Categorical Quantum Computing with Finite Fields

Matthew Varughese
candidate number 141034

Supervisor: Dr Jamie Vicary

Somerville College, Oxford, 2009

Submitted in partial fulfilment of the requirements for the

Degree of Master of Science

in

Mathematics and the Foundations of Computer Science

at the

University of Oxford

Contents

Abstract

In this dissertation we explore primarily the category of finite dimensional vector spaces over a finite field F, $\mathbf{FdVect}_F$, and its relevance and possible uses in quantum information theory. The main results will be related to Frobenius algebras in $\mathbf{FdVect}_F$, particularly:
1) The link between classical structures in **Rel** the category of finite relations and single valued classical structures in $\mathbf{FdVect}_{F_2}$, which I show are equivalent to abelian groupoids whose components are of odd order.
2) Monoidal structures in $\mathbf{FdVect}_{F_p}$ (dimension n) that are isomorphic to the finite field F_{p^n}. The main result here is that such monoidal structures always exist and each admits a special Frobenius algebra.
This work also provides a background to the use of category theory in quantum computing. We cover the use of symmetric monoidal categories, diagrammatic calculi, abstract categories in both quantum and classical systems and give an introduction to copying and deleting operations. We see $\mathbf{FdVect}_F$ in action with several examples of familiar quantum protocol and properties. Also we give some other interesting concrete categories worth studying in future work.

Acknowledgments

I'd like to give a special thanks for my supervisor Jamie Vicary, for the time and effort he has invested in helping me with this dissertation. I also thank Karin Erdmann for her help in pointing out the use of the 'normal basis theorem'. I thank my family, friends and fellow course mates for all their support during the time of writing. Finally I would like to thank Bob Coecke for providing such a fascinating introduction to quantum computing in his lecture course, my choice to write a dissertation in quantum computing was primarily down to the enjoyment I took in studying the subject in his course.

Introduction

Much of the mathematical foundations for quantum computing were made over 70 years ago by Von Neumann with the use of Hilbert spaces. In recent years significant work has been made in developing more advanced methods for quantum computing using category theory. This category theoretic approach to the subject will be the focus of my dissertation. I will discuss the importance of category theory in quantum mechanics more in chapter 2.

In this dissertation I will study the use in quantum computing of the category of finite dimensional vector spaces over finite fields (denoted $\mathbf{FdVect}_F$). I will aim to:-
1. Investigate which properties of quantum computing we can model using these categories, as well as which seem natural.
2. Find out how this can be used to give a different perspective on quantum computing, or as a tool in quantum computing.
3. Understanding how finite fields may be used in quantum computing in the future and where future study might be best focussed.

To give an outline of the structure of this dissertation, we start in chapter 1 by looking at finite dimensional vector spaces and finite fields. We discuss the properties that are going to be useful in quantum computing and the properties we may want, but not have.

Chapters 2-6 provides a background to the category theoretic approach to quantum mechanics, this should be accessible even for a reader completely unfamiliar with category theory. Chapter 2 introduces category theory, chapter 3 describes the diagrammatic calculi that makes such an approach so appealing. In chapter 4 we introduce the symmetric monoidal category which forms the basic structure to classical and quantum systems. In chapter 5 we look at categories defining properties, that are either classified as classical or quantum. Chapter 6 introduces copying and deleting operations.

In chapter 7 we focus on Frobenius algebras and in particular classical structures. We get back to $\mathbf{FdVect}_F$ here and look at what classical structures and special Frobenius algebras look like in this category. Chapter 8 provides examples of $\mathbf{FdVect}_F$ in action, we see many familiar quantum protocols and properties. Chapter 9 gives examples of other interesting categories worth studying in future work.

1 Finite dimensional vector spaces and finite fields

We first look at our usual setting for quantum mechanics the Hilbert space

Definition 1.1. A (finite dimensional) Hilbert space is vector space $\mathcal{H}$ over $\mathbb{C}$ which also comes with an inner product, i.e. a map

$$\langle -|-\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C} \tag{1}$$

satisfying,

$$\langle \psi | c_1 \cdot \phi_1 + c_2 \cdot \phi_2 \rangle = c_1 \langle \psi | \phi_1 \rangle + c_2 \langle \psi | \phi_2 \rangle \tag{2}$$

$$\langle c_1 \cdot \psi_1 + c_2 \cdot \psi_2 | \phi \rangle = \bar{c}_1 \langle \psi_1 | \phi \rangle + \bar{c}_2 \langle \psi_2 | \phi \rangle \tag{3}$$

$$\langle \psi | \phi \rangle = \overline{\langle \phi | \psi \rangle} \qquad \langle \psi | \psi \rangle \in \mathbb{R}^+ \qquad \langle \psi | \psi \rangle = 0 \Leftrightarrow \psi = 0 \tag{4}$$

The concrete categories $\mathbf{FdVect}_{\mathbb{K}}$ of finite dimensional vector spaces over field $\mathbb{K}$ and **FdHilb** of finite dimensional hilbert spaces, share properties that make them useful in quantum mechanics. For example both can be made dagger compact categories. This is shown by theorem 5.7 and the fact Hilbert spaces are finite dimensional vector spaces over the field $\mathbb{C}$. The other defining feature of a Hilbert space is its inner product, this leads to the question, can we define such an inner product on different finite dimensional vector spaces? We will discuss this more later.

Finite fields

Finite fields were first studied in the 17th and 18th centuries, they now play key roles in areas of maths such as number theory, group theory and algebraic geometry. They have also proved an important resource in more applied areas such as computer science, coding and cryptography. While little work has been done on their applications in quantum mechanics, finite fields do possess qualities that make them a good candidate to study in this area. Because of the finite number of elements we can often run computer simulations on all the elements in a finite field to check a result or search for patterns. They also have the nice multiplication and addition structure of a field.

The first obvious limitation as a full model of quantum mechanics is their discrete nature will not allow the study of continuous data which we see in quantum mechanics. However the does not rule out the possibility of creating finite field extensions or some sort of limit functions to handle continuous data. Besides, previous research has already shown us that discrete categories such as **Rel** the category of relations can produce enough resources to simulate a teleportation protocol or describe the notion of quantum entanglement.

The next limitation we face is when we look at inner products in $\mathbf{FdVect}_{\mathbb{K}}$. Let ψ and ϕ be elements of a vector space V, we can represent these as maps from the base field $\mathbb{K}$ to V, i.e. $|\phi\rangle : \mathbb{K} \to V :: 1 \mapsto \phi$. The adjoint of elements of V can be represented by $|\phi\rangle^{\dagger} : V \to \mathbb{K} :: \phi \mapsto 1$. We can use the transpose as our adjoint (see theorem 5.5) to give us a map from $\mathbb{K} \to \mathbb{K}$ via the square of the norm $\langle\psi|\phi\rangle = |\psi\rangle^{\dagger} \circ |\phi\rangle$. This map is also linear with respect to ψ and ϕ, however consider say the vector $\phi = (1,1)$ in GF(2) this gives $\langle\phi|\phi\rangle = 1 + 1 = 0$ violating the final condition of 4. A non-zero vector being orthogonal to itself is a property we want to avoid. However the base field having non-zero characteristic will always mean an inner product is difficult to define, because of this reason.

One attempt to get round this problem is to focus our attention on vectors ψ in our vector space which have non-zero inner product $\langle\psi|\psi\rangle$, we call this set S. While our vector space is not actually an inner product space, this inner product can still be applied in a useful way to chosen vectors. Scalar multiplication will be closed on S as we can see from

$$\langle s\psi|s\psi\rangle = s^2\langle\psi|\psi\rangle$$

and the fact that in any finite field (or any field) the product of non-zero elements is non-zero. It also makes sense to restrict our attention to operations which map vectors in S to other vectors in S. An obvious candidate would be unitary maps. For this to be the case the transpose would be equal to the inverse. Below is an example in GF(3)

$$U = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \qquad U^T = U^{-1} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We also have U preserving the inner product and therefore maps vectors in S to S.

$$\langle U\psi|U\phi\rangle = \psi^T \circ U^T \circ U \circ \psi = \psi^T \circ \phi = \langle\psi|\phi\rangle$$

The addition operation however will not be closed, for example in GF(2) we have

$$(1,0) + (0,1) = (1,1)$$

While this restriction would allow an inner product to have more meaning, the fact S cannot be preserved under addition means we would then not allow the possibility of superposition of states. This is essential in any model of quantum mechanics. Also the lack of an inner product gives less meaning to our adjoint. In the category of **Rel** the adjoint has an intuitive meaning i.e. y is related to x in $f^{\dagger}$ iff x is related to y in f; in $\mathbf{FdVect}_F$ the adjoint does not have such intuitive meaning behind it. We will continue to study the adjoint in $\mathbf{FdVect}_F$, which for the rest of this dissertation will be the transpose.

It is clear $\mathbf{FdVect}_F$ is not going to capture all the features of a full quantum system. However that is not to say we cannot observe concepts such as entanglement or quantum protocols, such as teleportation and superdense coding. Using the simplest finite field F_2 we see many similarities between the more studied category **Rel** and $\mathbf{FdVect}_{F_2}$. In fact we observe the difference boils down to a difference in matrix arithmetic.

Example 1.2. Semi-ring of Booleans in Rel

If we write an element $A \subseteq X$ as,

$$A = \bigcup_{i \in X} a_i \{i\}$$

we can think of our coefficients a_i as part of the Boolean $\mathbb{B}$ semi-ring (ring without additive inverses). We can use $+$ and $*$ to represent $\cup$ and $\cap$, giving the following arithmetic.

$$\begin{array}{ccc} 0+0=1 & 0+1=1+0=1 & 1+1=1 \\ 0*0=0 & 0*1=1*0=0 & 1*1=1 \end{array}$$

This allows us to multiply and add matrices in familiar ways and even makes our relations linear operators over this arithmetic.

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

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \left(\lambda \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \mu \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) = \lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \mu \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

2 Introducing category theory

While the traditional use of Hilbert spaces can describe our quantum systems, we often find very intuitive or simple results can seem excessively complicated or inaccessible. We not only lack the perspective to see the big picture, but find it hard to get to the essence of the result. The category theoretic approach allows us to do all of this. Maybe the three most appealing properties to this approach are, firstly we can immediately identify the property of our quantum systems that gives rise to a result. Secondly, we can represent results using easy to understand and intuitive diagrammatic form. We can manipulate this form in a formal way, much the same you would do with equations. Thirdly, category theory gives us a framework to study quantum mechanics outside the tradition Hilbert space setting. Not only does this give us a new perspective to quantum mechanics, but opens up the entire world of mathematics as possible places where quantum computing can take place.

This third property is probably the most relevant to this dissertation as I will be studying quantum computing out of its usual contexts. An analogy we make is that we can think of quantum mechanics as a group of animals all living inside a specific habitat which is our Hilbert spaces. It may seem daunting to take the animals out of the habitat where we know they can all live and to build a new home from scratch for all the animals would be a massive task. However category theory acts like a guide telling us where each animal can live and where it interacts with the environment in a natural way. With the help of this guide, we can find better places to use the animals (perform simulations or protocols), for example farming. Or just observe the animals in different types of environment, allowing us to understand them better. It also means we have the entire world (corresponding to the entire world of mathematics) to explore and find better homes for these animals.

I will now define some of the category theory that will be used in this dissertation.

Definition 2.1. A category is a structure containing objects, usually denoted A,B,C etc. and morphisms, depicted as arrows between objects and usually denoted f,g etc. More formally a category comprises

1. A collection of objects $|\mathbf{C}|$
2. A collection of morphisms (arrows). For any $A, B \in |\mathbf{C}|$ the hom-set $\mathbf{C}(A, B)$

is the set of all morphisms from A to B.
3. For any $A, B, C \in |\mathbf{C}|$, $f \in \mathbf{C}(A,B)$ and $g \in \mathbf{C}(B,C)$ there exists a composite $g \circ f \in \mathbf{C}(A,C)$, i.e. there is a composition operation

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

with the following properties
i. Associativity. For any $f \in \mathbf{C}(A,B)$, $g \in \mathbf{C}(B,C)$ and $h \in \mathbf{C}(C,D)$ we have

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

ii. Existence of identities. For any $A, B \in |C|$ there exists $1_A \in \mathbf{C}(A,A)$ and $1_B \in \mathbf{C}(B,B)$, such that for any $f \in \mathbf{C}(A,B)$ we have

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

Categories are found in a broad range of places. We can see examples in how we view natural and physical processes or in mathematical structures or even can be studied as a part of mathematics in its own right. We will split them into three different types

1. Real world categories. These are processes we see all around us in the world, for example processes in physics or chemistry or quantum mechanics. Our physical or chemical or quantum states become objects and the processes that take our system from one state to another are morphisms. In these categories the identity is the same as 'doing nothing' and the composite $g \circ f$ is to do process f followed by process g. We don't have to restrict ourselves to such scientific examples we could use category theory to look at the process of washing a car or even writing a dissertation.

2. Concrete categories. Here our objects are mathematical structures and morphisms are structure preserving maps between them; these will often be the structures used to model the real world processes. Examples are **Pos** or **Grp** where the objects are posets and groups respectively and the morphisms are order preserving maps for **Pos** and group homomorphisms for **Grp**. Below is another important example

Example 2.2. Let $\mathbf{FdVect}_{\mathbb{K}}$ be the concrete category with
1. Objects as finite dimensional vector spaces over $\mathbb{K}$
2. Morphisms as linear maps between these vector spaces
3. The composition of two linear maps as the ordinary function composition (giving another linear map) and the identity function (again linear).

3. Abstract categories. Here categories are studied as mathematical structures in their own right. By defining properties in these categories we can build a structure that can be used to model or simulate a physical system. We can also think of these categories as a way of axiomatising our system. The study of these categories can reveal often interesting and unusual information about our system. A strict monoidal category is an example of an abstract category, it provides the basic structure to most of the categories we see in quantum computing.

