

A Categorical Semantics for Topological Quantum Computation

Giovanni de Felice

April 2017

Contents

1	Introduction	2
2	Representation Theory	2
2.1	Monoidal categories	2
2.2	Hopf symmetry	3
2.2.1	Monoids and comonoids	3
2.2.2	The <i>Hopf</i> PROP	4
2.2.3	Hopf Algebras and Quantum groups	4
2.2.4	Categories of representations	4
2.3	Spherical Fusion categories	4
2.3.1	Spherical categories	4
2.3.2	Fusion categories	4
2.3.3	Graph invariants	5
2.4	Braided Fusion categories	5
2.4.1	Braiding and twisting	5
2.4.2	Modular categories	6
2.4.3	Knot invariants	7
3	The Physics of Anyons	7
3.1	Phases of Matter	7
3.1.1	Many-body Quantum Systems	7
3.1.2	Topological phases of matter	8
3.2	Algebraic theory of Anyons	10
3.3	Quantum Symmetry	11
3.3.1	The Quantum Double	11
3.3.2	Drinfeld center	13
3.3.3	Kitaev's lattice construction	13

4	Quantum Computation	14
4.1	Permutational Quantum Computing	14
4.1.1	Jordan's model	14
4.1.2	Categorical PQC	14
4.1.3	Spin Network Quantum systems	14
4.2	Topological Quantum Computation	15
4.2.1	The Topological Model	15
4.2.2	Anyon Vacuum on a Torus and Quantum Memory	15
4.2.3	Approximation of Dijkgraaf-Witten link invariants	15
5	A braided programming language	15
5.1	Non-commutative linear logic	15
5.2	Adjunction	15
5.3	Quantum Semantics	17

1 Introduction

Categories and diagrams

Symmetry, quantization and categorification

Categorification = replacing equalities with isomorphisms

quantization =

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

Definition categories, functors, natural transformations

2 Representation Theory

2.1 Monoidal categories

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 $\otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ 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 A monoidal category is a quintuple $(\mathcal{C}, \otimes, 1, a, i)$ where \mathcal{C} is a category, $\otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ is a bifunctor called tensor product.

$$a : - \otimes (- \otimes -) \xrightarrow{\sim} (- \otimes -) \otimes -$$

is a natural isomorphism. 1 is an object of \mathcal{C} subject to the following axioms:

1. Pentagon axiom: the following diagram commutes for all objects W, X, Y, Z in \mathcal{C} .
2. Unit axiom: the left and right unitors are equivalences $\mathcal{C} \rightarrow \mathcal{C}$.

Let us give three important examples of monoidal categories.

Example 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 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 above is the classical introduction to monoidal categories as a category with some extra structure. Monoidal categories can also be seen as degenerate 2-categories. Although this viewpoint requires one additional initial step of abstraction (the definition of a 2-category), we will see that it will give 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, vertically and horizontally. (DIAGRAMS-...) Taking the dual diagrams we obtain the diagrammatic language. Monoidal categories are 2-categories with only one 0-object called 1. We can think of it as the underlying plane or the empty diagram, 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 $1 \rightarrow 1$ which we will denote by 1.

Definition Given a system A , a state of is a morphism $1 \rightarrow A$. A costate (or effect) of A is a morphism $A \rightarrow 1$. We denote them as follows in the diagrammatic language.

Example In the category *Sets* states and costates of a set X are elements $x \in X$. In $Vect_k$ states are vectors and costates are functionals. Note that the diagrammatic notation provides a two-dimensional generalisation of Dirac's notation.

Definition Scalars in a monoidal category are morphisms $1 \rightarrow 1$.

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.

2.2 Hopf symmetry

Using the diagrammatic tools developed in the previous section we will now recover the most basic algebraic structures mathematicians use to talk about symmetry.

