Hopf Algebras in Quantum Computation

Giovanni de Felice

April 2017

Contents

1   Introduction

Categories and diagrams
Symmetry, quantization and categorification
Categorification = replacing equalities with isomorphisms [1].
For an account of the relationships between categorification and quantization consider [2].
Mathematically: from groups to quasitriangular hopf algebras, G to DG
Categorically: from symmetric fusion categories to modular categories
Physically: fermions/bosons to anyons, local symmetries to topological symmetries, 3D to 2D
Computation: from PQC to TQC, complexity theory
Logic: mirror the relationship, all statements about RepDG are statements in RepG, a modality, programming language

2   Diagrams and Hopf Algebras

2.1   Monoidal categories

In this section, we set in place the basic definitions and diagrammatic intuitions which we will use throughout the thesis. The standard reference about basic category theory results is [3]. Many of the definitions are taken from [?]. A more detailed and up to date survey on monoidal categories can be found in [4]. For an introduction to diagrammatic reasoning in monoidal categories consider the first two chapters of [?]. Many of the results in this section and their relationship to quantum mechanics can be found in [8].
Recall the definition of a category.

Definition 1 *A category $\mathcal{C}$ consists of the data:*

- *a collection of objects $obj(\mathcal{C})$*

- *a collection of morphisms (or arrows) $arr(\mathcal{C})$*

- *domain and codomain assignments $dom, cod : arr(\mathcal{C}) \to obj(\mathcal{C})$. For any two objects $a, b \in obj(\mathcal{C})$ we define the hom-set*

$$\mathcal{C}(a, b) := \{f \in arr(\mathcal{C}) : a = dom(f), b = cod(f)\}$$

- *for any triple of objects a, b, c a composition map*

$$c_{a,b,c} : \mathcal{C}(a, b) \times \mathcal{C}(b, c) \to \mathcal{C}(a, c)$$

We denote the composition by $g \circ f$, diagrammatically:

$$a \xrightarrow[g \circ f]{} c \quad \overset{f}{\nearrow} b \overset{g}{\searrow}$$

- *For any object a an identity morphism $id_a : a \to a$*

Satisfying the following axioms:

$$h \circ (g \circ f) = (h \circ g) \circ f \quad f \circ id_a = f = id_b \circ f$$

$$A \xrightarrow[g \circ f]{\overset{f \nearrow \; B \; \searrow g}{}} C$$

The commutativity of the above diagram is a statement about $\mathcal{C}$, and it has exactly the same information to its dual diagram. Where objects are one-dimensional wires and morphisms are (zero dimensional) boxes:

$$
\begin{array}{ccc}
C & & C \\
\uparrow & & \uparrow \\
\boxed{g} & = & \boxed{g \circ f} \\
B & & \\
\boxed{f} & & \\
\uparrow & & \uparrow \\
A & & A
\end{array}
$$

We will mainly use this second diagrammatic language in this work. When $\mathcal{C}$ is just a category we only have one way of composing morphisms and the language is one dimensional.

Example 1 *Examples of categories are: $Sets$ of sets and functions, $FSets$ of finite sets and functions, Rel of sets and relations, $Vect_k$ of vector spaces over k and linear maps and $FVect_k$ of finite dimensional vector spaces and linear maps.*

Category theory is a really good language for talking about equivalences and relationships between structures. This is achieved with the following tools.

Definition 2 (Functor) *A functor $F : \mathcal{C} \to \mathcal{D}$ is a mapping that*

- *associates an object $F(X)$ of $\mathcal{D}$ to each object X of $\mathcal{C}$.*

- *associates to each morphism $f : X \to Y$ a morphism $F(f) : F(X) \to F(Y)$ such that $F(id_X) = id_Y$ and $F(g \circ f) = F(g) \circ F(f)$ for all morphisms $f : X \to Y$ and $g : Y \to Z$.*

For instance there is a functor $Q : Sets \to Vect_k$ called '1st quantization' and taking a set to the free vector space generated by that set. Given two functors with matching source and target we can have natural transformations between them

Definition 3 (Natural Transformation) *Given categories $\mathcal{C}$ and $\mathcal{D}$ and functors $F, G : \mathcal{C} \to \mathcal{D}$ a natural transformation $\alpha : F \Rightarrow G$ is an assignment to every object a in $\mathcal{C}$ of a morphism $\alpha_a : F(a) \to G(a)$ in $\mathcal{D}$ such that for each morphism $f : a \to b$, the following commutes:*

$$G(a) \xrightarrow{\; G(f) \;} G(b)$$

$$\alpha_a \uparrow \qquad\qquad \uparrow \alpha_b$$

$$F(a) \xrightarrow[\; F(f) \;]{} F(b)$$

A natural isomorphism is a natural transformation such that all components are isomorphisms.

Recall that a monoid is a triple $(X, \times, 1)$ where X is a set, $1 \in X$ and $\times$ is an associative and unital multiplication on X. The notion of a monoidal category is the categorification of a monoid. Elements of the set are replaced by objects in a category $\mathcal{C}$, multiplication by a bifunctor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ and the equalities in the unit and association axioms are replaced by natural isomorphisms. In order for this new structure to be well-behaved we will also need to impose compatibility conditions. We obtain the following definition:

Definition 4 (Monoidal category) *A monoidal category is a category $\mathcal{C}$ equipped with a bifunctor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ called tensor product, an object 1 called unit object, a natural isomorphism*

$$a : - \otimes (- \otimes -) \overset{\sim}{\Rightarrow} (- \otimes -) \otimes -$$

called associator, a natural isomorphism

$$\lambda : 1 \otimes (-) \Rightarrow (-)$$

called left unitor and a natural isomorphism

$$\rho : (-) \otimes 1 \Rightarrow (-)$$

called right unitor. Subject to the following coherence conditions holding for all objects a, b, c, d in $\mathcal{C}$:

1. *Pentagon axiom: the following diagram commutes*

$$(a \otimes b) \otimes (c \otimes d)$$

$$\alpha_{a \otimes b, c, d} \nearrow \qquad\qquad \searrow \alpha_{a, b, c \otimes d}$$

$$((a \otimes b) \otimes c) \otimes d \qquad\qquad a \otimes (b \otimes (c \otimes d))$$

$$\alpha_{a,b,c} \otimes id_d \downarrow \qquad\qquad\qquad \uparrow id_a \otimes \alpha_{b,c,d}$$

$$(a \otimes (b \otimes c)) \otimes d \xrightarrow[\; \alpha_{a, b \otimes c, d} \;]{} a \otimes ((b \otimes c) \otimes d)$$

2. Triangle identity: the following diagram commutes

$$(a \otimes 1) \otimes b \xrightarrow{\;\;\alpha_{a,1,b}\;\;} (a \otimes 1) \otimes b$$

with downward arrows $\rho_a \otimes id_b$ and $id_a \otimes \lambda_b$ meeting at

$$a \otimes b$$

Let us give three important examples of monoidal categories.

Example 2 *The category Sets of sets and functions is monoidal with the cartesian product $\times$ as bifunctor and the singleton set as unit object.*
The category $Vect_k$ of finite dimensional vector spaces over a field k is monoidal with the usual tensor product $\otimes$ and the one dimensional vector space k as unit object.
*The category Rel of sets and relations is monoidal with the cartesian product $\times$ and the singleton as unit object.*

The more structure comes with a category the more complicated diagrams we can draw. Monoidal categories have a two-dimensional diagrammatic language. The presence of unitors and associators and the conditions they satisfy make sure that this graphical language is well behaved. This is known as the coherence theorem for monoidal categories and can be found in [3]. It says that any well formed diagram in a monoidal category, made up of associators and unitors commutes. When the associators are trivial morphisms (i.e identity morphisms) we say the category is strict monoidal. It is known that every monoidal category is equivalent to a strict one [3], but it is sometimes useful to take associators into account as we will see in our discussion on permutational quantum computation. We write the tensor of two morphisms $f \otimes g : A \otimes B \to C \otimes D$ simply putting them side by side:

$$
\begin{array}{cc}
C & D \\
\uparrow & \uparrow \\
\boxed{f} & \boxed{g} \\
| & | \\
A & B
\end{array}
$$

In our diagrams we can picture the unit I of the tensor as the plane on which we are drawing. Indeed we could imagine drawing as many copies as we wanted of id_I on the previous diagram to obtain obtain an equivalent diagram as $id_I \otimes f = f$ for any morphism f. So really the identity on I is just the empty diagram which we can stick next to any diagram we like.

