Topological Quantum Computation

Shawn X. Cui*

August 15, 2018

Abstract

This is the note for the 10-lecture course 'Topological Quantum Computation' (TQC) I taught at Stanford University during Spring 2018. The course is aimed at a basic introduction to TQC, with a focus on the mathematical side of the theory. Topics include toric code, quantum double model of finite groups, non-Abelian anyons, braid groups, modular tensor categories, Jones polynomial, etc. In particular, it contains a careful treatment of ribbon operators in the quantum double model.

Each section below covers the material for one lecture. *Please be aware that the note has not been proofread, so it may contain typos/errors. Use it at your caution.*

Contents

*Email: cuixsh@gmail.com

1 Topological quantum computation: an overview

1.1 Some Basics of Quantum Computation (QC)

Let's start with some basics ingredients in quantum computation. By a *qubit* is meant a 2-dimensional Hilbert space $\mathbb{C}^2$ with a preferred orthonormal basis $\{|0\rangle, |1\rangle\}$. In general, one can also talk about *qudit*, which is the d-dimensional Hilbert space $\mathbb{C}^d$ for some integer $d > 2$. A (1-qubit) quantum state is a non-zero vector $|\psi\rangle \in \mathbb{C}^2$. Usually, we normalize $|\psi\rangle$ so that it has norm $\langle\psi|\psi\rangle = 1$. The space of n-qubits is represented by the n-fold tensor product $(\mathbb{C}^2)^{\otimes n}$, and an n-qubit state is a non-zero vector in $(\mathbb{C}^2)^{\otimes n}$. Quantum gates are operators that transform quantum states. An n-qubit quantum gate is a unitary operator $U \in \mathbf{U}(2^n)$. The following are some 1-qubit gates. They are the Pauli matrices.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad Y = iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

A measurement is probabilistic operation on states. Given a normalized 1-qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$, measuring it (with respect to the standard basis) results in the state $|0\rangle$ with probability $|a|^2$ and the state $|1\rangle$ with probability $|b|^2$. More generally, we can measure states with respect to an observable $\mathcal{O}$, which is a Hermitian operator acting on certain n-qubits, that is, $\mathcal{O} = \mathcal{O}^\dagger$. The eigenvalues of $\mathcal{O}$ are all real and we have the spectral decomposition:

$$\mathcal{O} = \sum_i \lambda_i P_i, \tag{1}$$

where P_i is the projector onto the λ_i-eigenspace. Then if we measure an n-qubit state $|\psi\rangle$ with respect to $\mathcal{O}$, the probability to get the outcome λ_i is $\langle\psi|P_i|\psi\rangle$, and when the outcome

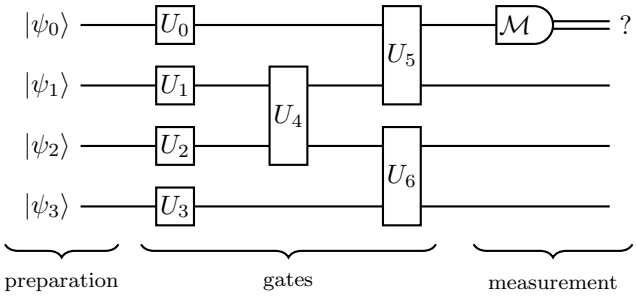
is λ_i, the resulting state becomes $P_i|\psi\rangle$. With this notation, the measurement with respect to the standard basis is equivalent to the measurement with respect to the observable Z.

It is direct to see that the P_i's in Equation 1 satisfy

$$P_i^\dagger = P_i, \quad P_i P_j = \delta_{i,j} P_i, \quad \sum_i P_i = Id. \tag{2}$$

A set of operators $\{P_i\}$ satisfying Equation 2 is called a complete set of projectors. Given an arbitrary complete set of projectors $\{P_i\}$, one can define an observable $\mathcal{O}$ by Equation 1 by choosing some mutually distinct real numbers $\{\lambda_i\}$. Thus an equivalent formulation of measurement is in terms of projectors. That is, given a complete set of projectors $P = \{P_i\}$, a measurement of $|\psi\rangle$ with respect to P will project $|\psi\rangle$ to $P_i|\psi\rangle$ with probability $\langle\psi|P_i|\psi\rangle$.

The process of quantum computation is illustrated as follows:



In the circuit above, the flow proceeds from left to right with time. Each wire represents a qubit, each box represents a quantum gate, and $\mathcal{M}$ means the measurement of the first qubit with respect to the standard basis.

In actual physical systems, the qubits will always interact with the environment which introduces noises (or errors). Another type of errors happens when applying quantum gates. Any gate can only be designed to a certain accuracy. There are two approaches to deal with errors. The 'software ' approach is by using error correcting codes, and the 'hardware ' approach is topological quantum computing (TQC).

1.2 Error Correcting Code

We will not go into much detail on error correcting code, but will only sketch the general idea. For references on this aspect, see for instance Chapter 10 [16]. The key to error correction is distinguishing the notion of *logical* qubits with *physical* qubits. We encode a logical qubit into a subspace of multiple physical qubits. Under certain assumptions, there is a way to detect errors and according to different syndromes we can even correct them. For instance, (a toy example), consider the encoding of logical qubit into three physical qubits:

$$\begin{aligned} \mathbb{C}^2 &\hookrightarrow \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \\ |0\rangle &\mapsto |0\rangle_L := |000\rangle \\ |1\rangle &\mapsto |1\rangle_L := |111\rangle \end{aligned}$$

outcome	measuring Z_1Z_2	measuring Z_2Z_3
no error: $a\|000\rangle + b\|111\rangle$	1	1
error X_1: $a\|100\rangle + b\|011\rangle$	-1	1
error X_2: $a\|010\rangle + b\|101\rangle$	-1	-1
error X_3: $a\|001\rangle + b\|110\rangle$	1	-1

Table 1: Outcomes of measurements

Thus a general logical state is $|\psi\rangle_L = a|0\rangle_L + b|1\rangle_L$. Assume each time the error will only happen to one of the three physical qubits (we do not know which ,a priori) and the only type of error is a bit flip, namely, the operator X, then we can detect and correct an error as follows. Let Z_i be the Pauli Z acting on the i-th qubit. It is clear that Z_1Z_2 has eigenvalue 1 on the subspace span$\{|00\rangle, |11\rangle\}$ and eigenvalue -1 on span$\{|01\rangle, |10\rangle\}$. Hence a measurement of Z_1Z_2 serves to check if the two qubits are aligned with the same direction. To detect if there is any error, we make two measurements, one with respect to Z_1Z_2 and the other with respect to Z_2Z_3. The outcomes of the measurements for each possible error are listed in Table 1. From the table, we see that the outcomes of measurements are different for each possible error (and the case with no error). Hence, based on the measurement outcome, we know to which qubit, if any, the error happens, and we can simply correct it by applying the X operator to that qubit.

Of course, this is only a toy model. More complicated encoding is required in order to correct other types of errors and also errors involving more than one qubit. For instance, the following nine-qubit code corrects arbitrary single qubit errors. See Chapter 10.2 [16].

$$\begin{aligned} \mathbb{C}^2 &\hookrightarrow (\mathbb{C}^2)^{\otimes 9} \\ |0\rangle &\mapsto |0\rangle_L := (|000\rangle + |1\rangle)^{\otimes 3} \\ |1\rangle &\mapsto |1\rangle_L := (|000\rangle - |1\rangle)^{\otimes 3} \end{aligned}$$

1.3 Topological Quantum Computing (TQC)

TQC is an approach to realizing quantum computing with non-Abelian anyons/quasi-particles in certain two dimensional quantum systems. The information is encoded in non-local degrees of the system making it fault-tolerant to local errors. The process of information is achieved by braiding of anyons, which effects a unitary transformation acting as quantum gates. Measurement of states is performed through fusing anyons. In terms of computational power, TQC is equivalent to the standard circuit model, but the former has the advantage of being automatically fault-tolerant to local errors.

The quantum medium to carry out TQC is a two dimensional topological phase of matter (TPM), the content of the 2016 Nobel Prize in physics. Roughly, a TPM is a quantum system with certain robust properties that depends on the topology of the underlying material. TPMs can be found in certain fractional quantum Hall states. As a concrete example, think of a plane of electrons subject to a strong magnetic field in the vertical direction where the temperature is lowered to close to absolute zero degree. See Figure 1. An important feature

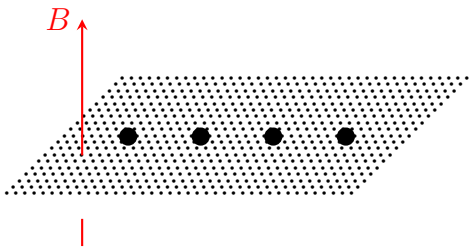


Figure 1: A collection of electrons subject to the plane. The anyons are point-like excitations.

of a TPM is that it harbors anyons/quasi-particles.

- They are low energy, point-like excitations.
- They can be locally moved, but can not be localled destroyed or created.
- Each anyon has a topological charge or type.
- The statistics for exchanging two anyons are more general than bosons/fermions.

Consider n anyons separated in space and each of them has type a. Denote the space of states with such a configuration by $V_{aa\cdots a}$. There is an energy gap $\Delta E > 0$ between such a configuration and other spectral. Hence the system will evolve within itself as long as the local perturbations are small enough. If $\dim V_{aa\cdots a} = 1$, we call the anyon type a Abelian. Otherwise, it is called non-Abelian. For a non-Abelian type a, we can encode information in $V_{aa\cdots a}$, which is not accessible by local errors.

When two anyons are swapped, the system undergoes a unitary transformation. See Figure 2. The world lines of the swap produce a braid diagram. We call such a process braiding of anyons. The unitary transformation only depends on the isotopy classes of the braid diagram, which means the only way the system evolves is by braiding anyons. These unitary transformations act as quantum gates and they form a representation of the n-strand braid group, which is defined by the presentation:

$$B_n = \langle \sigma_1, \cdots, \sigma_{n-1} \,|\, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \\ \sigma_i\sigma_j = \sigma_j\sigma_i, |i-j| > 1 \,\rangle.$$

If we bring two anyons close to each other and fuse them, some other anyon will emerge, and there are different possible outcomes. Abstractly, we denote the fusion by:

$$a \times b = c, d, \cdots$$

This corresponds to a projection to different superselection sectors, and can be used to perform measurement.

The general process of TQC is illustrated in Figure 3. We start by creating some anyons from the vaccum to initialize the state. Then we braid anyons to transform the state. Finally we fuse the anyons back to vaccum.

The study of TQC is closely related to a number of subjects, such as topological phase of matter, topological quantum field theories, modular tensor categories, knot invariants, etc. We will touch some of the relations later in the course.

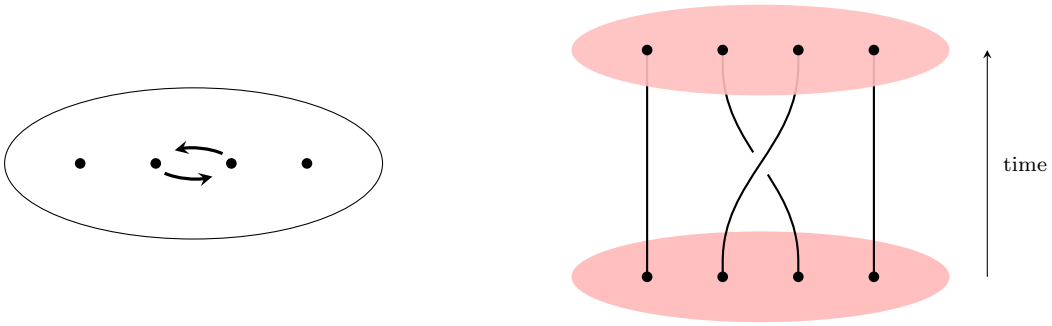


Figure 2: Braiding of two anyons

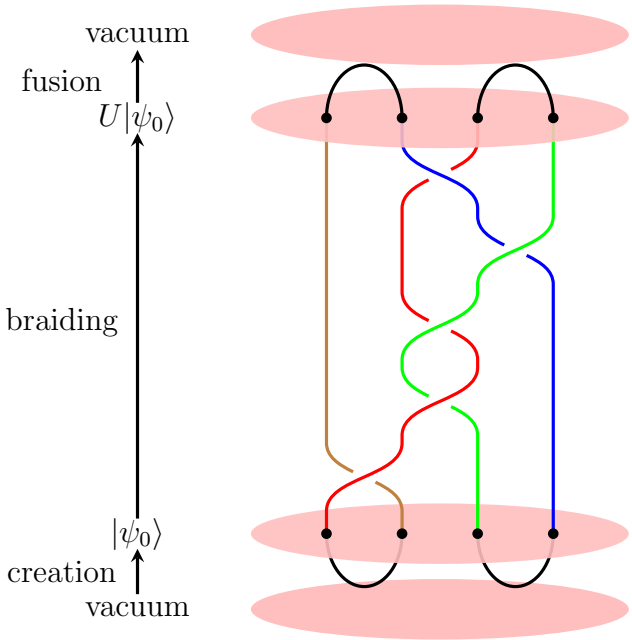


Figure 3: The process of TQC.

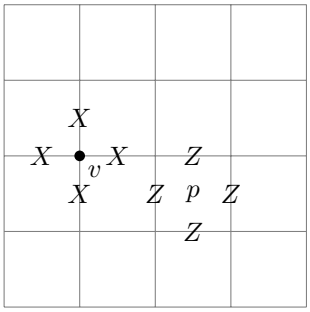


Figure 4: A $L \times L$ square lattice on the torus

2 Toric Code

Toric code [14] is an exactly solvable lattice model defined on a closed surface, i.e., a surface without boundary. It has a gapped Hamiltonian whose low energy excitations are anyons. Although all of the anyon types in toric code are Abelian and hence are not useful for TQC, the toric code is a beautiful theory that illustrates many concepts of topological phases. Thus it is worth studying the model to some details. Later, we will generalize it to Kitaev's quantum double model for any finite groups, where non-Abelian anyons can emerge.

Recall that the Pauli matrices are defined as follows.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad Y = iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Let $\mathcal{L}$ be a square lattice of size $L \times L$ with periodic boundaries both in the horizontal direction and in the vertical direction. See Figure 4. Namely, we identify the two horizontal boundaries as well the two vertical ones. In another word, $\mathcal{L}$ is a lattice on the torus.

Remark 2.1. The Hamiltonian model to be introduced below can be defined on lattices of any shape on any closed surface. Here we simply choose the square lattice on the torus as an illustrative example.

Denote by

$$\begin{aligned} V &= \{\text{vertices}\}, \\ E &= \{\text{edges}\}, \\ F &= \{\text{faces or plaquettes}\}. \end{aligned}$$

To each edge $e \in E$ associate a qubit $\mathcal{H}_e = \mathbb{C}^2$. The total Hilbert space $\mathcal{H}_{\text{tot}}$ is defined as

$$\mathcal{H}_{\text{tot}} := \bigotimes_{e \in E} \mathcal{H}_e.$$

To define the Hamiltonian, we first introduce some local operators. To each $v \in V$ and $p \in F$, define

$$A_v := \left(\bigotimes_{e \in \text{star}(v)} X_e \right) \bigotimes \left(\bigotimes_{e \in E - \text{star}(v)} Id_e \right), \quad B_p := \left(\bigotimes_{e \in \partial p} Z_e \right) \bigotimes \left(\bigotimes_{e \in E - \partial p} Id_e \right),$$

where star(v) is the set of edges adjacent to v, ∂p is the set of edges on the boundary of p, and X_e (resp. Z_e) is the operator X (resp. Z) acting on the qubit $\mathcal{H}_e$. Graphically, A_v and B_p are shown in Figure 4.

The following properties are easy to check. For any $v, v' \in V$ and $p, p' \in F$, we have

$$A_v^2 = Id, \quad B_p^2 = Id \tag{3}$$

$$A_v A_{v'} = A_{v'} A_v, \quad B_p B_{p'} = B_{p'} B_p, \quad A_v B_p = B_p A_v. \tag{4}$$

This means that all the A_v's and B_p's mutually commute with other, and hence they can be diagonalized simultaneously. Moreover, each A_v and each B_p has eigenvalue either 0 or 1.

The Hamiltonian is defined as

$$H := \sum_{v \in V} (1 - A_v) + \sum_{p \in F} (1 - B_p). \tag{5}$$

Since all the terms in the Hamiltonian are Hermitian operators that commute with each other, the Hamiltonian can be solved exactly. Moreover, as it will be shown below, the Hamiltonian is frustration free, namely, the ground states are achieved as the common eigenstates of all A_v's and B_p's with eigenvalue one. Denote the ground states manifold by V_{gs}, then

$$V_{gs} = \{|\psi\rangle \in \mathcal{H}_{\text{tot}} : A_v|\psi\rangle = |\psi\rangle, B_v|\psi\rangle = |\psi\rangle, \text{ for all } v \in V, p \in F\}. \tag{6}$$

2.1 Ground States

Now we compute the degeneracy of the ground states.

Let $\mathcal{L}^*$ be the dual lattice of $\mathcal{L}$ as shown in Figure 5, where solid lines represent the lattice $\mathcal{L}$ and dashed lines $\mathcal{L}^*$. Then a vertex v, edge e, and plaquette p in $\mathcal{L}$ correspond to the plaquette v^*, edge e^*, and vertex p^*, respectively, in $\mathcal{L}^*$. A basis element of $\mathcal{H}_{\text{tot}}$ is an assignment $\{x_e : e \in E\}$ of 0 or 1 to each edge. Given a basis element, we construct a graph G in $\mathcal{L}^*$ as follows. Initially, G has the same set of vertices as those of $\mathcal{L}^*$ with no edges. For each edge $e \in E$, if $x_e = 1$, then we add the dual edge e^* to G. See Figure 6. By this procedure, we have a one-to-one correspondence between basis elements of $\mathcal{H}_{\text{tot}}$ and graphs in $\mathcal{L}^*$. Denote by $|G\rangle$ the basis element corresponding to the graph G.

Note that $|G\rangle$ is an eigenstate of B_p for each p, and it has eigenvalue 1 if and only if the vertex of G inside p has even degree. Thus, an equivalent condition for $|G\rangle$ to be an eigenstate with eigenvalue 1 for all B_p's is that G has even degree at all vertices. That is, G is a collection of loops in $\mathcal{L}^*$, or in another word, a *multi-loop*. See Figure 7 for a local configuration of such G. The ground states manifold V_{gs} is a subspace of the space spanned by basis elements corresponding to multi-loops.

Now we look at the action of A_v on a multi-loop element $|G\rangle$. At each edge adjacent to v, A_v flips $|0\rangle$ and $|1\rangle$. Denote by v^* the plaquette in $\mathcal{L}^*$ dual to v. Then $A_v|G\rangle$ corresponds to the graph G' which is obtained from G by replacing the edges of G that belong to ∂v^* with their complement in ∂v^*. See Figure 8. Hence G' is obtained by deforming G through the dual plaquette v^*, and we say G' and G are homologous. In general, for arbitrary two

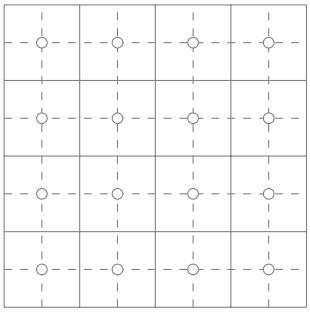


Figure 5: The lattice $\mathcal{L}$ (solid gray lines) and the dual lattice $\mathcal{L}^*$ (dashed gray lines).

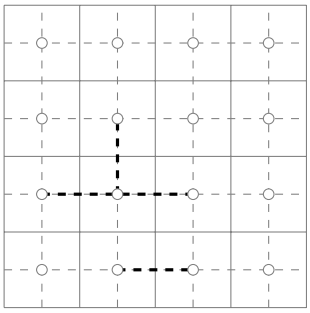


Figure 6: An example of a graph G in the dual lattice. The basis element $|G\rangle$ has component $|1\rangle$ on edges whose dual belongs to G and has component $|0\rangle$ otherwise.

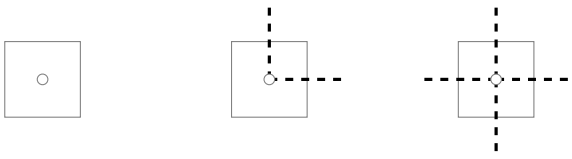


Figure 7: A local picture of a multi-loop around each dual vertex.