2.2.1 Monoids and comonoids

Definition monoids

Definition comonoid

Let us introduce some of the groups we will meet: \mathbb{Z}_2 , S_3 , $U(N)$. characters = costates

2.2.2 The Hopf PROP

Definition Bialgebra

Definition Hopf

2.2.3 Hopf Algebras and Quantum groups

quasitriangular hopf algebras

Definition Quantum double construction

2.2.4 Categories of representations

2.3 Spherical Fusion categories

2.3.1 Spherical categories

Definition monoidal categories, rigidity

Definition A pivotal category is a tensor category together with a left duality $*$ and a monoidal natural isomorphism $\gamma : id \rightarrow -^{**}$

In a pivotal category we can define traces by using the monoidal natural iso. γ .

Definition left and right trace, left and right dimension

Definition A pivotal category is called spherical if left and right traces coincide. categorical dimension.

Theorem 2.1 $Rep(H)$ for H a hopf algebra is spherical.

Proof With comonoid and rigid

2.3.2 Fusion categories

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

Definition 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 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 An object X in a \mathbb{C} -linear category is called simple if $\text{End}X = k\text{id}_X$.

Definition \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 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 2.2 $\text{Rep}(H)$ is a fusion category

Example Any group G is a hopf algebra (comonoid = copy). Therefore $\text{Rep}G$ can also be made monoidal and rigid.

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

$$\begin{aligned} \tau : \quad \sigma &\mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ g &\mapsto \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix} \end{aligned}$$

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

$$\mathbf{1} \otimes X \simeq X \simeq X \otimes \mathbf{1} - \mathbf{1} \otimes -1 \simeq \mathbf{1} - \mathbf{1} \otimes \tau \simeq \tau \simeq \tau \otimes -1 \tau \otimes \tau \simeq \mathbf{1} \oplus -1 \oplus \tau \quad (1)$$

2.3.3 Graph invariants

2.4 Braided Fusion categories

2.4.1 Braiding and twisting

Braid group, Yang-Baxter, Quasitriangular Hopf algebras.

Definition Braided monoidal categories (with braid c)

Definition Ribbon categories (twist θ)

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

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

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

Example 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 $Set \rightarrow Vect$. This gives still big categories, but can be quotiented out by an ideal defined in terms of link-invariants to give interesting cats.

Definition braided fusion category

Definition 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 2.3 *If \mathcal{C} is k -linear, spherical or a $*$ -category (k -linear dagger) then so is $Z_1(\mathcal{C})$*

Theorem 2.4 *If H is a quasitriangular Hopf Algebra then $Rep(H)$ is a braided fusion category.*

N-matrix, R-matrix

2.4.2 Modular categories

Definition 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 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 2.5 *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 2.6 *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 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 2.7 *\mathcal{C} is modular iff the S -matrix is invertible.*

Theorem 2.8 *The modular S -matrix diagonalises the N -matrix.*

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

2.4.3 Knot invariants

3 The Physics of Anyons

3.1 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

3.1.1 Many-body Quantum Systems

Definition 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 $\mathcal{H} : \mathcal{L} \rightarrow \mathcal{L}$, 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 describe by graphs.

Definition A Hamiltonian is k -local if...

Definition An MQS on a graph $T = (V, E)$ 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 3.1 *Let $\mathcal{H} : V \rightarrow V$ 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 $R_1 R_2 \mathcal{H} = R_1 \mathcal{H} R_2 = \mathcal{H} R_1 R_2$. Also $R^{-1} \mathcal{H} = R^{-1} \mathcal{H} R R^{-1} = R^{-1} R \mathcal{H} R^{-1} = \mathcal{H} R^{-1}$. The unit is the identity operator $id_{V^* \otimes V}$.

Proposition 3.2 *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} :

$$\mathcal{H}|\psi\rangle = E|\psi\rangle$$

Note that if $R \in G$ then

$$\mathcal{H}R|\psi\rangle = R\mathcal{H}|\psi\rangle = ER|\psi\rangle$$

So $R|\psi\rangle$ 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 $\text{End}(V_E) \simeq \mathbb{C}$. Indeed suppose $f : V_E \rightarrow V_E$ 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 corresponding 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 $\text{Rep}(G)$. Note there are no restrictions yet on the group of symmetries.