Definition 5 (States and costates) *Given a system A, a state of is a morphism $1 \to A$. A costate (or effect) of A is a morphism $A \to 1$. In the diagrammatic language we draw states and costates respectively:*
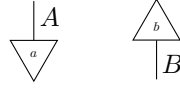
Remark It is perhaps useful to understand monoidal categories as degenerate 2-categories. Although this viewpoint requires one additional initial step of abstraction (the definition of a 2-category), it gives us the diagrammatic language for monoidal categories for free. For the rigorous definition of a 2-category we refer to [BAEZ], for our purposes we will only need the intuition. A 2-category is a collection of objects with 1-arrows between them and 2-arrows between the 1-arrows. Note that there are two ways of composing the 2-arrows:

- vertical composition:
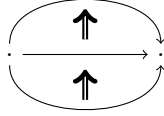
- parallel composition:
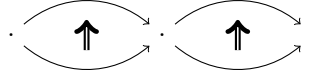
Taking the dual of the above diagrams we obtain the diagrammatic language. Monoidal categories are 2-categories with only one 0-object called 1. We can think of the 0-object as the underlying plane, wires carry systems (1-arrows), boxes are morphisms (2-arrows). We recover the given definition of monoidal category by calling 1-arrow objects, and 2-arrows morphisms. The unit object 1 is then the identity 1-arrow $1 \to 1$ which is simply denoted 1.

Example 3 *The cartesian product in Sets $A \times B$ of sets A and B, satisfies the universal properties of a categorical product, in the sense that we have projections p_1 and p_2 such that if f and g are maps from some set C there is a unique function h making the following diagram commute:*
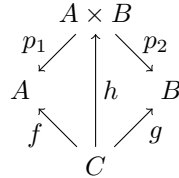
Because of this property all states of $(Sets, \times)$ are separable. This category is the ambient Cartesian world of classical physics.

Example 4 *In $Vect_k$ states are vectors and costates are functionals. Note that the diagrammatic notation provides a two-dimensional generalisation of Dirac's notation. The category $Hilb$ of Hilbert spaces and linear maps is monoidal when equipped with the usual tensor product $\otimes$. Note that $\otimes$ is not a categorical product, and in fact we can have entangled states. Quantum mechanics is based on $(Hilb, \otimes)$ [8].*

Definition 6 (Scalars) *Scalars in a monoidal category are morphisms $1 \to 1$.*

The category $Sets$ has only one scalar. Rel has two scalars forming the cyclic group $\mathbb{Z}_2$ under composition. $Vect_k$ has scalars from k. Given a vector and a functional we obtain a scalar by composing them analogously to Dirac's formalism.

Definition 7 (BMC) *A braided monoidal category is a monoidal category $\mathcal{C}$ equipped with a natural isomorphism $B_{a,b} : a \otimes b \to b \otimes a$ called braiding, subject to the following compatibility conditions (called hexagon equations):*

In the diagrammatic language this means we have braidings:

for any A and B, satifying:

$$(1)$$

The compatibility conditions are obvious statements in the diagrammatic calculus, for instance the first hexagon equation just says:

$$(2)$$

Both *Sets* and *Hilb* are examples of symmetric monoidal categories in the following sense.

Definition 8 (SMC) *A braided monoidal category is symmetric if the braiding $B_{a,b}$ satisfies*

$$B_{a,b} \circ B_{b,a} = id_{a \otimes b}$$

For all objects a, b

In a SMC the braiding is called symmetry morphism and is denoted

It satisfies:

We will now describe some new classes of examples of monoidal categories. These are of a different nature to the categories we have seen so far.

Definition 9 (PROPs) *A PROP (products and permutations category) is a strict symmetric monoidal category where every object is of the form $x^{\otimes n}$ for a single object x and $n \geq 0$.*

8

This means that we are only allowed one type of wire when drawing diagrams about $PROPs$ but we can use as many copies as we like and we can make swaps with them. Categories satisfying these properties are useful syntactic tools as we will see. One way to think of a $PROP\ A$ is as an abstract algebraic structure carrying some axioms, we can then instantiate those axioms in some other symmetric monoidal category $\mathcal{C}$ by considering symmetric monoidal functors $F : A \to \mathcal{C}$. We call such functors algebras or models of A in $\mathcal{C}$. If A is defined in terms of generators and relations (as is most often done), the choice of such functor corresponds to the choice of one object from $\mathcal{C}$ and morphisms on that object respecting the defining relations of A. On its own A has no clear interpretation, it just defines a syntax, but if $\mathcal{C}$ is a semantic category (i.e one with a clear interpretation) then F is a 'filling' of the syntax with meaning. This reasoning was first proposed in Lawvere's Phd thesis in 1963 [**?**].

It will sometimes be useful to drop the 'permutational' structure of $PROPs$.

Definition 10 (PRO) *A PRO (products category) is a strict monoidal category where every object is of the form $x^{\otimes n}$ for a single object x and $n \geq 0$.*

The semantic categories we will consider the most are $Sets$ and $Hilb$. One important difference between them is that $Hilb$ exhibits duality.

Definition 11 (Rigidity) *Let $\mathcal{C}$ be a monoidal category and $A \in obj(\mathcal{C})$. A left-dual of A is an object A^* with morphisms*

Satisfying the snake equations:
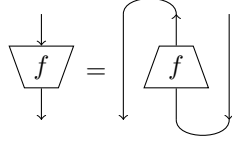
If every object has a left-dual, we say that $\mathcal{C}$ is left-rigid. Similarly we can define right-duals and right-rigid categories by interchanging the roles of A and $A^\star$ in the definition.

Given a (left/right) rigid structure we can define (left/right)transpose as follows.

Definition 12 (Transpose) *Given a (left/right) rigid category $\mathcal{C}$ and any process $f : A \to B$ the (left/right) transpose f^* (or left transpose f^l, right transpose*

f^r *if it is not clear from context) is:*

$$\text{(diagram)} \qquad (3)$$

Definition 13 (Trace) *In a symmetric monoidal category $\mathcal{C}$, if A has a left dual $A^\star$, the trace of some morphism $f : A \to A$ is defined as the following scalar:*
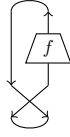
2.2 Hopf Algebras

Now that we have set in place a diagrammatic machinery based on monoidal categories, let us make use of it. In this section we will meet some mathematical structures which have been used by mathematicians to describe symmetry. The notion of Hopf algebras is a powerful generalization of that of a group. Since their discovery in the 1940s, Hopf algebras have been used in various fields of pure mathematics (such as number theory, algebraic geometry, and representation theory) and have found applications in Quantum mechanics. Most of the results of this section can be found in [**?**].

Definition 14 (Monoid) Δ *is a PRO generated by morphisms (,) satisfying associativity:*

$$\text{(diagram)} \qquad (4)$$

and the unit law:

$$\text{(diagram)} \qquad (5)$$

Models of Δ in monoidal categories are called monoids and they are very well known, examples include the natural numbers under addition, lists of some alphabet under concatenation and any group. Taking the opposite category Δ^{op} corresponds to flipping all the diagrams.

Definition 15 (Comonoid) Δ^{op} *is a PRO generated (,) satisfying coassociativity:*

$$\text{(diagram)} \qquad (6)$$

and the counit law:

$$\curlyvee = \; | \; = \curlyvee \tag{7}$$

Models of these are comonoids, the most common example is the copy map on any set with 'delete' as counit. Monoids and comonoids are simple structures that we can stick together to form more complicated ones. Bialgebras arise from one type of interaction of a monoid and comonoid.

Definition 16 (Bialg) *Bialg is a PROP generated by ($\curlywedge$, $\bullet$, $\curlyvee$, $\circ$), where $\curlywedge$ and $\bullet$ form a monoid, $\curlyvee$ and $\circ$ a comonoid and the morphisms additionally satisfy the following laws:*

$$\bowtie = \curlyvee\curlywedge \tag{8}$$

$$\curlyvee\hspace{-0.3em}\bullet = \bullet \; \bullet \tag{9}$$

$$\circ\hspace{-0.3em}\curlywedge = \circ \; \circ \tag{10}$$

$$\circ\hspace{-0.3em}\bullet = \tag{11}$$

Where the empty diagram is the identity on the tensor unit.

Models of *Bialg* in *Vect* are bialgebras. We leave examples for later as we are now ready to introduce one of the main topics of this thesis.

Definition 17 (Hopf) *Hopf is a PROP generated by ($\curlywedge$, $\bullet$, $\curlyvee$, $\circ$, $\boxdot$). Where ($\curlywedge$, $\bullet$, $\curlyvee$, $\circ$) is a bialgebra and the antipode S satisfies the Hopf law:*

$$\boxed{s} = \bullet\circ = \boxed{s} \tag{12}$$

We will argue that $Hopf$ is a good syntax to talk about symmetry. Let us start by instantiating $G : Hopf \rightarrow Sets$. This corresponds to choosing a set G, with a binary function $G \times G \rightarrow G$ (or multiplication) with a unit. Using the counit rule it is easy to see that the comultiplication in $Sets$ must be the copy map $g \mapsto (g, g)$ so that the antipode is the morphism $g \mapsto g^{-1}$ and G forms a group. Since the 19th century groups have been used by mathematicians and physicists to describe symmetry.