Definition 2.3. A strict monoidal category $\mathbf{C}$ is a category with the following properties

1. Objects come with a monoid structure $(|\mathbf{C}|, \otimes, I)$. I is the unit object, $\otimes$ the monoidal product. This means for all $A, B, C \in |\mathbf{C}|$

$$A \otimes (B \otimes C) = (A \otimes B) \otimes C \quad \textit{and} \quad I \otimes A = A = A \otimes I$$

2. for all objects $A, B, C, D \in |C|$ there exists an operation

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

which is associative and has 1_I as its unit:

$$f \otimes (g \otimes h) = (f \otimes g) \otimes h \quad \textit{and} \quad 1_I \otimes f = f = f \otimes 1_I$$

3. For all f, g, h, k such that f's output (codomain) matches g's input (domain) and h's output matches k's input.

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

4. For all objects $A, B \in |\mathbf{C}|$ we have

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

Finally in this section we will define a few of the most basic and important concepts to category theory. Feel free to skip to the next section if category theory is already familiar to you.

Definition 2.4. An isomorphism $f \in \mathbf{C}(A, B)$ is a morphism with an inverse, i.e. there exists a $g \in \mathbf{C}(B, A)$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. Two objects are isomorphic if there exists an isomorphism between them.

Definition 2.5. The opposite category $\mathbf{C}^{op}$ of a category $\mathbf{C}$ is a category with

1. The same objects as $\mathbf{C}$

2. Morphism are reversed i.e. for every $f \in \mathbf{C}(A, B)$ we get opposite morphism $f^{op} \in \mathbf{C}^{op}(B, A)$. Also,

- Identities in $\mathbf{C}^{op}$ are those $\mathbf{C}$, and
- If $h = g \circ f$ in $\mathbf{C}$ then $h^{op} = f^{op} \circ g^{op}$, in other words,

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

Definition 2.6. Let $\mathbf{C}$ and $\mathbf{D}$ be categories. A functor $F : \mathbf{C} \to \mathbf{D}$ is a map taking each object $A \in |\mathbf{C}|$ to an object $F(A) \in |\mathbf{D}|$ and taking each morphism $f \in \mathbf{C}(A, B)$ to a morphism $F(f) \in \mathbf{D}(F(A), F(B))$, such that for all objects A and morphisms f and g in category $\mathbf{C}$ we have
1. $F(1_A) = 1_{F(A)}$
2. $F(g \circ f) = F(g) \circ F(f)$

In the same way a functor is a structure preserving map from one category to another, a natural transformation is a structure preserving map from one functor to another.

Definition 2.7. Let $\mathbf{C}$ and $\mathbf{D}$ be categories and let F and G be functors from $\mathbf{C}$ to $\mathbf{D}$. A natural transformation from F to G denoted $\eta : F \dot{\to} G$ is a function that assigns to every object $A \in \mathbf{C}$ a morphism in $\mathbf{D}$ $\eta_A : F(A) \to G(A)$ such that for any $f \in \mathbf{C}(A, B)$ the below diagram commutes (we will talk more about commutative diagrams in the next section)

$$\begin{tikzcd}
F(A) \arrow[r, "\eta_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\
F(B) \arrow[r, "\eta_B"'] & G(B)
\end{tikzcd}$$

3 Diagrams and notation

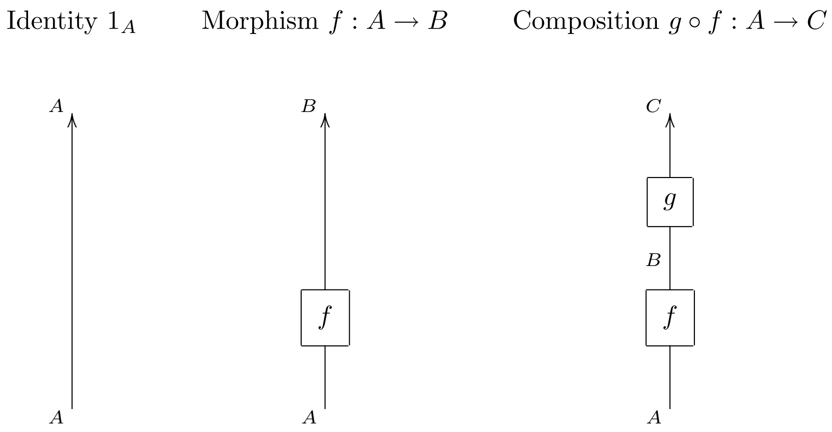
One of the most important features of using categories in quantum mechanics is that the systems and processes we encounter can be represented in a purely diagrammatic calculus. This means that situations which may look extremely complicated and at first glance uninterpretable, in the form of equations, now become very intuitive and easy to read. Abstract categorical structures, the axioms that define them and derivable equations all have purely diagrammatic counterparts. Below we see what these counterparts are

The diagrams are read from bottom to top.

- Identities 1_I are an empty diagram

- Identities on object A, 1_A, are depicted as an arrow from bottom to top.

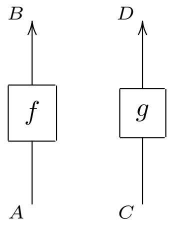
- Morphisms are depicted as a box and the composition of f then g is shown as a box f connected to a box g above it.


Identity 1_A Morphism $f : A \to B$ Composition $g \circ f : A \to C$

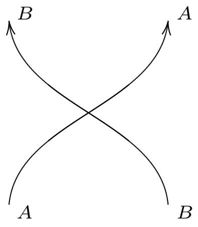
Tensor products are depicted as lining the diagrams up side by side. For example $f \otimes g$ is a morphism f on the left of a morphism g.

The symmetry operation is shown as swapping of the lines.

Tensor $f \otimes g : A \otimes C \to B \otimes D$



Symmetry $\sigma_{AB} : A \otimes B \to B \otimes A$

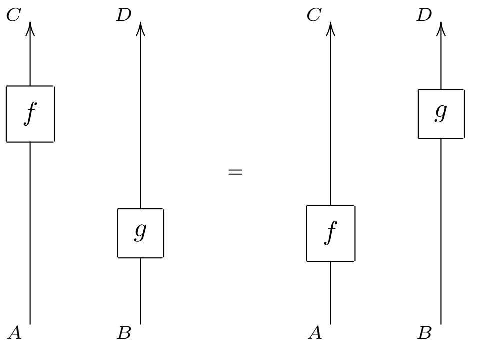


Another form of diagram we will see a lot is the commutative diagram. This is very similar to an equation with the different paths of the diagram forming different sides to the equation.

Example 3.1. In any strict monoidal category with $f \in \mathbf{C}(A, C), g \in \mathbf{C}(B, D)$ we have

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

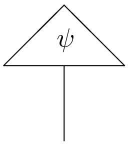
In terms of a graphical calculus this looks like

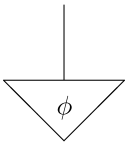


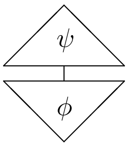
In terms of a commutative diagram this looks like

$$\begin{tikzcd}
A \otimes B \arrow[r, "f\otimes 1_B"] \arrow[d, "1_A\otimes g"'] & C \otimes B \arrow[d, "1_C\otimes g"] \\
A \otimes D \arrow[r, "f\otimes 1_D"'] & C \otimes D
\end{tikzcd}$$

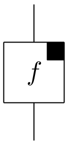
One type of notation commonly used in quantum mechanics is Dirac notation. Bras and kets also have graphical counterparts via a 90° clockwise rotation. Inner products and projectors can also be represented in our graphical calculus.

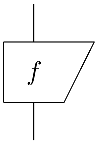
$|\psi\rangle =$ 

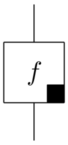
$\langle\phi| =$ 

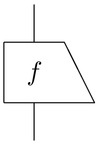
$\langle\phi|\psi\rangle =$ 

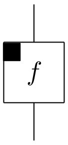
By introducing an asymmetry to the box used to represent function f it is possible to represent notions of transpose, conjugate and adjoint. The transpose is made through a 180° rotation, adjoint by a vertical flip and conjugate by horizontal flip (or vertical flip and 180° rotation). This will come up more in chapter 4 when we introduce a unit.

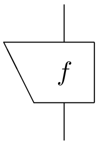
$f =$ 

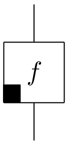
or 

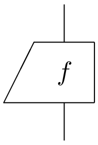
$f^\dagger =$ 

or 

$f^* =$ 

or 

$f^T =$ 

or 

For the rest of this paper I will interchange between the use of equations, Dirac notation, commutative diagrams and graphical calculus. I will aim to use the most appropriate representation to make the definition or theorem as intuitive and informative as possible.

4 Building structure with abstract categories

At the end of section 1 I defined a strict monoidal category. While this is the basic structure to the real world categories we encounter in quantum mechanics, the mathematical structures used to represent these systems do not admit the required properties. The strictness of the equalities is where the connection fails. In the concrete categories of groups, topological spaces, vector spaces and Hilbert spaces we do not have

$$A \otimes (B \otimes C) = (A \otimes B) \otimes C \quad \textit{or} \quad I \otimes A = A = A \otimes I$$

We do however have instead of an equality, an isomorphism.

$$A \otimes (B \otimes C) \simeq (A \otimes B) \otimes C \quad \textit{and} \quad I \otimes A \simeq A \simeq A \otimes I$$

These are in fact natural isomorphisms. Natural isomorphisms are natural transformations which are also isomorphisms. We introduce the natural transformations α (associativity) to switch the brackets and λ and ρ (left and right units) to introduce new objects relative to an existing one. Later we will also encounter the symmetry natural isomorphism σ which is used to switch objects across the monoidal product. These natural isomorphisms allow us to define the abstract categories needed to model our concrete categories (as well as the real world ones).

Definition 4.1. A monoidal category $\mathbf{C}$ is a category with the following properties

1. There exists an object $I \in |\mathbf{C}|$

2. A bifunctor $- \otimes -$, which is an operation on objects and morphisms such that

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

and also for all objects A, B and morphisms f,g,h,k of appropriate type

$$(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h) \text{ and } 1_A \otimes 1_B = 1_{A \otimes B} \tag{5}$$

3. Three natural isomorphisms

$$\begin{aligned} \alpha =& \{A \otimes (B \otimes C) \overset{\alpha_{A,B,C}}{\longrightarrow} (A \otimes B) \otimes C |\ A, B, C \in |\mathbf{C}|\} \\ \lambda =& \{A \overset{\lambda_A}{\longrightarrow} I \otimes A |\ A \in |\mathbf{C}|\} \\ \rho =& \{A \overset{\rho_A}{\longrightarrow} A \otimes I |\ A \in |\mathbf{C}|\} \end{aligned}$$

and for all A,B,C,D,A',B',C' and f,g,h of appropriate types, the below diagrams commute:-

Naturality conditions, showing these isomorphisms interact with morphisms in the appropriate way.

$$\begin{tikzcd}
A \otimes (B \otimes C) \arrow[r, "\alpha_{A,B,C}"] \arrow[d, "f\otimes(g\otimes h)"'] & (A \otimes B) \otimes C \arrow[d, "(f\otimes g)\otimes h"] \\
A' \otimes (B' \otimes C') \arrow[r, "\alpha_{A',B',C'}"'] & (A' \otimes B') \otimes C'
\end{tikzcd} \tag{6}$$

$$\begin{tikzcd}
A \arrow[r, "\lambda_A"] \arrow[d, "f"'] & I \otimes A \arrow[d, "1_A\otimes f"] \\
B \arrow[r, "\lambda_I"'] & I \otimes B
\end{tikzcd} \qquad
\begin{tikzcd}
A \arrow[r, "\rho_A"] \arrow[d, "f"'] & A \otimes I \arrow[d, "f\otimes 1_A"] \\
B \arrow[r, "\rho_I"'] & B \otimes I
\end{tikzcd} \tag{7}$$

Another associativity condition.

$$\begin{tikzcd}
A \otimes (B \otimes (C \otimes D)) \arrow[r, "\alpha"] \arrow[d, "1_A\otimes\alpha"'] & (A \otimes B) \otimes (C \otimes D) \arrow[r, "\alpha"] & ((A \otimes B) \otimes C) \otimes D \\
A \otimes ((B \otimes C) \otimes D) \arrow[rr, "\alpha"'] & & (A \otimes (B \otimes C)) \otimes D \arrow[u, "\alpha\otimes 1_D"']
\end{tikzcd} \tag{8}$$

Coherence conditions, showing the isomorphisms interact with each other in the correct way.

$$\begin{tikzcd}
A \otimes B \arrow[r, "1_A\otimes\lambda_B"] \arrow[dr, "\rho_A\otimes 1_B"'] & A \otimes (I \otimes B) \arrow[d, "\alpha_{A,I,B}"] \\
& (A \otimes I) \otimes B
\end{tikzcd} \qquad \lambda_I = \rho_I \tag{9}$$

Definition 4.2. A symmetric monoidal category is a monoidal category with a fourth natural isomorphism called symmetry

$$\sigma = \{A \otimes B \stackrel{\sigma_{A,B}}{\longrightarrow} B \otimes A |\ A, B \in |\mathbf{C}|\}$$

Such that for all A, B, C, D and f, g of appropriate types, the following diagrams commute:-

Naturality condition

$$\begin{tikzcd}
A \otimes B \arrow[r, "\sigma_{A,B}"] \arrow[d, "f \otimes g"'] & B \otimes A \arrow[d, "g \otimes f"] \\
C \otimes D \arrow[r, "\sigma_{C,D}"'] & D \otimes C
\end{tikzcd} \tag{10}$$

Another condition of the symmetry isomorphism

$$\begin{tikzcd}
A \otimes B \arrow[r, "\sigma_{A,B}"] \arrow[dr, "1_{A \otimes B}"'] & B \otimes A \arrow[d, "\sigma_{B,A}"] \\
& A \otimes B
\end{tikzcd} \tag{11}$$

Coherence conditions

$$\begin{tikzcd}
A \arrow[r, "\lambda_A"] \arrow[dr, "\rho_A"'] & I \otimes A \arrow[d, "\sigma_{I,A}"] \\
& A \otimes I
\end{tikzcd} \tag{12}$$

$$\begin{tikzcd}
A \otimes (B \otimes C) \arrow[r, "\alpha"] \arrow[d, "1_A \otimes \sigma_{B,C}"'] & (A \otimes B) \otimes C \arrow[r, "\sigma_{(A \otimes B),C}"] & C \otimes (A \otimes B) \arrow[d, "\alpha"] \\
A \otimes (C \otimes B) \arrow[r, "\alpha"'] & (A \otimes C) \otimes B \arrow[r, "\sigma_{A,B} \otimes 1_C"'] & (C \otimes A) \otimes B
\end{tikzcd} \tag{13}$$

It is also useful to add structure to our abstract categories to represent the idea of adjoints which we see in **FdHilb**. These adjoints in **FdHilb** also play a key part in defining the inner product. We therefore introduce a dagger monoidal category.