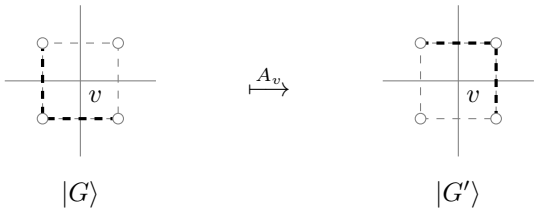


Figure 8: The action of A_v on a multi-loop.

multi-loops G_1 and G_2, they are called homologous to each other if one is obtained from the other by a sequence of deformations through dual plaquettes. This defines an equivalence relation on the set of multi-loops. For each equivalence class $[G]$, define the state

$$|[G]\rangle := \sum_{G' \in [G]} |G'\rangle.$$

It is direct to check that

$$A_v|[G]\rangle = |[G]\rangle, \quad \text{for any } v \in V,$$

since A_v simply permutes the terms in the summation of $|[G]\rangle$.

Hence $|[G]\rangle$ is a ground state. Apparently, the states $|[G]\rangle$ corresponding to different equivalence classes of multi-loops are linearly independent. It is not hard to see that they actually span all of V_{gs}. In summary, a basis of V_{gs} is given by $\{|[G]\rangle : [G] \text{ equivalence class of multi-loops}\}$, and the dimension of V_{gs} is the number of equivalence classes.

In the language of homology, multi-loops are 1-cycles (with $\mathbb{Z}_2$ coefficients). Two multi-loops are homologous or equivalent if they belong to the same homology class. Equivalence classes of multi-loops are homology classes 1-cycles, and thus the dimension of V_{gs} is equal to $|H_1(\text{torus}; \mathbb{Z}_2)|$, the number of elements in the first homology of the torus with $\mathbb{Z}_2$ coefficients. One can also use the notion of cohomology, but the two notions are equivalent by Poincare duality.

On the torus, there are four equivalence classes of multi-loops. They are represented by $\{[\emptyset], [m], [l], [d]\}$, where (See Figure 9) $\emptyset$ is the empty set or any contractible loop, m is the horizontal loop, l is the vertical loop, and d is the diagonal loop. Note that d is in the same equivalence class as the multi-loop which is the union of m and l. Also note that all the loops are on the dual lattice. Thus on the torus, the ground state degeneracy is four. On the sphere, the ground state degeneracy is 1 since all multi-loops are contractible.

2.2 Excitations

We have seen that a ground state $|\psi\rangle$ is defined by the following constraints:

$$A_v|\psi\rangle = |\psi\rangle, \quad v \in V, \tag{7}$$
$$B_p|\psi\rangle = |\psi\rangle, \quad p \in F. \tag{8}$$

An elementary excitation or a 1-particle excitation is a state $|\psi\rangle$ for which at most one constraint in Equation 7 is violated. More generally, an n-excitation corresponds to $|\psi\rangle$ for which at most n constraints are violated.

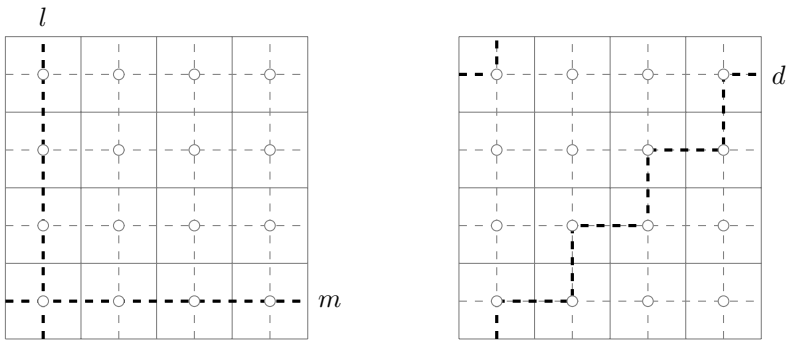


Figure 9: A representative for each equivalence class of multi-loops.

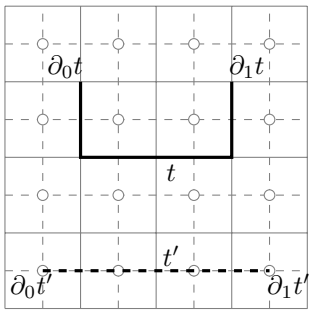


Figure 10: Connected paths (strings) in the lattice and dual lattice.

The A_v's and B_v's are not independent operators, since they satisfy

$$\prod_{v \in V} A_v = Id, \quad \prod_{p \in F} B_p = Id. \tag{9}$$

Therefore, it is impossible to have exactly one A_v or one B_p violated, which means single-particle excitations do not exist, or rather, the only single-particle excitation is the vacuum. Now we consider two-particle excitations.

Let t be connected path in the lattice $\mathcal{L}$ and denote the two end points of t by $\partial_0 t$ and $\partial_1 t$. Define

$$S^Z(t) := \prod_{e \in t \cap E} Z_e. \tag{10}$$

See Figure 10. Clearly $S^Z(t)$ commutes with all B_p's and all A_v's except the two vertex operators at the end points of t where they anti-commute:

$$S^Z(t) A_{\partial_i t} = -A_{\partial_i t} S^Z(t), i = 0, 1.$$

Let $|\mathcal{E}\rangle$ be a ground state and let $|\psi^Z(t)\rangle = S^Z(t)|\mathcal{E}\rangle$. Then $|\psi^Z(t)\rangle$ violates exactly two constraints, one at $\partial_0 t$ and one at $\partial_1 t$, since

$$A_{\partial_i t}|\psi^Z(t)\rangle = A_{\partial_i t} S^Z(t)|\mathcal{E}\rangle = -S^Z(t) A_{\partial_i t}|\mathcal{E}\rangle = -|\psi^Z(t)\rangle.$$

Hence we have a pair of particles located at the vertices $\partial_0 t$ and $\partial_1 t$. We call them quasi-particles of Z-type or "electric" charges. These quasi-particles have energy 4. The operator

$S^Z(t)$ is called a string operator of Z-type. While the operator itself depends on the string t, the state $|\psi^Z(t)\rangle$ is unchanged as we deform t keeping the end points fixed. Hence, only the isotopy class of strings matter to the state $|\psi^Z(t)\rangle$.

Similarly, we can consider a path t' in the dual lattice $\mathcal{L}^*$. The two end points, $\partial_0 t'$ and $\partial_1 t'$ correspond to two plaquettes in the original lattice. See Figure 10. Define the string operator of X-type by

$$S^X(t') = \prod_{e \in E \cap (t')^*} X_e. \tag{11}$$

Then $S^X(t)$ commutes with all A_v's and all B_p's except at the two plaquettes $(\partial_0 t')^*$ and $(\partial_1 t')^*$, where they anti-commute. Let $|\psi^X(t')\rangle = S^X(t')|\mathcal{E}\rangle$. Then $|\psi^X(t')\rangle$ represents a pair of quasi-particles at the plaquettes $(\partial_0 t')^*$ and $(\partial_1 t')^*$. They are called quasi-particles of X-type or "magnetic" charges, and they have energy 4. Again the $|\psi^X(t')\rangle$ only depends on the isotopy class of the path t'.

Thus, there are two types of quasi-particles. The electric charges live on vertices while magnetic charges live on plaquette. There is another type of quasi-particle which is the composite of an electric charge and a magnetic charge. Note that this composite has energy 8, and it occupies a plaquette and a vertex on it. If we think of the vacuum as a particular type of quasi-particle, we have in total four types of quasi-particles. (Note that the degeneracy of the ground states on the torus is also four; this is not a coincidence.)

We could have arbitrarily even number of quasi-particles of each type. To obtain this configuration, we simply connect each pair of quasi-particles of the same type by a string. The space of each configuration has dimension exactly 4. However, the degeneracy arises purely due to the degeneracy of the ground states on the torus. If the lattice is on a sphere, then there will no degeneracy. Hence, all the quasi-particles are Abelian. The only topological degree of freedom is the charge configuration and the only local degrees are phase factors.

Nonetheless, let's take a look at their braiding statistics. Consider a pair of electric charges and a pair of magnetic charges $|\psi\rangle = S^Z(t_1)S^X(t_2)|\mathcal{E}\rangle$ (See Figure 11). If we move an electric charge around a magnetic charge, then resulting state would be $|\psi'\rangle = S^Z(t_1 \cup t)S^X(t_2)|\mathcal{E}\rangle$. Thus,

$$|\psi'\rangle = S^Z(t_1)S^Z(t)S^X(t_2)|\mathcal{E}\rangle = -S^Z(t_1)S^X(t_2)S^Z(t)|\mathcal{E}\rangle = -|\psi\rangle,$$

where we have used the fact that $S^Z(t)$ acts on the ground state by identity for any contractible loop t. So by dragging an electric charge around a magnetic charge, the state changes by a global phase (actually a only minus sign). This is the nature of Abelian quasi-particles. In the case of non-Abelian quasi-particles, as we will see later, the braiding process can produce nontrivial transformations in some higher dimensional space.

Finally, to fuse two particles of the same type, we simply draw another string connecting them to form a closed loop. The result would always be the vacuum. This implies any quasi-particle is its own antiparticle.

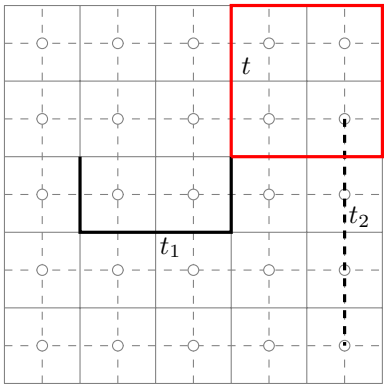


Figure 11: Dragging an electric charge around a magnetic charge.

3 Quantum Double of Finite Groups

3.1 Representations of Finite Groups

We start with some basics on representation theory of finite groups. Let G be finite group whose identity element is denoted by e. A unitary representation of G is a pair (V, χ), where V is a finite dimensional Hilbert space, and χ is a group morphism

$$\chi : G \longrightarrow \mathbf{U}(V),$$

where $\mathbf{U}(V)$ is the group of unitary transformations on V. For $g \in G, v \in V$, when no confusion arises, we usually write $\chi(g)(v)$ simply as $g.v$ and call it the action of g on v. We also say the group G acts on the space V by the representation χ. Sometimes, we also call χ itself the representation, and denote the corresponding Hilbert space by V_χ. Finitely, denote by $|\chi| := \dim V$. Let $\{|j\rangle : j = 1, \cdots, |\chi|\}$ be an orthonormal basis of V, and denote the matrix elements of g by $\Gamma^\chi_{ij}(g)$, namely,

$$g.|j\rangle = \sum_{i=1}^{|\chi|} \Gamma^\chi_{ij}(g)|i\rangle.$$

In the following, when talking about representations, we always assume a basis for the Hilbert space has been chosen and hence each group element corresponds to a unitary matrix.

We call a representation (V, χ) irreducible (or an irrep, for short), if V does not contain a proper subspace except 0 which is invariant under the action of G. Every group has a trivial irrep which is one dimensional and all elements of the group act by the identity operator. Denote this trivial irrep by $\mathbf{1}$. Let's look at some examples.

Let $\mathbb{Z}_d = \{0, 1, \cdots, d-1\}$ be the cyclic group of d elements. It has a generator $a := [1]$ with order d, namely, $a^d = e$. Let S_3 be the group of permutations on three elements. It has two generators $\mu = (123)$ and $\sigma = (23)$ with the relations $\mu^3 = \sigma^2 = (\mu\sigma)^2 = e$. When defining a representation, it suffices to specify the matrices of generators of a group and verify the relations of the generators are preserved.

$\mathbb{Z}_d$ has d inequivalent irreps, all of which are dimensional. (More generally, all irreps of a finite Abelian group are one dimensional.) For each $i = 0, 1, \cdots, d-1$, there is an irrep, denoted by $[\omega_d^i]$, mapping the generator a to the 1×1 matrix (ω_d^i), where $\omega_d := e^{\frac{2\pi\sqrt{-1}}{d}}$.

	dimension	matrix of μ	matrix of σ
$[+]$	1	(1)	(1)
$[-]$	1	(1)	(-1)
$[2]$	2	$\begin{pmatrix} \omega_3 & 0 \\ 0 & \bar{\omega}_3 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Table 2: Irreps of S_3.

S_3 has three irreps, which we denote by $\{[+], [-], [2]\}$, the matrices of the generators μ and σ for each irrep are listed in Table 2. From the table, we see that $[+]$ is the trivial irrep $\mathbf{1}$ and $[-]$ is called the 'sign' irrep as it maps a permutation to its signature.

It is fact that every finite group G has only finitely many inequivalent irreps. Denote by $\mathrm{Irr}(G)$ the set of all inequivalent irreps. For each irrep $\chi \in \mathrm{Irr}(G)$, assume an orthonormal basis for V_χ has been chosen and the matrix elements of $g \in G$ are given by $\Gamma^\chi_{ij}(g)$. The following relation is well known and important in representation theory.

Shur Orthogonality Relation: for any two irreps $\chi, \chi' \in \mathrm{Irr}(G)$, and $i, j = 1, \cdots, |\chi|$, $i', j' = 1, \cdots, |\chi'|$, we have

$$\sum_{g \in G} \Gamma^\chi_{ij}(g) \overline{\Gamma^{\chi'}_{i'j'}(g)} = \frac{|G|}{|\chi|} \delta_{\chi,\chi'} \delta_{i,i'} \delta_{j,j'}. \tag{12}$$

The orthogonality relation has many implications. For instance, take χ' to be the trivial irrep $\mathbf{1}$ and $i' = j' = 1$, then $\Gamma^{\chi'}_{i'j'}(g) = 1$ for all g, and hence we have

$$\sum_{g \in G} \Gamma^\chi_{ij}(g) = |G| \delta_{\chi,\mathbf{1}} \delta_{i,1} \delta_{j,1}. \tag{13}$$

3.2 Quantum Double

The quantum double of a finite group G is an algebra DG with two set of generators $\{A_g : g \in G\}$ and $\{B_h : h \in G\}$. The multiplication of the generators is given as follows:

$$\begin{aligned} A_{g_1} A_{g_2} &= A_{g_1 g_2} \\ B_{h_1} B_{h_2} &= \delta_{h_1,h_2} B_{h_2} \\ A_g B_h &= B_{ghg^{-1}} A_g, \end{aligned} \tag{14}$$

where, and throughout the context, $\bar{g}$ means g^{-1}. The identity element with respect to multiplication is given by both $\sum_{h \in G} B_h$ and A_e. From the multiplication rules, we see that the A-type generators (i.e., the A_g) span a subalgebra isomorphic to the group algebra $\mathbb{C}[G]$ and the B-type generators (i.e., the B_h) span a subalgebra isomorphic to the dual of $\mathbb{C}[G]$, that is, the algebra of functions on G. The quantum double has a basis given by

$$\{D_{(h,g)} := B_h A_g : h, g \in G\}. \tag{15}$$

DG has more structures than being an algebra. In fact, it is a quasi-triangular Hopf algebra with the maps (Δ, ϵ, S, R) defined as follows.

- Δ is the co-multiplication $\Delta : DG \longrightarrow DG \otimes DG$,

$$\Delta(A_g) = A_g \otimes A_g, \quad \Delta(B_h) = \sum_{h=h_1h_2} B_{h_2} \otimes B_{h_1}. \tag{16}$$

Δ is an algebra morphism, hence the image of any element under Δ is known. For instance,

$$\begin{aligned}\Delta(D_{(h,g)}) = \Delta(B_h)\Delta(A_g) &= \sum_{h=h_1h_2} (B_{h_2} \otimes B_{h_1})(A_g \otimes A_g) \\ = \sum_{h=h_1h_2} B_{h_2}A_g \otimes B_{h_1}A_g &= \sum_{h=h_1h_2} D_{(h2,g)} \otimes D_{(h_1,g)}.\end{aligned}$$

- ϵ is the counit $\epsilon : DG \longrightarrow \mathbb{C}$ which is also an algebra morphism. On generators, it is defined by:

$$\epsilon(A_g) = 1, \quad , \epsilon(B_h) = \delta_{h,e}. \tag{17}$$

- S is the antipode $S : DG \longrightarrow DG$,

$$S(A_g) = A_{\bar{g}}, \quad S(B_h) = B_{\bar{h}}. \tag{18}$$

But note that S is an anti-algebra morphism, that is $S(ab) = S(b)S(a)$. Hence $S(D_{(h,g)}) = S(A_g)S(B_h) = D_{(\bar{g}\bar{h}g,\bar{g})}$. Clearly, $S^2 = Id$.

- R is the universal R-matrix $R \in DG \otimes DG$ which is given by

$$R = \sum_g A_g \otimes B_g = \sum_{h,g} D_{(h,g)} \otimes D_{(g,e)}. \tag{19}$$

As an element of $DG \otimes DG$, R is invertible, and its inverse is given by

$$R^{-1} = \sum_g A_{\bar{g}} \otimes B_g. \tag{20}$$

3.3 Representations of DG

Irreducible representations of DG are closely related with those of G. We give a complete characterization of irreps of DG. Let G acts on itself by conjugation, namely, for $g, x \in G$, the action of g sends x to $gx\bar{g}$. An orbit under this action is called a conjugacy class. Clearly, G is partitioned into several conjugacy classes:

$$G = \sqcup_i C_i,$$

where C_i is a conjugacy class. For any element $r \in G$, the conjugacy class containing r is given by $C(r) = \{gr\bar{g} : g \in G\}$. The stabilizer (or centralizer) $Z(r)$ of r is the subgroup which fixes r by conjugation, that is, $Z(r) = \{g \in G : gr = rg\}$. For each $c \in C(r)$, arbitrarily choose $q_c \in G$ such that $q_c r \bar{q}_c = c$. The choice of q_c is not unique, and any other q_c' satisfying the required condition is equal to $q_c z$ for some $z \in Z(r)$. In particular, we always assume $q_r = e$. It is direct to check that $\{q_c : c \in C(r)\}$ is a coset representative for $Z(r)$, namely,

$$G = \sqcup_{c \in C} q_c Z(r).$$

Lemma 3.1. For any $g \in G, c \in C$, we have $\bar{q}_{gc\bar{g}} g q_c \in Z(r)$.

Proof.

$$(\bar{q}_{gc\bar{g}} g q_c) r (\bar{q}_{gc\bar{g}} g q_c)^{-1} = \bar{q}_{gc\bar{g}} g q_c r \bar{q}_c \bar{g} q_{gc\bar{g}} = \bar{q}_{gc\bar{g}} (gc\bar{g}) q_{gc\bar{g}} = r.$$

□

An irrep of DG is characterized by a pair (C, χ), where C is a conjugacy class of G, and (assuming an element $r \in C$ has been arbitrarily chosen and fixed,) χ is an irrep of $Z(r)$. The Hilbert space corresponding to (C, χ) is given by $V_{(C,\chi)} = \mathbb{C}[C] \otimes V_\chi$. Thus a basis is given by

$$\{|c\rangle \otimes |j\rangle : c \in C, j = 1, \cdots, |\chi|\}.$$

The action of DG on $V_{(C,\chi)}$ is given by

$$\begin{aligned} B_h |c\rangle \otimes |j\rangle &= \delta_{h,c} |c\rangle \otimes |j\rangle \\ A_g |c\rangle \otimes |j\rangle &= |gc\bar{g}\rangle \otimes \chi\left(\bar{q}_{gc\bar{g}} g q_c\right) |j\rangle \\ &= \sum_i \Gamma^\chi_{ij} \left(\bar{q}_{gc\bar{g}} g q_c\right) |gc\bar{g}\rangle \otimes |i\rangle. \end{aligned} \tag{21}$$

It is straight forward to check the above equations indeed defines a representation of DG and it is in fact irreducible. In defining the actions, we need to arbitrarily choose the $q_c{}'$s, but the resulting representations for different choices of $q_c{}'$s turn out to be isomorphic. Also, the second part in the pair (C, χ) depends on the choice of an element $r \in C$. For different $r\,'s$, the corresponding centralizer $Z(r)\,'$s are isomorphic, we will not obtain any new representations of DG.

The action of A_g in Equation 21 is simplified in certain cases. If $\chi = \mathbf{1}$ is the trivial irrep of $Z(r)$, then $V_{(C,\chi)} \simeq \mathbb{C}[C]$, and

$$A_g |c\rangle = |gc\bar{g}\rangle. \tag{22}$$

If, on the other hand, C is the trivial conjugacy class $\{e\}$, then $Z(r) = Z(e) = G$. Hence χ is an irrep of G, and $V_{(C,\chi)} \simeq V_\chi$, and

$$A_g |j\rangle = \chi(g) |j\rangle. \tag{23}$$

If both C and χ are trivial, then the representation is one dimensional, and the scalar corresponding to the generators of DG are given by

$$A_g \mapsto 1, \quad B_h \mapsto \delta_{h,e}. \tag{24}$$

Note that this is exactly the counit map ϵ in Equation 17.