Example 5 (Finite groups) *We will only make use of the following classes of finite groups:*

- $\mathbb{Z}_n$ *the cyclic group with n elements.*

- S_n *the symmetric group, can be seen as the group of permutations of a set with n elements, has order n!. S_3 is the smallest non-abelian group up to isomorphism.*

Example 6 (Groups of matrices) *Here we will fix some notation on the infinite groups of matrices we will meet. All matrices we will consider are over the complex numbers. $GL(n)$ is the group of invertible n by n complex matrices. $U(n)$ is the group of unitary $n \times n$ matrices (i.e such that $U^\dagger U = UU^\dagger = I$). The special unitary group $SU(n)$ is the subgroup of $U(n)$ consisting of matrices with determinant 1. The representation theory of $SU(n)$ is widely used in particle physics, for instance representations of $SU(2)$ model the behaviour of spin-$\frac{1}{2}$ particles.*

If we take a model of $H : Hopf \to Vect$ we obtain what is known as a Hopf Algebra.

Example 7 (Group algebras) *If G is a group with unit e, the group algebra $\mathbb{C}G$ (of dimension $|G|$) is a hopf algebra with multiplication linearly generated by $|g\rangle \otimes |h\rangle \to |gh\rangle$, unit $|e\rangle$, comultplication generated by $|g\rangle \to |g\rangle \otimes |g\rangle$ and counit $\sum_g \langle g|$.*

The previous example gives the usual definition of a group algebra which, for finite sets and finite dimensional vector spaces is just the composition $Q \circ G$ (as shown in the diagram) where Q is the 1st quantization functor. It is easy to see that Q preserves the monoidal structure as well as the symmetry morphisms (we say Q is a symmetric monoidal functor) so that the composition is also symmetric monoidal and $Q \circ G$ is a model of $Hopf$.

$$
\begin{array}{ccc}
 & Hopf & \\
G \swarrow & & \searrow \mathbb{C}G \\
FSets & \xrightarrow{\quad Q \quad} & FVect
\end{array}
$$

In this case the comultiplication in $Hilb$ is the linearisation of the copy map (the copy map on some basis extended linearly to the whole Hilbert space) which is co-commutative. For a general $H : Hopf \to Vect$ this doesn't have to be the case. Hopf algebras provide a broader framework to talk about symmetry, as we can have non co-commutative Hopf algebras. We can see it as a quantization of the notion of symmetry, it will allow us to describe symmetries of quantum systems. Physically we will see that Hopf algebras allow to talk about local symmetries and exchange statistics on the same footing [**?**]. In particular if the Hopf algebra is not cocommutative the exchange statistics can be highly nontrivial, in which case they will describe the symmetries of anyons. The following

two propositions are simple but important results about the antipode of a hopf algebra.

Proposition 1 *The antipode of a Hopf algebra is unique. It follows that being a Hopf algebra is a property of bialgebras.*

Proof Suppose S and S' are two antipodes for some Hopf algebra, then:

$$\tag{13}$$

■

Proposition 2 *The antipode is an anti-(co)algebra homomorphism.*

$$\tag{14}$$

Proof First note that:

$$\tag{15}$$

So that is a left convolution inverse to .
Also:

$$\tag{16}$$

So that is a right convolution inverse to . And it is easy to see using associativity and co-associativity that right and left convolution inverses must coincide. We deduce that the antipode is an anti-coalgebra homomorphism. For a proof that the antipode is an anti-algebra morphism simply flip all the diagrams and interchange white with black.

■

Definition 18 (Quasitriangularity) *A Hopf algebra H is quasitriangular if there is an invertible element $R \in H \otimes H$ satisfying the following equations:*
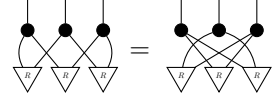
$$\text{(17)}$$

$$\text{(18)}$$
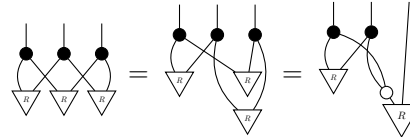
$$\text{(19)}$$

R is called the 'universal R-matrix', and it can be thought as controlling the non-cocommutativity of the Hopf algebra. Quasitriangular hopf-algebras are sometimes called Quantum groups. We will see that they exhibit topological behaviour, as the following proposition hints to.
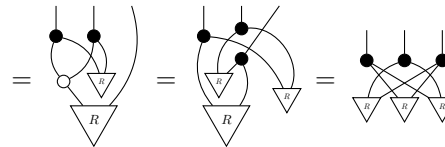
Proposition 3 *The universal R-matrix satisfies the Quantum Yang-Baxter equation:*

$$\text{(20)}$$

Proof First using isotopy invariance and the second rule of quaitriangularity we get:

$$\text{(21)}$$

Then using the first rule:

$$\text{(22)}$$

$\blacksquare$

14

Example 8 *The most trivial example of quasitriangular hopf algebras are the cocommutative ones. It is easy to check that if H is cocommutative, it is quasi-triangular with* ●|●| *as R-matrix.*

We will only be considering finite dimensional Hopf Algebras, as for finite dimensional vector spaces, these always have duals.

Definition 19 (Dual Hopf Algebra) *For a finite dimensional Hopf Algebra H the dual Hopf algebra is the vector space $H^\star$ of linear functionals on H with Hopf Algebra structure given by transposing all of the structure.*

Given any finite dimensional hopf algebra H with invertible antipode there is a standard way of constructing a Quasitriangular Hopf Algebra first introduced by Drinfeld [**?**]. It will be implicit from now on that all Hopf algebras (and vector spaces) are finite-dimensional unless stated otherwise.

Definition 20 (Quantum double of a Hopf algebra) *The quantum double of a Hopf algebra $(H, \mu, 1, \Delta, \epsilon, S)$ with invertible antipode is the vector space $H \otimes H^\star$, with the following structure:*

- *multiplication and unit:*
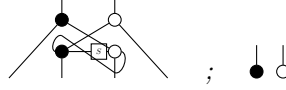
- *comultiplication and counit:*

- *antipode:*

It is easy to check this is indeed a Hopf algebra and that it is quasitriangular with universal R-matrix:

2.3 Representations of Hopf algebras

Recall that a group describes the symmetries of some space X when it acts on it (e.g crystals, classical symmetries= symmetries of sets). If we apply the same reasoning to Hopf Algebras we have to make H act on some quantum state space (i.e Hilbert space). So our object of study is not H on its own but rather a module (or representation) of H.

Where V is a finite dimensional vector space. Note that the above diagram represents a linear map, all diagrams we will be drawing in this section are diagrams in $Hilb$. In order for V to be a representation the following must hold.

Definition 21 (Module) *Let H be bialgebra, a (left) H-module (or representation of H) is a vector space V together with a (left) action of H on V.*

$$H \quad V$$
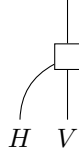
Satisfying the following conditions:

$$\tag{23}$$

$$\tag{24}$$

A right H-module is defined similarly with a right H-action.

Suppose V and W are representations of H, then we say $f : V \to W$ (a linear map) is a H-module homomorphism (or intertwiner) if:

$$\tag{25}$$

Where the black square denotes the action of H on W.
Dually we can define H-comodules and H-comodule homorphisms as follows.

Definition 22 (Comodule) *Let H be bialgebra, an H-comodule is a vector space V together with a coaction of H on V.*

$$H$$

$$V$$
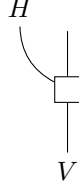
Satisfying the following conditions:

$$(26)$$

$$(27)$$

A right H-comodule is defined similarly with a right H-coaction. And H-comodule homomorphisms are linear maps which commute with the H-coaction.

Let us consider, the category $Rep(H)$ where objects are representations of H and morphisms intertwiners. It is easy to see that the axioms of a category are satisfied, composition is just lifted from vector spaces. This category has really nice structure induced from the defining axioms of hopf algebras.

Proposition 4 *$Rep(H)$ is a monoidal category for any bialgebra H with tensor unit the trivial one-dimensional representation $(\mathbb{C}, \varphi)$.*

Proof Given H-modules V and W (with white and black actions respectively), $V \otimes W$ has natural H-module structure induced by the comultiplication:

$$H \quad V \quad W$$
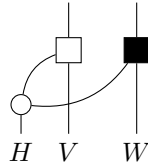
And $V \otimes W$ with this action is indeed a module as:

$$(28)$$

17

Also:

$$\text{(diagram)} = \text{(diagram)} = \text{(diagram)} \tag{29}$$

Using the bialgebra law and the fact that V and W are H-modules. Showing that $(\mathbb{C}, \curlyvee)$ is the tensor unit is a trivial application of the counit law.