Definition 4.3. A dagger monoidal category $\mathbf{C}$ is a monoidal category with a identity-on-objects contravariant involutive functor

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

satisfying the below equations,
1. for all objects $A, A^\dagger = A$ (identity on objects),
2. for all morphisms $f, f^{\dagger\dagger} = f$ (involutive),
3.

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

Also all unit and associativity natural isomorphisms are unitary, i.e. the inverse and adjoint (defined by †) coincide.

A dagger symmetric monoidal category is both a dagger monoidal category and a symmetric monoidal category in which the symmetry natural isomorphism is unitary.

5 Quantum and classical tensors

Until now the structure we have imparted on our categories can be used as much in classical information systems as it can in quantum information systems. In both classical and quantum systems it seems natural that we want to have composition of operation as well as the ability to perform operations simultaneously. This is why symmetric monoidal categories form a basis for a categorical approach for both. However we must choose a suitable monoidal tensor to allow further either classical properties or quantum properties to be defined on our mathematical structure. For example in $\mathbf{FdVect}_{\mathbb{K}}$ defining our monoidal tensor as the direct sum $\oplus$ gives us classical-like properties and using the tensor product $\otimes$ we get quantum-like properties. We see below both describe a dagger symmetric monoidal category.

Theorem 5.1. $\mathbf{FdVect}_{\mathbb{K}}$ *with respect to* $\oplus$*, the direct sum, is a dagger symmetric monoidal category.*

Proof. In example 2.2 I describe how $\mathbf{FdVect}_{\mathbb{K}}$ forms a category, however to show it is a monoidal category requires 8 (eq 5-9) conditions to be satisfied, for symmetry another 4 (eq 10-13) and for it to be dagger another 7 (1-3 in def 4.3 and unitary conditions on the 4 natural isomorphisms). To save myself from a monstrous proof spanning many pages I will therefore define the natural isomorphisms and prove a couple of the conditions.

The monoidal unit is given by the 0-dimensional space $\{0\}$ containing just the 0 vector.

$$\alpha_{V_1,V_2,V_3} : V_1 \oplus (V_2 \oplus V_3) \to (V_1 \oplus V_2) \otimes V_3 :: v' \oplus (v'' \oplus v''') \mapsto (v' \oplus v'') \otimes v'''$$

$$\lambda_V : V \to \{0\} \oplus V :: v \mapsto 0 \oplus v \qquad \rho_V : V \to V \oplus \{0\} :: v \mapsto v \oplus 0$$

$$\sigma_{V_1,V_2} : V_1 \oplus V_2 \to V_2 \oplus V_1 :: v' \oplus v'' \mapsto v'' \oplus v'$$

We are often given a choice of †, for example when our underlying field is $\mathbb{C}$ the most obvious choice of † is to take the conjugate transpose. However whatever our underlying field the transpose (defined with respect to a given basis) will provide a † structure. We will use the transpose for the purposes of this proof.

Condition 13
The below diagram commutes

$$\begin{tikzcd}
v' \otimes (v'' \otimes v''') \arrow[r, "\alpha"] \arrow[d, "1_{V_1} \otimes \sigma_{V_2,V_3}"'] & (v' \otimes v'') \otimes v''' \arrow[r, "\sigma_{(V_1 \otimes V_2),V_3}"] & v''' \otimes (v' \otimes v'') \arrow[d, "\alpha"] \\
v' \otimes (v''' \otimes v'') \arrow[r, "\alpha"'] & (v' \otimes v''') \otimes v'' \arrow[r, "\sigma_{V_1,V_2} \otimes 1_{V_3}"'] & (v''' \otimes v') \otimes v''
\end{tikzcd}$$

Condition 3 from def 4.3
Taking f to be an m_1 by n_1 matrix F (with respect to the same basis as our transpose is defined against) and g an m_2 by n_2 matrix G. $f \oplus g$ is an $m_1 + m_2$ by $n_1 + n_2$ matrix as below.

$$\begin{aligned}
f \oplus g &= \begin{pmatrix} F & 0 \\ 0 & G \end{pmatrix} \\
(f \oplus g)^T &= \left(\begin{array}{cc} F & 0 \\ 0 & G \end{array} \right)^T \\
&= \left(\begin{array}{cc} F^T & 0 \\ 0 & G^T \end{array} \right) = f^T \oplus g^T
\end{aligned}$$

□

Theorem 5.2. $\mathbf{FdVect}_{\mathbb{K}}$ with monoidal tensor $\otimes$, the tensor product, is a dagger symmetric monoidal category.

Proof. The monoidal unit for $\otimes$ is given by the underlying field $\mathbb{K}$. The natural isomorphisms α and σ are defined as in the $\oplus$ case. Again we take the transpose to be our †.

$$\begin{aligned}
\lambda_V &: V \to \mathbb{K} \oplus V :: v \mapsto 1 \otimes v & \rho_V &: V \to V \oplus \mathbb{K} :: v \mapsto v \oplus 1 \\
\lambda_V^{-1} &: \mathbb{K} \oplus V \to V :: k \otimes v \mapsto k \cdot v
\end{aligned}$$

Condition 6
The below diagram commutes

$$\begin{tikzcd}
v \otimes (v' \otimes v'') \arrow[r, "\alpha_{V_1,V_2,V_3}"] \arrow[d, "f \otimes (g \otimes h)"'] & (v \otimes v') \otimes v'' \arrow[d, "(f \otimes g) \otimes h"] \\
f(v) \otimes (g(v') \otimes h(v'')) \arrow[r, "\alpha_{V_1',V_2',V_3'}"'] & (f(v) \otimes g(v')) \otimes h(v'')
\end{tikzcd}$$

Condition 9
The below diagram commutes

$$\begin{tikzcd}
v \otimes v' \arrow[r, "1_{V_1} \otimes \lambda_{V_2}"] \arrow[dr, "\rho_{V_1} \otimes 1_{V_2}"'] & v \otimes (1 \otimes v') \arrow[d, "\alpha_{V_1,\mathbb{K},V_2}"] \\
& (v \otimes 1) \otimes v'
\end{tikzcd}$$

and

$$\lambda_{\mathbb{K}} k = 1 \otimes k = k = k \otimes 1 = \rho_{\mathbb{K}} k$$

□

Quantum categories

We now introduce one of the defining features of quantum-like systems, distinguishing them from their classical counterparts. The unit and counit in a compact closed category will give us the notion of entanglement and be key in protocols such as teleportation or entanglement swapping.

Definition 5.3. A compact closed category is a symmetric monoidal category with the following :-

1. For every $A \in |\mathbf{C}|$, there exists A^* the dual of A,
2. A pair of morphisms

$$\eta_A : I \to A^* \otimes A \qquad \text{and} \qquad \epsilon_A : A \otimes A^* \to I,$$

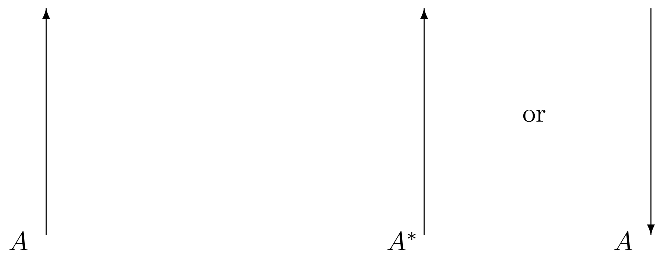
called the unit and counit respectively (sometimes referred to as cup and cap) , with the below diagrams commuting

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

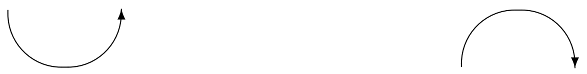
$$\begin{tikzcd}
A^* \arrow[r, "\lambda_{A^*}"] \arrow[d, "1_{A^*}"'] & (I \otimes A^*) \arrow[r, "\eta_A \otimes 1_{A^*}"] & (A^* \otimes A) \otimes A^* \arrow[d, "\alpha^{-1}_{A^*,A,A^*}"] \\
A^* & (A^* \otimes I) \arrow[l, "\rho^{-1}_{A^*}"'] & A^* \otimes (A \otimes A^*) \arrow[l, "1_{A^*} \otimes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

These objects and morphisms have a diagrammatic representation

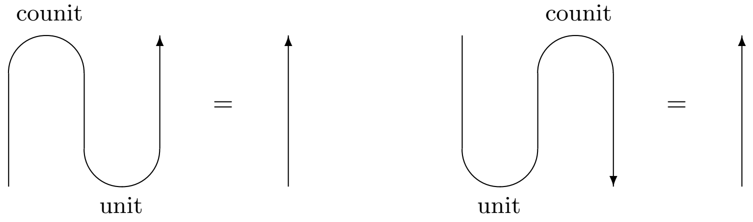
A is depicted as an upwards arrow as before. A^* is depicted as a upwards arrow labelled A^* or a downward arrow labelled A. A and A^* are shown below respectively.



η_A the unit and ϵ_A the counit will be depicted as,



The commutation of the diagrams above looks like



Definition 5.4. A dagger compact category is a compact closed category and a dagger symmetric monoidal category where for all $A \in |C|$,

$$\epsilon_A = \eta_A^{\dagger} \circ \sigma_{A,A^*}$$

Theorem 5.5. $\mathbf{FdVect}_{\mathbb{K}}$ is compact closed with respect to the tensor product.

Proof. We take the dual space V^* to be the usual linear algebraic dual space. Let $\{|i\rangle\}_i$ be a basis for V and $\{\langle i|\}_i$ be a basis for V^* such that $\langle i|j\rangle = \delta_{ij}$ (note that $\langle\psi|\phi\rangle$ may not necessarily define an inner product). We take the unit to be,

$$\eta_V : \mathbb{K} \to V^* \otimes V :: 1 \mapsto \sum_{i=1}^{n} \langle i| \otimes |i\rangle$$

and the counit to be,

$$\epsilon_V : V \otimes V^* \to \mathbb{K} :: |i\rangle \otimes \langle j| \mapsto \langle i|j\rangle$$

We note that the linear maps η_V and ϵ_V do not depend on the choice of basis $\{|i\rangle\}_i$ we can see this by the fact there is a canonical isomorphism called the name $\ulcorner\ \urcorner$(see ref [categories for the practicing physicist])

$$\ulcorner\ \urcorner : \mathbf{FdVect}_{\mathbb{K}}(V,V) \to \mathbf{FdVect}_{\mathbb{K}}(\mathbb{K}, V^* \otimes V) :: \sum m_{ij}|i\rangle\langle j| \mapsto \sum m_{ij}\langle i| \otimes |j\rangle$$

Notice this canonical isomorphism does not depend on the choice of basis. Also as η_V is the image in this isomorphism of 1_V, which also does not depend on the choice of basis, we see η_V is defined independently of the choice of basis. By a similar argument it follows ϵ_V also does not depend on the choice of basis.

The compactness conditions on a general state $|\psi\rangle = \Sigma\psi_i|i\rangle$

$$\begin{aligned}(\epsilon_V \otimes 1_V) \circ (1_V \otimes \eta_V) \circ \left(\left(\sum_{i=1}^{n} \psi_i|i\rangle\right) \otimes 1_V \otimes 1_V\right) \\ = (\epsilon_V \otimes 1_V) \circ \left(\sum_{i,j=1}^{n} \psi_i|i\rangle \otimes \langle j| \otimes |j\rangle\right) \\ = 1_V \otimes 1_V \otimes \left(\sum_{j=1}^{n} \psi_j|j\rangle\right)\end{aligned}$$

and for $\langle\psi| = \Sigma\psi_i\langle i|$

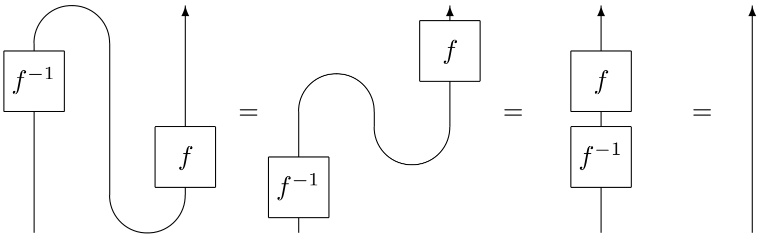
$$\begin{aligned}(1_V \otimes \epsilon_V) \circ (\eta_V \otimes 1_V) \circ \left(1_V \otimes 1_V \otimes \left(\sum_{i=1}^{n} \psi_i\langle i|\right)\right) \\ = (1_V \otimes \epsilon_V) \circ \left(\sum_{i,j=1}^{n} \psi_i\langle j| \otimes |j\rangle \otimes \langle i|\right) \\ = \left(\sum_{j=1}^{n} \psi_j\langle j|\right) \otimes 1_V \otimes 1_V\end{aligned}$$

□

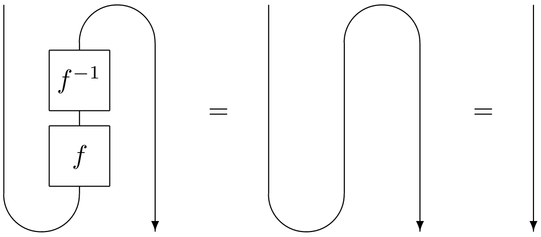
There are also other possibilities to turn $\mathbf{FdVect}_{\mathbb{K}}$ into a compact category. Given an invertible function $f : V \to V$ we can use,

$$\eta'_V := (1_{V^*} \otimes f) \circ \eta_V \qquad \text{and} \qquad \epsilon_V \circ (f^{-1} \otimes 1_{V^*})$$

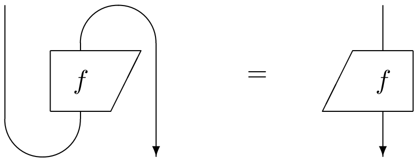
It is fairly easy to see the compactness conditions hold using diagrammatic form,



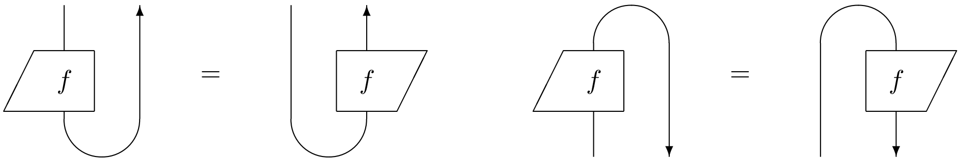
and



Using previous asymmetrical notation for a morphism f we can now define our transpose.

