Coecke and Aleks Kissinger. Interacting Frobenius Algebras and the Structure of Multipartite Entanglement. PRG-RR-09-12, Dec 2009.

[11] Bob Coecke and Aleks Kissinger. The compositional structure of multipartite quantum entanglement. *ICALP 2010*, quant-ph, Feb 2010.

[12] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest and H.-J. Briegel. Entanglement in Graph States and its Applications. *Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos", Varenna, Italy, July, 2005*, quant-ph, Feb 2006.

[13] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett. 67, 661663 (1991)*, Aug 1991.

[14] Daniel Gottesman and Isaac L. Chuang. Quantum Teleportation is a Universal Computational Primitive. *Nature 402, 390-393 (1999)*, Aug 1999.

[15] Aleks Kissinger. Entanglement, Monoidal Categories, and Frobenius Algebras, Jan 2010.

[16] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press India Pvt. Ltd., New Delhi, India, Fourth South Asian printing edition, 2008. Special edition for sale in South Asia only, not for export elsewhere.

[17] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett. 70, 18951899 (1993)*, Mar 1993.

[18] M. Rédei. Why John von Neumann did not like the Hilbert Space Formalism of Quantum Mechanics (and what he liked instead). *Stud. Hist. Phil. Mod. Phys. 27*, pages 493–510.

[19] L. Lamata, J. León, D. Salgado and E. Solano. Inductive Entanglement Classification of Four Qubits under SLOCC. *Phys. Rev. A 75, 022318 (2007)*, quant-ph, Feb 2007.

[20] Peter Selinger. A survey of graphical languages for monoidal categories. *arXiv*, quant-ph, Aug 2009.

[21] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J.Sci.Statist.Comput. 26 (1997) 1484*, Jan 1996.

[22] P. Mathonet, S. Krins, M. Godefroid, L. Lamata, E. Solano and T. Bastin. Entanglement Equivalence of n-qubit Symmetric States. *Phys. Rev. A 81, 052315 (2010)*, quant-ph, Aug 2009.

[23] W. Dür, G. Vidal and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A 62, 062314 (2000)*, quant-ph, Jun 2000.

[24] Saman Zarandioon. Quantum Computation, NP-completeness and Physical Reality.

[25] M. Żukowski, A. Zeilinger, M. A. Horne and A. K. Ekert. "Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett. 71, 42874290 (1993)*, 1993.