∎

Proposition 5 *If H is cocommutative, then $Rep(H)$ is symmetric.*

Proof Cocommutativity means:

$$\text{(diagram)} = \text{(diagram)} \tag{30}$$

So the symmetry morphism on $V \otimes W$ from $Vect$ is an intertwiner:

$$\text{(diagram)} = \text{(diagram)} = \text{(diagram)} \tag{31}$$

∎

Recall that when H is cocommutative, it is trivially quasitriangular. The following is an important generalisation of the previous result.

Proposition 6 *If H is quasitriangular, then $Rep(H)$ is braided.*

Proof For any H-modules V and W, using the symmetry morphism from $Vect$ define:

$$\text{(diagram)} := \text{(diagram)} \tag{32}$$

$$\text{(diagram)} = \text{(diagram)} \tag{33}$$

It is easy to see these are inverses of each other, we just need to check they are intertwiners.

$$\text{(diagram)} = \text{(diagram)} = \text{(diagram)} \tag{34}$$

18

Using H-module definition and the defining relation for R.

$$= \quad \text{(diagram)} \quad = \quad \text{(diagram)} \tag{35}$$

And a similar proof works for the inverse.

∎

Proposition 7 *If H is a Hopf algebra, then $Rep(H)$ is left-rigid.*

Proof For any H-module V let $V^\star$ be its dual in $Vect$, we can define a dual H-action on $V^\star$ using the antipode:

$$\text{(diagram)} \quad := \quad \text{(diagram)} \tag{36}$$
$$H \ V^\star \qquad\qquad H \ V^\star$$

Then the usual cups and caps from $Hilb$ are intertwiners.

$$\text{(diagram)} \quad = \quad \text{(diagram)} \quad = \quad \text{(diagram)} \quad = \quad \text{(diagram)} \tag{37}$$

Using the module laws and the antipode law. A similar derivation holds for the cap.

∎

We can see that the proof relies on the existence of the antipode. If a skew-antipode $\bar{S}$ exists, $Rep(H)$ is right-rigid, where the right dual is defined:

$$\text{(diagram)} \quad := \quad \text{(diagram)} \tag{38}$$
$$H \ V^\star \qquad\qquad H \ V^\star$$

The proof that this choice works is very similar to the one above. In particular, $\bar{S}$ exists when the antipode is an invertible morphism as we can define $\bar{S} = S - S^{-1}$ If the antipode coincides with the skew antipode then $Rep(H)$ then left and right duals in $Rep(H)$ coincide, we say it is rigid.

19

3 The Algebra of Anyons

In this section we introduce the physics of Anyons and use the framework developed in the first section to define categorical models for theories of these particles. For an introduction to the physics of anyons consider the foundational paper [**?**] or Simon's notes [**?**], for a categorical presentation [**?**] and for a thorough survey of the mathematical aspects of anyons [2].

In the first section we introduce the physics and make the link with braided fusion categories, in the second part of we will develop the categorical formalism and the third part is dedicated to one result where quantification and categorical constructions play an important role.

To understand how anyons arise physically, let us consider n indistinguishable particles evolving in space. The quantum amplitude for a space-time evolution of the system will depend on the topology of the particle word-lines and not on the detailed geometry. This means that isotopic space-time evolution will yield the same amplitude.

To formalize the situation suppose we have n indistinguishable particles in D dimensions, the configuration space can be written as:

$$C = (\mathbb{R}^{nD} - \Delta)/S_n$$

Where Δ is the space of coincidences (where at least two of the n particles occupy the same position in $\mathbb{R}^D$). We are quotienting the space by S_n to account for the indistinguishability of the particles (i.e we do not care about the order of the n coordinates in D dimensions). Let us fix the starting and endpoint in the configuration space, the space of paths from starting to endpoint C divides into topologically distinct classes, described by the fundamental group $\pi_1(C)$. These classes account for the different possible exchange statistics of the particles.

We can then describe the evolution of the wave function for the system via unitary transformations induced from the element of the fundamental group corresponding to particles word-lines. In mathematical terms this corresponds to a representation of $\pi_1(C)$.

If space-time has $D = 3 + 1$ dimensions, the topological class of paths is completely determined by the corresponding permutation of the particles, because there are no knots in 4 dimensions. Therefore the evolution of the system under particle exchanges will be described by a representation of the symmetric group S_n. In $2 + 1$ dimensions we have more exotic behaviour, as the paths in configuration space can braid. The time evolution of the wave function is then described by a representation of the braid group on n strands, denoted B_n.

Definition 23 (Braid group) *The braid group on n strands B_n is the group generated by $\{\sigma_i : i = 1, .., n - 1\}$ satisfying the following relations:*

- *$\sigma_i \sigma_j = \sigma_j \sigma_i$ for $i + 1 < j$*

- *$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ for $1 < i < n$.*

The second relation is called Yang-Baxter equation and can be drawn as follows:

$$
\begin{array}{c}
\text{(diagram)}
\end{array}
=
\begin{array}{c}
\text{(diagram)}
\end{array}
\tag{39}
$$

$$i-1 \quad i \quad i+1 \qquad i-1 \quad i \quad i+1$$

- Abelian case

We say the system is abelian if the wave function lives in a one-dimensional representation of the group of paths in configuration space. In $3+1$ dimensions, this means we have to consider the one-dimensional representations of S_N. Note that there are only two possibilities (namely the trivial and the sign representations) corresponding to the two possible types of particle statistics in $3+1$ dimensions (Bose and Fermi statistics respectively). In $2+1$ dimensions we have many more possibilities as the evolution of the wave function will be described by a one-dimensional representation of the braid group B_N. There are infinitely many one dimensional representations of the braid group connecting the fermions and bosons case. These are described by a single parameter θ. Only one parameter because using Yang-Baxter we can show that all N phases have to be the same, also can show θ has to be a fraction from physical considerations. We obtain abelian anyons.

- Non-abelian case

In the non-abelian case, the wave function lives in a higher-dimensional representation of In $3+1$ dimensions we don't get anything more than bosons and fermions if we also want to consider creation, annihilation (splitting, fusion) of particles (Doplicher-Roberts theorem). In $2+1$ dimensions we obtain degeneracy, non-abelian anyons, braidings give all unitaries.

In the previous section, we only considered groups of symmetries of a Hamiltonian. In order take topological symmetries of a system into account, we need the more general framework of Hopf Algebras. In particular, as those symmetries arise from braids, we need quasitriangular hopf algebras (or quantum groups) to treat all symmetries on the same level. We will see that the universal R-matrix plays an important role in the description of topological dependencies.

3.1 Models of anyons

We want to construct a category $\mathcal{C}$ that models the behaviour of anyons. Ojects of $\mathcal{C}$ will correspond to quantum systems and morphisms to their possible evolutions, or to the processes we can perform on them.
Let us first set a finite set of labels $\{a, b, c...\}$ of distinct particle types, these will be objects of $\mathcal{C}$. In our theory we must be able to consider many particles at

the same time, so $\mathcal{C}$ must be monoidal [?]. The unit of the tensor $\mathbf{1}$ corresponds to the vacuum particle type (or "no-particle") and must be within our labels. So for the moment our theory is a monoidal category $\mathcal{C}$ and we can already use the diagrammatic language. A particle of type a evolving trivially in time is denoted:

$$\Big\uparrow a$$
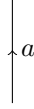
Where we have adopted the convention that time flows upwards.
Two particles of types a and b can fuse to a third particle of type c. So we have fusion morphisms:

$$c \quad \phi \quad a \quad b$$
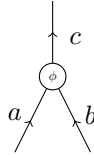
Similarly a particle c can split to give two particles a and b. And $\mathcal{C}$ contains splitting morphism:

$$a \quad b \quad \psi \quad c$$
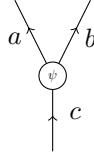
Any particle a in quantum physics comes with its antiparticle a^* which we can picture as a particle of type a travelling backwards in time.

$$\Big\downarrow a$$
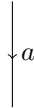
It has the property of fusing to the vacuum when it encounters a. Dually the vacuum can yield a particle-antiparticle pair, so we have cups and caps morphisms
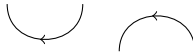
Categorically this corresponds to a rigid structure on $\mathcal{C}$, we will assume it is a well behaved category i.e it is spherical and $1^* = 1$. So we can define the quantum numbers for each particle type a to be the following scalar:

$$\bigcirc \, a$$

22
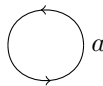
At this point we need to linearise the theory to take superpositions into account. We enrich the category over commutative monoids and introduce a biproduct $\oplus$ and zero object $\mathbf{0}$ as additional structure on $\mathcal{C}$. In order for the fusion to behave well with superpositions we must require that our particle types be simple objects in the category. At this point, our category $\mathcal{C}$ is a spherical fusion category (see appendix) and the fusion rules look like this:

$$a \otimes b \simeq \oplus_c N_{ab}^c c \tag{40}$$

Where $N_{ab}^c \in \mathbb{N}$.