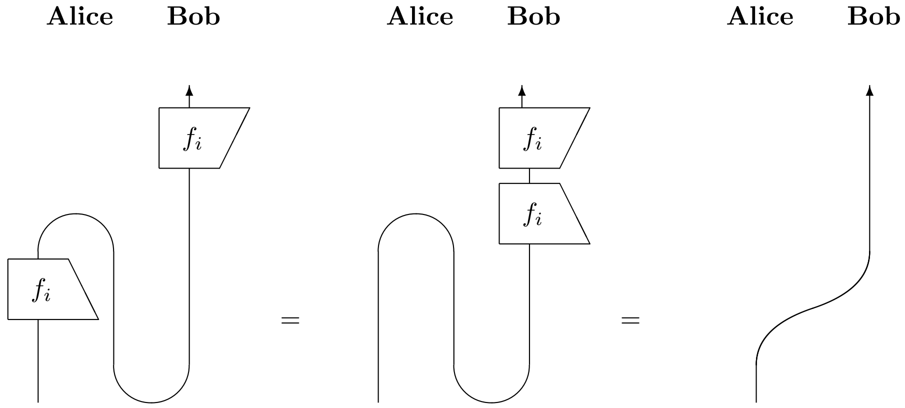


In example 3.1 we came across the idea of sliding morphisms, depicted as boxes, along identity lines. We now introduce the concept of sliding these boxes around the U-bends of the unit and counit.



Example 5.6. The quantum teleportation protocol is one of the most interesting and remarkable consequences of entanglement in quantum systems. It also provides a good example of compact closed categories in action. Let $X \in |\mathbf{FdHilb}|$ be the 2-dimensional space with basis elements $|0\rangle$ and $|1\rangle$ with $X^* = X$. We now set up the necessary parts to the protocol in three steps:-

1. We use the method of 5.5 to create the Bell state unit $|\Phi^+\rangle = |00\rangle + |11\rangle$ and counit $\langle\Phi^+| = \langle 00| + \langle 11|$.
2. Using the Bell matrices f_i, which are invertible (with $f^\dagger = f^{-1}$), we can create the Bell basis (the method for creating units and counits from invertible functions is explained above) $|\Phi^+\rangle, |\Phi^-\rangle = |00\rangle - |11\rangle$, $|\Psi^+\rangle = |01\rangle + |10\rangle$ and $|\Psi^-\rangle = |01\rangle - |10\rangle$. Each of these defines a unit and counit.
3. The teleportation protocol then reduces to just sliding boxes and one use of the compactness condition to simplify.



Corollary 5.7. $\mathbf{FdVect}_{\mathbb{K}}$ is dagger compact with respect to the tensor product

Proof. Follows from theorem 5.2, theorem 5.5 and that for η_V and ϵ_V we have

$$\epsilon_V = \eta_V^\dagger \circ \sigma_{V,V^*}$$

□

Classical categories

In the same way compact closed categories form the basis for defining what makes a system quantum-like we can also add categorical structure to help us define classical properties. Cartesian categories can be thought of the classical counterparts to compact closed categories in that they provide the first steps in defining classical properties in a system. They will allow us to describe uniform copying and deleting operation that do not exist in quantum systems due to the no-cloning and no-deleting theorems.

Definition 5.8. A product of A_1 and $A_2 \in |\mathbf{C}|$ is a triple consisting of

1. Object $A_1 \times A_2 \in |\mathbf{C}|$
2. Morphism $\pi_1 : A_1 \times A_2 \to A_1$
3. Morphism $\pi_2 : A_1 \times A_2 \to A_2$

Such that for all $B, A_1, A_2 \in |\mathbf{C}|$ the operation

$$(\pi_1 \circ -, \pi_2 \circ -) : \mathbf{C}(B, A_1 \times A_2) \to \mathbf{C}(B, A_1) \times \mathbf{C}(B, A_2)$$

admits an inverse $\langle -, - \rangle_{B,A_1,A_2}$

Definition 5.9. A category $\mathbf{C}$ is Cartesian if any pair of objects in $\mathbf{C}$ admit a product.

Note that in a Cartesian category the products are not necessarily unique, however two distinct products of a pair of objects will be isomorphic. Using the disjoint union $+$ we now define the coproduct.

Definition 5.10. A coproduct of A_1 and $A_2 \in |\mathbf{C}|$ is a triple consisting of

1. Object $A_1 + A_2 \in |\mathbf{C}|$
2. Morphism $\iota_1 : A_1 \to A_1 + A_2$
3. Morphism $\iota_2 : A_2 \to A_1 + A_2$

Such that for all $B, A_1, A_2 \in |\mathbf{C}|$ the operation

$$(- \circ \iota_1, - \circ \iota_2) : \mathbf{C}(A_1 + A_2, B) \to \mathbf{C}(A_1, B) \times \mathbf{C}(A_2, B)$$

admits an inverse $\langle -, - \rangle_{B,A_1,A_2}$

Equivalently a category $\mathbf{C}$ is co-Cartesian if any pair of objects in $\mathbf{C}$ admit a coproduct.

We combine the notions of product and co-product with biproducts or direct sums. Firstly we remark that a zero object is one with exactly one morphism to and from each object (including itself). The zero map $0_{A,B}$ is the canonical map composing the unique morphism from A to the zero object with the unique morphism from the zero object to B.

Definition 5.11. In a category $\mathbf{C}$, with a zero object, a biproduct (or direct sum) of A_1 and $A_2 \in |\mathbf{C}|$ is a quintuple consisting of object $A_1 \oplus A_2 \in |\mathbf{C}|$ and four morphism:

$$\begin{tikzcd}
A_1 \arrow[r, bend left, "\iota_1"] & A_1 \oplus A_2 \arrow[l, bend left, "\pi_1"] \arrow[r, bend right, "\pi_1"'] & A_2 \arrow[l, bend right, "\iota_1"']
\end{tikzcd}$$

satisfying

$$\pi_1 \circ \iota_1 = 1_{A_1} \qquad \pi_2 \circ \iota_1 = 0_{A_1,A_2}$$
$$\pi_1 \circ \iota_2 = 0_{A_2,A_1} \qquad \pi_2 \circ \iota_2 = 1_{A_2}$$

A category $\mathbf{C}$ is a biproduct category if any pair of objects in $\mathbf{C}$ admits a biproduct.

Theorem 5.12. $\mathbf{FdVect}_{\mathbb{K}}$ *is a Cartesian category with respect to the direct sum* $\oplus$

Proof. Take objects V_1 and V_2, n and m dimensional vector spaces respectively, then we let $V_1 \oplus V_2, \pi_1, \pi_2$ be the product. π_1 is a matrix with the first n columns an $n \times n$ identity matrix followed by m columns of 0s. Similarly π_2 is a matrix with the first n columns 0s followed by an $m \times m$ identity matrix.

$$\pi_1 = \left.\begin{pmatrix} \underbrace{\begin{matrix} 1 & 0 & \dots \\ 0 & 1 & \dots \\ \vdots & \vdots & \ddots \end{matrix}}_{\text{n columns}} & \underbrace{\begin{matrix} 0 & 0 & \dots \\ 0 & 0 & \dots \\ \vdots & \vdots & \ddots \end{matrix}}_{\text{m columns}} \end{pmatrix}\right\}\text{n rows}$$

$$\pi_2 = \left.\begin{pmatrix} \underbrace{\begin{matrix} 0 & 0 & \dots \\ 0 & 0 & \dots \\ \vdots & \vdots & \ddots \end{matrix}}_{\text{n columns}} & \underbrace{\begin{matrix} 1 & 0 & \dots \\ 0 & 1 & \dots \\ \vdots & \vdots & \ddots \end{matrix}}_{\text{m columns}} \end{pmatrix}\right\}\text{m rows}$$

Take any space W a p dimensional space and morphism $f : W \to V_1 \oplus V_2$ represented by the $(n+m) \times p$ matrix F. The operation $(\pi_1 \circ -, \pi_2 \circ -)$ takes f to (f_1, f_2) where f_1 is represented by a matrix F_1 containing the top n rows of F and equivalently F_2 the bottom m rows of F. The inverse $\langle -, - \rangle_{W,V_1,V_2}$ is obtained by simply putting the two halves back together again i.e.

$$\langle f_1, f_2 \rangle_{W,V_1,V_2} = \begin{pmatrix} F_1 \\ F_2 \end{pmatrix}$$

$\square$

Note also that if we let $\iota_1 = \pi_1^T$ and $\iota_2 = \pi_2^T$ it is easy to see that $V_1 \oplus V_2$ is a biproduct and therefore $\mathbf{FdVect}_{\mathbb{K}}$ a biproduct category with respect to $\oplus$. Here the zero object is the zero-dimensional vector space and the zero map, just a matrix of 0s.

6 Copying, deleting and classical structures

In classical computing the idea of copying and deleting information seems fundamental in any practical device. However this is one area where quantum computers and classical computers differ significantly; in quantum computing we cannot copy or delete arbitrary qubits.

Example 6.1. The CNOT gate will negate the second qubit when the first qubit is 1 and leave the second qubit unchanged when the first qubit is 0, it will always leave the first qubit unchanged.

The CNOT gate in classical computing can be used to copy one qubit if we place a zero bit next to it. If we choose an arbitrary qubit however the result is not the same.

Classical case

$$00 \xrightarrow{CNOT} 00 \qquad 10 \xrightarrow{CNOT} 11$$

Quantum case

$$(a|0\rangle + b|1\rangle)|0\rangle \xrightarrow{CNOT} a|00\rangle + b|11\rangle$$

We can see in the quantum case the only states which will be copied are $|0\rangle$ and $|1\rangle$.

In fact it is easy to show for any linear map we can at best only copy orthogonal states, giving rise to the no-cloning theorem. There exists an equivalent theorem called the no-deleting theorem showing the reverse, i.e. that we cannot take two identical qubits and transform them into a single qubit of the same state. These theorems are consistent with other results in physics, for example both the ability to delete qubits or copy qubits would allow us to transfer data faster than the speed of light. Also the ability to copy qubits would also contradict the uncertainty principle, because we could make measurements on many copies allowing arbitrary precision. The no-cloning theorem also plays a key role in quantum cryptography.

We can study the concepts behind copying and deleting information using a category theory approach. I will define internal monoidal and comonoidal structures below. In classical-like systems (more formally Cartesian categories) these structures are exactly copying and deleting operations. In quantum-like systems these structures will not copy all states, often copying certain states. They allow the generation of entangled states, needed in protocols such as quantum teleportation.

Definition 6.2. An internal monoid (X, m, e) is an object X with a pair of morphism m, the multiplication, and e (sometimes denoted u), the multiplicative unit,

$$X \otimes X \xrightarrow{m} X \xleftarrow{e} I$$

such that the below diagrams commute,

$$\begin{tikzcd}
X & X \otimes X \arrow[l, "m"'] \\
X \otimes X \arrow[u, "m"] & X \otimes X \otimes X \arrow[l, "m\otimes 1_X"] \arrow[u, "1_X\otimes m"']
\end{tikzcd}
\qquad
\begin{tikzcd}
 & X & \\
I \otimes X \arrow[ur, "\simeq"] \arrow[r, "e\otimes 1_X"'] & X \otimes X \arrow[u, "m"] & X \otimes I \arrow[ul, "\simeq"'] \arrow[l, "1_X\otimes e"]
\end{tikzcd}$$

Definition 6.3. An internal comonoid (X, δ, ϵ) is an object X with a pair of morphism δ, the comultiplication, and ϵ, the comultiplicative unit,

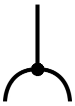
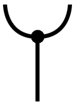
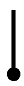
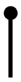
$$X \otimes X \xleftarrow{\delta} X \xrightarrow{\epsilon} I$$

such that the below diagrams commute,

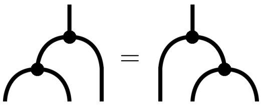
$$\begin{tikzcd}
X \arrow[r, "\delta"] \arrow[d, "\delta"'] & X \otimes X \arrow[d, "1_X\otimes\delta"] \\
X \otimes X \arrow[r, "\delta\otimes 1_X"'] & X \otimes X \otimes X
\end{tikzcd}
\qquad
\begin{tikzcd}
 & X \arrow[dl, "\simeq"'] \arrow[d, "\delta"'] \arrow[dr, "\simeq"] & \\
I \otimes X & X \otimes X \arrow[l, "\epsilon\otimes 1_X"] \arrow[r, "1_X\otimes\epsilon"'] & X \otimes I
\end{tikzcd}$$

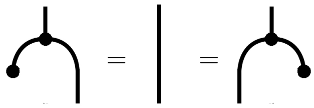
Strictly we should only refer to internal (co)monoids by (X, m, e) or (X, δ, ϵ). However as the (co)unit will be unique, we sometimes refer to a (co)monoid simply by its (co)multiplication, implying that a (co)unit does exist.