Example Suppose $\mathcal{H} = \sigma_Z$ be the Hamiltonian of a qubit living in \mathbb{C}^2 . It has eigenvalues ± 1 and corresponding eigenvectors $|0\rangle$ and $|1\rangle$. 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

3.1.2 Topological phases of matter

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 world-lines and not on the detailed geometry.

example: particle-antiparticle creation, swap and annihilation

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). The space of paths through configuration space C divides into topologically distinct classes, described by the fundamental

group $\pi_1(C)$.

If we fix the starting and endpoint in the configuration space, we can 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 the group of homotopy classes of paths from starting to endpoint on the configuration space.

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 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 .

- 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 $3 + 1$ 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 taht the universal R -matrix plays an important role in the description of topological dependencies.

3.2 Algebraic theory of Anyons

In this section we describe the algebraic framework of modular categories, as theories of anyons.

Let us first set some labels a, b, c, \dots for our particle types. Let us label by $\mathbf{1}$ the vacuum particle type "no-particle". It has the property that it leaves other particle types unchanged under fusion: $\mathbf{1} \otimes a \simeq a \simeq a \otimes \mathbf{1}$. So for the moment our theory is a monoidal category \mathcal{C} and we can already use the diagrammatic language, the wires carry particle types (image). Now note that fusion $a \otimes b \xrightarrow{\sim} c$ and splitting $c \xrightarrow{\sim} a \otimes b$ are really dual concepts. This duality is witnessed by the existence of antiparticles. Each particle a comes with its antiparticle a^* such that $a \otimes a^* \simeq \mathbf{1} \simeq a^* \otimes a$. So the category must be rigid, we will assume it is a well behaved category i.e it is spherical and $\mathbf{1}^* = \mathbf{1}$. So we can define the quantum numbers for each particle type (image). 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 and the fusion rules look like this:

$$a \otimes b \simeq \oplus_c N_{ab}^c c \quad (2)$$

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

We still have one question to ask to the theory, what happens when a particle is passed around another one? 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. 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.

Example Suppose we start from a set of labels and define the fusions to form a group. In fact $\mathbf{1}$ 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 $\text{Rep}G$, in which the allowed linear processes (intertwiners) preserve the fusion rules. Doing the process and then fusing the system with a particle (action of the group) is the same as doing the fusion and then the process. The category $\text{Rep}(G)$ for G a group is a spherical fusion category. Linearity

and tensor are given by the underlying *Vect* structure, simple objects are the irreducible representations of G , duality is proved by using the group inverse (hopf algebra antipode). 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.

Let us consider the object $V = \mathbb{C}G$ of $\text{Rep}G$. (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.

Theorem 3.3 *$\text{Rep}G$ is a braided fusion category*

3.3 Quantum Symmetry

Recall our discussion from the subsection Algebraic theory of anyons. We distinguished degenerate anyons theories (symmetric fusion categories) to modular tensor categories. In this section we will look at physically implementable examples of those two cases, and discuss a general construction for taking a degenerate anyon theory and making it modular.

Local symmetries are very well described by the theory of groups. In order to describe symmetries of Hamiltonians exhibiting topological phases of matter we need to use the more general notion of Hopf Symmetry.

3.3.1 The Quantum Double

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 measuring 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 Let us consider the case where $G \simeq \mathbb{Z}_2$. We obtain a lattice of spins. Those particles we want to 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:

$$g P_h = P_{ghg^{-1}} g \quad (3)$$

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

Definition Lagrangian, Noether's theorem

Definition 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 $\text{Rep} D(G)$ 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 $\{|k, v_j^\alpha\rangle\}_{j=1, \dots, \dim \alpha}^{k \in C_i}$ and forms an irreducible representation of $D(G)$ under the action

$$P_h g |k, v_j^\alpha\rangle = \delta_{h, gkg^{-1}} |h, \alpha(h^{-1} g k) v_j^\alpha\rangle \quad (4)$$

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

3.3.2 Drinfeld center

Definition The braided (Drinfeld) centre of \mathcal{C} is the category $Z_1(\mathcal{C})$ 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.