We still have one question to ask to the theory, what happens when the position of two particles is exchanged? To answer this question the theory must have a braid structure and we obtain a braided fusion category (see section 1). The braid structure determines the long-distance, topological interactions between particles.

Example 9 *Suppose we start from a set of labels and define the fusions to form a group. In fact 1 is the identity particle type, for any particle type a, a^* will be its inverse. We have defined the skeleton of a spherical fusion category, which we obtain by linearising, i.e taking a functor to $Hilb$. We obtain the category Vec_G, of G graded vector spaces over $\mathbb{C}$. The category Vec_G for G a group is a symmetric spherical fusion category. Linearity and tensor are given by the underlying $Vect$ structure, simple objects are indexed by the elements of G, duality is proved by using the group inverse. It is easy to chow that $Vec_G \simeq Rep(Func(G))$ where $Func(G)$ is the function algebra on G. For $G = \mathbb{Z}_2$ we have two irreducible representations τ_+ and τ_-, both one dimensional with the obvious fusion rules given by the cyclic group of order 2.*

Remark In the case where the theory is described by the category $RepG$. Let us consider the object $V = \mathbb{C}G$ of $RepG$. (Note $V \simeq \oplus_i V_i$ where V_i's are the simple objects.) Simple objects correspond to particle types so the states of V are superpositions of particle types. In the case where G is abelian there is only one way two particles can fuse to a third, so the fusions are deterministic and the irreducible representations will be one dimensional, each corresponding to an element of the group. If G is not abelian, say $a \otimes b \simeq c_1$ and $b \otimes a \simeq c_2$ then taking the representations category defines a 2-dimensional object c spanned by $\{c_1, c_2\}$ which is an irreducible representation of G. So from now on we will call particle types the irreducible representations and particles subtypes the elements of the group G. The action of G permutes the basis vectors, multiplying by an element of G, but an element of G is precisely a particle subtype and multiplication is fusion. So acting with $g \in G$ on a state $v \in V$ corresponds to fusing a particle of type g with one that is in a superposition v of particle types. The allowed processes are intertwiners which commute with the action and therefore preserve fusions. If the group G is abelian, then the particles are abelian anyons.

3.2 Braided Fusion Categories

We can place braided fusion categories in a spectrum by asking what their symmetric center Z_2 is. The two antipodal points of this spectrum are symmetric fusion categories on one side (such that $Z_2(\mathcal{C}) = \mathcal{C}$) and modular tensor categories (such that the symmetric centre is trivial, i.e its objects are direct products of the tensor unit $\mathbf{1}$). In the first case, we have only symmetric exchange symmetries so that all particles in the theory are either bosons or fermions. Such categories are degenerate anyon theories with no topological dependencies between particles. Modular tensor categories are really the opposite situation, the theory doesn't contain any bosons or fermions but only non-degenerate anyons, i.e anyons with non-trivial twist factor.

Definition 24 *The symmetric center $Z_2(\mathcal{C})$ is the full subcategory of $\mathcal{C}$ defined by:*
$$obj\, Z_2(\mathcal{C}) = \{X \in \mathcal{C} : c_{X,Y} \circ c_{Y,X} = id_{Y \otimes X} \quad \forall Y \in \mathcal{C}\}$$

Definition 25 *A braided fusion category is:*

- *pre-modular if it is spherical,*

- *non-degenerate if $Z_2(\mathcal{C})$ is trivial*

- *modular if it is pre-modular and non-degenerate.*

Theorem 8 *Let $\mathcal{C}$ be a spherical symmetric fusion category with trivial twists. Then $\mathcal{C} \simeq Rep(G)$ for some group G (unique up to iso).*

Theorem 9 *If $\mathcal{C}$ is a spherical fusion category then $Z_1(\mathcal{C})$ is modular.*

Modular tensor categories are particularly well behaved types of braided fusion categories. To any modular category $\mathcal{C}$ we can assign the so called modular S-matrix which will contain all the information of the fusion rules as well as the braided structure.

Definition 26 *Let $\mathcal{C}$ be a spherical braided fusion category and let I be the set of isomorphism classes of simple objects in $\mathcal{C}$. We define $S_{i,j}$ for $i,j \in I$ to be the following: (diagram)*

Theorem 10 *$\mathcal{C}$ is modular iff the S-matrix is invertible.*

Theorem 11 *The modular S-matrix diagonalises the N-matrix.*

splitting, fusion rules, braided, R,T matrices, modular S matrix.

Example 10 (Knot invariants)

3.3 The Drinfeld center

In the previous section we saw that BFCs can be put on a spectrum ranging from symmetric fusion categories to modular categories. Physically, symmetric fusion categories are degenerate theories of anyons as they exhibit no topological behaviour. Conversely modular categories are very well behaved anyons theories. In this section we introduce a general construction that turns braided fusion categories into modular categories, and we show its relationship with the Quantum double construction on a Hopf Algebra introduced in the first chapter. Topological dependencies between objects in fusion categories are captured by the braided structure.

Definition 27 (Half-braiding) *A half-braiding on some object X in a monoidal category $\mathcal{C}$ is a natural isomorphism*

$$e^X : X \otimes (-) \Rightarrow (-) \otimes X$$

satisfying:

$$e^X_{Y \otimes Z} = (id_Y \otimes e^X_Z) \circ (e^X_Y \otimes id_Z)$$

Definition 28 (Drinfeld center) *The braided (Drinfeld) center of a category $\mathcal{C}$ is the category $Z(\mathcal{C})$ with objects pairs (X, e^X) where $X \in \mathcal{C}$ and e_X is a half-braiding, and with morphisms given by the morphisms of $\mathcal{C}$ which commute with the half-braiding.*

Definition 29 (Yetter-Drinfeld modules) *Let H be a bialgebra, the category $\mathcal{D}_H^{lr}$ is the category of left-right Yetter-Drinfeld modules where objects are left H-modules which are simultaneously right H-comodules satisfying the following compatibility condition:*

 (41)

where the white box denotes the H coaction and the black box defines the right coaction. Morphisms of $\mathcal{D}_H^{lr}$ are both H-module and H-comodule morphisms. Left-left Yetter-Drinfeld modules are defined in the obvious way and form a category $\mathcal{D}_H^{ll}$. The compatibility condition then looks like this:

 (42)

Fix a bialgebra H and suppose $\left(V, \overset{\bullet}{\uparrow}\right) \in obj(Rep(H))$ and (V, e_V) is in $Z(RepG)$. Note that H has a natural H-module structure given by right multiplication. Consider the component of the half-braiding of V at H.

Define a right coaction of H on V by:

$$ \text{(diagram)} \quad := \quad \text{(diagram)} \tag{43} $$

Note that from the bialgebra laws (diagram) and (diagram) , seen as morphisms on the H-module H are intertwiners in $Rep(H)$. Therefore by naturality of the half braiding we get:

$$ \text{(diagram)} \quad = \quad \text{(diagram)} \quad = \quad \text{(diagram)} \tag{44} $$

and

$$ \text{(diagram)} \quad = \quad \text{(diagram)} \quad = \quad \text{(diagram)} \tag{45} $$

So that the coaction indeed defines a left H-comodule.

Claim 1

$$ \text{(diagram)} \quad = \quad \text{(diagram)} \tag{46} $$

Proof As the braiding is an intertwiner, it commutes with the action of H on $V \otimes H$, therefore:

$$ \text{(diagram)} \quad = \quad \text{(diagram)} \quad = \quad \text{(diagram)} \tag{47} $$

Now note that $\left(H \otimes H, \text{(diagram)} \right)$ is in $Rep(H)$ and

$$ \text{(diagram)} : \left(H \otimes H, \text{(diagram)} \right) \to \left(H, \text{(diagram)} \right) $$

is an intertwiner by associativity. Also it is easy to check that the symmetry morphism lifted from $Vect$

$$ \left(H, \text{(diagram)} \right) \otimes V \to V \otimes \left(H, \text{(diagram)} \right) $$

is an intertwiner. Therefore by naturality of the braid:

$$\tag{48}$$

∎

We have defined a functor $F_1 : Z(Rep(H)) \to \mathcal{D}_H^{lr}$ which is identity on arrows and sends (V, e_V) to the left-right Yetter-Drinfeld module with black H action and white H coaction. To see that it is well defined to say it is identity on arrows (and so faithful) note that if an H-module morphism f is in $Z(Rep(H))$ then it commutes with the half-brading, in particular it commutes with the H-component of the half-braiding and therefore it commutes with the H-coaction as defined.