We can also represent these morphisms in diagrammatic form,

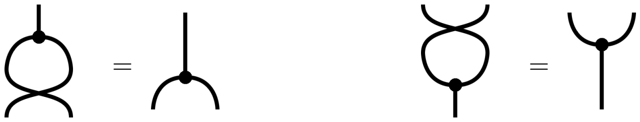
$m :=$  $\delta :=$  $e :=$  $\epsilon :=$ 

For example the two commutative diagrams used to define a monoid (the associative law and unit law) can be represented as below





We see below the respective conditions for commutativity in an internal monoid and comonoid.



In a dagger monoidal category we can use the adjoint to find an internal comonoid given we know an internal monoid or vice versa.

Lemma 6.4. Given an internal (commutative) monoid (X, m, e), $(X, m^\dagger, e^\dagger)$ defines an internal (commutative) comonoid

Proof. It is fairly easy to see that taking the adjoint of one of the above diagrams is the same as flipping the diagram upside. More formally from the associative law on (X, m, e) we get,

$$\begin{aligned} m \circ (m \otimes 1) &= m \circ (1 \otimes m) \\ (m \circ (m \otimes 1))^\dagger &= (m \circ (1 \otimes m))^\dagger \\ (m \otimes 1)^\dagger \otimes m^\dagger &= (1 \otimes m)^\dagger \otimes m^\dagger \\ (m^\dagger \otimes 1) \otimes m^\dagger &= (1 \otimes m^\dagger) \otimes m^\dagger \end{aligned}$$

giving the associative law in $(X, m^\dagger, e^\dagger)$. Also from the unit law on (X, m, e) we get,

$$\begin{aligned} m \circ (e \otimes 1) &= 1 = m \circ (1 \otimes e) \\ (m \circ (e \otimes 1))^\dagger &= 1 = (m \circ (1 \otimes e))^\dagger \\ (e^\dagger \otimes 1) \otimes m^\dagger &= 1 = (1 \otimes e^\dagger) \otimes m^\dagger \end{aligned}$$

giving the unit law in $(X, m^\dagger, e^\dagger)$. Finally from commutativity in (X, m, e) we get,

$$\begin{aligned} m \circ \sigma &= m \\ (m \circ \sigma)^\dagger &= m^\dagger \\ \sigma^\dagger \circ m^\dagger = \sigma \circ m^\dagger &= m^\dagger \end{aligned}$$

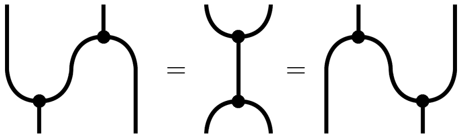
□

Definition 6.5. An internal dagger monoidal structure is an internal monoidal structure (X, m, e) together with an internal comonoidal structure (X, δ, ϵ) such that the comonoidal structure is the dagger of the monoidal structure. I.e. $m^\dagger = \delta$ and $e^\dagger = \epsilon$. Note that the combination of a monoidal and comonoidal structure is often written as $(X, m, e, \delta, \epsilon)$.

Definition 6.6. Frobenius algebra (also called Frobenius monoidal category) have internal monoidal and comonoidal structures $(X, m, e, \delta, \epsilon)$ satisfying the Frobenius condition, shown below.

$$\begin{tikzcd}
X \otimes X \arrow[rr, "1\otimes\delta"] \arrow[dd, "\delta\otimes 1"'] \arrow[dr, "m"] & & X \otimes X \otimes X \arrow[dd, "m\otimes 1"] \\
& X \arrow[dr, "\delta"] & \\
X \otimes X \otimes X \arrow[rr, "1\otimes m"'] & & X \otimes X
\end{tikzcd}$$

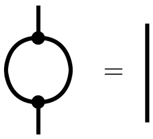
Alternatively here are the conditions in diagrammatic form,



Definition 6.7. A Frobenius category is called special if

$$m \circ \delta = 1$$

In diagrammatic form,



Definition 6.8. A morphism $f : X \to Y$ is a monoid homomorphism for internal monoids (X, m, e) and (Y, m', e') if

$$f \circ m = m' \circ (f \otimes f) \qquad \text{and} \qquad f \circ e = e'$$

and a comonoid homomorphism for internal comonoids (X, δ, ϵ) and (Y, δ', ϵ') if

$$\delta' \circ f = (f \otimes f) \circ \delta \qquad \text{and} \qquad \epsilon' \circ f = \epsilon$$

Definition 6.9. A copyable element (or classical element) of a †-Frobenius monoid (X, m, e) is a comonoid homomorphism $\alpha : I \to X$, i.e. the below diagrams commute

$$\begin{tikzcd}
I \arrow[r, "\alpha"] \arrow[d, "\delta"'] & X \arrow[d, "\delta"] \\
I \otimes I \arrow[r, "\alpha\otimes\alpha"'] & X \otimes X
\end{tikzcd}
\qquad
\begin{tikzcd}
I \arrow[d, "\alpha"'] \arrow[dr, "1_I"] & \\
X \arrow[r, "\epsilon"'] & I
\end{tikzcd}$$

Note these two diagrams show the element is copyable and deletable respectively, even though it is still only referred to as copyable. The name classical comes from the classical properties it possesses. As we see in theorem 6.10 given an internal comonoid in $\mathbf{FdVect}_{\mathbb{K}}$, with monoidal tensor $\oplus$, every element is a classical element. In fact in general, the existence of an internal comonoid structure making every element classical is an equivalent definition of a Cartesian category, also if such an internal comonoid exists it will be the only possible internal comonoid, see [3].

Theorem 6.10. The only possible internal comonoids in $\mathbf{FdVect}_{\mathbb{K}}$ with monoidal tensor $\oplus$ are universal copying and deleting operations.

Proof. Let (X, δ, ϵ) define a comonoid in $\mathbf{FdVect}_{\mathbb{K}}$. We can split up our δ into two parts $\delta_1 = \pi_1 \circ \delta$ and $\delta_2 = \pi_2 \circ \delta$, so for $x \in X$ $\delta(x) = (\delta_1(x), \delta_2(x))$. We now use the unit law to give

$$x = \lambda_A^{-1} \circ (\epsilon \oplus 1_X) \circ \delta(x) = \lambda_A^{-1} \circ (\epsilon \circ \delta_1(x), \delta_2(x)) = k \cdot \delta_2(x)$$

So $\delta_2(x)$ is a scalar multiple k'' of x. By the right unit law we get similarly $\delta_1(x)$ is a scalar multiple k' of x, note our multiple must be invertible and therefore non-zero. Next by associativity we see.

$$(1_X \oplus \delta) \circ \delta = (\delta \oplus 1_X) \circ \delta$$
$$(\delta_1, \delta_1 \circ \delta_2, \delta_2 \circ \delta_2) = (\delta_1 \circ \delta_1, \delta_2 \circ \delta_1, \delta_2)$$

While we already know $\delta_1 \circ \delta_2 = \delta_2 \circ \delta_2$ due to commutativity of scalars, we also get $\delta_1 = \delta_1 \circ \delta_1$ telling us that $k' = k'^2$ therefore $k' = 1$, and similarly we get $k'' = 1$. Therefore $\delta(x) = (x, x)$ for all $x \in X$ we also note that $\epsilon(x) = 1$. □

Definition 6.11. A classical structure is a dagger Frobenius algebra which is also commutative and special.

While at first the name may seem misleading as classical-like categories such as Cartesian categories will not have a classical structure, however the name comes about through the role of extracting classical resources of the structure via classical elements. However classical structures also provides many important quantum resources, for example we can use them to create quantum structures.

Definition 6.12. A quantum structure in a dagger monoidal category is a pair (X, η) such that $\eta : I \to X \otimes X$ and $\eta^\dagger : X \otimes X \to I$ defines a unit (not to be confused with the multiplicative unit) and counit, making our category a compact closed category with X the dual of itself.

Theorem 6.13. Every classical structure induces a quantum structure with the unit $\eta : I \xrightarrow{e} X \xrightarrow{\delta} X \otimes X$ and counit $\eta^{\dagger} : X \otimes X \xrightarrow{m} X \xrightarrow{\epsilon} I$, also making the category dagger-compact.

Proof. The compact closed conditions are easily seen when written in diagrammatic form and by use of the Frobenius equations. □

While every classical structure induces a quantum structure, not all quantum structures arise from classical structures. By applying the copying operation of a classical structure to a non-classical element we obtain an entangled state, in the case of a quantum structure via the non-classical multiplicative unit e.

7 Classical structures in FdHilb, Rel and FdVect over GF(p)

Classical structures form a key part to any quantum-like category. Not only do they allow construction of quantum structures which are used in many quantum protocols, but they often have an interesting structure within their mathematical contexts.

Classical structures in FdHilb

In finite dimensional Hilbert spaces classical structures correspond to orthonormal bases (the set of classical elements forming the basis). We can also characterise orthogonal bases and in fact any arbitrary basis using weaker conditions. These theorems are stated below, see [11] for proofs of these results.

Theorem 7.1. Commutative special Frobenius categories correspond to arbitrary bases.

Theorem 7.2. Commutative †-Frobenius categories correspond to orthogonal bases.

Theorem 7.3. Commutative special †-Frobenius categories correspond to orthonormal bases.

It is interesting to see that commutative Frobenius categories do not display such nice characteristic as the structures above and can come in a wide range of forms. One of the dagger or special condition is needed for the structures to correspond to a basis. We also note that classical structures are often refered to as basis structures because of the connection in theorem 7.3

Classical structures in Rel

In **Rel** we can define a basis in a similar way to a vector space, for example every element can be written as composition of basis elements below we show how this is done in **FdVect** and **Rel**,

$$|\psi\rangle = \sum_{i\in X} \psi_i \cdot |i\rangle \qquad\qquad A = \bigcup_{i\in X} a_i\{i\}$$

In **Rel** the sum becomes a union and coefficient become Boolean valued. However we see classical structures that do not copy basis element, called nonstandard classical structures. For example taking X to be the two element set denoted $II = \{0,1\}$ we can define comultiplication δ and comultiplicative unit ϵ to be,

$$\begin{aligned} \delta(0) &= \{00,11\} & \epsilon(0) &= \{*\} \\ \delta(1) &= \{01,10\} & \epsilon(1) &= \emptyset \end{aligned}$$

Here 00 represents $0 \otimes 0$. This provides a classical structure but only copies one element $\{0,1\}$.

It turns out that the classical structures in **Rel** correspond exactly to abelian groupoids. The different categorical conditions give us the needed properties for our structure to form an abelian groupoid, these are summarised below.

Categorical condition	Groupoid condition
Associativity of multiplication	Associativity
Multiplicative unit	Identity
Special condition	Closure over elements of X
Frobenius and special condition	Inverses
Commutativity	Commutativity

Before a more formal proof, we define the term single-valued internal monoid in **Rel**.

Definition 7.4. An internal monoid in **Rel** is single-valued iff for all $a, b \in X$, $m(a \otimes b) = \emptyset$ or $m(a \otimes b) = c$, where c is a single element of X.

Theorem 7.5. Any abelian groupoid defines a classical structures in **Rel**.

Proof. This proof is based on the proof given in [4], I have included some diagrams to make the proof easier to follow. For $a, b, c \in X$ if $a \cdot b = c$ in our groupoid then we define $m(a \otimes b) = c$ in our internal multiplication (we will denote $a \otimes b$ as ab). Associativity, commutativity and identity of the groupoid (or set of identities of components) then directly translate into a commutative internal monoidal structure (and therefore also the internal comonoidal structure).

It remains to show the special and Frobenius conditions. For all $a, b \in X$, $m(a, b)$ is a single element of the set X (m is single-valued), therefore for all $x \in X$, $\delta(x) = \{ab | a, b \in X \wedge m(ab) = x\}$. By considering xe_x where $e_x = xx^{-1}$, $\delta(x) \neq \emptyset$, it follows $m(\delta(x)) = x$, the special condition. We can write the

Frobenius condition as,

$$\forall x, y \in X \ \{ab|a, b \in X \wedge m(ab) = m(xy)\} = \{cm(d, y)|c, d \in X \wedge m(cd) = x\}$$
$$= \{m(x, c)d|c, d \in X \wedge m(cd) = y\}$$

Consider $cm(d, y)$ on the RHS(top), by associativity $m(cm(d, y)) = m(x, y)$ and therefore it will appear on the LHS. Similarly for $m(x, c)d$. Now take an a, b from the LHS, consider $c = a$ and $d = m(by^{-1})$, so by associativity

$$cm(d, y) = am(m(by^{-1})y) = ab$$

c(m(d,y)) appears on the RHS(top) as (again making use of associativity),

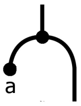
$$m(cd) = m(am(by^{-1})) = m(m(xy)y^{-1}) = x$$

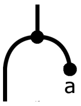
giving the top equality. By considering $c = m(x^{-1}a)$ and $d = b$, we get the bottom equality. □

Before we start on proving the other direction we start with a useful lemma

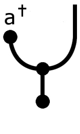
Lemma 7.6. Given a single-valued internal monoid in **Rel** the left and right action are partial bijections.

Proof. We now define the left and right action and an involution * on elements of X. $R_a(b) = m(ab)$ and $L_a(b) = m(ba)$ are the right and left action of a respectively, we will depict these as below:-

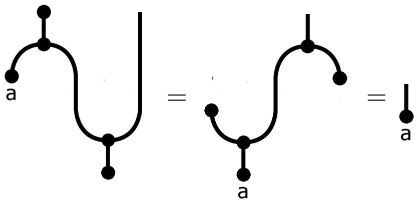
$L_a =$ 

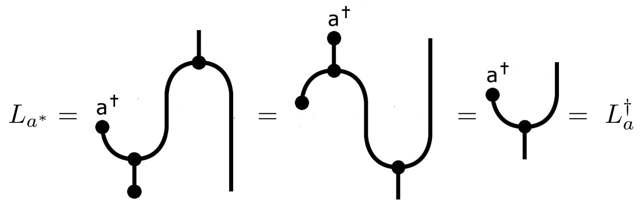
$R_a =$ 

We define the involution * by $a^* = (a^\dagger \otimes 1) \circ \delta \circ e$. In diagrammatic form,

$a^* =$ 

Making use of the Frobenius equations and the unit law we show this is in fact an involution and therefore a bijection on X. Also that $L_{a^*} = L_a^\dagger$.