Theorem 3.4 $Z(\text{Rep}G) \simeq \text{Rep}DG$

3.3.3 Kitaev's lattice construction

The following argument seems to work for abelian groups. Being a spherical fusion category, $\text{Rep}G$ 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 $\text{Rep}G$ 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 $\text{Rep}G$. 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 exhaust 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 $\text{Rep}(G)$. Indeed the category we obtained is $Z(\text{Rep}(G)) \simeq \text{Rep}(DG)$.

Theorem 3.5 *The lattice construction and the Drinfeld construction coincide*

Example In the case $G = \mathbb{Z}_2$, recall $\text{Rep}\mathbb{Z}_2$ has two simple objects 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.

4 Quantum Computation

4.1 Permutational Quantum Computing

4.1.1 Jordan's model

Here we give a categorical description of Jordan's model for Permutational Quantum computation [REFERENCE].

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

4.1.2 Categorical PQC

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

Theorem 4.1 *Any symmetric fusion category induces representations of the symmetric group S_n for any $n \in \mathbb{N}$.*

Theorem 4.2 *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 4.3 *Jordan's model \mathcal{J}*

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

4.1.3 Spin Network Quantum systems

The model described by Jordan is implementable by defining a hamiltonian on a network of spins.

Generalised spin network systems for arbitrary group G

4.2 Topological Quantum Computation

4.2.1 The Topological Model

Hard to actually get qubits

Take the fusion space to be our topological hilbert space.

Topological qudits are usually encoded as fusion tree basis elements

Topological gates: braids (can express as action of the braid group) + measurements (=fusions and associators).

4.2.2 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.

4.2.3 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?)

5 A braided programming language

5.1 Non-commutative linear logic

5.2 Adjunction

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:

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

$$\square : \text{Rep}G \rightarrow \text{Rep}DG \simeq Z(\text{Rep}G)$$

Theorem 5.1 Let $\{X_i\}_{i \in I}$ be the set of representatives of the isomorphism classes of simple objects in $\text{Rep}G$. Let $\mathbb{C}G$ be the regular representation, then

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

Theorem 5.2 $\square V = \bigoplus_{i \in I} X_i^* \otimes V \otimes X_i$ with action of DG given by

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

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

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

$$P_h g [P_k e] v = \delta_{h, gkg^{-1}} [P_h e] \pi(g) v \quad (5)$$

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 $\mathbb{C}G \simeq \bigoplus_i \mathbb{C}C_i$ and we could try to decompose:

$$\square V \simeq \bigoplus_i \mathbb{C}C_i \otimes V \quad (6)$$

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

\square 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 $\square V$

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

Example 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 $\square\tau_-$, it has basis $\{[P_e e] =: w_e, [P_a e] =: w_a\}$ and

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

And we see from the table (see Lahtinen "The Toric Code and the Quantum Double" for table of reps) that $\square\tau_- \simeq X \oplus Y$. Similarly $\square\tau_+ \simeq 1 \oplus Z$.

Consider the regular representation $V := \mathbb{C}\mathbb{Z}_2 \simeq \tau_+ \oplus \tau_-$, then $\square V \simeq 1 \oplus X \oplus Z \oplus Y \simeq (1 \oplus X) \otimes (1 \oplus Z)$.

What happens if we braid the two components of $\square V$? In $Rep D\mathbb{Z}_2$ 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 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

References

- [1] Kitaev A. Yu. *Anyons in an exactly solved model and beyond*. Annals of Physics 321, pp 2-111, 2006
- [2] Kitaev A. Yu. *Fault-tolerant Quantum Computation by Anyons*. Annals Phys. 30, pp2-30, 2003.
- [3] Majid Sh. *Foundations of Quantum Group Theory*. Cambridge University Press, 1995.
- [4] Gould M. *Quantum double finite group algebras and their representations*. Bulletin of the Australian Mathematical Society, 1993.
- [5] Bakalov B., Kirillov A. *Lectures on tensor categories and modular functors*. American Mathematical Society, University Lectures Series vol 21, 2000.