The conjugacy classes and centralizer of certain elements of S_3 are given in Table 3. With the chosen elements r and $q_c{}'s$ for each conjugacy class as shown in Table 3, we derive all irreps of $D(S_3)$. See Table 4, where a basis for each irrep and the action of A_μ and A_σ are

	$\{c : c \in C_i\}$	$r \in C_i$	$\{q_c : c \in C_i\}$	$Z(r)$
C_1	$\{e = (1)\}$	e	$\{e\}$	S_3
C_2	$\{(12), \sigma = (23), (13)\}$	σ	$\{(13), e, (12)\}$	$\{e, \sigma\} \simeq \mathbb{Z}_2$
C_3	$\{\mu = (123), (132)\}$	μ	$\{e, \sigma\}$	$\{e, \mu, \mu^2\} \simeq \mathbb{Z}_3$

Table 3: Conjugacy classes C_1, C_2, C_3 of S_3. Here for each C_i, we arbitrarily choose $r \in C_i$ and arbitrarily choose $q_c{}'s$ for $c \in C_i$. Note that the order of the elements in $\{q_c : c \in C_i\}$ is the same as that in $\{c : c \in C_i\}$. For instance, $q_{(12)} = (13)$.

(C, χ)		basis	dimension	matrix of A_μ	matrix of A_σ
C_1	$[+]$	$\lvert+\rangle$	1	(1)	(1)
	$[-]$	$\lvert-\rangle$	1	(1)	(-1)
	$[2]$	$\lvert 2_+\rangle, \lvert 2_-\rangle$	2	$\begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
C_2	$[1]$	$\lvert(12)\rangle, \lvert(23)\rangle, \lvert(13)\rangle$	3	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$
	$[-1]$	$\lvert(12), -\rangle, \lvert(23), -\rangle, \lvert(13), -\rangle$	3	$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$
C_3	$[1]$	$\lvert(123)\rangle, \lvert(132)\rangle$	2	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	$[\omega]$	$\lvert(123), \omega\rangle, \lvert(132), \omega\rangle$	2	$\begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	$[\bar{\omega}]$	$\lvert(123), \bar{\omega}\rangle, \lvert(132), \bar{\omega}\rangle$	2	$\begin{pmatrix} \bar{\omega} & 0 \\ 0 & \omega \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Table 4: Irreps of DS_3 where $\omega = \omega_3$.

given. Since μ and σ generate S_3, we can deduce the action of all A_g's. The action of B_h is simple in all cases, which we ignore in the table.

If V is a representation of DG, V^* is also a representation. Given a co-vector $\phi \in V^*$, the action is given by

$$(D_{(h,g)}.\phi)(v) := \phi\left(S(D_{(h,g)})v\right), \quad v \in V.$$

If we choose any basis $\{|j\rangle : j = 1, \cdot, \dim V\}$ for V and let the dual basis be $\{\langle j| : j = 1, \cdots, \dim V\}$, then

$$D_{(h,g)}\langle j| = \sum_{i=1}^{\dim V} \langle j|S(D_{(h,g)})|i\rangle\langle i|.$$

Given two representations V, W of DG, $V \otimes W$ is a representation whose action is given by the co-multiplication Δ, namely, for $v \in V, w \in W$,

$$D_{(h,g)}.(v \otimes w) := \Delta(D_{(h,g)})v \otimes w.$$

Explicitly,

$$A_g.(v \otimes w) = A_g v \otimes A_g w, \quad B_h.(v \otimes w) = \sum_{h=h_1h_2} h_2 v \otimes h_1 w.$$

$W \otimes V$ becomes a representation in the same way. It is easy to check the naive swap map $\mathrm{Flip}_{V,W}$ between $V \otimes W$ and $W \otimes V$ is not covariant under the action of DG if G is non-Abelian. (Check the action of B_h before and after the swap.) It turns out the correct "covariant swap" is the composition of the naive one with the action of the universal R-matrix. Recall that $R \in DG \otimes DG$ is an invertible element. We let the first factor of R act on V and the second factor act on W, then R can be viewed as a map from $V \otimes W$ to $V \otimes W$. Define

$$c_{V,W} := \mathrm{Flip}_{V,W} \circ R : V \otimes W \xrightarrow{R} V \otimes W \xrightarrow{\mathrm{Flip}_{V,W}} W \otimes V. \tag{25}$$

It is direct to check $c_{V,W}$ commutes with the action of DG. The explicit formula for $c_{V,W}$ is given by

$$c_{V,W}(v \times w) = \sum_g B_g w \otimes A_g v. \tag{26}$$

Then

$$c_{W,V}c_{V,W}(v \times w) = \sum_{g,h} B_h A_g v \otimes A_h B_g w.$$

Thus in general $c_{W,V}c_{V,W} \neq Id_{V\otimes W}$. The inverse of $c_{V,W}$ is given by

$$c_{V,W}^{-1} = R^{-1} \circ \mathrm{Flip} : W \otimes V \xrightarrow{\mathrm{Flip}_{W,V}} V \otimes W \xrightarrow{R^{-1}} V \otimes W. \tag{27}$$

4 Kitaev's Quantum Double Model

Now we study Kitaev's quantum double model based on a finite group G [14]. When the group is taken to be $\mathbb{Z}_2$, the model reduces to the well-known toric code. For non-Abelian groups, the model produces quasi-particles which are non-Abelian. Generalization of the model from finite groups to C^* Hopf algebras was pointed out in [14], and was explicitly studied in [6]. The model was later further generalized to C^* weak Hopf algebras (quantum groupoids) in [7]. For a detailed exposition of the Kitaev's model, we recommend [4].

4.1 The Hamiltonian of the Model

Let Σ be any oriented surface without boundary such as the sphere or the torus, and let $\mathcal{L}$ be an arbitrary lattice on Σ. For convenience, we still assume $\mathcal{L}$ is a square lattice, but this assumption is not essential. As before, V, E, and F denote the set of vertices, edges, and plaquettes, respectively. *Now we arbitrarily fix an orientation on each edge.* Associate to each edge the Hilbert space $\mathbb{C}[G]$ with the orthonormal basis $\{|g\rangle : g \in G\}$. The total Hilbert space $\mathcal{H}_{\text{tot}}$ is the tensor product of the $\mathbb{C}[G]$'s over all edges. *Throughout the context, by a site is meant a pair $s = (v, p)$, where $v \in V, p \in F$ and $v \in \partial p$.* See Figure 12. For a site $s = (v, p)$, we connect v to the center of p by a red segment.

For each site $s = (v, p)$ and $g, h \in G$, we define the local operators $A_g(s)$ and $B_h(s)$ as shown in Figure 13. $A_g(s)$ acts on edges which are adjacent to v. For each such edge, the action is multiplication on the left by g if the edge is pointed away from v, and multiplication on the right by $\bar{g}$ otherwise. Note that $A_g(s)$ does not depend on the plaquette, but only on v, hence we also write $A_g(s) = A_g(v)$. The action of $B_h(s)$ is described as follows. Given a basis element in $\mathcal{H}_{\text{tot}}$, one starts from v, travels along the boundary of p in the *counterclockwise* direction, and multiply the group elements in the order as they are met. But if one edge is oriented opposite to the traveling direction, then one multiplies the inverse of the group element on that edge instead of the group element itself. Then $B_h(s)$ acts as identity if h equals the product just obtained, and as 0 otherwise. In another word, $B_h(s)$ projects to the subspace spanned by those basis elements for which the product along p starting from v is equal to h. Note that $B_h(s)$ does depend on both v and p. The following identities are easily verified.

$$A_{g_1}(s)A_{g_2}(s) = A_{g_1 g_2}(s), \quad B_{h_1}(s)B_{h_2}(s) = \delta_{h_1,h_2} B_{h_2}(s), \tag{28}$$

$$A_g(s)B_h(s) = B_{ghg^{-1}}A_g(s), \quad A_e(s) = \sum_{h \in G} B_h(s) = Id \tag{29}$$

$$\tag{30}$$

Hence the operators $\{A_g(s), B_h(s)\}$ define a representation of the quantum double DG. Namely, A_g and B_h from DG act on $\mathcal{H}_{\text{tot}}$ as $A_g(s)$ and $B_h(s)$, respectively. We denote by $D(s)$ the algebra generated by the A_g's and B_h's, and call it the algebra of local operators at site s.

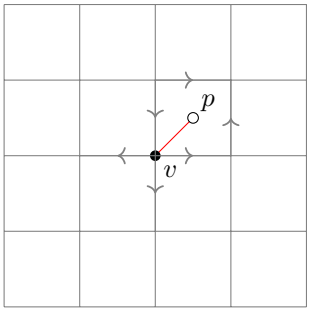


Figure 12: A lattice $\mathcal{L}$ on the surface Σ whose edges are arbitrarily oriented.

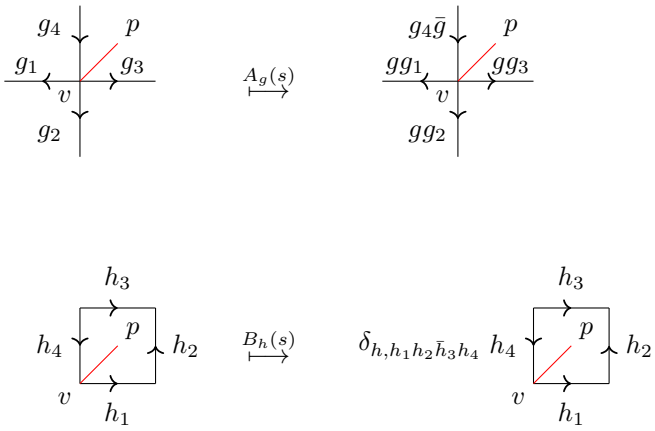


Figure 13: The definition of local operators $A_g(s)$ and $B_h(s)$

Now we introduce the vertex and plaquette operators.

$$A(v) := \frac{1}{|G|} \sum_{g \in G} A_g(v), \quad B(p) := B_e(v, p). \tag{31}$$

Note that while in general $B_h(v, p)$ depends both on v and p, $B_e(v, p)$ only depends on p since the property that a product of group elements equals the identity is cyclic. It is direct to check that $A(v)$ and $B(p)$ are both projectors and they mutually commute with each other. The Hamiltonian is defined by

$$H = \sum_{v \in V} (1 - A(v)) + \sum_{p \in F} (1 - B(p)), \tag{32}$$

and the ground state is given by

$$V_{gs} = \{|\psi\rangle \in \mathcal{H}_{\text{tot}} : A(v)|\psi\rangle = |\psi\rangle, B(p)|\psi\rangle = |\psi\rangle\}. \tag{33}$$

It is direct to check that

$$A_g(s)A(v) = A(v), \quad B_h(s)B(p) = \delta_{h,e}B(p).$$

Hence we have $|\psi\rangle \in V_{gs}$ if and only if

$$A_g(s)|\psi\rangle = |\psi\rangle, \quad B_h(s)|\psi\rangle = \delta_{h,e}|\psi\rangle. \tag{34}$$

Note that Equation 34 means that $D(s)$ acts on V_{gs} by the trivial representation. Thus, V_{gs} is the subspace corresponding to trivial representation of DG at every site s.

4.2 Ground State Space of the Model (Optional)

In this subsection, we compute the ground state degeneracy. Denote by $\pi_1(\Sigma)$ the fundamental group of Σ and by $\text{Hom}(\pi_1(\Sigma), G)$ the set of all group morphisms from $\pi_1(\Sigma)$ to G. There is an action G on $\text{Hom}(\pi_1(\Sigma), G)$ by conjugation. Namely, for $g \in G, \phi \in \text{Hom}(\pi_1(\Sigma), G)$, $g.\phi := g\phi(\cdot)\bar{g}$.

Proposition 4.1. The dimension of $V_{gs}(\Sigma)$ is equal to the number of orbits in $\text{Hom}(\pi_1(\Sigma), G)$ under the G-action.

Proof. A basis element of the total Hilbert space is an assignment of a group element to each edge. Let $|g\rangle$ be any basis element where $g = \{g_\alpha \in G : \alpha \in E\}$. Let γ be any oriented path in the lattice. Denote by g_γ the group element obtained by multiplying the group elements along the path γ. But if one edge in the path is oriented opposite to the path, then multiply the inverse of the group element on that edge instead.

Then the constraint $B(p)|g\rangle = |g\rangle$ is equivalent to the condition that $g_{\partial p} = e$, where ∂p is the boundary of p oriented *counterclockwise*. Note that the condition $g_{\partial p} = e$ is independent of the choice of a starting vertex on ∂p. Hence the subspace fixed by all B_p's is spanned the following set:

$$\begin{aligned} \mathcal{S} &= \{|g\rangle : g_{\partial p} = e, \quad \forall p\} \\ &= \{|g\rangle : g_\gamma = e, \quad \text{for any contractible closed } \gamma\}. \end{aligned}$$

For any $h \in G$, we call the operator $A_h(v)$ a gauge transformation at the vertex v. For two basis elements $|g\rangle, |g'\rangle \in \mathcal{S}$, we call $|g\rangle$ and $|g'\rangle$ gauge equivalent or $|g\rangle \sim |g'\rangle$ if $|g'\rangle$ can be obtained from $|g\rangle$ by applying some gauge transformations at several vertices. Gauge equivalence defines an equivalence relation on $\mathcal{S}$ and denote by $[\mathcal{S}]$ the set of equivalence classes. For each $[g] \in [\mathcal{S}]$, define

$$|[g]\rangle := \sum_{|g'\rangle \sim |g\rangle} |g'\rangle. \tag{35}$$

It is direct to check $\{|[g]\rangle : [g] \in [\mathcal{S}]\}$ forms a basis of $V_{gs}(\Sigma)$.

Now we build a correspondence between $[\mathcal{S}]$ and orbits in $\mathrm{Hom}(\pi_1(\Sigma), G)$.

Choose any vertex v_0 as the base point and choose a maximal spanning tree T containing v_0. By definition, a maximal spanning tree is a subgraph of the lattice $\mathcal{L}$ (with plaquettes ignored) which contains all vertices of $\mathcal{L}$ and does not contain any loop. Thus any maximal spanning tree contains exactly $N := |V| - 1$ edges. Define a map

$$\Phi : \mathcal{S} \longrightarrow \mathrm{Hom}(\pi_1(\Sigma, v_0), G) \tag{36}$$

as follows. Let γ be any closed path starting and ending at v_0. For any $|g\rangle \in \mathcal{S}$, define $\Phi(|g\rangle)([\gamma]) := g_\gamma$, namely, $\Phi(|g\rangle)$ maps a closed path γ to the product of the group elements on it. The fact that $g_{\gamma_0} = e$ for any contractible loop γ_0 implies that $\Phi(|g\rangle)(\gamma)$ only depends on the homotopy class of γ. Hence $\Phi(|g\rangle)$ is a well defined map from $\pi_1(\Sigma, v_0)$ to G. It is clear that it is also a group morphism, hence

$$\Phi(|g\rangle) \in \mathrm{Hom}\left(\pi_1(\Sigma, v_0), G\right).$$

Now we show that map Φ is onto and in fact $|G|^N$-to-1. Given any $\tau \in \mathrm{Hom}(\pi_1(\Sigma, v_0), G)$, we construct a preimage $|g\rangle$ of τ as follows. The value of g on edges of the maximal spanning tree T is arbitrary, and the value on other edges is to be determined. For any edge α not in T, let $\partial_0\alpha$ and $\partial_1\alpha$ be the two end vertices of α. By construction, there is a unique path γ_i in T connecting v_0 to $\partial_i\alpha$, $i = 0, 1$. Let $\gamma = \gamma_0\alpha\bar{\gamma}_1$ be the closed path, where $\bar{\gamma}_1$ means the path γ_1 with reversed direction. Namely, γ reaches $\partial_0\alpha$ along γ_0 from v_0, travels through the edge α, and then goes back to v_0 along $\bar{\gamma}_1$. Define g_α to be the unique group element such that

$$g_{\gamma_0} g_\alpha g_{\bar{\gamma}_1} = \tau(\gamma).$$

It can be checked that such defined $|g\rangle$ is in $\mathcal{S}$, and $\Phi(|g\rangle) = \tau$. Since we have $|G|^N$ choices when defining $|g\rangle$, the map Φ is $|G|^N$-to-1

On the other hand, for each given $|g\rangle$, if we only allow to apply gauge transformations on $|g\rangle$ at vertices other than v_0, there are in total $|G|^N$ such transformations. (One needs to check all the possible $|G|^N$ transformations are indeed different with each other.) If two $|g\rangle, |g'\rangle$ are related by gauge transformations at vertices other than v_0, then $\Phi(|g\rangle) = \Phi(|g'\rangle)$. We conclude that the preimage of τ contains precisely those $|g\rangle$'s which are related by gauge transformations at vertices other than v_0. If we perform a gauge transformation $A_h(v_0)$ at v_0 to $|g\rangle$, then it is easy to see that $\Phi(A_h(v_0)|g\rangle) = h\Phi(|g\rangle)\bar{h}$. Thus we have a one-to-one correspondence between gauge classes in $\mathcal{S}$ and orbits in $\mathrm{Hom}(\pi_1(\Sigma), G)$. □

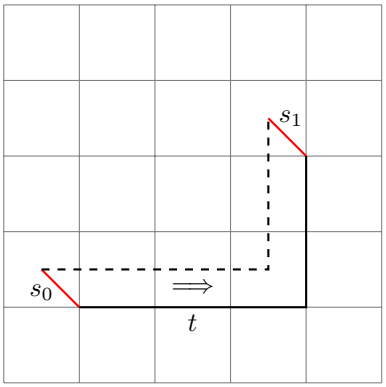


Figure 14: An example of a ribbon t connecting the site s_0 to s_1.

Since the fundamental group of the sphere is trivial, the ground state degeneracy on the sphere is 1. On the torus, the fundamental group is $\mathbb{Z} \times \mathbb{Z}$. A morphism from $\mathbb{Z} \times \mathbb{Z}$ to G is given by a pair of group elements (g_1, g_2) such that $g_1 g_2 = g_2 g_1$. The action of G on the pair (g_1, g_2) is given by conjugation: $(g_1, g_2) \mapsto (g g_1 \bar{g}, g g_2 \bar{g})$. Hence the ground state degeneracy on the torus is given by the number of commuting pairs in $G \times G$, up to conjugation by G; this is equal to the number of irreps of DG.

4.3 Excitations of the Model (Summary)

We give a summary of excitations, fusion, and braiding, delaying the technical details until next section. *From now on, assume the lattice is on a sphere and denote by $|\mathcal{E}\rangle$ the unique ground state.*

In general, an excitation occupies a site. However, as in the case of toric code, single site excitation does not exist. (But such excitation can exist on surfaces with nontrivial topology.)

The tool to study excitations is ribbon operators which are analogous to string operators in toric code. Just as a string connects two vertices, a ribbon connects two sites. See Figure 14. A ribbon t can be thought of as a thin strip with a pair of parallel strings, one in the lattice and the other in the dual lattice. The ribbon t is assumed to be directed; it starts from the site $s_0 := \partial_0 t$ and ends at the site $s_1 := \partial_1 t$. (More precise definition of ribbons will be given in next section.) As a notation, a site s_i always means the pair (v_i, p_i). Associated with each ribbon t are a set of operators $\{F^{(h,g)}(t) : h, g \in G\}$. Each $F^{(h,g)}(t)$ acts non-trivially only on edges that are contained in or crossed by t. We give several properties of these operators (without proof) and use them to study excitations. (We have not shown what the operators $F^{(h,g)}(t)$ actually are. But hopefully this will not affect understanding of the statements below.)

1. Let

$$\mathcal{F}(t) = \mathrm{span}_{\mathbb{C}}\{F^{(h,g)}(t) : h, g \in G\}. \tag{37}$$

Elements in $\mathcal{F}(t)$ are called ribbon operators. The dimension of $\mathcal{F}(t)$ is $|G|^2$. Hence $\{F^{(h,g)}(t) : h, g \in G\}$ is a basis of $\mathcal{F}(t)$; it is called the group elements basis. A differ-

ent basis, which is a "Fourier transformation" of the group elements basis, is given by

$$\{F^{(C,\chi;u,u')}(t) : (C,\chi) \in \mathrm{Irr}(DG), u \text{ and } u' \text{ each enumerates a basis of } V_{(C,\chi)}.\} \tag{38}$$

This is called the representation basis.