$(a^*)^* =$ 



As m is single-valued for any $a \in X$ L_a is a partial map on X. Also as L_{a^*} must also be a partial map, $(L_a)^\dagger$ is a partial map, more precisely that for each $b \in X$ there is at most one $x \in X$ such that $m(a, x) = b$. This makes L_a a partial bijection. We can show R_a is a partial bijection with a very similar argument. □

Theorem 7.7. Any classical structure in **Rel** defines an abelian groupoid.

Proof. In the reverse to theorem 7.5 we externalise our internal monoidal structure to define a multiplication on elements of X. The special condition gives two important properties meaning the multiplication is single valued and for each $x \in X$ there exists $a, b \in X$ such that $a \cdot b = x$. Again associativity, commutativity and the unit (we will look more at the unit later in the proof) of the internal monoid directly translate into our multiplication.

Next we show we can partition X into disjoint sets X_i such that each X_i has a single element of X, e_i as its identity. Let $e = \{e_i\}_i$ with $e_i \in X$, it is easy to see for any $x \in X$ that for each e_i $m(x, e_i) = x$ or $m(x, e_i) = \emptyset$. For each $x \in X$ there exist exactly one e_i such that $m(x, e_i) = x$ as L_x is injective, we therefore place x in X_i.

We now show these sets X_i: firstly do not interact with each other and secondly that each one forms a group. Take $x_i \in X_i$ and $x_j \in X_j$ and $(i \neq j)$,

$$m(x_i, x_j) = m(x_i, m(e_j, x_j)) = m(m(x_i, e_j), x_j)) = m(\emptyset, x_j) = \emptyset$$

Take $a, b \in X_i$, if $m(a, b) = c \neq \emptyset$ then if $c \in X_j$, $m(m(a, b), e_j) = m(a, m(b, e_j))$ is defined and therefore $m(b, e_j)$ which implies $i = j$. Consider now $a \in X_i$ and $a^* \in X_j$, so $a^* = L_{a^*}(e_j) = L_a^\dagger(e_j)$ therefore $m(a, a^*) = e_j$. We see a^* is the inverse of a and also here $i = j$, so $a^* \in X_i$ (by considering $L_a = L_{(a^*)^\dagger}$ we get $m(a^*, a) = e_i$ without needing commutativity). Now we have inverses it remains to show that our multiplication is total over X_i. Consider $a, b \in X_i$, so

$$b = m(e_i, b) = m(m(a^*, a), b) = m(a^*, m(a, b)) \tag{14}$$

therefore $m(a, b)$ is defined. □

Theorem 7.8. Classical structures in **Rel** are precisely the abelian groupoids over the set X

Proof. This follows from theorem 7.5 and 7.7. □

Note that we only used commutativity in making our group abelian and vice versa, therefore the non-commutative special Frobenius algebras correspond exactly to non-abelian groupoids.

Classical structures in $\mathbf{FdVect}_{F_p}$

Before this project very little was known about the different categorical structures of $\mathbf{FdVect}_{F_p}$ or for that matter vector spaces over any finite field. To investigate this problem I started by using the mathematical program Mathematica to calculate different structures in $\mathbf{FdVect}_{F_2}$. These structures include commutative internal monoids (the transpose provides the commutative comonoid see lemma 6.4), commutative Frobenius algebras, special commutative Frobenius algebras, dagger commutative Frobenius algebras and classical structures (special dagger commutative Frobenius algebras). This analysis was done firstly using $X = F_2^2$ then $X = F_2^3$. These results can be found in Appendix A. Theorems 7.13, 7.14, 7.15, 7.16, 7.19, 7.20 and 7.21 are all original work (with most theorems that provide lead up to these results either original or the proof constructed from scratch).

From the 2-dimensional case over F_2 we get two classical structures with monoids as below (positions in matrix from left to right correspond to 00, 01, 10 and 11 and going down 0 and 1)

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

Immediately we can see we have one standard classical structure and one non-standard classical structure. For the case of more than 2 dimensions we also get at least one standard classical structure. We generalise this with the following result. Note below the abstract notion of orthonormal basis.

Theorem 7.9. Given a vector space X over field $\mathbb{K}$ with our † involution defined over the direct sum as well as the tensor product (ie. $(f \oplus g)^\dagger = f^\dagger \oplus g^\dagger$). Given any choice of basis $|0\rangle, |1\rangle, ..., |n\rangle \in X$ such that $\langle i|j\rangle = \delta_{ij}$ (if $\langle\phi|\psi\rangle$ defines an inner product then this is an orthonormal basis) then the base copying operation $\delta|i\rangle = |ii\rangle$ and comultiplicative unit $\epsilon|i\rangle = 1$ gives a classical structure in $\mathbf{FdVect}_{\mathbb{K}}$.

Proof. Firstly we rewrite the comultiplication and unit in terms of morphisms from $V \to I$ and $I \to V \otimes V$

$$\delta = \sum_i |ii\rangle \circ \langle i| \qquad\qquad \epsilon = \sum_i \langle i|$$

we can now take the adjoint to give our multiplication

$$\begin{aligned} m = \delta^\dagger &= \left(\sum_i |ii\rangle \circ \langle i|\right)^\dagger \qquad\qquad e = \epsilon^\dagger = \sum_i |i\rangle \\ &= \sum_i |i\rangle \circ \langle ii| \end{aligned}$$

Next we show that (X, δ, ϵ) defines a commutative internal comonoid and therefore by lemma 6.4 (X, m, e) defines a commutative internal monoid. For general element $|\psi\rangle = \Sigma\psi_i \cdot |i\rangle$,

Commutativity

$$\begin{aligned} \sigma \circ \delta \circ |\psi\rangle &= \sigma \circ \left(\sum_j |jj\rangle \circ \langle j|\right) \circ \left(\sum_k \psi_k \cdot |k\rangle\right) \\ &= \sigma \circ \left(\sum_j \psi_j \cdot |jj\rangle\right) \\ &= \left(\sum_j \psi_j \cdot |jj\rangle\right) = \delta \circ |\psi\rangle \end{aligned}$$

Associativity

$$\begin{aligned} (\delta \otimes 1) \circ \delta \circ |\psi\rangle &= \left(\sum_i |ii\rangle \circ \langle i| \otimes 1\right) \circ \left(\sum_j \psi_j \cdot |jj\rangle\right) \\ &= \sum_i \psi_i \cdot |iii\rangle \\ &= \left(1 \otimes \sum_i |ii\rangle \circ \langle i|\right) \circ \left(\sum_j \psi_j \cdot |jj\rangle\right) = (1 \otimes \delta) \circ \delta \circ |\psi\rangle \end{aligned}$$

Left unit

$$\begin{aligned}(\epsilon \otimes 1) \circ \delta \circ |\psi\rangle &= \left(\sum_i \langle i| \otimes 1\right) \circ \left(\sum_j \psi_j \cdot |jj\rangle\right)\\ &= \left(\sum_i \psi_i \cdot |i\rangle\right) = |\psi\rangle\end{aligned}$$

Right unit follows from the left unit and commutativity

Next the Frobenius conditions, with general element $|\phi\rangle = \Sigma\phi_{i,j} \cdot |ij\rangle$

$$\begin{aligned}\delta \circ m \circ |\phi\rangle &= \left(\sum_i |ii\rangle \circ \langle i|\right) \circ \left(\sum_j |j\rangle \circ \langle jj|\right) \circ \sum_{k,l} \phi_{k,l} \cdot |kl\rangle\\ &= \left(\sum_i |ii\rangle \circ \langle i|\right) \circ \sum_j \phi_{j,j} \cdot |j\rangle\\ &= \sum_i \phi_{i,i} \cdot |ii\rangle\\ (m \otimes 1) \circ (1 \otimes \delta) \circ |\phi\rangle &= \left(\sum_i |i\rangle \circ \langle ii| \otimes 1\right) \circ \left(1 \otimes \sum_j |jj\rangle \circ \langle j|\right) \circ \sum_{k,l} \phi_{k,l} \cdot |kl\rangle\\ &= \left(\sum_i |i\rangle \circ \langle ii| \otimes 1\right) \circ \sum_{k,j} \phi_{k,j} \cdot |kjj\rangle\\ &= \sum_i \phi_{i,i} \cdot |ii\rangle\\ (1 \otimes m) \circ (\delta \otimes 1) \circ |\phi\rangle &= \left(1 \otimes \sum_i |i\rangle \circ \langle ii|\right) \circ \left(\sum_j |jj\rangle \circ \langle j| \otimes 1\right) \circ \sum_{k,l} \phi_{k,l} \cdot |kl\rangle\\ &= \left(1 \otimes \sum_i |i\rangle \circ \langle ii|\right) \circ \sum_{j,l} \phi_{j,l} \cdot |jjl\rangle\\ &= \sum_i \phi_{i,i} \cdot |ii\rangle\end{aligned}$$

Finally the special condition

$$\begin{aligned} m \circ \delta \circ |\psi\rangle &= \left(\sum_i |i\rangle \circ \langle ii| \right) \circ \left(\sum_j |jj\rangle \circ \langle j| \right) \circ \sum_k \psi_k \cdot |k\rangle \\ &= \left(\sum_i |i\rangle \circ \langle ii| \right) \circ \sum_j \psi_j \cdot |jj\rangle \\ &= \sum_i \psi_i \cdot |i\rangle = |\psi\rangle \end{aligned}$$

□

From now on in this section we will assume a basis to X, $|0\rangle, |1\rangle, ..., |n\rangle$ and take the † to be the transpose of the map defined over this basis. This means that we get the condition above that $\langle i|j\rangle = \delta_{ij}$.

Theorem 7.10. Given classical structures $(X, m, e, \delta, \epsilon)$ and $(Y, m', e', \delta', \epsilon')$ vector spaces X and Y respectively over field $\mathbb{K}$. We can define a classical structure in $X \oplus Y$.

Proof. Take the basis $|0\rangle, |1\rangle, ..., |n\rangle$ for X and $|n+1\rangle, |n+2\rangle, ..., |n+m\rangle$ for Y. We define our new multiplication m'' to be:-

$$m''(|i\rangle, |j\rangle) = \begin{cases} m(i,j) & i \leq n, j \leq n \\ m'(i,j) & i > n, j > n \\ 0 & i \leq n, j > n \\ 0 & i > n, j \leq n \end{cases}$$

the new unit e'' is just $e + e'$. Any element a in $X \oplus Y$ we can write uniquely as $a = a_x + a_y$ with $a_x \in X$ and $a_y \in Y$. We also have

$$\begin{aligned} a + b &= (a_x + b_x) + (a_y + b_y) \\ m''(a, b) &= m(a_x, b_x) + m'(a_y, b_y) \\ \delta(a) &= \delta(a_x) + \delta(a_y) \\ a^\dagger &= a_x^\dagger + a_y^\dagger \end{aligned}$$

All the required properties of a classical structure in $X \oplus Y$ now follow directly from the equivalent properties in X and Y. □

In $\mathbf{FdVect}_{F_2}$ we can define a similar notion of single-valued as in **Rel**.

Definition 7.11. An internal monoid in $\mathbf{FdVect}_{F_2}$ is single-valued iff for all basis element $|i\rangle$ and $|j\rangle$, $m|ij\rangle = 0$ or $m|ij\rangle = |k\rangle$, where $|k\rangle$ is a basis element.

When comparing $\mathbf{FdVect}_{F_2}$ to **Rel** (as pointed out in chapter 1) the arithmetic only differs with $1+1=1$ in **Rel** and $1+1=0$ in F_2, and this situation rarely comes up in the conditions for a classical structure when the monoid is single-valued. This leads to the fact that single-valued internal monoids correspond exactly to abelian groupoids with components of odd order. We start with a lemma about abelian groups.

Lemma 7.12. A finite abelian group X has odd order if and only if for all elements $x \in X$, $|\{y|y^2 = x\}|$ is odd.

Proof. All finite abelian groups can be expressed as the direct sum of cyclic groups of prime power order. E.g. any abelian group of order 12 would be isomorphic to either $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Take an odd order abelian group we can describe it as isomorphic to $\mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus ... \oplus \mathbb{Z}_{k_n}$ where $k_1, ..., k_n$ are all odd. In any cyclic group of odd order m each element x has one square root, if x is even then $x/2$ or odd then $x/2 + m/2$. It follows that in the direct sum of odd order cyclic groups each element $(x_1, x_2, ..., x_n)$ has one square root $(\sqrt{x_1}, \sqrt{x_2}, ..., \sqrt{x_n})$.

Similarly if we take an abelian group of even order, then at least one of our $\mathbb{Z}_{k_i}$ will be even. In an even order cyclic group every element has two square roots, $x/2$ and $x/2 + m/2$. It follows that the number of square roots of any element of our abelian group must therefore be a multiple of 2. □

In theorems 7.13 to 7.15 we let X be an n-dimensional vector space over F_2. N denotes a set of n elements.

Theorem 7.13. Any abelian groupoids with each component of odd order defines a single-valued classical structure in $\mathbf{FdVect}_{F_2}$.

Proof. Again we internalise the groupoid multiplication of N, so for $i, j, k \in N$, if $i \cdot j = k$ then $m(|i\rangle \otimes |j\rangle) = |k\rangle$ (we will denote $m(|i\rangle \otimes |j\rangle)$ as $m|ij\rangle$). Associativity, commutativity and identity again translate directly to X, note that while the identity in X may be the sum of basis vectors, $|i\rangle$, only one $|i\rangle$ will interact with any given basis element at a time. Also notice that our structure is again single valued.