Similarly we can define a functor $F_2 : Z(Rep(H)) \to \mathcal{D}_H^{ll}$ by considering the V component of the half braiding on the H-module H and defining the following left-coaction:

$$\tag{49}$$

Claim 2

$$\tag{50}$$

Proof The proof is very similar to that of the previous claim. Using the fact that the braid is an intertwiner we obtain

$$\tag{51}$$

Then using the unit law and the same trick as before we see that

$$\tag{52}$$

∎

For the same reasons as for F_1, F_2 is faithful. To show F_1 and F_2 are equivalences of categories we still need to show they are full and essentially surjective.

- F_1 is full:
  Suppose f is a morphism $V \to W$ in $\mathcal{D}_H^{lr}$,

We now show that or any $\left(W, \square\!\!\!\!\square\right)$ define

$$\overset{\diagdown \ \diagup}{\underset{W \ V}{\diagup}} := \square\!\!\!\!\square \quad ; \quad \overset{\diagup \ \diagdown}{\underset{V \ W}{}} := \square\!\!\!\!\square \qquad (53)$$

Claim 3

$$\langle \text{diagram} \rangle = | \ | \ | \quad \Longleftrightarrow \quad \square = \bullet \ | \qquad (54)$$

$$\langle \text{diagram} \rangle = | \ | \ | \quad \Longleftrightarrow \quad \square = | \ \bullet \qquad (55)$$

Proof We will only proove the first statement, the second proof is very similar. First note that from the definition and as W is a H-module:

$$\langle \text{diagram} \rangle = \boxed{x} = \boxed{x} \qquad (56)$$

$(\Longleftarrow)$ is straightforward. To show $(\Longrightarrow)$ set $W = H$ with the natural left module structure given by left multiplication, then inserting the unit state $\bullet$ on the left of the tensor we obtain the required identity.

$\blacksquare$

Proposition 12 *If H is a finite-dimensional Hopf Algebra then right-right Yetter Drinfeld modules are DH-modules.*

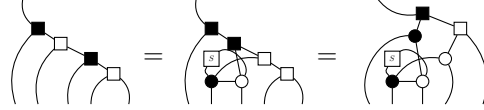**Proof** The previous claims only assumed the bialgebra laws. Making use of the antipode and the compatibility condition we obtain:

$$\boxed{s} = \boxed{s} = \qquad (57)$$

When H is finite dimensional, we can define the action of DH on V as follows (where thick wires carry DH and thin wires carry H)

$$\underset{DH \ \ V}{\square} := \qquad (58)$$

28

This action gives V a DH-module structure as:

$$(59)$$

■

Corollary 1 *If H is a finite dimensional Hopf algebra with invertible antipode $Z(RepH) \simeq RepDH$*

4 Quantum Computation

4.1 Phases of Matter

Classical phases of matter: solid, liquid and gas.
Temperature is proportional to energy
Close to zero temperature, phases of matter are quantized. We obtain exotic behaviours of matter.
In order to talk about quantum phases of matter we need to consider many-body quantum systems. We will use the definitions of Zhenghan

Definition 30 (Many Body Quantum Systems) *A Many-body Quantum system (MQS), is a triple $(\mathcal{L}, b, \mathcal{H})$, where $\mathcal{L}$ is a Hilbert space with a distinguished ONB b and a hermitian operator $\mathcal{H} : \mathcal{L} \to \mathcal{L}$, called Hamiltonian.*

The eigenvalues of the Hamiltonian correspond to the energy levels of the system. The elements of the basis b are the initial classical states of the system. Many-body quantum systems will usually be obtained from spatial configurations of particles, which we will descibe by graphs.

Definition 31 *A Hamiltonian is k-local if...*

Definition 32 *An MQS on a graph $\mathrm{T} = (V, E)$ with $\mathbb{C}^d$ degrees of freedom (qudit space) is an MQS $(\mathcal{L}, b, \mathcal{H})$ where*

$$\mathcal{L} = \otimes_{e \in E} \mathbb{C}^d$$

b is obtained from the standard basis of $\mathbb{C}^d$ and $\mathcal{H}$ is a local Hamiltonian.

Many interesting spatial configurations of matter are obtained from triangulations of manifolds by taking their 1-skeleton graph.
Let us consider unitary operators which commute with the Hamiltonian $\mathcal{H}$. These are operators which leave the energy of the system unchanged. These transformations form a group G under composition and a particle subject to the Hamiltonian $\mathcal{H}$ will be described by irreducible representations of G. G is the group of symmetries of the system under $\mathcal{H}$.

Proposition 13 *Let $\mathcal{H} : V \to V$ be the Hamiltonian for some physical system described by a hilbert space V. Then the unitary operators which commute with $\mathcal{H}$ form a group G.*

Proof Suppose $R_1\mathcal{H} = \mathcal{H}R_1$ and $R_2\mathcal{H} = \mathcal{H}R_2$, then $R_1R_2\mathcal{H} = R_1\mathcal{H}R_2 = \mathcal{H}R_1R_2$. Also $R^{-1}\mathcal{H} = R^{-1}\mathcal{H}RR^{-1} = R^{-1}R\mathcal{H}R^{-1} = \mathcal{H}R^{-1}$. The unit is the identity operator $id_{V^* \otimes V}$.

∎

Proposition 14 *If G is the group of symmetries of a Hamiltonian $\mathcal{H}$ then each energy eigenspace carries an irreducible representation of G.*

Proof Note that under the obvious G-action, V is a representation of G. The eigenvalues of the Hamiltonian, correspond to energy levels of the physical system which we previously called 'particle types'. Fix any eigenvalue E of $\mathcal{H}$, the allowed states of a particle with energy E live in the corresponding eigenspace V_E. Indeed these are invariant under the action of $\mathcal{H}$:

$$\mathcal{H}\ket{\psi} = E\ket{\psi}$$

Note that if $R \in G$ then

$$\mathcal{H}R\ket{\psi} = R\mathcal{H}\ket{\psi} = ER\ket{\psi}$$

So $R\ket{\psi}$ is an eigenvector with eigenvalue E. Therefore G acts on V_E for any energy level. We prove V_E is irreducible by showing that $End(V_E) \simeq \mathbb{C}$. Indeed suppose $f : V_E \to V_E$ is an intertwiner, then $fR = Rf \;\forall R \in G$ TO PROVE

∎

Starting with a hamiltonian $\mathcal{H}$ we have shown that energy levels (or particle types) correspond to the irreducible representations of the group G of symmetries of $\mathcal{H}$. The particle theory correponding to the hamiltonian $\mathcal{H}$ has irreducible representations of G as objects and intertwiners, preserving the energy of the system, as processes. This is the definition of the category $Rep(G)$. Note there are no restrictions yet on the group of symmetries.

Example 11 *Suppose $\mathcal{H} = \sigma_Z$ be the Hamiltonian of a qubit living in $\mathbb{C}^2$. It has eigenvalues ± 1 and corresponding eigenvectors $\ket{0}$ and $\ket{1}$.. The group algebra of symmetries of $\mathcal{H}$ is generated by id and $\mathcal{H}$ and it is isomorphic to $\mathbb{C}\mathbb{Z}_2$. $\mathbb{Z}_2$ has two irreducible representations (the trivial and the sign) representations which correspond to the one-dimensional eigenspaces of $\mathcal{H}$. Note that*

4.2 Kitaev's model

Let us consider a two dimensional lattice of particles (situated on the edges of the lattice) under the influence of a magnetic field and an electric field. Anyonic behaviour is exhibited by excitations of the particles on the lattice. In

our process theory the allowed processes are charge-flux composites, the states are lattice configurations (determined by the states of the particles, which are generally given by an element $g \in G$) . By mearuring the flux in certain regions of the lattice and acting on the charge of the corresponding flux sector we can create and control the behaviour of excitations on the material.