2. $F^{(h,g)}(t)$ commutes with all $A(v)$ and $B(p)$ where $v \neq v_0, v_1$ and $p \neq p_0, p_1$. The space of 2-particle excitations at s_0 and s_1 is given by

$$L(s_0, s_1) = \{F|\mathcal{E}\rangle : F \in \mathcal{F}(t)\}, \tag{39}$$

and it has two orthonormal bases,

$$\begin{aligned}&\{|h,g\rangle := F^{(h,g)}(t)|\mathcal{E}\rangle : h,g \in G\},\\ &\{|C,\chi;u,u'\rangle := F^{(C,\chi;u,u')}|\mathcal{E}\rangle : (C,\chi) \in \mathrm{Irr}(DG), u \text{ and } u' \text{ each enumerates a basis of } V_{(C,\chi)}\},\end{aligned} \tag{40}$$

which are respectively again called the group elements basis and the representation basis.

3. The local operators $D(s_0)$ and $D(s_1)$ preserve the space $L(s_0, s_1)$. They are the commutant of each other in the space of operators on $L(s_0, s_1)$, hence validate the notion of being called 'local operators'. Indeed, any local operator that acts on a few qudits near the site s_0 must commute with the action of $D(s_1)$. Although the action of the local operator does not necessarily preserve the subspace $L(s_0, s_1)$, when projecting the action to $L(s_0, s_1)$, it will coincide with one of the operators in $D(s_0)$. The action of $D(s_i)$ on the representation basis has a particularly nice form. Explicitly, the action of $D(s_1)$ on $|C,\chi;u,u'\rangle$ transforms the u part according to the irrep (C,χ) while the action of $D(s_0)$ transforms the u' part according to the the dual irrep $(C,\chi)^*$. For instance,

$$B_h(s_1)A_g(s_1)|C,\chi;u,u'\rangle = \sum_{\tilde{u'}} \Gamma^{(C,\chi)}_{\tilde{u'}u'}\left(D_{(h,g)}\right)|C,\chi;u,\tilde{u'}\rangle. \tag{41}$$

Thus the representation basis gives a decomposition of $L(s_0, s_1)$:

$$L(s_0, s_1) = \bigoplus_{(C,\chi)\in\mathrm{Irr}(DG)} V^*_{(C,\chi)} \otimes V_{(C,\chi)}, \tag{42}$$

and under this decomposition $D(s_0)$ (resp. $D(s_1)$) acts on the first (resp. second) factor. When fixing (C,χ), we can think of the u index as living on site s_0 and the u' index as living on site s_1. Moreover, the local operators only change the indices u and u', but not the irrep (C,χ). Therefore, we call (C,χ) a quasi-particle type or an anyon type, and the types of quasi-particles are in one-to-one correspondence with the irreps of DG (strictly speaking, with isomorphism classes of irreps).

4. The state $F^{(h,g)}(t)|\mathcal{E}\rangle$ is unchanged as we deform the ribbon t.

5. To obtain the space of 3-particle excitations at sites s_0, s_1, s_2, we simply connect one of the sites, say s_0, to each of the other two by a ribbon. See Figure 15 (Left). Then

$$L(s_0, s_1, s_2) = \mathrm{span}\{|h_1, g_1; h_2, g_2\rangle := F^{(h_2,g_2)}(t_2)F^{(h_1,g_1)}(t_1)|\mathcal{E}\rangle : h_i, g_i \in G\}. \tag{43}$$

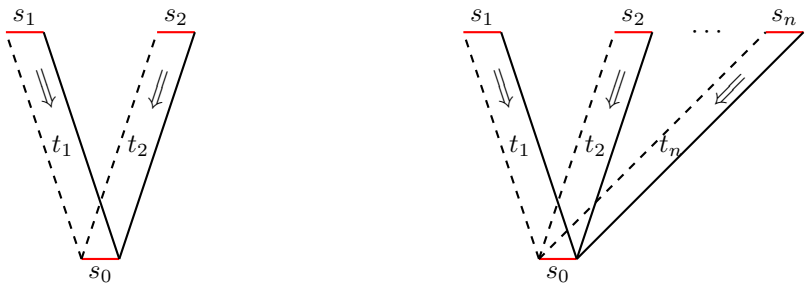


Figure 15: Ribbons connecting more than two sites

We also have the representation basis:

$$\{|C_1, \chi_1; u_1, u_1'; C_2, \chi_2; u_2, u_2'\rangle\}. \tag{44}$$

One can think of the u_1 index as living on s_1, u_2 on s_2, u_1' and u_2' on s_0. The local operators $D(s_i), i = 1, 2$ transform u_i according to $(C_i, \chi_i)^*$, while $D(s_0)$ transforms $u_1' \otimes u_2'$ according to $(C_1, \chi_1) \otimes (C_2, \chi_2)$. (Note that the latter statement is not obvious.) By general representation theory, $(C_1, \chi_1) \otimes (C_2, \chi_2)$ decomposes into direct sums of irreps:

$$(C_1, \chi_1) \otimes (C_2, \chi_2) = (C_3, \chi_3) \oplus (C_4, \chi_4) \oplus \cdots \tag{45}$$

Each irrep in the decomposition is called a total charge/type of (C_1, χ_1) and (C_2, χ_2). In general, given any two types $\alpha, \beta \in \mathrm{Irr}(DG)$, we can decompose

$$\alpha \otimes \beta = \bigoplus_{\gamma \in \mathrm{Irr}(DG)} N_{\alpha\beta}^{\gamma} \gamma, \tag{46}$$

where $N_{\alpha\beta}^{\gamma} = 0, 1$ and these $\{N_{\alpha\beta}^{\gamma}\}$ are called fusion rules.

6. More generally, consider the space $L(s_0, s_1, \cdots, s_n)$. We connect s_i to s_0 with a ribbon t_i, $i = 1, \cdots, n$. See Figure 15(Right). Assume each ribbon t_i is associated with the type $\alpha_i := (C_i, \chi_i)$. For $i = 1, \cdots, n$, $D(s_i)$ acts on $|u_i\rangle$ according to α_i^* and $D(s_0)$ acts on $|u_1', \cdots, u_n'\rangle$ according to the product $\alpha_1 \otimes \cdots \otimes \alpha_n$. Let $\mathrm{Inv}(\alpha_1 \otimes \cdots \otimes \alpha_n)$ be the subspace of $\alpha_1 \otimes \cdots \otimes \alpha_n$ corresponding to the trivial representations of $D(s_0)$. Then the space $\alpha_1^* \otimes \alpha_n^* \otimes \mathrm{Inv}(\alpha_1 \otimes \cdots \otimes \alpha_n)$ corresponds to the subspace without excitation at the site s_0. In another word, this is the space of n quasi-particles of types $\alpha_1, \cdots, \alpha_n$ whose total type is trivial. Note that the local operators $D(s_i)$ have no access to the space $\mathrm{Inv}(\alpha_1 \otimes \cdots \otimes \alpha_n)$; this is the logical space where we can encode information. For $n > 3$, the space $\mathrm{Inv}(\alpha_1 \otimes \cdots \otimes \alpha_n)$ could have dimension greater than one, but in general it lacks a tensor product structure.

5 Ribbon Operators

In this section, we study ribbon operators and excitations. An elementary and detailed discussion of ribbon operators can be found in [6].

Let $\mathcal{L}$ be a lattice on which the Hamiltonian is defined, and let $\mathcal{L}^*$ be its dual lattice. Recall that each edge α in $\mathcal{L}$ is arbitrarily assigned a direction (orientation). We now orient

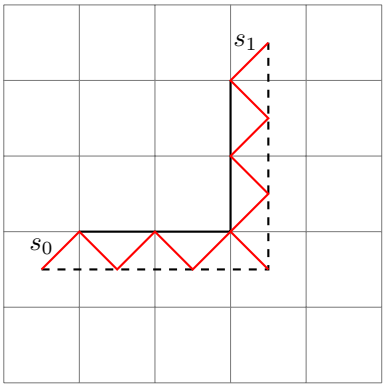


Figure 16: A ribbon consisting of a sequence of triangles.

Figure 17: (Left) a type-I (or dual) triangle; (Right) a type-II (or direct) triangle

the dual edge α^* so that α^* crosses α from right to left. (This only makes sense if the surface is oriented, which is always our assumption.)

Roughly speaking, a ribbon is a thin strip in the combined lattice $\mathcal{L} \cup \mathcal{L}^*$ that connects two sites. See Figure 16, where, and throughout the section, we will draw an edge in $\mathcal{L}$ as a solid black line, an edge in $\mathcal{L}^*$ as a dashed black line, and a site as a solid red line. More precisely, a ribbon is built up from two types of triangles, called type-I triangles (or dual triangles) and type-II triangles (or direct triangles). See Figure 17. A dual triangle consists of two sites and a dual edge, while a direct triangle consists of two sites and a direct edge (that is, an edge in $\mathcal{L}$). For a dual/direct triangle τ, by choosing one site as $\partial_0\tau$ and the other as $\partial_1\tau$, we say τ is directed and it starts at $\partial_0\tau$ and ends at $\partial_1\tau$. We often use an arrow to indicate the direction. See Figure 17. A (directed) ribbon t is defined to be a sequence $(\tau_1, \cdots, \tau_n)$ of triangles (type I or II) such that $\partial_1\tau_i = \partial_0\tau_{i+1}$, and that the edge contained in any τ_i (not including the sites) is not the same as and also not dual to the edge in any other τ_j. The second condition above means the ribbon does not repeat or cross itself. Denote by $\partial_0 t = \partial_0\tau_1$ and $\partial_1 t = \partial_1\tau_n$. We say t is a directed ribbon, starting at $\partial_0 t$ and ending at $\partial_1 t$. Similarly, we also use an arrow to indicate the direction. Note that it is possible that $\partial_0 t = \partial_1 t$. Such a ribbon is called a closed ribbon, (though we will not talk about it here).

For each pair of group elements $(h, g) \in G \times G$ and a directed ribbon t, we wish to define an operator $F^{(h,g)}(t)$. We first define it for the case of a triangle. See Figure 18 for a graphical illustration. Namely, if t is a triangle, then $F^{(h,g)}(t)$ acts non-trivially only on the edge contained in it. If t is a type-I triangle and $|x\rangle$ is a basis state in the Hilbert space of the edge α_t contained in t, the action $F^{(h,g)}(t)$ sends $|x\rangle$ to $\delta_{g,e}|hx\rangle$ if the direction of t coincides with that of α_t, and to $\delta_{g,e}|x\hat{h}\rangle$ otherwise. If t is a type-II triangle and again $|x\rangle$ is a basis state, then the action sends $|x\rangle$ to $\delta_{g,x}|x\rangle$ if the direction of t coincides with that of its edge, and to $\delta_{\bar{g},x}|x\rangle$ otherwise. Note that for type-II triangle, the action is a projector

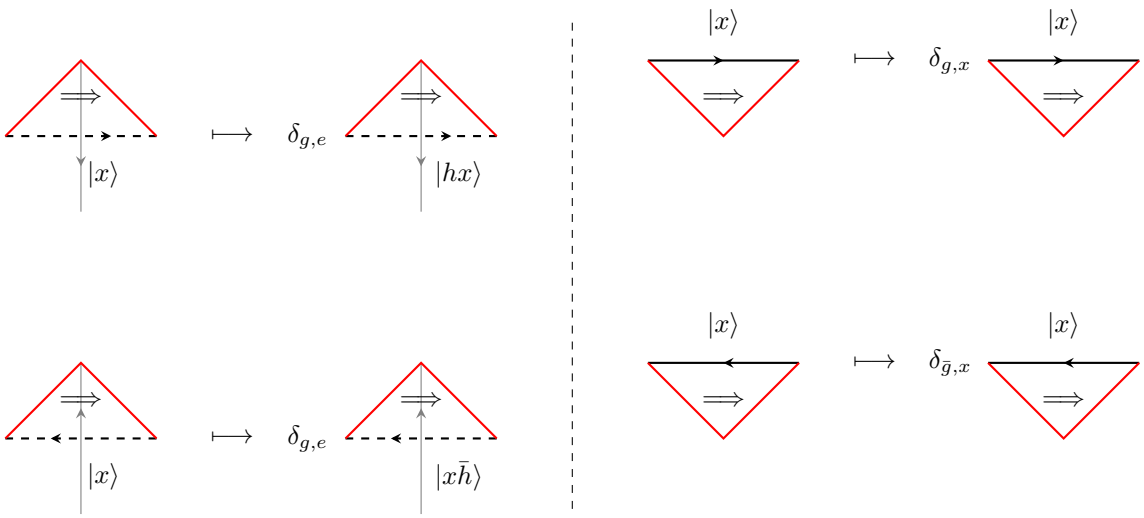


Figure 18: (Left block) The action of $F^{(h,g)}(\tau)$ for a type-I triangle τ; (Right block) The action of $F^{(h,g)}(\tau)$ for a type-II triangle τ. For each type, there are two cases determined by whether the direction of the triangle coincides with the direction of the edge in it. In all cases, $x \in G$ is a group element such that $|x\rangle$ represents a basis state in the corresponding Hilbert space.

and it does not depend on h.

We now define the operator $F^{(h,g)}(t)$ for a general ribbon t inductively. If t consists of more than one triangle, then split $t = t_1 \sqcup t_2$ as a disjoint union of two sub ribbons, and define

$$F^{(h,g)}(t) := \sum_{k\in G} F^{(h,k)}(t_1)F^{(\bar{k}hk,\bar{k}g)}(t_2). \tag{47}$$

With Equation 47, we can define $F^{(h,g)}(t)$ inductively for ribbons of arbitrary length. However, one must check that $F^{(h,g)}(t)$ does not depend on the way the ribbon is split. To prove this, it suffices to show the following. Let $t = t_1 \sqcup t_2 \sqcup t_3$. To compute $F^{(h,g)}(t)$, one can first split t into $t_1 \sqcup t_2$ and t_3, and then split the former into t_1 and t_2, or one can instead first split t into t_1 and $t_2 \sqcup t_3$, and then split the latter into t_2 and t_3. One needs to check the two ways of splitting give the same answer. This is straight forward:

$$\begin{aligned}
F^{(h,g)}(t) &= \sum_{k\in G} F^{(h,k)}(t_1 \sqcup t_2)F^{(\bar{k}hk,\bar{k}g)}(t_3) \\
&= \sum_{k,l\in G} F^{(h,l)}(t_1)F^{(\bar{l}hl,\bar{l}k)}(t_2)F^{(\bar{k}hk,\bar{k}g)}(t_3), \\
F^{(h,g)}(t) &= \sum_{l\in G} F^{(h,l)}(t_1)F^{(\bar{l}hl,\bar{l}g)}(t_2 \sqcup t_3) \\
&= \sum_{m,l\in G} F^{(h,l)}(t_1)F^{(\bar{l}hl,m)}(t_2)F^{(\bar{m}\bar{l}hlm,\bar{m}\bar{l}g)}(t_3) \\
&\overset{lm\to k}{=} \sum_{k,l\in G} F^{(h,l)}(t_1)F^{(\bar{l}hl,\bar{l}k)}(t_2)F^{(\bar{k}hk,\bar{k}g)}(t_3),
\end{aligned} \tag{48}$$

where in the last equality, we applied a change of variable $lm \to k$.

Remark 5.1. Although it is direct to verify that $F^{(h,g)}(t)$ is well defined, it is still not clear how the particular combination on the right hand side of Equation 47 is chosen. In fact, we can rewrite Equation 47 as

$$F^{(h,g)}(t) = \sum_{h_1,g_1,h_2,g_2} \Omega^{(h,g)}_{(h_1,g_1),(h_2,g_2)} F^{(h_1,g_1)}(t_1) F^{(h_2,g_2)}(t_2), \tag{49}$$

for some tensor $\Omega^{(h,g)}_{(h_1,g_1),(h_2,g_2)}$. For compactness, we use bold letters $\mathbf{a}, \mathbf{b}, \mathbf{c}, \cdots$, to represent a pair of group elements. Then we have

$$F^{\mathbf{c}}(t) = \sum_{\mathbf{a},\mathbf{b}} \Omega^{\mathbf{c}}_{\mathbf{ab}} F^{\mathbf{a}}(t_1) F^{\mathbf{b}}(t_2). \tag{50}$$

That $F^{\mathbf{a}}(t)$ does not depend on the way the ribbon is split is equivalent to the condition,

$$\sum_{\mathbf{m}} \Omega^{\mathbf{m}}_{\mathbf{ab}} \Omega^{\mathbf{d}}_{\mathbf{mc}} = \sum_{\mathbf{n}} \Omega^{\mathbf{d}}_{\mathbf{an}} \Omega^{\mathbf{n}}_{\mathbf{bc}} \tag{51}$$

If we take a $|G|^2$ dimensional Hilbert space with basis given by $\{f_{\mathbf{a}} : \mathbf{a} \in G \times G\}$ and define a multiplication by

$$f_{\mathbf{a}} f_{\mathbf{b}} := \sum_{\mathbf{c}} \Omega^{\mathbf{c}}_{\mathbf{ab}} f_{\mathbf{c}}, \tag{52}$$

then Equation 51 is equivalent to the property that the multiplication is associative, which makes the Hilbert space an associative algebra. In fact, one can check directly that the $\Omega^{\cdot}_{\cdot,\cdot}$ tensor here is exactly the multiplication tensor in the quantum double DG:

$$D_{\mathbf{a}} D_{\mathbf{b}} = \sum_{\mathbf{c}} \Omega^{\mathbf{c}}_{\mathbf{ab}} D_{\mathbf{c}}. \tag{53}$$

By the inductive formula, the operator $F^{(h,g)}(t)$ acts non-trivially only on edges contained in or crossed by the ribbon. For a typical ribbon, the explicit formula is given in Figure 19.

Let

$$\mathcal{F}(t) = \mathrm{span}_{\mathbb{C}}\{F^{(h,g)}(t) : h, g \in G\}. \tag{54}$$

Any operator in $\mathcal{F}(t)$ is called a ribbon operator. We state some properties of ribbon operators. Although they all can be proved formally, it is easier to use the explicit expression in Figure 19 to verify the properties.

Let t be a ribbon with $\partial_i t = s_i = (v_i, p_i), i = 0, 1$. It is straight forward to show

$$F^{(h_1,g_1)}(t) F^{(h_2,g_2)}(t) = \delta_{g_1,g_2} F^{(h_1 h_2, g_2)}(t). \tag{55}$$

Hence $\mathcal{F}(t)$ is an algebra.