Next we see a difference from **Rel** when we look at the special condition. For $i \in N$, $\delta|i\rangle$ is the set of all pairs j, k that multiply to make i. Notice if $j \neq k$ then we get the pair jk and kj due to commutativity. Therefore these pairs will not play a role in $m\delta|i\rangle$ and we only need to consider pair jj that multiply to i.

The special condition is therefore satisfied if the number of these is odd for all $i \in N$, by lemma 7.12 this is equivalent to when all components of the groupoid are of odd order. Finally for the Frobenius condition we need to show that given inputs $|i\rangle, |j\rangle$ basis elements we do not get any repeat pairs as outputs then our $1+1=0$ arithmetic of F_2 comes into play. The only way this can happen is if for some $i, j, k, l \in N$ you get two pairs jk and jl that multiply to i (by commutativity we do not need to consider when kj and lj multiply to i). However the existence of inverses prevents this as $m|j^{-1}i\rangle = m(m|jj^{-1}\rangle \otimes |k\rangle) = |k\rangle$, but similarly $m|j^{-1}i\rangle = l$ contradicting the fact m is single-valued. □

Theorem 7.14. Any single-valued classical structure in $\mathbf{FdVect}_{F_2}$ defines an abelian groupoids with each component of odd order.

Proof. We start by externalising our internal monoidal structure, so for $i, j, k \in N$ if $m|ij\rangle = |k\rangle$ then we let $i \cdot j = k$. Associativity and commutativity directly translate into our external multiplication. We notice importantly that lemma 7.6 holds in $\mathbf{FdVect}_{F_2}$.

Next we partition X into disjoint sets X_i, again like in **Rel** so we have a single element of X_i, e_i as its identity. Take $e = \sigma|e_i\rangle$ where $e_i \in N$ are the identities of the components of the groupoid. The next step we need to take carefully as it differs to the **Rel** case. For any $x \in N$ and for any $y \neq x \in N$ there must be an even number of i such that $m(x, e_i) = y$ and an odd number such that $m(x, e_i) = x$, however as L_x is an injection there will be no e_i such that $m(x, e_i) = y$ and exactly one e_i such that $m(x, e_i) = x$, we therefore place x in X_i. The rest of the proof that a classical structure defines an abelian groupoid follows exactly as in **Rel**. It remains to show that this abelian groupoid has each component of even order, like in theorem 7.13 we see the special condition applied to an abelian groupoid restricts the groupoid to having only components of odd order.

□

Theorem 7.15. Single-valued classical structures in $\mathbf{FdVect}_{F_2}$ are precisely the abelian groupoids with each component of odd order.

Proof. This follows from theorem 7.13 and 7.14. □

Going back to the 2-dimensional case we see a structure which does not copy basis elements and also is not single-valued:

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

When we look carefully at this however we see some interesting properties. Consider the non zero elements of X, $\{|0\rangle, |1\rangle, (|0\rangle + |1\rangle)\}$ this is isomorphic to the group $\mathbb{Z}_3$ with respect to the multiplication, where $(|0\rangle + |1\rangle)$ is the identity. Furthermore as the elements of X form a group with respect to addition (with the 0 element different to the 1 element) and the multiplication distributing over addition due to linearity we get a finite field.

It may seem like a finite field is bound to have enough structure to it to satisfy the conditions needed to make it a classical structure, however this is not the case. If we consider the monoid below:

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

this defines three Frobenius algebras with respect to the three comonoids below: the first will make our structure dagger but not special, the second special but not dagger and the third neither dagger or special.

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

Theorem 7.16. In $\mathbf{FdVect}_{F_p}$ given any n-dimensional vector space X it is always possible to construct an internal monoid on X that forms a finite field isomorphic to F_{p^n} with respect to the multiplication m and addition.

Proof. We can assign each basis element to powers of x in the usual polynomial representation, then assign the same multiplication as in the finite field. This multiplication must be linear as in a field the multiplication distributes over addition. The unit and associativity translate directly into our monoid from the field's multiplicative structure.

□

Any such internal monoid will automatically be commutative from commutativity of the finite field. Also importantly a finite field structure on X given by a monoid (X, m, e) has enough structure to guarantee there exists a special Frobenius algebra, however there will not always exist a dagger Frobenius algebra. Before we get to this theorem we lay the groundwork with some more general statements about Frobenius algebras.

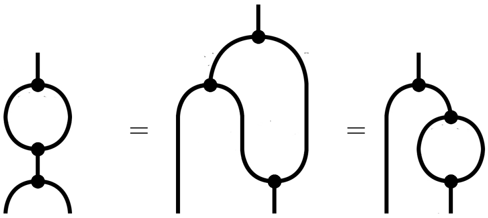
Theorem 7.17. Take an internal monoidal category (X, m, e) in $\mathbf{FdVect}_{\mathbb{K}}$ and an element of the usual algebraic dual space $\epsilon : X \to I$, called a Frobenius form, such that the nullspace of the Frobenius form $\{x \in X | \epsilon \circ x = 0\}$ contains no nontrivial left ideals. This will uniquely define a δ such that $(X, m, e, \delta, \epsilon)$ is a Frobenius algebra.

Proof. We have used an alternative definition of Frobenius algebra found in [9] def 2.2.1. The main theorem of chapter 2 in this ref is to prove that the ϵ Frobenius form uniquely determines a comonoid satisfying our usual definition of Frobenius algebra in definition 6.6. This proof should be easy to follow owing to much of the proof being written in diagrammatic form, using a slightly different looking left to right tubes, instead of bottom to top wires. □

Given an Frobenius form ϵ and an invertible element a we can define a new Frobenius form $\epsilon' = \epsilon \circ m(a \otimes 1_X)$. While they have different nullspaces, because a is invertible the respective nullspaces will have the same left ideals.
We also make the remark here that if every non-zero element in X forms a group then any non-trivial left ideal in X is the entire space X, therefore the only element in the dual space which contains a left ideal in its nullspace is the 0 element. This means every non-zero element of the dual space X^* defines a Frobenius form.

Lemma 7.18. Let $(X, m, e, \delta, \epsilon)$ be a Frobenius algebra in $\mathbf{FdVect}_{\mathbb{K}}$. The handle operation $\omega := m \circ \delta$, is a left X-module homomorphism. i.e. $\omega \circ m = m(1_X \otimes \omega)$. For more on the handle operator see [9].

Proof. With the use of the Frobenius condition and then associativity the result follows, with a simple diagrammatic proof.



□

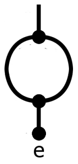
Note we also get ω as a right X-module homomorphism by a similar proof.

The next theorem is the main theorem of this section, it relates to the category $\mathbf{FdVect}_{F_p}$. This theorem along with theorem 7.16 and corollary 7.20 are original work.

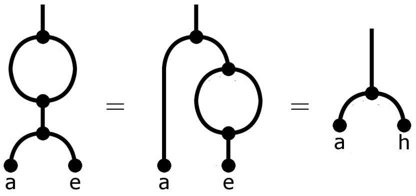
Theorem 7.19. Given a monoid (X, m, e) in $\mathbf{FdVect}_{F_p}$ which forms a finite field on the set of elements in X, there exists exactly one special Frobenius algebra $(X, m, e, \delta, \epsilon)$.

Proof. Firstly we show that the handle operator is the same as multiplication by a particular element, which we call the handle element, h.

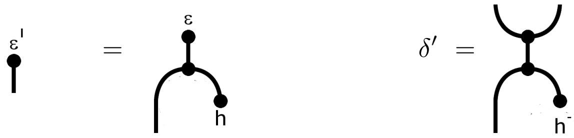
let h =



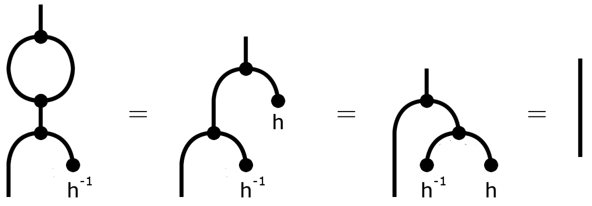
$\omega \circ a =$



Note we if we had split a into $m(ea)$ we would get the handle operator as left multiplication by h, therefore without commutativity of m we still see that h commutes with every element of X. Next we take any Frobenius form ϵ (as mentioned before we have the choice of any element in the X^*) with respective comultiplication δ, the corresponding handle element we call h. We now define a new $\epsilon' = \epsilon \circ m(1_X \otimes h)$ and $\delta' = \delta \circ m(1_X \otimes h^{-1})$, see below



With a bit of playing about with diagrams it is fairly easy (although time consuming) to show $(X, m, e, \delta', \epsilon')$ defines a Frobenius algebra. With the below calculations we show this is special.



□

Corollary 7.20. In $\mathbf{FdVect}_{F_p}$ given any n-dimensional vector space X it is always possible to construct a special Frobenius algebra on X that forms a finite field isomorphic to F_{p^n} with respect to the multiplication m and addition.

Proof. The result follows from theorem 7.16 and 7.19. □

Theorem 7.21. Let X be an n-dimensional vector space over F_2. There exists a dagger special internal monoid which is isomorphic to the finite field F_{2^n}.

Proof. As mentioned before, to create an internal monoid that has a finite field structure all we need to do is choose n elements of X that span X with respect to addition, and the associated multiplication structure will always be linear. If we choose a generator x for the multiplication group (the multiplication group is isomorphic to $\mathbb{Z}_{2^n-1}$), then the basis elements $x, x^2, x^4, ..., x^{2^{n-1}}$ have a useful property that taking the square cycles the basis elements, this is enough to show the monoid is special. For some generators these n elements will be a basis and for some not, however using the 'normal basis theorem' see [6] (a note to Karin Erdmann for helping point this out) such a basis will always exist. □

This result is original, although considerably less interesting than the previous result as the dagger special internal monoids produced are not necessarily Frobenius; out of the three properties this is certainly the most important. The hope of extending this proof to include Frobenius is also lost as in the 4-dimensional case the only two classical structures (up to isomorphism of basis element) isomorphic to the finite field F_{2^n} are not of this form (below is one of them as an example).

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

It is not known whether there always (for any p and n) exist classical structures which are isomorphic to a finite field. In the case over F_2 there does for dimensions 2-4 at least. However I would not be surprised if this did not hold in higher dimensions, due to the lack of pattern between these classical structures in different dimensions.

In our analysis of classical structures in $\mathbf{FdVect}_{F_2}$ we are left with one more case which does not fit into a single-valued groupoid or finite field structure. It is shown below.

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

Unlike the other classical structures (as well as many other non-dagger or special structures) it does not form any sort of group structure, with the element 0+1+2 not having an inverse. We must gain more understanding of this fascinating and unexpected new structure before we gain complete knowledge of classical structures in $\mathbf{FdVect}_{F_2}$.

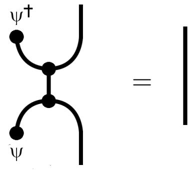
In conclusion to this section we find the existence of special Frobenius algebras isomorphic to finite fields, in theorem 7.19 and corollary 7.20, probably the most interesting results in this section. Despite this the classification of classical structures in $\mathbf{FdVect}_{F_2}$ or $\mathbf{FdVect}_{F_p}$ remain open questions. I will discuss this more in the conclusion.

8 The uses of FdVect over GF(2)

In this section we see some examples of vector spaces over finite fields in action. We look at basis structures (classical structures) and teleportation protocols and also discuss some of the limitations of $\mathbf{FdVect_F}$.

As mentioned before we sometimes refer to classical structures as basis structures due to the fact the classical elements form an orthonormal bases in **FdHilb** (see theorem 7.3). In **FdHilb** unbiased elements with respect to an orthogonal basis correspond to elements which, when a measurement is made over the basis we are equally likely to get any of the outcomes, i.e. for basis $|a_i\rangle$ the normalised state $|\psi\rangle$ satisfies $|\langle\psi|a_i\rangle|^2 = 1/dim(\mathcal{H})$ for all i. We now introduce the abstract notion of unbiased elements with respect to a classical structure

Definition 8.1. Given a classical structure (X, m, e) a state $\psi : I \to X$ is unbiased iff its left action L_ψ is unitary, i.e. $L_\psi^{-1} = L_\psi^\dagger$. Below we see this in diagrammatic form.



An important concept is the notion of complementary basis. In **FdHilb** they correspond to two bases where the basis elements of the first are unbiased with respect to the second and vice verse.

Definition 8.2. Two classical structures (X, m, e) and (X, m', e') are complementary iff:
1. Whenever $\phi : I \to X$ is classical for (X, m, e) it is unbiased for (X, m', e')
2. Whenever $\psi : I \to X$ is classical for (X, m', e') it is unbiased for (X, m, e)
3. e is classical for (X, m', e') and e' is classical for (X, m, e)

For $\mathbf{FdVect}_{F_2}$, in the 2-dimensional case the two possible classical structures are not complementary, the monoid

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \tag{15}$$

has no classical elements (it needs at least the unit of the other classical structure to be a classical element).

However in the 3-dimensional case we see the classical structures (X, m_A, e_A) and (X, m_B, e_B), depicted below, are complementary. Note, instead of (X, m_A, e_A) we could pick a structure with $|0\rangle$ being copied and then the structure seen in (15), on the second and third basis elements (we will comment on this alternative choice of complementary basis structures later).

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

The structure (X, m_A, e_A) corresponds to the familiar basis copying operation on $|0\rangle$, $|1\rangle$ and $|2\rangle$. The structure (X, m_B, e_B) corresponds to $\mathbb{Z}_3$ on the three basis elements with $|0\rangle$ as the unit. The classical elements of (X, m_A, e_A) are $|0\rangle$, $|1\rangle$ and $|2\rangle$ which are also the unbiased elements of (X, m_B, e_B). The only classical element of (X, m_B, e_B) is $|0\rangle + |1\rangle + |2\rangle$ which is the only unbiased element of (X, m_A, e_A). Also both units are classical elements in the other classical structures.