Example 12 *Let us consider the case where $G \simeq \mathbb{Z}_2$. We obtain a lattice of spins. Those particles we wont use as our qubits, indeed we will impose that their state is in a basis state $\{|0\rangle, |1\rangle\}$. One way to picture the states of the system is to draw the lattice and colour the edges red when the corresponding particle is in state $|0\rangle$. Note that the lattice can be embedded in any manifold (e.g. subsection quantum memory is a lattice on a torus, if we used a more layered lattice we could implement error correction). What we obtain is a picture of paths on the lattice which we call excitations.*

The magnetic flux of a particle is given by an element $h \in G$, this indexes the superselection sectors so that the charge lives in a unitary irreducible representation of the centralizer $N(h)$ of the flux h carried by the particle. We have two possible operations on our states: flux measurement and symmetry transformations on the charge. Flux measurements correspond to a projection $P_h \in \mathbb{C}G^*$ onto flux sector h. The residual global symmetry transformations are then implemented via some $g \in N(h)$.
Naturally the projectors form a Von Neumann family and satisfy

$$P_h P_{h'} = \delta_{h,h'} P_h.$$

A general element $g \in G$ is a global symmetry transformation and affects the fluxes via conjugation:

$$g P_h = P_{ghg^{-1}} g \tag{60}$$

The quantum double construction allows to capture both global symmetry transformations and projective measurements in one algebraic structure.

Definition 33 *Lagrangian, Noether's theorem*

Definition 34 *For any finite group G, its quantum double $D(G)$ is the algebra generated by $\{P_h g\}_{h,g \in G}$ with multiplication induced by (1). $D(G) \simeq \mathbb{C}G^* \otimes \mathbb{C}G$ and inherits their hopf algebra structure (comultiplication and antipode are given by tensoring).*

$D(G)$ has a natural quasi-triangular structure witnessed by the universal R-matrix $R = \sum_{g,h \in G} P_h e \otimes P_h g$, making $RepDG$ braided. Particle states then live in irreducible representations of $D(G)$. Let $\{C_i\}_{i=1}^n$ be the distinct conjugacy classes in G. To each of those conjugacy classes corresponds a centralizer subgroup N_i (two choices of representatives for C_i yield isomorphic centralizer subgroups). Then for any irreducible representation (α, V_α^i) of N_i with basis elements v_j^α, let $V_{i,\alpha} = \mathbb{C}C_i \otimes V_\alpha^i$, this has basis $\{|k, v_j^\alpha\rangle\}_{j=1,\ldots,dim\alpha}^{k \in C_i}$ and forms an irreducible representation of $D(G)$ under the action

$$P_h g |k, v_j^\alpha\rangle = \delta_{h,gkg^{-1}} |h, \alpha(h^{-1}gk)v_j^\alpha\rangle \tag{61}$$

and the $\{V_{i,\alpha}\}$ is the complete set of irreducible representations.

Remark Can we generalise the lattice construction? The following argument seems to work for abelian groups. Being a spherical fusion category, $RepG$ is well suited to be a process theory of particles. As we pointed out earlier what is missing is the braided structure, but let us ignore this for the moment. We have simple objects corresponding to particle types and fusion rules determined by the group structure.

Now suppose we have particles whose fusion is described by a $RepG$ and let us consider a lattice with those particles located at the edges. This lattice could be embedded in any space but let us assume it is a lattice on a torus. The states of our system are then configurations of particle types on the edges. So edges are coloured by simple representations from $RepG$. Now we can act on the lattice with vertex and plaquette operators which basically implement measurements at vertices and flips (fusion with other simple reps) of the particles on a plaquette. By now we have produced a theory where states are lattice configurations and processes are generated by vertex V_α and plaquette P_β operators. We want to extract the topological degrees of freedom of this theory. First we note that using vertex operators we can make sure that the product of all particles incident at all vertices is 1, i.e $V_\alpha = 1 \; \forall \alpha$. We restrict our states to satisfy this local property and we drop vertex operators (in the sense that they are not allowed processes anymore), indeed we fixed their value at all points of the lattice. By also setting $P_\beta = 1$ at all plaquettes we quotient further the theory. So we obtain a theory where all vertex and plaquette measurements have value 1. We finally declare two configurations to be equal if there is a sequence of plaquette operations taking us from one to the other. Noting that plaquette operators are local isometries we see this corresponds to quotienting out the category by an equivalence relation. This doesn't exaust the degrees of freedom of the theory because of the topology of the torus. Those topological degrees of freedom will be the simple objects our newly created category, their fusion rules are completely determined by the structure of $Rep(G)$. Indeed the category we obtained is $Z(Rep(G)) \simeq Rep(DG)$.

Example 13 *In the case $G = \mathbb{Z}_2$, recall $Rep\mathbb{Z}_2$ has two simple object of dimension one τ_+ and τ_- with fusions given by group structure. Let us draw the states of our system as colourings of the edges of the lattice. The condition on the vertex operators results in no endlines and no triple intersections on the lattice. The condition on plaquette operators only allows loop configurations. Quotienting out by plaquette operators relation we obtain 4 distinct classes, namely the vacuum 1, the first cycle of the torus X, the second cycle Z, and both cycles $X \otimes Z \simeq Y$ and we have the fusion rules. The theory we have obtained is $RepD\mathbb{Z}_2$ which has in fact 4 simple objects with same fusions. We are therefore treating the topological defects of a theory in $Rep\mathbb{Z}_2$ as particles particles in their own right, with their own theory. All those representations are one-dimensional and in fact we just formulated a theory of abelian anyons.*

Example 14 (Anyon Vacuum on a Torus and Quantum Memory) *If we*

consider the torus as our configuration space. Let C_1, C_2 be the two cycles. Consider the process T_i for $i = 1, 2$ which creates a particle-antiparticle pair, moves them in opposite directions around cycle C_i so that they meet on the other side of the torus and annihilate. Then we can show T_i do not commute with each other if the particles are abelian anyons with $\theta \neq 0, \pi$. We know θ must be a fraction p/q with p and q coprime. Then we can show that the system has degenerate ground states. We have q different ground state, so the vacuum state lives in a q dimensional space. If we initialise it in some superposition it will remain in that state unless a T_1 or T_2 operation is implemented. Because of their topological nature it is very unlikely that such processes occur spontaneously, and therefore the quantum information stored in the superposition is protected.

4.3   Permutational Quantum Computing

This section is about a model of quantum computation introduced by Jordan [**?**]. We will give a categorical presentation of the model which is not present in the literature and will allow us to compare the model to other computational models.

Definition 35 *Let $\mathcal{J}$ be the symmetric fusion category with positive half integers as simple objects, fusions etc.*

The construction given by Jordan can be generalised. In this section we argue that Symmetric Fusion categories are models fo permutational quantum computation.

Theorem 15 *Any symmetric fusion category induces representations of the symmetric group S_n for any $n \in \mathbb{N}$.*

Theorem 16 *If $\mathcal{C}$ is a symmetric fusion categories, then $\mathcal{C}$ is symmetrically monoidally equivalent to $Rep(G)$ for G some group (if the twist is trivial) or some supergroup (if the twist is -1).*

Proof Doplicher-Roberts theorem

∎

Proposition 17 *Jordan's model $\mathcal{J}$*

Example 15 *Permutational quantum computation in $Rep(S_3)$.*

Remark The model described by Jordan is implementable by defining a hamiltonian on a network of spins.
Generalised spin network systems for arbitrairy group G

Example 16 (Approximation of Dijkgraaf-Witten link invariants) *The link invariant essentially counts homomorphisms from the fundamental group of the link complement to the group G. (cite Zhenghan?)*

4.4 Topological Quantum Computation

Take the fusion space to be our topological hilbert space.
Topological qudits are usually encoded as fusion tree basis elements
Topologial gates: braids (can express as action of the braid group) + measurements (=fusions and associators).

5 A braided programming language

5.1 Non-commutative linear logic

5.2 An adjunction between fPQC and TQC

This section is dedicated to the relationship between a category $\mathcal{C}$ and its braided centre $Z(\mathcal{C})$. In the first part we will talk about non-commutative logic and modalities. In the second part we will see

Free forgetful adjunction:

$$\Box : \mathcal{C} \rightleftarrows Z(\mathcal{C}) : U$$

$$\Box : RepG \to RepDG \simeq Z(RepG)$$

Theorem 18 *Let* $\{X_i\}_{i \in I}$ *be the set of representatives of the isomorphism classes of simple objects in RepG. Let* $\mathbb{C}G$ *be the regular representation, then*

$$\mathbb{C}G \simeq \oplus_{i \in I} X_i \otimes X_i^*$$

Theorem 19 $\Box V = \oplus_{i \in I} X_i^* \otimes V \otimes X_i$ *with action of* DG *given by ....*

Let G be a group, DG its quantum double, (π, V) a representation of G.
The induced representation $\Box V$ is the coequalizer of:

$$DG \otimes \mathbb{C}G \otimes V \rightrightarrows DG \otimes V$$

Where the top arrow is given by the right action of G on $DG \simeq \mathbb{C}G^* \otimes \mathbb{C}G$

$$(P_h g, k) \mapsto P_h(gk^{-1})$$

(this satisfies the axioms of an action but do we have to make the action conjugate the flux projection component?) and the bottom arrow is given by the π action on V.
To compute the coequalizer we consider the orbits of the action of G on DG, these form a partition of DG:

$$\{[P_k e] : k \in G\}$$

34

So, as a vector space $\Box V \simeq \mathbb{C}G \otimes V$ and the action of DG on $\Box V$ is given by:

$$P_h g[P_k e]v = \delta_{h,gkg-1}[P_h e]\pi(g)v \tag{62}$$

So that element $P_h g$ implements residual symmetry g and projects onto flux sector gkg^{-1}.