Also, $F^{(h,g)}(t)$ commutes with all the $A(v)$ and $B(p)$ for which $v \neq v_i, p \neq p_i, i = 0, 1$. In fact, $F^{(h,g)}(t)$ even commutes with all $A_{g'}(v)$ for any $g' \in G$. Recall that at each site s

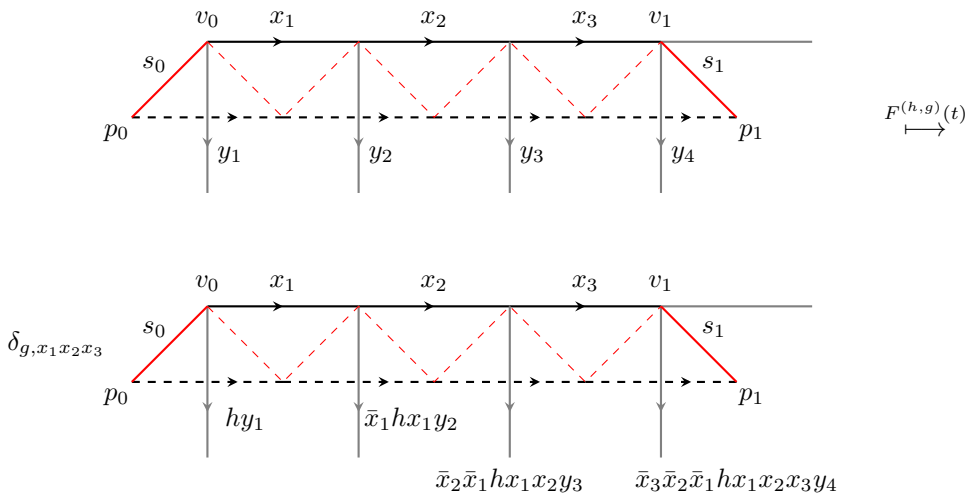


Figure 19: Explicit formula for the operator $F^{(h,g)}(t)$, where t starts at $s_0 = (v_0, p_0)$ and ends at $s_1 = (v_1, p_1)$. Each x_i, y_j is a group element representing a basis state of the total Hilbert space. The action is zero unless $g = x_1x_2x_3$.

we have the algebra of operators $D(s)$ which gives the action of DG on the total Hilbert space. The ribbon operator in general does not commute with the operators in $D(s_i)$. Their commutation relations are given as follows.

$$\begin{aligned} A_{g'}(s_0)F^{(h,g)}(t) &= F^{(g'hg\bar{g}',g'g)}(t)A_{g'}(s_0) \\ B_{h'}(s_0)F^{(h,g)}(t) &= F^{(h,g)}(t)B_{h'h}(s_0) \end{aligned} \tag{56}$$

$$\begin{aligned} A_{g'}(s_1)F^{(h,g)}(t) &= F^{(h,g\bar{g'})}(t)A_{g'}(s_1) \\ B_{h'}(s_1)F^{(h,g)}(t) &= F^{(h,g)}(t)B_{\bar{g}\bar{h}gh'}(s_1) \end{aligned} \tag{57}$$

Denote by $|\mathcal{E}\rangle$ the unique ground state (assuming the surface is a sphere). Let $|0\rangle$ be the basis state in the total Hilbert space which has value e at each edge. Hence $|0\rangle$ is fixed by all $B(p)$'s. Then up to normalization, $|\mathcal{E}\rangle$ is given by

$$|\mathcal{E}\rangle = \prod_v A(v)|0\rangle. \tag{58}$$

In particular, all the basis states contained in the expansion of $|\mathcal{E}\rangle$ have positive coefficients. Moreover, for any basis state in the expansion, the product of the group elements along any closed loop is the identity e.

Assume t is not closed and define

$$|h, g\rangle := F^{(h,g)}(t)|\mathcal{E}\rangle. \tag{59}$$

By the formula in Figure 19, $F^{(h,g)}(t)$ projects out all basis states in $|\mathcal{E}\rangle$ for which the product of the group elements along any path connecting v_0 to v_1 is not equal to g, and it modifies all remaining terms by expressions involving h. Then the basis states in the expansion of $|h, g\rangle$

are characterized as follows. The product of the group elements along any path connecting v_0 to v_1 is equal to g, and the product along the boundary of the plaquette p_0 starting from v_0 in counterclockwise direction is equal to $\bar{h}$. Therefore the $|h,g\rangle\,'s$ are orthogonal and do not depend on the choice of t.

Let

$$L(s_0,s_1)=\{F|\mathcal{E}\rangle : F\in\mathcal{F}(t)\}=\mathrm{span}_{\mathbb{C}}\{|h,g\rangle : h,g\in G\}. \tag{60}$$

The space $L(s_0,s_1)$ contains all states with excitations at s_0 and s_1. The local operators $D(s_i), i=0,1$ preserves $L(s_0,s_1)$. By Equations 5657 and the fact that $D(s_i)$ acts on the ground state by the trivial representation, it is direct to see that the actions are given by

$$\begin{aligned} A_{g'}(s_0)|h,g\rangle &= |g'h\bar{g'},g'g\rangle \\ B_{h'}(s_0)|h,g\rangle &= \delta_{h',\bar{h}}|h,g\rangle \end{aligned} \tag{61}$$

$$\begin{aligned} A_{g'}(s_1)|h,g\rangle &= |h,g\bar{g'}\rangle \\ B_{h'}(s_1)|h,g\rangle &= \delta_{h',\bar{g}hg}|h,g\rangle. \end{aligned} \tag{62}$$

Apparently, $D(s_0)$ commutes with $D(s_1)$ since they act on non-overlapping edges. By general representation theory of quantum doubles, the space $L(s_0,s_1)$ decomposes as

$$L(s_0,s_1)=\bigoplus_{(C,\chi)\in\mathrm{Irr}(DG)} V^*_{(C,\chi)}\otimes V_{(C,\chi)}, \tag{63}$$

where $D(s_0)$ acts on $V^*_{(C,\chi)}$ and $D(s_1)$ acts on $V_{(C,\chi)}$. We then have another basis corresponding to the decomposition:

$$\{|C,\chi;u,u'\rangle : (C,\chi)\in\mathrm{Irr}(DG), u=(c,j), u'=(c',j'), c,c'\in C, j,j'=1,\cdots,|\chi|\}. \tag{64}$$

Explicitly, the translation between the two bases are given by:

$$|C,\chi;u,u'\rangle=\frac{|(C,\chi)|}{|G|}\sum_{h,g}\Gamma^{(C,\chi)}_{u,u'}\left(D_{(h,g)}\right)|h,g\rangle, \tag{65}$$

$$|h,g\rangle=\sum_{(C,\chi)}\sum_{u,u'}\overline{\Gamma^{(C,\chi)}_{u,u'}\left(D_{(h,g)}\right)}|C,\chi;u,u'\rangle, \tag{66}$$

where $\Gamma^{(C,\chi)}_{u,u'}\left(D_{(h,g)}\right)$ is the matrix element of the irrep (C,χ). We also define the ribbon operators $F^{(C,\chi;u,u')}(t)$ by

$$F^{(C,\chi;u,u')}(t)=\frac{|(C,\chi)|}{|G|}\sum_{h,g}\Gamma^{(C,\chi)}_{u,u'}\left(D_{(h,g)}\right)F^{(h,g)}(t). \tag{67}$$

Hence,

$$|C,\chi;u,u'\rangle=F^{(C,\chi;u,u')}(t)|\mathcal{E}\rangle. \tag{68}$$

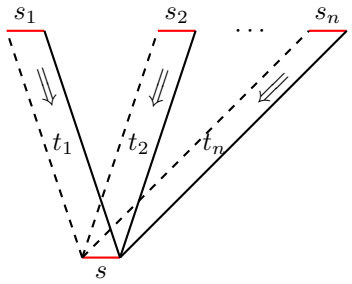


Figure 20: n ribbons are used to create excitations at $n+1$ sites.

Remark 5.2. Simplifications of the formula for $|C,\chi;u,u'\rangle$ is possible, although we will not be using it in later context. Note that the matrix elements of the irrep (C,χ) is given by,

$$\Gamma^{(C,\chi)}_{u,u'}\left(D_{(h,g)}\right) = \delta_{h,gc'\bar{g}}\delta_{h,c}\Gamma^{\chi}_{jj'}(\bar{q}_h g q_{c'}), \quad u=(c,j), u'=(c',j'). \tag{69}$$

Substituting the expression in Equation 65, we get

$$|C,\chi;u,u'\rangle = \frac{|\chi|}{|Z(r)|}\sum_{n\in Z(r)}\Gamma^{\chi}_{jj'}(n)|c, q_c n\bar{q}_{c'}\rangle, \quad u=(c,j), u'=(c',j'), \tag{70}$$

where $r\in C$ is the pre-selected element. For $|h,g\rangle$, let $C(h)$ be the conjugacy class containing h and $r\in C(h)$ the pre-selected element in $C(h)$, then

$$|h,g\rangle = \sum_{\chi\in \mathrm{Irr}(Z(r))}\sum_{j,j'=1}^{|\chi|}\overline{\Gamma^{\chi}_{jj'}(\bar{q}_h g q_{\bar{g}hg})}\ |C(h),\chi;(h,j),(\bar{g}hg,j')\rangle. \tag{71}$$

Under the basis $\{|C,\chi;u,u'\rangle\}$, $D(s_0)$ changes the u index according to $(C,\chi)^*$ and $D(s_1)$ changes the u' index according to (C,χ). But, both actions will not change the (C,χ) index. We call (C,χ) an anyon/quasi-particle type. Thus anyon types are in one-to-one correspondence with (isomorphism classes of) irreps of DG. We can think of the u index as living at s_0 and the u' index as living at s_1. Each state $|C,\chi;u,u'\rangle$ is obtained by applying the ribbon operator $F^{(C,\chi;u,u')}(t)$ to the ground state.

Now we consider excitations at $n+1$ sites $s,s_1\cdots,s_n$. For each $i=1,\cdots,n$, we choose a ribbon t_i connecting s_i to s. These ribbons are disjoint except near the site s. See Figure 20. Then the space $L(s,s_1\cdots,s_n)$ with excitations at these sites has a basis given by

$$\{|h_1,g_1;\cdots;h_n,g_n\rangle := F^{(h_n,g_n)}(t)\cdots F^{(h_1,g_1)}(t)|\mathcal{E}\rangle : h_i,g_i\in G\} \tag{72}$$

or

$$\{|C_1,\chi_1,u_1,u_1';\cdots;C_n,\chi_n,u_n,u_n'\rangle := F^{(C_n,\chi_n;u_n,u_n')}(t)\cdots F^{(C_1,\chi_1;u_1,u_1')}(t)|\mathcal{E}\rangle : \\ (C_i,\chi_i)\in \mathrm{Irr}(DG), u_i,u_i'=1,\cdots,|(C_i,\chi_i)|\}. \tag{73}$$

$D(s_i)$ acts on the u_i index according to $(C_i,\chi_i)^*$ and $D(s)$ acts on the indices $u_1'\otimes\cdots\otimes u_n'$

according to the product action $(C_1,\chi_1)\otimes\cdots\otimes(C_n,\chi_n)$. This can be derived from Equations 56 and 57. For instance,

$$\begin{aligned} B_{h'}(s)|h_1,g_1;\cdots;h_n,g_n\rangle &= B_{h'}(s)F^{(h_n,g_n)}(t)\cdots F^{(h_1,g_1)}(t)|\mathcal{E}\rangle \\ &= F^{(h_n,g_n)}(t)B_{\overline{g_n}\overline{h_n}g_nh'}\cdots F^{(h_1,g_1)}(t)|\mathcal{E}\rangle \\ &= F^{(h_n,g_n)}(t)\cdots F^{(h_1,g_1)}(t)B_{\overline{g_1}\overline{h_1}g_1\cdots\overline{g_n}\overline{h_n}g_nh'}|\mathcal{E}\rangle \\ &= \delta_{h',\overline{g_n}h_ng_n\cdots\overline{g_1}h_1g_1}|h_1,g_1;\cdots;h_n,g_n\rangle \\ &= \sum_{h'=h'_n\cdots h'_1}\left(B_{h'_1}(s)\otimes\cdots B_{h'_n}(s)\right)|h_1,g_1;\cdots;h_n,g_n\rangle. \end{aligned} \tag{74}$$

We view the operators $D(s_i)$ as local operators and $D(s)$ as logical/topological operators. Denote by $\alpha_i=(C_i,\chi_i)$, and let $\mathrm{Inv}(\alpha_1,\cdots,\alpha_n)\subset\alpha_1\otimes\cdots\otimes\alpha_n$ be the subspace where $D(s)$ acts by the trivial representation. Then the subspace

$$\alpha_1^*\otimes\cdots\otimes\alpha_n^*\otimes\mathrm{Inv}(\alpha_1,\cdots,\alpha_n)\subset\alpha_1^*\otimes\cdots\otimes\alpha_n^*\otimes\alpha_1\otimes\cdots\otimes\alpha_n \tag{75}$$

contains no excitation at s and the action of $D(s_i)$ does not affect the $\mathrm{Inv}(\alpha_1,\cdots,\alpha_n)$ part. Therefore, we call $\mathrm{Inv}(\alpha_1,\cdots,\alpha_n)$ the logical subspace. In contrast, the α_i^*'s are called the local subspaces. Since local operators do not have access to the logical subspace, quantum information encoded in this subspace is protected from local errors. From now on, we will drop the local degrees α_i^* and only consider the logical degrees $\alpha_1\otimes\cdots\otimes\alpha_n$. That is, we will suppress the u_i indices and denote a basis state by $|\alpha_1,u'_1;\cdots;\alpha_n,u'_n\rangle$ or $|u'_1,\cdots,u'_n\rangle$ when the types α_i are fixed.

6 Braiding and Fusion

We start with a brief review of some representation theory that will be used later. Let α,β be two representations of DG, denote by $\mathrm{Hom}(\alpha,\beta)$ the space of morphisms, namely, linear maps from α to β commuting with the action of DG.

Lemma 6.1 (Schur's Lemma)**.** If α and β are two irreps of DG, then

$$\mathrm{Hom}(\alpha,\beta)\simeq\begin{cases}\mathbb{C} & \text{if } \alpha\simeq\beta,\\ 0 & \text{otherwise.}\end{cases} \tag{76}$$

Also recall that we have defined the invertible element R and its inverse R^{-1},

$$R=\sum_{g\in G}A_g\otimes B_g,\qquad R=\sum_{g\in G}A_{\bar{g}}\otimes B_g. \tag{77}$$

If α and β are two representations, then there is an isomorphism $c_{\alpha,\beta}$,

$$c_{\alpha,\beta}:\alpha\otimes\beta\xrightarrow{R}\alpha\otimes\beta\xrightarrow{\text{Flip}}\beta\otimes\alpha, \tag{78}$$

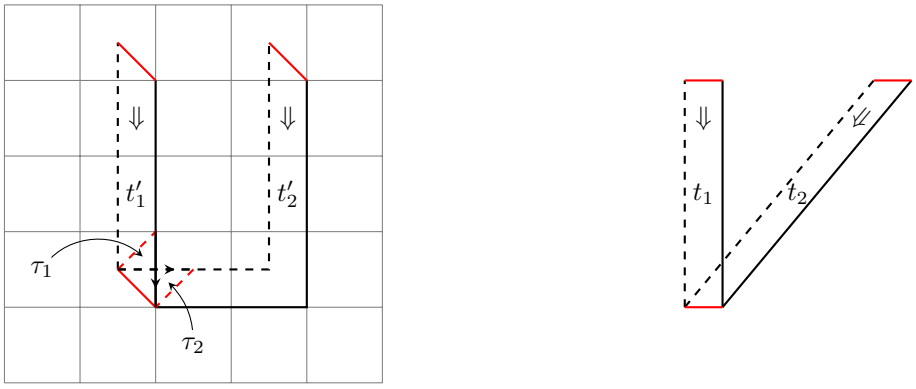


Figure 21: (Left)Two ribbons $t_1 = t_1'\tau_1$ and $t_2 = t_2'\tau_2$. They share one common site and are directed toward this site. (Right) A schematic picture of two ribbons t_1 and t_2 whose configuration is given by that on the left.

where the first factor of R acts on α, the second acts on β, and Flip swaps the two factors. It is direct to check $c_{\alpha,\beta} \in \mathrm{Hom}(\alpha \otimes \beta, \beta \otimes \alpha)$ and its inverse is given by

$$c_{\alpha,\beta}^{-1} : \beta \otimes \alpha \xrightarrow{\text{Flip}} \alpha \otimes \beta \xrightarrow{R^{-1}} \alpha \otimes \beta. \tag{79}$$

More generally, for n representations $\alpha_1, \cdots, \alpha_n$, we can apply the isomorphism c to $\alpha_i \otimes \alpha_{i+1}$:

$$\alpha_1 \otimes \cdots \alpha_i \otimes \alpha_{i+1} \cdots \otimes \alpha_n \xrightarrow{id_{\alpha_1} \otimes \cdots c_{\alpha_i,\alpha_{i+1}} \cdots \otimes id_{\alpha_n}} \alpha_1 \otimes \cdots \alpha_{i+1} \otimes \alpha_i \cdots \otimes \alpha_n \tag{80}$$

We denote the above the isomorphism by $c_{i,i+1}$.

Lemma 6.2. The following equations hold:

$$c_{i,i+1}\ c_{i+1,i+2}\ c_{i,i+1} = c_{i+1,i+2}\ c_{i,i+1}\ c_{i+1,i+2}, \tag{81}$$

$$c_{i,i+1}\ c_{j,j+1} = c_{j,j+1}\ c_{i,i+1}, \quad |i-j| \geq 1. \tag{82}$$

Before introducing braiding, we need a technical lemma. Let t_1, t_2 be two ribbons as shown in Figure 21(Left), namely, $t_i = t_i'\tau_i, i = 0, 1$, the t_i's are disjoint, and τ_1 (resp. τ_2) is a type-II (resp. type-II) triangle. Moreover, τ_1 and τ_2 share the same edge. (Strictly speaking, their edges are dual to each other.) So the ribbon operators associated with τ_1 and τ_2 act on the same edge. When the background lattice is not drawn, we use the schematic picture in Figure 21(Right) to represent two ribbons whose configuration is described by that in Figure 21(Left).

Lemma 6.3. Let t_1, t_2 be as above, then

$$F^{(h_2,g_2)}(t_2)F^{(h_1,g_1)}(t_1) = F^{(h_1,g_1\bar{g}_2\bar{h}_2g_2)}(t_1)F^{(h_2,g_2)}(t_2). \tag{83}$$

Proof. Consider first the special case when $t_i = \tau_i, i = 0, 1$. Let the common edge of τ_1 and τ_2 be oriented as shown in Figure 21(Left), and let $|x\rangle$ be a basis state on that edge where x is a group element. Then we check the action of both sides of Equation 83 on $|x\rangle$.

$$\begin{aligned} \text{LHS:} \quad |x\rangle &\mapsto \delta_{g_1,x}\delta_{g_2,e}|x\bar{h}_2\rangle, \\ \text{RHS:} \quad |x\rangle &\mapsto \delta_{g_2,e}\delta_{g_1\bar{g}_2\bar{h}_2g_2,x\bar{h}_2}|x\bar{h}_2\rangle. \end{aligned} \tag{84}$$

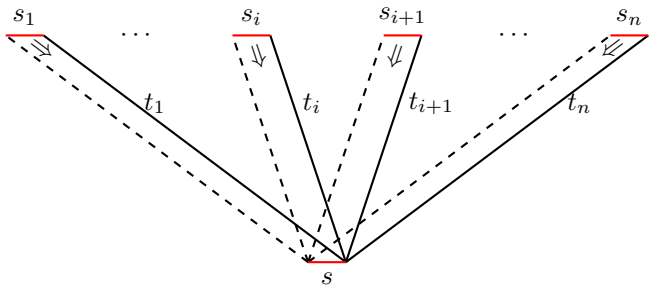


Figure 22: A configuration of $n+1$ excitations

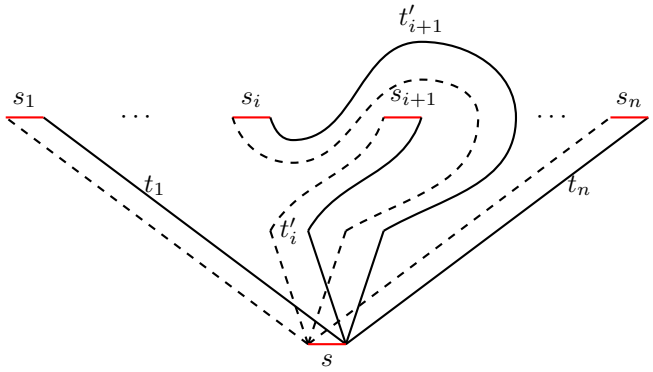


Figure 23: The configuration after we swap, in counterclockwise direction, the excitation at s_i with that at s_{i+1}.

The coefficients in front of $|x\bar{h}_2\rangle$ in both expressions are obviously equal, and thus we have proved Equation 83 in the special case. The general case can be proved using the inductive formula for ribbon operators.

$$\begin{aligned} F^{(h_2,g_2)}(t_2)F^{(h_1,g_1)}(t_1) &= \sum_{k_1,k_2} F^{(h_2,k_2)}(t'_2)F^{(\bar{k}_2 h_2 k_2, \bar{k}_2 g_2)}(\tau_2)\, F^{(h_1,k_1)}(t'_1)F^{(\bar{k}_1 h_1 k_1, \bar{k}_1 g_1)}(\tau_1) \\ &= \sum_{k_1,k_2} F^{(h_1,k_1)}(t'_1)F^{(\bar{k}_1 h_1 k_1, \bar{k}_1 g_1 \bar{g}_2 \bar{h}_2 g_2)}(\tau_1)\, F^{(h_2,k_2)}(t'_2)F^{(\bar{k}_2 h_2 k_2, \bar{k}_2 g_2)}(\tau_2) \\ &= F^{(h_1, g_1\bar{g}_2\bar{h}_2 g_2)}(t_1)F^{(h_2,g_2)}(t_2). \end{aligned} \tag{85}$$

In the first and last equality above, we applied the inductive formula for ribbon operators. In the second equality, we applied Equation 83 for τ_1 and τ_2 which we already proved. (The relevant terms are colored in red.) Note that the ribbons t'_1, t'_2 are disjoint with each and are also disjoint from the τ_i, thus their corresponding operators commute with each other. □

Now consider a configuration of $n+1$ excitations at $s, s_1, \cdots, s_n$. We use a ribbon t_i to connect s_i to s. See Figure 22. Consider a basis state

$$|h_1, g_1; \cdots; h_i, g_i; h_{i+1}, g_{i+1}; \cdots; h_n, g_n\rangle := F^{(h_n,g_n)}(t_n)\cdots F^{(h_{i+1},g_{i+1})}(t_{i+1})F^{(h_i,g_i)}(t_i)\cdots F^{(h_1,g_1)}(t_1)|\mathcal{E}\rangle. \tag{86}$$

Note the ordering in which the ribbon operators are applied. A different ordering will give a different basis. If we swap the excitations at s_i and s_{i+1} in counterclockwise direction

Figure 24: (Left) The trajectory of a counterclockwise swap; (Right) The trajectory of a clockwise swap.