Example 8.3. We outline how to simulate a teleportation protocol in the same way as the sketch proof [10] (proposition 2.2). Firstly we note that we can see that given any pair of complementary classical structures on X we can define a classical structure $(X \otimes X, (1_X \otimes \sigma_{X,X} \otimes 1_X) \circ (m_A \otimes m_B), e_A \otimes e_B)$. We now consider the structure $(X, (m_A \otimes 1_X) \circ (1_X \otimes m_B^\dagger) : X \otimes X \to X \otimes X)$, in [16] we see this defines a 'bell-basis' with respect to the classical structure described on $X \otimes X$. This paper goes on to show any 'bell-basis' will support a teleportation protocol.

In our case we see our 'bell basis' is $|00\rangle + |11\rangle + |22\rangle$, $|01\rangle + |12\rangle + |20\rangle$ and $|02\rangle + |10\rangle + |21\rangle$ and the corresponding unitary bell matrices.

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

Example 8.4. The superdense coding protocol is also a result of the 'bell basis' described above, see [16]. Using the same example of complementary bases we apply one of three unitaries to half of our shared entangled state. Then we transfer our quantum piece of information and get out one of three possible measurement outcomes. We see the term superdense is slightly out of place here as we could just have transfered a prepared state corresponding to one of the basis elements $|0\rangle$, $|1\rangle$ or $|2\rangle$ then perform a measurement over the basis structure (X, m_A, e_A), without having to use entanglement. However it may still be possible with a more complicated example to perform a useful superdense coding in $\mathbf{FdVect}_{F_2}$.

Both these results are very interesting. The fact our 'bell basis' only contains 3 elements in a 9 dimensional space seems slightly unusual, although given the varying nature of the classical structures in $\mathbf{FdVect}_{F_2}$ the fact we are able to reproduce such a familiar teleportation protocol at all is remarkable. We only have to look at the other choice of complementary basis in the three dimensional case of $\mathbf{FdVect}_{F_2}$, to find some stranger results. In this alternative case applied to the teleportation protocol, the measurement has only one outcome and therefore we need to transfer no classical information. However if this were physically possible, then it would allow information to be teleported instantly and therefore allow faster than light communication. In our superdense coding example we now lose all our information as the measurement has only one outcome.

Overall it seems that some complementary basis structures will produce protocols similar to those seen in **FdHilb** while others give different or unexpected results. These unexpected results and the classical structures that create them are intriguing, giving us a new perspective on these protocols, it will take further study to fully understand their importance.

9 Other interesting concrete categories

In this section we will take a look at vector spaces over other fields and types of arithmetic. As far as I know no work has been done in quantum computing on these categories. We will identify some basic properties which are likely to be of interest in any further study of them.

Example 9.1. $\mathbf{FdVect}_{F^{alg}}$ is the category of vector spaces over the algebraic closure of finite field F.

Here we have extended our finite field to make it algebraically closed (the smallest such extension), meaning that any polynomials over the base field will now have solutions. This can be useful in say normalising vectors. However any field extension of F will have the same characteristic, therefore the algebraic closure still has non-zero characteristic. This will prove problematic in any attempt to define an inner product. When our finite field is of order p the algebraic closure is the union of copies of F_{p^n} for all n, so we are likely to see at least some properties similar to the categories $\mathbf{FdVect}_{F_{p^n}}$.

The category of relations **Rel** has been pivotal in the development of category theory in quantum mechanics. We have already compared the similarities between $\mathbf{FdVect}_{F_2}$ and this well studied category. Now we look at slightly modified versions

Example 9.2. **Rel2** is the category of vector spaces over the following semi-ring arithmetic $(+_2, *_2)$ on the set of integers $\{0,\ 1,\ 2\}$:-

$$i +_2 j = \min(i+j, 2)$$
$$i *_2 j = \min(i * j, 2)$$

This category is likely to have similar properties to **Rel**, there might also be connections between this and $\mathbf{FdVect}_{F_3}$, which has similar matrix arithmetic. The fact this arithmetic has zero characteristic means we can define an inner product on the vector space.

Example 9.3. **RelC** is the category of vector spaces over the following semi-ring arithmetic $(+_c, *_c)$ on the continuous interval of the real line [0,1]:-

$$i +_c j = \min(i+j, 1)$$
$$i *_c j = i * j$$

Here we have a continuous form of **Rel** and possibly the most interesting of these examples. Again zero characteristic will mean it is possible to define a meaningful inner product. One way we can think of this category is in terms of probabilities of events being related, i.e. in the one element case $\{*\} \xrightarrow{f} \{*\} \xrightarrow{g} \{*\}$, the composition will give us the probabilities multiplied together. With more than one element we introduce addition. However addition will only have an intuitive meaning in terms of probability, if events are mutually exclusive. One way to keep meaning is to apply restrictions to our relations, i.e. that the column vectors in our matrices do not sum to more than 1. We now lose the direct connection between this category and **Rel**, in that we cannot have a surjective map, taking relations of value 1 in **RelC** to relations in **Rel**. We still observe however observe the map from **RelC** to **Rel**, mapping non-zero relations in **RelC** to relations in **Rel**. In terms of our probabilistic interpretation this is the move from observing relations that are certain to relations that have some probability of occurrence.

The fact **RelC** takes continuous values may allow more properties of quantum systems to be simulated and could help bridge the gap between **Rel** and **FdHilb**. We also note that there are likely to be many other such structures that have been studied thoroughly in other areas of mathematics, waiting to be introduced to the world of quantum computing.

10 Conclusion and further areas of research

In this project we have seen how a category theoretic approach to quantum computing can give a whole new perspective to the systems and processes we study. The use of diagrammatic representation and ability to reduce complex concepts to their absolute essence within the framework of an abstract category makes this approach instantly appealing.

We go back to our analogy of using category theory as a guide to where quantum mechanics can live in the world of mathematics outside Hilbert spaces. Where does finite fields fit into our new world for quantum computing? It has many nice feature, already providing useful setting for areas such as coding, cryptography, elliptic curves etc. In this project we have shown even simple finite fields have the necessary resources to perform protocols such as quantum teleportation and we can also observe concepts of entanglement. To make the claim that the whole of quantum mechanics can live within the finite field setting would be too much and finding out which parts of quantum computing do not naturally fit in with finite fields is an aim of this project. Certainly I could imagine vector spaces over finite fields in the future being a new home for some parts of quantum computing. I would hope at the very least that they would help us come to a better understanding of quantum computing.

The study of Frobenius algebras on vector spaces over finite fields provides us with several interesting results. We see a link between single valued classical structures in $\mathbf{FdVect}_{F_2}$ and the classical structures of **Rel**, due to the similarities in the matrix arithmetic. Despite the fact there are relatively few classical structures in $\mathbf{FdVect}_{F_2}$, without restricting our attention to single-valued monoids, the classical structures do not have a great deal of pattern to them, and there is currently no way to classify them. The existence of special Frobenius algebras isomorphic to finite fields is probably the most useful result in this section. Also while special Frobenius structures take on a much wider range of forms than our classical structures, it may be worth dropping the slightly unnatural dagger condition (except for in the case of single-valued monoids) and in further analysis focus attention more on special Frobenius structures.

Further research could also be done on categories $\mathbf{FdVect}_{F_{p^n}}$ where n is greater than 1. These categories have hardly been touched upon in this dissertation. Also an obvious follow up to some of the work done on $\mathbf{FdVect}_{F_2}$ would be to see if any similar results hold in $\mathbf{FdVect}_{F_p}$ for $p > 2$. In chapter 8 we examine a teleportation protocol in $\mathbf{FdVect}_{F_2}$, it would be interesting to see if we can simulate the same protocols using vector space over different finite fields, or if for example we can describe the category **Spek** in $\mathbf{FdVect}_{F_2}$ like we can in **Rel**. Also further work could be done on other protocols and quantum properties in $\mathbf{FdVect}_{F}$. In chapter 9 we also introduced several new semi-ring arithmetic which could provide the base to a vector space, studying these in more depth I feel would provide some interesting results.

A Mathematica results

2-dimensional results, $X = F_2^2$

Internal monoidal structures. Monoids in the first row have $|0\rangle$ unit, second row $|1\rangle$ unit and third row $|0\rangle + |1\rangle$ unit. Positions in matrix from left to right correspond to 00, 01, 10 and 11 and going down 0 and 1.

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

Commutative Frobenius algebras

$$\left\{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^T\right\}\left\{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}^T\right\}\left\{\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^T\right\}\left\{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}^T\right\}\left\{\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}^T\right\}\left\{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}^T\right\}\left\{\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}^T\right\}\left\{\begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}^T\right\}\left\{\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}^T\right\}\left\{\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}^T\right\}$$

$$\left\{\begin{pmatrix}1&1&1&0\\1&0&0&1\end{pmatrix},\begin{pmatrix}1&1&1&0\\1&0&0&1\end{pmatrix}^T\right\}\left\{\begin{pmatrix}1&1&1&0\\1&0&0&1\end{pmatrix},\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix}1&0&0&0\\0&1&1&1\end{pmatrix},\begin{pmatrix}1&1&1&0\\0&0&0&1\end{pmatrix}^T\right\}\left\{\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix},\begin{pmatrix}0&1&1&1\\1&1&1&0\end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix},\begin{pmatrix}1&1&1&0\\1&0&0&1\end{pmatrix}^T\right\}\left\{\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix},\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix}^T\right\}$$

Commutative dagger Frobenius algebras

$$\left\{\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix},\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix}^T\right\}\left\{\begin{pmatrix}0&1&1&1\\1&1&1&0\end{pmatrix},\begin{pmatrix}0&1&1&1\\1&1&1&0\end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix}1&0&0&0\\0&0&0&1\end{pmatrix},\begin{pmatrix}1&0&0&0\\0&0&0&1\end{pmatrix}^T\right\}\left\{\begin{pmatrix}0&1&1&0\\1&0&0&1\end{pmatrix},\begin{pmatrix}0&1&1&0\\1&0&0&1\end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix}1&1&1&0\\1&0&0&1\end{pmatrix},\begin{pmatrix}1&1&1&0\\1&0&0&1\end{pmatrix}^T\right\}\left\{\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix},\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix}^T\right\}$$

Commutative special Frobenius structures

$$\left\{\begin{pmatrix}0&1&1&1\\1&1&1&0\end{pmatrix},\begin{pmatrix}0&1&1&1\\1&1&1&0\end{pmatrix}^T\right\}\left\{\begin{pmatrix}1&0&0&0\\0&0&0&1\end{pmatrix},\begin{pmatrix}1&0&0&0\\0&0&0&1\end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix}1&1&1&0\\0&0&0&1\end{pmatrix},\begin{pmatrix}1&0&0&0\\0&1&1&1\end{pmatrix}^T\right\}\left\{\begin{pmatrix}1&1&1&0\\1&0&0&1\end{pmatrix},\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix}^T\right\}$$
$$\left\{\begin{pmatrix}1&0&0&0\\0&1&1&1\end{pmatrix},\begin{pmatrix}1&1&1&0\\0&0&0&1\end{pmatrix}^T\right\}\left\{\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix},\begin{pmatrix}1&1&1&0\\1&0&0&1\end{pmatrix}^T\right\}$$

Classical structures

$$\left\{\begin{pmatrix}0&1&1&1\\1&1&1&0\end{pmatrix},\begin{pmatrix}0&1&1&1\\1&1&1&0\end{pmatrix}^T\right\}\left\{\begin{pmatrix}1&0&0&0\\0&0&0&1\end{pmatrix},\begin{pmatrix}1&0&0&0\\0&0&0&1\end{pmatrix}^T\right\}$$

3-dimensional results, $X = F_2^3$

Classical structures (monoids shown). Rows 1-3 have units $|0\rangle$, $|1\rangle$ and $|2\rangle$ respectively, rows 4-6 have unit $|0\rangle + |1\rangle + |2\rangle$ Positions in matrix from left to right correspond to 00, 01, 02, 10, 11, 12, 20, 21 and 22 and going down 0,1 and 2.

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

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

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

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

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

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

References

[1] Bob Coecke. *Quantum Computer Science, lecture notes, Oxford University* (Hilary term 2008)

[2] Michael A.Nielsen and Isaac L.Chuang. *Quantum Computation and Quantum Information* (Cambridge University Press 2000)

[3] Bob Coecke. and Eric Oliver Paquette. *Categories for the practising physicist* (arXiv:0905.3010)

[4] Dusko Pavlovic. *Quantum and classical structures in nondeterministic computation* (arXiv:0812.2266)

[5] Bob Coecke. *Kindergarten Quantum Mechanics* (arXiv:quant-ph/0510032)

[6] Rudolf Lidl and Harald Niederreiter. *Finite Fields* (Cambridge University Press 1997)

[7] Bob Coecke. *Introducing categories to the practising physicist* (arXiv:0808.1032)

[8] Benjamin C.Pierce. *Basic Category Theory for Computer Scientists* (The MIT Press 1991)

[9] Joachim Kock. *Frobenius Algebras and 2D Topological Quantum Field Theories* (Cambridge University Press 2003)

[10] Bob Coecke and Bill Edwards. *Toy quantum categories* (arXiv:0808.1037)

[11] Bob Coecke, Dusko Pavlovic and Jamie Vicary. *A new description of orthogonal bases* (arXiv:0810.0812)

[12] Samson Abramsky and Bob Coecke. *Categorical quantum mechanics* (arXiv:0808.1023)

[13] John Baez. *This Week's Finds in Mathematical Physics 268* (math.ucr.edu/home/baez/TWF.html also see n-category cafe golem.ph.utexas.edu/category/)

[14] Bob Coecke. *Quantum picturalism* (arXiv:0908.1787)

[15] Samson Abramsky and Bob Coecke. *Categorical Quantum Mechanics* (arXiv:0808.1023)

[16] Bob Coecke and Dusko Pavlovic. *Quantum measurements without sums* (arXiv:quant-ph/0608035)