Note that if C_i are the conjugacy classes of G then $\mathbb{C}G \simeq \oplus_i \mathbb{C}C_i$ and we could try to decompose:

$$\Box V \simeq \oplus_i \mathbb{C}C_i \otimes V \tag{63}$$

The action (3) factors through the conjugacy classes, (4) gives us a decomposition of $\Box V$ into irreducibles if V is simple in $RepG$? (this hold for abelian groups, should be generalised given decomposition of V into Z_i modules).

$\Box$ is clearly not monoidal if we take $\otimes$ as tensor, is it monoidal under $\oplus$? i.e is it additive? (Note that the induced representation functor Ind_H^G for H subgroup of G is additive). If it is additive then it is left and right exact and could use this to find the decomposition of $\Box V$

Is the $\Box$ functor representable? In the sense $\Box \simeq Hom(\mathbb{C}G, \_)$?

Example 17 *If $G = \mathbb{Z}_2 = \{e, a\}$, irreducible representations are the trivial τ_+ and the one dimensional sign representation τ_-. $DG \simeq \mathbb{C}\mathbb{Z}_2^* \otimes \mathbb{C}\mathbb{Z}_2$ and the orbits of the right action of $\mathbb{Z}_2$ on $D\mathbb{Z}_2$ are given by*

$$\{[P_e e], [P_a e]\}$$

Recall that $D\mathbb{Z}_2$ has 4 irreducible one dimensional representations which we denoted 1,X,Z,Y. With fusion rules generated by $A \otimes A \simeq 1$ and $X \otimes Y \simeq Z$. Now let us calculate $\Box\tau_-$, it has basis $\{[P_e e] =: w_e, [P_a e] =: w_a\}$ and

$$P_e e(xw_e + yw_a) = xw_e \quad P_a e(xw_e + yw_a) = yw_a \quad P_e a(xw_e + yw_a) = -xw_e \quad P_a a(xw_e + yw_a) = -yw_a$$

And we see from the table (see Lahtinen "The Toric Code and the Quantum Double" for table of reps) that $\Box\tau_- \simeq X \oplus Y$. Similarly $\Box\tau_+ \simeq 1 \oplus Z$. Consider the regular representation $V := \mathbb{C}\mathbb{Z}_2 \simeq \tau_+ \oplus \tau_-$, then $\Box V \simeq 1 \oplus X \oplus Z \oplus Y \simeq (1 \oplus X) \otimes (1 \oplus Z)$. What happens if we braid the two components of $\Box V$? In $RepD\mathbb{Z}_2$ the braid is implemented by acting on the components with $R = \sum_{g,h \in \mathbb{Z}_2} P_g e \otimes P_g h \in D\mathbb{Z}_2 \otimes D\mathbb{Z}_2$ and swapping coordinates. I claim this implements a CNOT gate followed by a swap.

Example 18 *If $G = S_3 = \langle \sigma, \rho \rangle$ where σ is a reflection and ρ a rotation. S_3 has three irreducible representations: the trivial τ_+, the sign representation τ_- and the two dimensional τ_2.*

5.3 Quantum Semantics

6 Conclusion

References

[1] J. Baez and D. James. Categorification. *eprint arXiv:math/9802029*, 1998.

[2] E. Rowell and W. Zhenghan. Mathematics of topological quantum computing. *eprint arXiv:1705.06206*, 2017.

[3] S. Mac Lane. *Categories for the working mathematician*. Springer Verlag, 1971.

[4] P. Etingof, S. Gelaki, D. Nikshych, and V. Ostrik. *Tensor Categories*, volume 205 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2015.

[5] M. Mueger. Tensor categories: A selective guided tour. *eprint arXiv:0804.3587*, 2008.

[6] B. Bartlett. Fusion categories via string diagrams. *eprint arXiv:1502.02882*, 2015.

[7] Peter Freyd. *Abelian Categories*. Harper Row, 1966.

[8] J. Vicary and C. Heunen. Lectures on categorical quantum mechanics. https://www.cs.ox.ac.uk/files/4551/cqm-notes.pdf, 2012.

A Fusion categories

Many of the results we will see in this section can be found in [5], [6] and [7].

Definition 36 *The category $\mathcal{C}$ is Ab if it is enriched over abelian groups. That is all hom-sets have abelian group structures and composition of morphisms is a group homomorphism.*

Definition 37 *An Ab-category $\mathcal{C}$ is additive if it has zero object and every pair of objects has a direct sum $\oplus$.*

Definition 38 *An abelian category is an additive category where every morphism has a kernel and a cokernel and every monic (epic) is a kernel (cokernel).*

Definition 39 *Let k be field, we say $\mathcal{C}$ is k-linear if all hom-sets are k-vector spaces and composition is bilinear.*

We will assume throughout the thesis that $k = \mathbb{C}$ so in particular the field is algebraically closed.

Definition 40 *An object X in a $\mathbb{C}$-linear category is called simple if $EndX = k id_X$.*

Definition 41 *$\mathcal{C}$ is semisimple if every object is isomorphic to a direct sum of simple objects. $\mathcal{C}$ is finite if there are finitely many isomorphism classes of simple objects.*

Definition 42 *A $\mathbb{C}$-linear tensor category is a fusion category if it has finite-dimensional hom-spaces, is semisimple with finitely many isomorphism classes of simple objects, the unit $\mathbf{1}$ is simple and all objects have duals.*

Theorem 20 *$Rep(H)$ is a fusion category*

Example 19 *Any group G is a hopf algebra (comonoid = copy). Therefore $RepG$ can also be made monoidal and rigid.*

Example 20 *Recall the group $S_3 = \{e, g, g^2, \sigma, \sigma g, \sigma g^2\}$. The category $Rep(S_3)$ is a fusion category. By the known representation theory of S_3, $Rep(S_3)$ has three simple objects: the trivial representation 1, the sign representation -1 and the geometric two dimensional representation τ:*

$$\tau : \quad \sigma \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$g \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}$$

These satisfy the following fusion rules $\forall X$ simple object:

$$1 \otimes X \simeq X \simeq X \otimes 1 \ -1 \otimes -1 \simeq 1 \ -1 \otimes \tau \simeq \tau \simeq \tau \otimes -1 \ \tau \otimes \tau \simeq 1 \oplus -1 \oplus \tau \quad (64)$$

Example 21 (Graph invariants from spherical fusion categories)

We now explore an important class of categories. Braided fusion categories (BFCs) are very closely related to categories of representations via the Tannaka reconstruction theorem and its variations. BFCs have found numerous applications to Quantum computer science as we will see in the remaining sections. Braid group, Yang-Baxter, Quasitriangular Hopf algebras.

Definition 43 *Braided monoidal categories (with braid c)*

Definition 44 *Ribbon categories (twist θ)*

Definition 45 *The symmetric centre $Z_2(\mathcal{C})$ of a braided tensor category $\mathcal{C}$ is the full subcategory with the following objects:*

$$\{X \in \mathcal{C} : c_{X,Y} \circ c_{Y,X} = id_{Y \otimes X} \forall Y \in \mathcal{C}\}$$

Example 22 *Braid group B_n, free braid category, free construction Tensor categories $\rightarrow$ BTCs (2-adjunction)*

Example 23 *categories of tangles = free rigid braided categories.*
Tangle categories are not linear over a field but can be linearised by using the free vector space functor $Set \to Vect$. This gives still big categories, but can be quotiented out by an ideal defined in terms of link-invariants to give interesting cats.

Definition 46 *braided fusion category*

Definition 47 *Let $\mathcal{C}$ be a tensor category, $X \in \mathcal{C}$. A half-braiding e_X is a family $\{e_X(Y) : X \otimes Y \xrightarrow{\sim} Y \otimes X\}$ such that $e_X(\mathbf{1}) = id_X$ and*

$$e_X(Y \otimes Z) = id_Y \otimes e_X(Z) \circ e_X(Y) \otimes id_Z \quad \forall Y, Z \in \mathcal{C}$$

Theorem 21 *If $\mathcal{C}$ is k-linear, spherical or a *-category (k-linear dagger) then so is $Z_1(\mathcal{C})$*

Theorem 22 *If H is a quasitriangular Hopf Algebra then $Rep(H)$ is a braided fusion category.*

    N-matrix, R-matrix