(we can think that we drag the ribbons t_i, t_{i+1} to make such a swap), then the ribbons are changed as shown in Figure 23. Namely, t_i is changed to t'_i, t_{i+1} is changed to t'_{i+1}, and all other ribbons remain unaltered. Note that the ribbons can be freely deformed as long as they do not cross any excitation. Hence we can deform t'_i to t_{i+1}. We cannot deform t'_{i+1} to t_i since that would cross the excitation at s_{i+1}. Then the resulting state is given by

$$\begin{aligned}
|\psi_{fi}\rangle \quad &\overset{}{=\!=\!=} \quad \cdots F^{(h_{i+1},g_{i+1})}(t'_{i+1})F^{(h_i,g_i)}(t'_i)\cdots|\mathcal{E}\rangle \\
&\overset{t'_i\to t_{i+1}}{=\!=\!=} \quad \cdots F^{(h_{i+1},g_{i+1})}(t'_{i+1})F^{(h_i,g_i)}(t_{i+1})\cdots|\mathcal{E}\rangle \\
&\overset{\text{Equ 83}}{=\!=\!=} \quad \cdots F^{(h_i,g_i\bar{g}_{i+1}\bar{h}_{i+1}g_{i+1})}(t_{i+1})F^{(h_{i+1},g_{i+1})}(t'_{i+1})\cdots|\mathcal{E}\rangle \\
&\overset{t'_{i+1}\to t_i}{=\!=\!=} \quad \cdots F^{(h_i,g_i\bar{g}_{i+1}\bar{h}_{i+1}g_{i+1})}(t_{i+1})F^{(h_{i+1},g_{i+1})}(t_i)\cdots|\mathcal{E}\rangle \\
&=\!=\!= \quad |\cdots;h_{i+1},g_{i+1};h_i,g_i\bar{g}_{i+1}\bar{h}_{i+1}g_{i+1};\cdots\rangle \\
&=\!=\!= \quad \left[\text{Flip}\circ\left(\sum_g A_g(s)\otimes B_g(s)\right)\right]_{i,i+1}|\cdots;h_i,g_i;h_{i+1},g_{i+1};\cdots\rangle, \qquad (87)
\end{aligned}$$

where in the fourth equality we can now deform the ribbon t'_{i+1} to t_i since the ribbon operator on t_{i+1} has not been applied yet when the ribbon operator on t'_{i+1} is being applied. In the last equality, $[\cdot]_{i,i+1}$ means we apply the operator inside the square bracket to i-th and $(i+1)$-th position. Thus a counterclockwise swap of the excitations at s_0 and s_1 induces the action

$$\left[\text{Flip}\circ\left(\sum_g A_g(s)\otimes B_g(s)\right)\right]_{i,i+1}. \qquad (88)$$

If we consider state in the representation basis

$$|\alpha_1,u_1,u'_1;\cdots;\alpha_n,u_n,u'_n\rangle, \qquad (89)$$

where $\alpha_1,\cdots,\alpha_n$ are irreps of DG, then $A_g(s)$ in Equation 88 acts on the u'_i index according to α_i and $B_g(s)$ acts on the u'_{i+1} index according to α_{i+1}. The map Flip swaps the the pair (u_i,u'_i) with the pair (u_{i+1},u'_{i+1}). Now if we fix the excitation types and drop the local degrees $u_1,\cdots,u_n$, the topological degrees $u'_1,\cdots,u'_n$ span the Hilbert space $\alpha_1\otimes\cdots\otimes\alpha_n$, and the action in Equation 88 on topological degrees is precisely the map $c_{i,i+1}$. (See Equation 80.) A counterclockwise swap followed by a clockwise swap must act as identity, hence a clockwise swap induces the action $c^{-1}_{i,i+1}$. We call the swap of two excitations a *braiding*.

The trajectories of a counterclockwise and a clockwise swap are each represented by the diagram as shown in See Figure 24. These diagrams are called braid diagrams on n

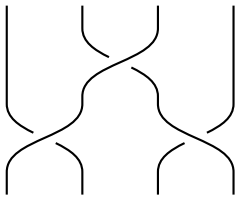


Figure 25: An example of a braid diagram on four strands.

strands. More generally, we can stack one braid diagram on top of another one to get more complicated braid diagrams. See Figure 25 for an example. These diagrams are considered up to isotopy. Namely, if two diagrams can be deformed to each other with their end points fixed, then they are considered equivalent. Equivalence classes of braid diagrams form a group called the braid group B_n. The multiplication of two diamgrams is given by stacking the first one on top of the second one. For an introduction to braid groups, see for instance [13]. Algebraically, B_n has a presentation as

$$B_n = \langle \sigma_1, \cdots, \sigma_{n-1} \,|\, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \tag{90}$$

$$\sigma_i\sigma_j = \sigma_j\sigma_i, |i-j| > 1 \,\rangle, \tag{91}$$

where σ_i (resp. σ_i^{-1}) corresponds to the braid diagram in Figure 24(Left) (resp. (Right)). Hence σ_i is the trajectory of counterclockwise braiding of s_i with s_{i+1}. A general element in B_n corresponds to a sequence of braidings.

Now assume all excitation types are the same $\alpha_1 = \cdots = \alpha_n = \alpha$. Then $c_{i,i+1} \in \mathbf{U}(\alpha^{\otimes n})$, and by Lemma 6.2 we obtain a representation of the braid group:

$$\begin{aligned} \rho_{n,\alpha}: \quad B_n &\longrightarrow \mathbf{U}(\alpha^{\otimes n}) \\ \sigma_n &\longmapsto c_{i,i+1}. \end{aligned} \tag{92}$$

Since each $c_{i,i+1}$ commutes with the DG-action, it also preserves the subspace $\mathrm{Inv}(\alpha^{\otimes n})$ on which DG acts by the trivial representation. Hence, $\rho_{n,\alpha}$ restricts to a representation on $\mathrm{Inv}(\alpha^{\otimes n})$:

$$\rho_{n,\alpha}: \quad B_n \longrightarrow \mathbf{U}\left(\mathrm{Inv}(\alpha^{\otimes n})\right). \tag{93}$$

But remember the subspace $\mathrm{Inv}(\alpha^{\otimes n})$ is the logical/protected subspace where information is encoded. Thus the image of $\rho_{n,\alpha}$ serve as quantum gates that process information.

Example 6.4. Let $\alpha = (C, \mathbf{1})$, where C is a conjugacy class and $\mathbf{1}$ is the trivial irrep . A basis for α is given by $\{|c\rangle : c \in C\}$. A counterclockwise braiding of α with another α induces the map:

$$\begin{aligned} c_{1,2}: \quad \alpha\otimes\alpha &\longrightarrow \alpha\otimes\alpha, \\ |c_1, c_2\rangle &\longmapsto |c_2, c_2c_2\bar{c}_2\rangle. \end{aligned} \tag{94}$$

Finally we consider the process of fusing excitations. Let $|\psi\rangle \in \alpha\otimes\beta$ be a state with excitations at s_1, s_2 and s. See Figure 26(Left). Here we have ignored the local degrees α^*

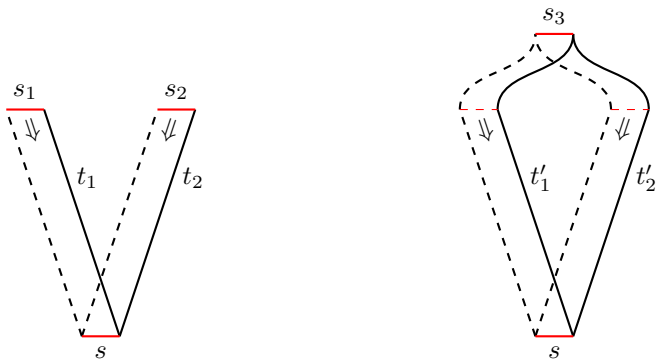


Figure 26: (Left) A configuration with three excitations. (Right) Fusing the excitations at s_1 and s_2 to get an excitation at s_3.

and β^* at s_1 and s_2, respectively. We bring the two excitations at s_1 and s_2 to a common location s_3 and measure the type of the excitation at s_3. This is called a fusion process. If the measurement shows the excitation at s_3 is γ, then the state $|\psi\rangle$ is transformed by a map:

$$\phi_{\alpha\beta}^{\gamma} : \alpha \otimes \beta \longrightarrow \gamma. \tag{95}$$

Moreover, $\phi_{\alpha\beta}^{\gamma}$ should commute with the DG-action at site s since the fusion takes place away from s. Hence, we have

$$\phi_{\alpha\beta}^{\gamma} \in \mathrm{Hom}(\alpha \otimes \beta, \gamma). \tag{96}$$

Note that as a representation of DG we have the decomposition of $\alpha \otimes \beta$,

$$\alpha \otimes \beta \simeq \bigoplus_i \gamma_i, \tag{97}$$

where the γ_i's are irreps and they are mutually non-isomorphic. Hence $\phi_{\alpha\beta}^{\gamma}$ is not zero if and only if γ is one of the γ_i's. And if $\gamma = \gamma_i$, then $\phi_{\alpha\beta}^{\gamma}$ is unique up to a scalar multiplication by Schur's Lemma (Lemma 6.1). We normalize $\phi_{\alpha\beta}^{\gamma_i}$ so that it is an isometry on the subspace $\gamma_i \subset \alpha \otimes \beta$. Hence, we call γ_i a total charge/type of α and β. We call the triple (α, β, γ) *admissible* if γ is a total charge of α and β, in which case, we use the graph in Figure 27(Left) to represent $\phi_{\alpha\beta}^{\gamma}$. $\phi_{\alpha\beta}^{\gamma}$ is called a fusion channel. The fusion process corresponds to a measurement which projects the state to one of its total charges via the fusion channel. Explicitly, α and β fuses to γ with the probability $|\phi_{\alpha\beta}^{\gamma}|\psi\rangle|^2$ and the resulting state is $\phi_{\alpha\beta}^{\gamma}|\psi\rangle$ (unnormalized).

We can also think of the reverse process to fusion, namely, a splitting process. If γ is a total charge of α and β, and $|\psi\rangle \in \gamma \subset \alpha \otimes \beta$, then of course fusing α and β will always produce γ. In this case, we may as well think that α and β is split from γ. The splitting process is represented by a morphism

$$\phi_{\gamma}^{\alpha\beta} \in \mathrm{Hom}(\gamma, \alpha \otimes \beta), \tag{98}$$

whose graphical representation is shown in Figure 27(Middle). We choose the normalization so that (see Figure 27 (Right))

$$\phi_{\alpha\beta}^{\gamma} \circ \phi_{\gamma}^{\alpha\beta} = id_{\gamma}. \tag{99}$$

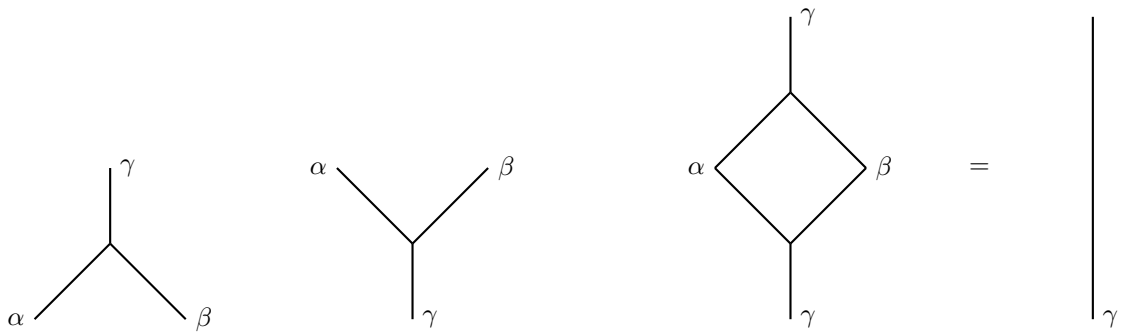


Figure 27: (Left) the fusion channel $\phi_{\alpha\beta}^{\gamma}$; (Middle) the splitting channel $\phi_{\gamma}^{\alpha\beta}$; (Right) the normalization condition.

Figure 28: (Left): a splitting tree represented by $(\phi_{\gamma}^{\alpha_1,\alpha_2}\otimes id_{\alpha_3})\phi_{\beta}^{\gamma,\beta_3}$. (Right) another splitting tree represented by $(id_{\alpha_1}\otimes\phi_{\gamma'}^{\alpha_2,\alpha_3})\phi_{\beta}^{\alpha_1,\gamma'}$.

Now consider a morphism in $\mathrm{Hom}(\beta,\alpha_1\otimes\alpha_2\otimes\alpha_3)$ given by $(\phi_{\gamma}^{\alpha_1,\alpha_2}\otimes id_{\alpha_3})\phi_{\beta}^{\gamma,\beta_3}$. It corresponds to the process of splitting β into γ and α_3 followed another splitting of γ into α_1 and α_3. See Figure 33(Left), where the graph representing the process is called a splitting/fusion tree. It turns out that as we vary γ among all possibilities, namely, all those γ such that $(\alpha_1,\alpha_2,\gamma)$ and (γ,α_3,β) are both admissible, then

$$\{(\phi_{\gamma}^{\alpha_1,\alpha_2}\otimes id_{\alpha_3})\phi_{\beta}^{\gamma,\alpha_3} : (\alpha_1,\alpha_2,\gamma),(\gamma,\alpha_3,\beta)\text{ admissible}\} \tag{100}$$

forms a basis of $\mathrm{Hom}(\beta,\alpha_1\otimes\alpha_2\otimes\alpha_3)$. This basis is called a splitting/fusion tree basis. But we also have another splitting/fusion tree as shown in Figure 33(Right) and by varying γ' we also get another splitting/fusion tree basis:

$$\{(id_{\alpha_1}\otimes\phi_{\gamma'}^{\alpha_2,\alpha_3})\phi_{\beta}^{\alpha_1,\gamma'} : (\alpha_2,\alpha_3,\gamma'),(\alpha_1,\gamma',\beta)\text{ admissible}\}. \tag{101}$$

The matrix relating these two bases is called F-matrix and its matrix elements are called F-symbols. The process of changing one basis to the other is called an F-move. See Figure 34. We will explore properties of F-symbols later.

More generally, a splitting tree basis of $\mathrm{Hom}(\beta,\alpha_1\otimes\cdots\otimes\alpha_n)$ is given by splitting tree shown in Figure 30 by varying $\gamma_1,\cdots,\gamma_{n-2}$. Of course, one can also consider other shapes of splitting trees and they will give other bases. Every two such bases are related by a sequence of F-moves.

Note that the invariant subspace $\mathrm{Inv}(\alpha^{\otimes n})$ can be identified with the space $\mathrm{Hom}(\mathbf{1},\alpha^{\otimes n})$, where $\mathbf{1}$ is the 1-dimensional trivial irrep of DG. Hence for $\mathrm{Inv}(\alpha^{\otimes n})$, we can use a splitting tree basis as the computational basis.

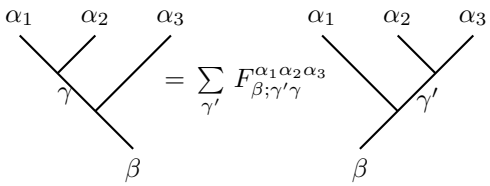


Figure 29: The F-matrix (F-symbols) related two splitting bases.

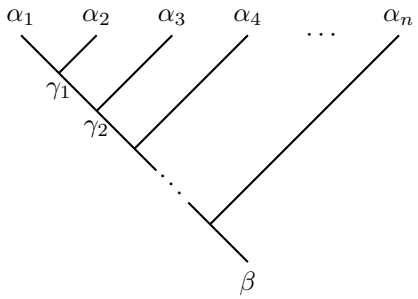


Figure 30: A splitting tree for n anyons

7 Quantum Computing with Kitaev's Model

We have discussed Kitaev's quantum double model based on any finite group G. Here we give a summary of the algebraic structures of anyons in the model, and show explicitly how they can be used to perform topological quantum computing. These structures form the abstract notion of a (unitary) modular tensor category, which is the algebraic foundation of an anyon system and will be introduced next section.

The types of excitations/anyons in the quantum double model are in one-to-one correspondence with (isomorphism classes of) irreps of DG. To be precise, an anyon type corresponds to an isomorphism class of irreps, while an anyon corresponds to a specific irrep, namely, a representative in the class. But we will not strictly distinguish these two notions. Denote by $L = \mathrm{Irr}(DG)$ the set of anyon types. Given two anyons $\alpha, \beta \in L$, we have the decomposition

$$\alpha \otimes \beta = \bigoplus_{\gamma \in L} N^{\gamma}_{\alpha\beta} \gamma, \tag{102}$$

where $N^{\gamma}_{\alpha\beta}$ is a non-negative integer indicating the multiplicity of γ in $\alpha \otimes \beta$. In general, $N^{\gamma}_{\alpha\beta}$ could be greater than 1. But for simplicity, let's assume $N^{\gamma}_{\alpha\beta} = 0, 1$, which is the case for most groups which we are interested in such as S_3. These integers $N^{\gamma}_{\alpha\beta}$ are called fusion coefficients or fusion rules. If $N^{\gamma}_{\alpha\beta} = 1$, then γ is called a total charge of α and β, and the triple (α, β, γ) is said to be *admissible*.

For each admissible triple (α, β, γ), we have the fusion channel $\phi^{\gamma}_{\alpha\beta} \in \mathrm{Hom}(\alpha \otimes \beta, \gamma)$ and the splitting channel $\phi^{\alpha\beta}_{\gamma} \in \mathrm{Hom}(\gamma, \alpha \otimes \beta)$ such that

$$\phi^{\gamma'}_{\alpha\beta} \phi^{\alpha\beta}_{\gamma} = \delta_{\gamma,\gamma'} id_{\gamma}. \tag{103}$$

These channels are represented by certain graphs in Figure 31. If $|\psi\rangle \in \alpha \otimes \beta$ is the

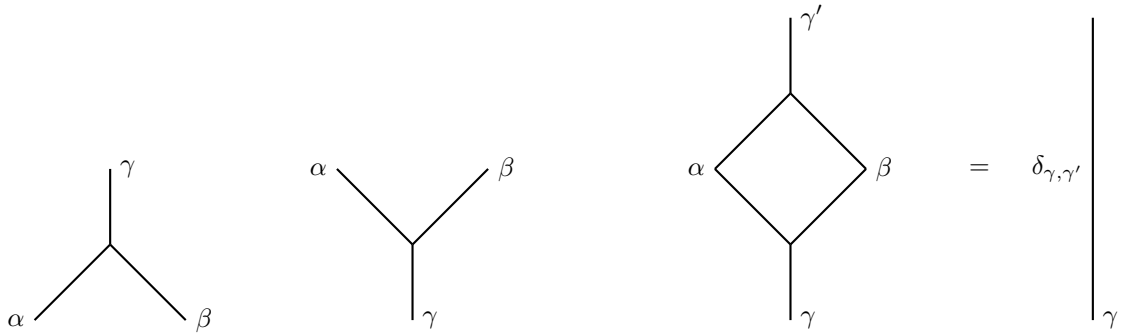


Figure 31: (Left)the fusion channel $\phi^{\gamma}_{\alpha\beta}$; (Middle) the splitting channel $\phi^{\alpha\beta}_{\gamma}$; (Right) the normalization condition.

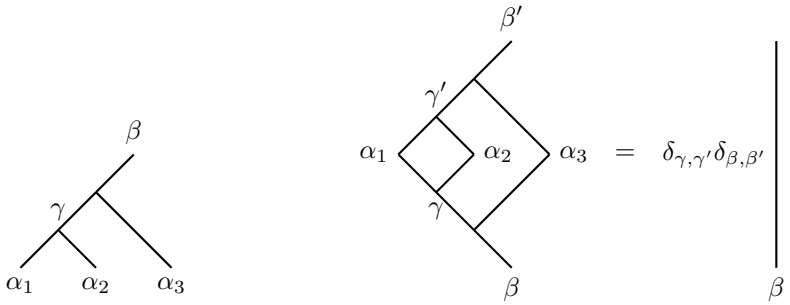


Figure 32: (Left) a fusion tree basis; (Right) the composition of a fusion tree basis with its dual splitting tree basis.

state before fusion, then fusing α and β corresponds to projecting $|\psi\rangle$ to one of their total charges. The probability to fuse into the anyon γ is $|\phi^{\gamma}_{\alpha\beta}|\psi\rangle|^2$, and given that outcome, the state becomes $\phi^{\gamma}_{\alpha\beta}|\psi\rangle$ (unnormalized). Note that any state $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{\gamma} c_{\gamma}\phi^{\alpha\beta}_{\gamma}|\psi_{\gamma}\rangle, \tag{104}$$

where $|\psi_{\gamma}\rangle$ is a state in γ and c_{γ} is some complex number. Then by the normalization condition in Equation 103, the probability to fuse into γ is given by $|c_{\gamma}|^2$ and the state is $|\psi_{\gamma}\rangle$ when that happens. Thus fusion corresponds to the measurement with respect to the splitting channel.

Now let's consider fusion channels of three anyons $\alpha_1, \alpha_2, \alpha_3$. We can first fuse α_1, α_2 into

Figure 33: Two splitting tree bases

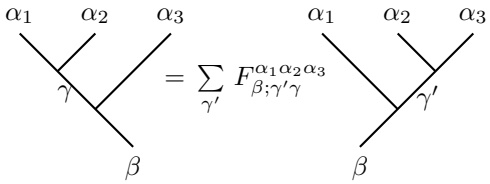


Figure 34: The F-move relating two splitting tree bases

γ, and then fuse γ, α_3 into β. This is represented by the process

$$\phi^{\beta}_{\gamma\alpha_3} \circ (\phi^{\gamma}_{\alpha_1\alpha_2} \otimes id_{\alpha_3}) \in \mathrm{Hom}(\alpha_1 \otimes \alpha_2 \otimes \alpha_3, \beta), \tag{105}$$

whose graphical interpretation is given in Figure 32(Left). By varying all possible intermediate γ, we obtain a basis for $\mathrm{Hom}(\alpha_1 \otimes \alpha_2 \otimes \alpha_3, \beta)$:

$$\{\phi^{\beta}_{\gamma\alpha_3} \circ (\phi^{\gamma}_{\alpha_1\alpha_2} \otimes id_{\alpha_3}) : (\alpha_1, \alpha_2, \gamma), (\gamma, \alpha_2, \beta) \text{ admissible}\}. \tag{106}$$

This basis is called a fusion tree basis. Analogously, we can consider the splitting process in Figure 33(Left), which corresponds to the morphism

$$(\phi^{\alpha_1\alpha_2}_{\gamma} \otimes id_{\alpha_3}) \circ \phi^{\gamma\alpha_3}_{\beta}, \tag{107}$$

and again by varying the intermediate γ, these give a basis of the space $\mathrm{Hom}(\beta, \alpha_1 \otimes \alpha_2 \otimes \alpha_3)$, called a splitting tree basis.

$$\{(\phi^{\alpha_1\alpha_2}_{\gamma} \otimes id_{\alpha_3}) \circ \phi^{\gamma\alpha_3}_{\beta} : (\alpha_1, \alpha_2, \gamma), (\gamma, \alpha_3, \beta) \text{ admissible}\}. \tag{108}$$

These fusion tree basis in Equation 106 is dual to the splitting tree basis in Equation 108 in the sense that

$$\left(\phi^{\beta'}_{\gamma'\alpha_3} \circ (\phi^{\gamma'}_{\alpha_1\alpha_2} \otimes id_{\alpha_3})\right) \circ \left((\phi^{\alpha_1\alpha_2}_{\gamma} \otimes id_{\alpha_3}) \circ \phi^{\gamma\alpha_3}_{\beta}\right) = \delta_{\gamma,\gamma'}\delta_{\beta,\beta'} id_{\beta}, \tag{109}$$

which is better illustrated with graphical calculations as shown in Figure 32(Right).

Apparently, we also have another splitting basis associated with three anyons (see Figure 33(Right)),

$$\{(id_{\alpha_1} \otimes \phi^{\alpha_2\alpha_3}_{\gamma})\phi^{\alpha_1\gamma}_{\beta} : (\alpha_1, \gamma, \beta), (\alpha_2, \alpha_3, \gamma) \text{ admissible}\}. \tag{110}$$

The two splitting bases in Equation 108 and 110 are related by a matrix transformation. See Figure 34, where $F^{\alpha_1\alpha_2\alpha_3}_{\beta}$ is called an F-matrix and its matrix elements $F^{\alpha_1\alpha_2\alpha_3}_{\beta;\gamma\gamma'}$ are called F-symbols. We also call the basis change an "F-move".

More generally, we have splitting/fusion tree bases for n anyons. Take $n = 4$ as an illustration. Figure 35 shows some examples of splitting tree bases for the same space $\mathrm{Hom}(\beta, \alpha_1 \otimes \alpha_2 \otimes \alpha_3 \otimes \alpha_4)$. Basically, each splitting tree represents a process of creating the anyons α_i's from the anyon β. Two different bases are related by a sequence of F-moves. For instance, see Figure 36.

Now let's consider the splitting process shown in Figure 35(Left), namely, we split β into γ_2, α_4, followed by splitting γ_2 into γ_1, α_3, followed by splitting γ_1 into α_1, α_2. Denote this

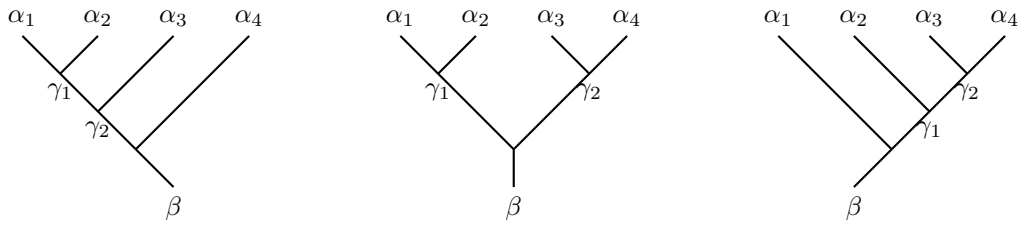


Figure 35: Some examples of splitting tree bases in $\mathrm{Hom}(\beta, \alpha_1 \otimes \alpha_2 \otimes \alpha_3 \otimes \alpha_4)$.

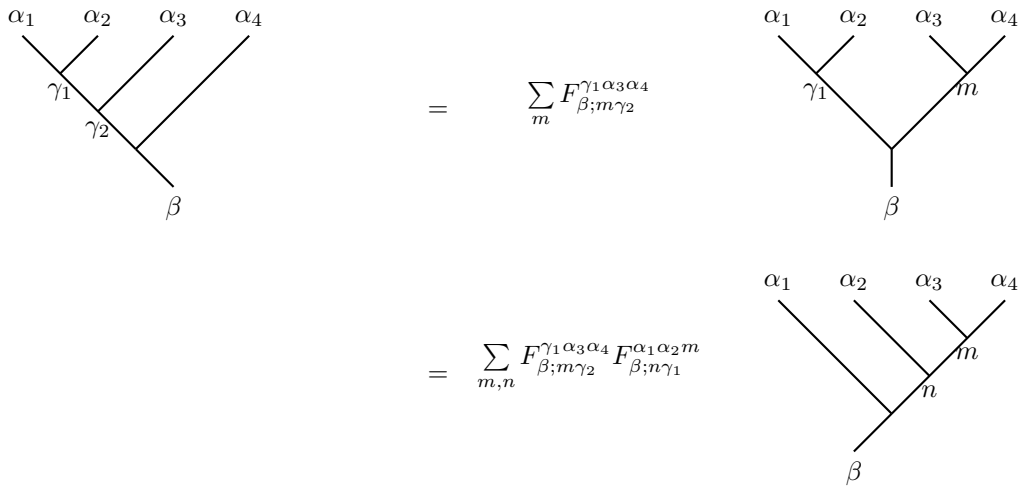


Figure 36: F-moves relating different bases

process temporarily by $P(\gamma_1, \gamma_2)$. Then for any state $|\psi_\beta\rangle \in \beta$, $P(\gamma_1, \gamma_2)$ produces a state $P(\gamma_1, \gamma_2)|\psi_\beta\rangle \in \alpha_1 \otimes \alpha_2 \otimes \alpha_3 \otimes \alpha_4$. If we change $|\psi_\beta\rangle$, then the final state also changes. However, the total charges of (α_1, α_2), (γ_1, α_3), and (γ_2, α_4) all remain fixed. We refer $|\psi_\beta\rangle$ as internal degrees. Fusion outcomes do not depend on internal degrees. Therefore, we will not use internal degrees to encode information [1]. Rather, information is encoded in the splitting channels. In this case, γ_1 and γ_2 label a specific channel. In another word, we encode information in the morphism space $\mathrm{Hom}(\beta, \alpha_1 \otimes \alpha_2 \otimes \alpha_3 \otimes \alpha_4)$, and use any splitting tree basis as the computational basis. Measurement with respect to a splitting tree basis is obtained by fusing anyons in the order according to the splitting tree. For the basis in Figure 35(Left), we fuse α_1, α_2 into some γ_1', fuse γ_1', α_3 into some γ_2', and finally fuse γ_2', α_4 to get β. The final state can be obtained by applying the dual fusion tree basis as shown in Figure 37.

As a special case, if $\beta = \mathbf{1}$, the trivial irrep or the ground state, then $\dim \beta = 1$. The only internal degree is the ground state $|\mathcal{E}\rangle \in \beta$, and $\mathrm{Hom}(\mathbf{1}, \alpha_1 \otimes \alpha_2 \otimes \alpha_3 \otimes \alpha_4)$ can be identified with the subspace $\mathrm{Inv}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \subset \alpha_1 \otimes \alpha_2 \otimes \alpha_3 \otimes \alpha_4$ on which DG acts by the trivial representation. This is the logical subspace we discussed before.

Finally, let's consider braiding. Braiding α_1 and α_2 in counterclockwise direction produces the transformation

$$c_{\alpha_1,\alpha_2} : \alpha_1 \otimes \alpha_2 \longrightarrow \alpha_2 \otimes \alpha_1. \tag{111}$$

[1] We will give another reason below why internal degrees are not used.

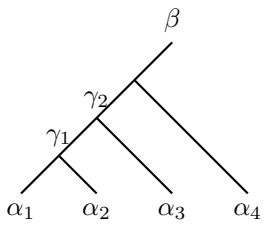


Figure 37: a fusion tree basis of four anyons

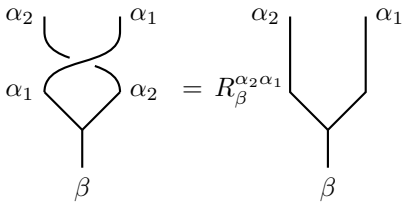


Figure 38: the R-move

Compose c_{α_1,α_2} with the splitting channel $\phi_\beta^{\alpha_1\alpha_2}$, we get $c_{\alpha_1,\alpha_2} \circ \phi_\beta^{\alpha_1\alpha_2} \in \mathrm{Hom}(\beta, \alpha_2 \otimes \alpha_1)$. Since the dimension of $\mathrm{Hom}(\beta, \alpha_2 \otimes \alpha_1)$ is 1, there exists a scalar $R_\beta^{\alpha_2\alpha_1}$ such that

$$c_{\alpha_1,\alpha_2} \circ \phi_\beta^{\alpha_1\alpha_2} = R_\beta^{\alpha_2\alpha_1} \phi_\beta^{\alpha_2\alpha_1}. \tag{112}$$

See Figure 38 for a graphical definition. The scalars $R_\beta^{\alpha_2\alpha_1}$ are called R-symbols, and the process of removing a crossing is called an "R-move". From the above equation, we can also see that $R_\beta^{\alpha_2\alpha_1}$ is independent of the internal degrees of β, which is the second reason why we will not make use of internal degrees.

With the fusion rules, F-symbols, and R-symbols, we can do explicit calculations. For some anyons α, β, take $\mathrm{Hom}(\beta, \alpha^{\otimes 4})$ as the computational space and choose the splitting tree basis in Figure 35(Middle) as the computational basis. Denote by $|\gamma_1, \gamma_2\rangle$ the splitting tree with labels γ_1, γ_2. Note that in general γ_1 and γ_2 are not independent, so we do not have a tensor product structure on $\mathrm{Hom}(\beta, \alpha^{\otimes 4})$. Braiding of the four α anyons gives a representation of the four strand braid group B_4 on $\mathrm{Hom}(\beta, \alpha^{\otimes 4})$. The generator $\sigma_i, i = 1, 2, 3$, of B_4 corresponds to braiding of the i-th α with the $(i+1)$-th. The action of σ_1 is easy to compute as we just need to perform one R-move. See Figure 39. Hence, we have

$$\sigma_1 |\gamma_1, \gamma_2\rangle = R_{\gamma_1}^{\alpha\alpha} |\gamma_1, \gamma_2\rangle, \tag{113}$$

and the action is a diagonal matrix. The same is true for σ_3. The action of σ_2 is more involved since we cannot apply an R-move directly. Instead, we will need to perform two F-moves to convert the current basis to another one, apply R-move in that basis, and perform another two F-moves to convert back to the current basis. See Figure 40. Hence, σ_2 is expressed as

$$\sigma_2 |\gamma_1, \gamma_2\rangle = \sum_{m,n,\gamma_1'\gamma_2'} F_{\beta;m\gamma_1}^{\alpha\alpha\gamma_2} (F_m^{\alpha\alpha\alpha})_{n\gamma_2}^{-1} R_n^{\alpha\alpha} F_{m;\gamma_2' n}^{\alpha\alpha\alpha} (F_\beta^{\alpha\alpha\gamma_2'})_{\gamma_1' m}^{-1} |\gamma_1', \gamma_2'\rangle. \tag{114}$$

The fusion rules, F-symbols, R-symbols, together with some additional data form the notion of a unitary modular tensor category, which is the algebraic model for anyons. In

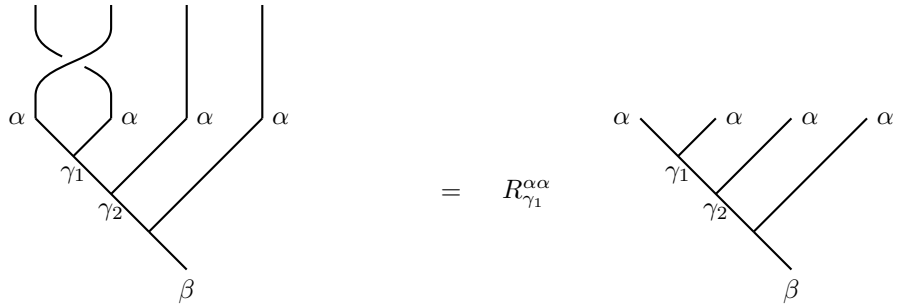


Figure 39: The action of σ_1.

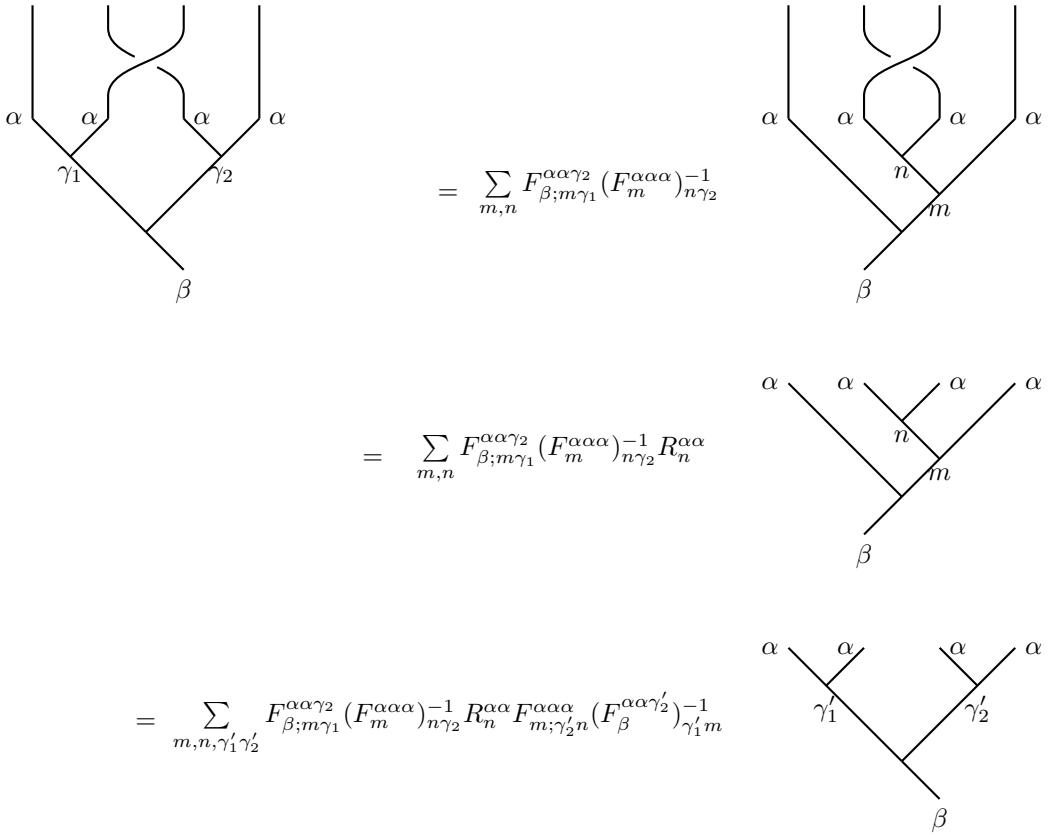


Figure 40: The action of σ_2.

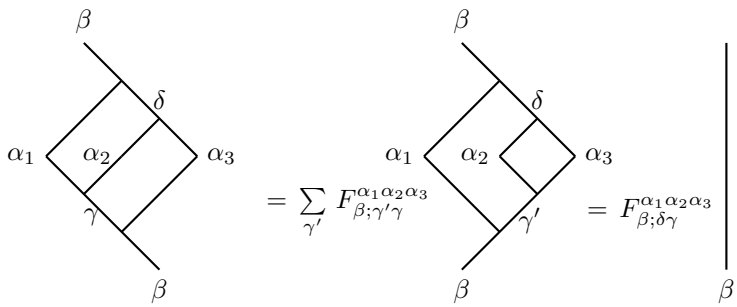


Figure 41: Expressing the F-symbols in terms of splitting/fusion channels.

(C,χ)		basis	dimension	matrix of A_μ	matrix of A_σ
C_1	$[+]$	$\|+\rangle$	1	(1)	(1)
	$[-]$	$\|-\rangle$	1	(1)	(-1)
	$[2]$	$\|2_+\rangle, \|2_-\rangle$	2	$\begin{pmatrix}\omega & 0\\ 0 & \bar\omega\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
C_2	$[1]$	$\|(12)\rangle, \|(23)\rangle, \|(13)\rangle$	3	$\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{pmatrix}$
	$[-1]$	$\|(12),-\rangle, \|(23),-\rangle, \|(13),-\rangle$	3	$\begin{pmatrix}0 & 0 & 1\\ -1 & 0 & 0\\ 0 & -1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 0 & -1\\ 0 & -1 & 0\\ -1 & 0 & 0\end{pmatrix}$
C_3	$[1]$	$\|(123)\rangle, \|(132)\rangle$	2	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
	$[\omega]$	$\|(123),\omega\rangle, \|(132),\omega\rangle$	2	$\begin{pmatrix}\omega & 0\\ 0 & \bar\omega\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
	$[\bar\omega]$	$\|(123),\bar\omega\rangle, \|(132),\bar\omega\rangle$	2	$\begin{pmatrix}\bar\omega & 0\\ 0 & \omega\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$

Table 5: Irreps of DS_3 where $\omega = \omega_3$.

general, the F-symbols are obtained by solving certain equations (to be discussed later). However, in the case of quantum double model, they can be computed directly from the data of splitting/fusion channels. Explicitly, this is illustrated in Figure 41, namely $F^{\alpha_1\alpha_2\alpha_3}_{\beta;\delta\gamma}$ is the unique scalar such that the first term in Figure 41 is equal to $F^{\alpha_1\alpha_2\alpha_3}_{\beta;\delta\gamma}$ times id_β.

As an illustration, we show how to compute the splitting/fusion channels and R-symbols for $G = S_3$. Recall that $D(S_3)$ has eight in-equivalent irreps. For convenience, we copy the table of irreps of $D(S_3)$ from a previous lecture. Denote the eight irreps in the order of appearance in Table 5 by A, B, C, D, E, F, G, H, respectively. Figuring out the fusion rules requires knowledge of representation theory. Here we simply work out a specific example. For a complete set of data on $D(S_3)$, see [8].

Take the irrep F corresponding to the conjugacy class $C_3 = \{\mu = (123), \bar\mu = (132)\}$. It has an orthonormal basis $\{|\mu\rangle, |\bar\mu\rangle\}$. We claim

$$F \otimes F = A \oplus B \oplus F. \tag{115}$$

The splitting channels are defined in Equations 116,117, and 118.

$$\begin{aligned}
\phi_A^{FF}: \quad A &\longrightarrow & F\otimes F \\
|+\rangle &\longmapsto & \frac{1}{\sqrt{2}}(|\mu,\bar{\mu}\rangle + |\bar{\mu},\mu\rangle). \qquad (116)\\
\phi_B^{FF}: \quad B &\longrightarrow & F\otimes F \\
|-\rangle &\longmapsto & \frac{1}{\sqrt{2}}(|\mu,\bar{\mu}\rangle - |\bar{\mu},\mu\rangle). \qquad (117)\\
\phi_F^{FF}: \quad F &\longrightarrow & F\otimes F \\
|\mu\rangle &\longmapsto & |\bar{\mu},\bar{\mu}\rangle \\
|\bar{\mu}\rangle &\longmapsto & |\mu,\mu\rangle. \qquad (118)
\end{aligned}$$

Recall that the braiding has the following transformation on $F\otimes F$:

$$\begin{aligned}
c_{F,F}: \quad F\otimes F &\longrightarrow & F\otimes F \\
|c_1,c_2\rangle &\longmapsto & |c_2, c_2c_1\bar{c}_2\rangle. \qquad (119)
\end{aligned}$$

Since the two elements $\mu, \bar{\mu}$ in C_3 commute, the above map is simply the swap map: $|c_1,c_2\rangle \mapsto |c_2,c_1\rangle$. We obtain that

$$R_A^{FF} = R_F^{FF} = 1, \quad R_B^{FF} = -1. \qquad (120)$$

Unfortunately, the computational power of braiding in the quantum double is limited for any finite group G. It is a theorem of [10] that the image of the braiding on the space $\mathrm{Hom}(\beta, \alpha^{\otimes n})$ is always a finite group for any α, β and n. This implies one always gets a finite set of quantum gates by braiding, which is of course not universal. To obtain universality, we either need to introduce extra resources such as ancilla and special measurement or use anyon models beyond the quantum double model. This is will be discussed in next section.

8 Unitary Modular Tensor Category(UMTC)

We give a minimal introduction to the notion of a unitary modular tensor category (UMTC), which is the algebraic structure describing a general anyon system. Apart from applications in topological quantum computing, UMTCs are also central in a number of subjects such as 3-dimensional topological quantum field theories, 2-dimensional conformal field theories, representation of quantum groups, etc. For aspects of UMTCs related with topological quantum computing and anyon systems, see [15, 5, 20, 17]. A UMTC can be defined abstractly within the framework of fusion categories. See, for instance, [2, 18]. However, the formalism involved is rather complicated and would be too much distraction to go through. Rather, we follow the approach in [15, 3] to define a UMTC in a concrete manner, building a direct connection with anyon systems. The downside of this approach is that certain properties which are obvious in the framework of fusion categories are highly nontrivial in the discrete setup. Readers who are interested in learning UMTCs to some depth are suggested to refer to some of the math literature such as [20].

Roughly, UMTCs are characterized by a set of data satisfying certain rules. The rules are to be obeyed by all anyon systems, and are also complete in the sense that any set of data satisfying these rules determines an anyon system. A UMTC is any particular set of data satisfying these rules, and thus corresponds to a particular anyon system.

Label set. First of all, a UMTC contains a label set

$$L = \{a, b, c, \cdots\}, \tag{121}$$

which describes all possible anyon types in an anyon system. L assumed to be a finite set. There is a special type in L, denoted by $\mathbf{1}$, which represents the ground state or the vacuum. Also, for each type $a \in L$, there is a unique type $\bar{a} \in L$ dual to a. The $\bar{a}$ is characterized as the unique type such that a and $\bar{a}$ can be combined to produce $\mathbf{1}$. It is natural to require that

$$\bar{\bar{a}} = a, \text{ and } \bar{\mathbf{1}} = \mathbf{1}. \tag{122}$$

If $\bar{a} = a$, we say a is self dual.

Fusion rules. For any two types $a, b \in L$, their combined type or total charge is formally written as

$$a \otimes b = \bigoplus_{c \in L} N_{ab}^c \, c, \tag{123}$$

where N_{ab}^c is a non-negative integer representing the possible ways of combining a and b to obtain c. *For simplicity, we assume N_{ab}^c is either 0 or 1, but note that there are anyon systems for which N_{ab}^c could be greater than one.* A theory with this property is called multiplicity free. If $N_{ab}^c = 1$, then c is called a total charge of a and b, and there is a unique channel of combining a and b to produce a type c. We call the triple (a, b, c) *admissible* in this case. We emphasize that the '$\otimes$' and '$\bigoplus$' in the above equation are treated as formal operations, although they can be defined to function as what they originally mean. Also note that some authors write '$\times$' and '$\sum$' to replace '$\otimes$' and '$\bigoplus$', respectively. The numbers N_{ab}^c's are called fusion rules.

Some natural properties need to be satisfied for the fusion rules if they describe an anyon system. The total charge of a and b should be the same as that of b and a. That is, formally, $a \otimes b = b \otimes a$, implying

$$N_{ab}^c = N_{ba}^c, \quad \forall a, b, c. \tag{124}$$

If c is a total charge of a and b, then $\bar{c}$ is a total charge of $\bar{a}$ and $\bar{b}$,

$$N_{ab}^c = N_{\bar{a}\bar{b}}^{\bar{c}}, \quad \forall a, b, c. \tag{125}$$

The total charge of $\mathbf{1}$ and a should always be a, implying

$$N_{\mathbf{1}a}^b = \delta_{a,b}, \quad \forall a, b. \tag{126}$$

As mentioned in the definition of a dual type, in order for the total charge of a and b to possibly be $\mathbf{1}$, a and b have to be dual to each other, and hence

$$N_{ab}^{\mathbf{1}} = \delta_{a,\bar{b}}, \quad \forall a, b. \tag{127}$$

Also, we require the fusion rules to be 'associative' whose meaning is as follows. If we want to combine three anyons a, b, and c to produce an anyon d, we can either combine a, b first to produce an intermediate anyon p followed by combining p, c to produce d, or combining b, c first to produce an intermediate q followed by combining a, q to produce d. The number of different ways to combining a, b, c to produce d is equal to the number of all possible p's, as well as to the number of all possible q's. It is reasonable to require these two numbers to be the same. Therefore, we have

$$\sum_{p\in L} N_{ab}^{p} N_{pc}^{d} = \sum_{q\in L} N_{aq}^{d} N_{bc}^{q}, \quad \forall a, b, c, d, \tag{128}$$

or written formally, $(a \otimes b) \otimes c = a \otimes (b \otimes c)$. It is not hard to check the above equation actually guarantees that for an arbitrary number of anyons the total number of ways of combining them into a single anyon does not depend on the specific ordering in which the anyons are combined. To summarize, the fusion rules are required to satisfy Equations 124 - 128.

Remark 8.1. Equations 124 - 128 impose many degrees symmetries on fusion rules. As an exercise, one can show the following,

$$N_{ab}^{c} = N_{c\bar{b}}^{a} = N_{c\bar{a}}^{b} = N_{\bar{c}a}^{\bar{b}} = N_{\bar{c}b}^{\bar{a}} = N_{\bar{a}\bar{b}}^{\bar{c}}. \tag{129}$$

One can of course swap the two lower indexes in any of the $N_{\cdot\cdot}^{\cdot}$ terms in the above equation.

Hilbert space of states and splitting/fusion tree bases. If $N_{ab}^{c} = 1$, there is a splitting channel ϕ_c^{ab} which creates a pair of anyons a and b from their total charge c. One can think that for any state $|\psi_c\rangle$ representing the anyon c, the channel creates a state $\phi_c^{ab}|\psi_c\rangle$ representing the two anyons a and b. The state $|\psi_c\rangle$ is interpreted as the internal degrees of the anyon c and is suppressed in the formalism of UMTCs. Hence, one can also think of the channel itself as a quantum state representing a pair of anyons a and b whose total charge is c. We will use these two interpretations interchangeably. Denote by V_c^{ab} the space of states corresponding to two anyons a and b with total charge c. V_c^{ab} has dimension 1 if c is indeed a total charge, and 0 otherwise. In the former case, a basis element in V_c^{ab} is given by ϕ_c^{ab}, whose graphical representation is shown in Figure 42 (Middle). More generally, denote by $V_c^{a_1 a_2 \cdots a_n}$ the space of states representing n anyons $a_1, \cdots, a_n$, whose total charge is c. An orthonormal basis of $V_c^{a_1 a_2 \cdots a_n}$ is specified by a splitting tree. See Figure 43. The splitting tree in Figure 43(Left) represents a state in $V_c^{a_1 \cdots a_4}$ such that the total charge of a_1, a_2 is b_1, the total charge of b_1, a_3 is b_2, and the total charge of b_2, a_4 is c. By varying all possible intermediate b_1, b_2, we obtain an orthonormal basis of $V_c^{a_1 \cdots a_4}$. Thus the dimension of $V_c^{a_1 \cdots a_4}$ is

$$\sum_{b_1, b_2} N_{a_1 a_2}^{b_1} N_{b_1 a_3}^{b_2} N_{b_2 a_4}^{c}. \tag{130}$$

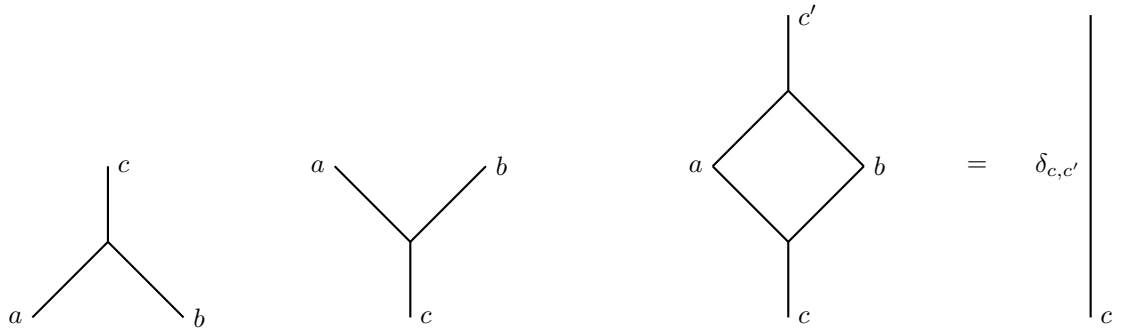


Figure 42: (Left) the fusion channel ϕ_{ab}^{c}; (Middle)the splitting channel ϕ_{c}^{ab}; (Right) the normalization condition.

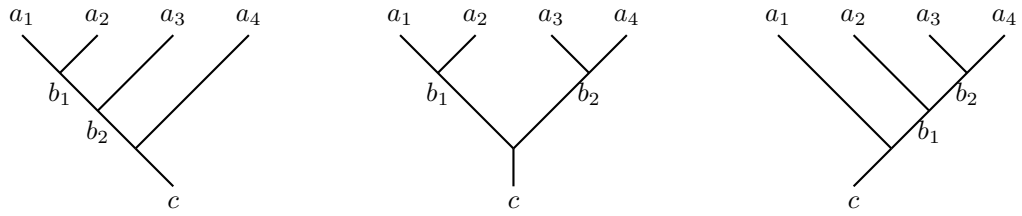


Figure 43: Three splitting tree bases for the space $V_c^{a_1\cdots a_4}$.

Another splitting tree such as the one in Figure 43 (Middle) gives a different orthonormal basis, from which the count for the dimension of $V_c^{a_1\cdots a_4}$ is equal to

$$\sum_{b_1,b_2} N_{a_1a_2}^{b_1} N_{a_3a_4}^{b_2} N_{b_1b_2}^{c}. \tag{131}$$

It is not surprising that Equation 128 guarantees that Equation 130 and Equation 131 give the same number, and actually guarantees that from any splitting tree one gets the same count of the dimension. An basis specified a splitting tree is called a splitting tree basis. In general, one formula expressing the dimension of $V_c^{a_1\cdots a_n}$ (with the splitting tree in Figure 44(Left)) is

$$\sum_{b_1,\cdots,b_{n-2}} N_{a_1a_2}^{b_1} N_{b_1a_3}^{b_2} \cdots N_{b_{n-2}a_n}^{c}. \tag{132}$$

If $N_{ab}^{c} = 1$, there is also a 1-dimensional Hilbert space V_{ab}^{c} spanned by the fusion channel ϕ_{ab}^{c} as shown in Figure 42(Left). V_{ab}^{c} is dual to V_{c}^{ab} in the sense that $\phi_{ab}^{c'}\phi_{c}^{ab} = \delta_{c,c'} id_c$, where id_c is interpreted as the identity channel on c. Graphically, this is illustrated in Figure 42 (Right), where a vertical line with a label a represents the identity process on a. More generally, there is a Hilbert space $V_{a_1\cdots a_n}^{c}$ spanned by fusion channels dual to $V_c^{a_1\cdots a_n}$. A basis of $V_{a_1\cdots a_n}^{c}$ is given by first choosing a fusion tree (See Figure 44(Right)) and then varying all intermediate anyons. Any such basis is called a fusion tree basis. If we have a state $|\psi\rangle \in V_c^{a_1\cdots a_n}$ and fuse the n anyons from left to right, then the amplitude for obtaining the intermediate anyons $b_1', \cdots, b_{n-2}'$ is given by applying the fusion channel in Figure 44(Right) with the specific $b_1', \cdots, b_{n-2}'$ on its internal edges to the state $|\psi\rangle$.

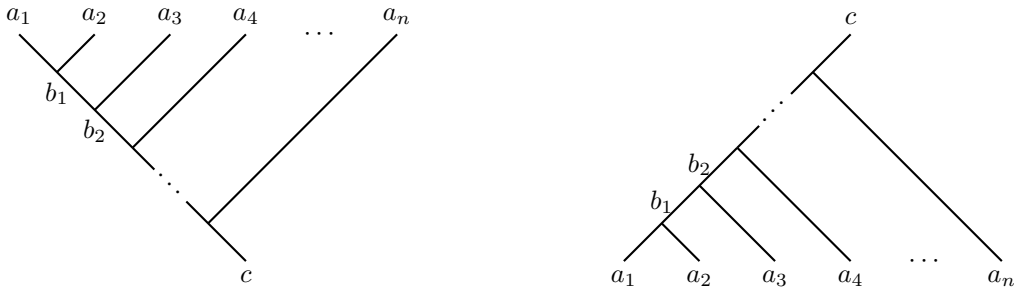


Figure 44: (Left) a splitting tree for the space $V_c^{a_1\cdots a_n}$; (Right) a fusion tree for the space $V_{a_1\cdots a_n}^c$

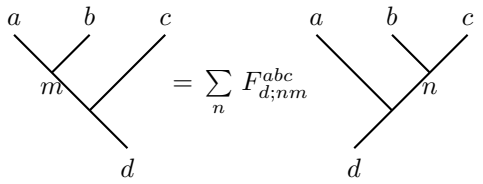


Figure 45: The F-matrix relating two bases.

F-symbols. The space V_d^{abc} has two sets of orthonormal bases given respectively by the two splitting trees shown on either side of the equation in Figure 45. Hence, we can express each state in one basis as a linear combination of the states in the other basis. Denote by F_d^{abc}, called an F-matrix, the unitary matrix relating the two bases. Explicitly, the definition of F_d^{abc} is shown in Figure 45, where $F_{d;nm}^{abc}$ denotes the (n, m) matrix element of F_d^{abc}, and is called an F-symbol or $6j$-symbol. Note that here n, m are labels of anyon types. In particular, m ranges over all types for which (a, b, m) and (m, c, d) are both admissible, and n ranges over all types for which (b, c, n) and (a, n, d) are both admissible. If either m or n violates the above constraints, we define $F_{d;nm}^{abc} = 0$. We call the change from one basis to the other an F-move. Straightly speaking, there are two types of F-moves inverse to each other depending on which basis to start with. Some authors call the transformation in Figure 45 an F-move and call the inverse transformation an inverse F-move.

The F-symbols need to satisfy some consistency conditions. Consider the space V_e^{abcd}. There are in total five splitting tree bases. One can convert one to another by a sequence of F-moves. But there are different sequences of F-moves achieving this purpose. It is natural to require that different sequences of F-moves give the same transformation. More precisely, in the space V_e^{abcd}, to convert one basis to another, there are exactly two sequences of F-moves. See Figure 46. To convert the splitting tree basis labeled by ① to the basis labeled by ③, one can follow either the path ① → ② → ③ or the path ① → ⑤ → ④ → ③. Denote by $|ⓘ; x, y\rangle$ the basis state in the basis labeled by ⓘ. For example, $|①; m, n\rangle$, $|③; z, y\rangle$, and $|④; x, y\rangle$ represent the basis states shown in Figure 45 corresponding to the bases ①, ③,

and ④, respectively. Then following the path ① → ② → ③, we have

$$\begin{aligned}|①; m, n\rangle &= \sum_z F^{mcd}_{e;zn} |②; m, z\rangle \\ &= \sum_{y,z} F^{mcd}_{e;zn} F^{abz}_{e;ym} |③; z, y\rangle. \end{aligned} \tag{133}$$

And following the path ① → ⑤ → ④ → ③, we have

$$\begin{aligned}|①; m, n\rangle &= \sum_x F^{abc}_{n;xm} |⑤; x, n\rangle \\ &= \sum_{x,y} F^{abc}_{n;xm} F^{axd}_{e;yn} |④; x, y\rangle \\ &= \sum_{x,y,z} F^{abc}_{n;xm} F^{axd}_{e;yn} F^{bcd}_{y;zx} |③; z, y\rangle \end{aligned} \tag{134}$$

By requiring these two sequences to give the same transformation, we arrive at the following equation, known as Pentagon Equation.

$$F^{mcd}_{e;zn} F^{abz}_{e;ym} = \sum_{x \in L} F^{abc}_{n;xm} F^{axd}_{e;yn} F^{bcd}_{y;zx}, \quad \forall a, b, c, d, e, m, n, y, z. \tag{135}$$

In general, it is a very hard problem to solve the equation. The Pentagon Equation makes the F-moves consistent not only for the case of four anyons a, b, c, d, but also for the case of arbitrary n anyons. Namely, any two sequences of F-moves relating one splitting tree basis to another give the same transformation. This is known as MacLane Coherence Theorem.

R-symbols. Consider the state (or channel) $\phi_c^{ab} \in V_c^{ab}$, if we swap (or braid) a and b counterclockwise, this should not change the total charge of a and b, but it will change ϕ_c^{ab} to ϕ_c^{ba} times a phase denoted by R_c^{ba}. We call R_c^{ba} an R-symbol. Graphically, see Figure 47(Left) for the definition of R_c^{ba}. A clockwise braiding followed immediately by a counterclockwise braiding should fix the initial state. Hence a clockwise braiding applied to ϕ_c^{ab} is equal to ϕ_c^{ba} times the phase $(R_c^{ab})^{-1}$. See Figure 47(Right). We call the transformation in either left or right of Figure 47 an R-move. There are also consistency conditions that need to be imposed on the R-symbols introduced below.

The effect of braiding an anyon d with a followed by braiding d with b should be the same as that of braiding d with (a, b) as a composite particle. The effect of the latter should be, in turn, the same as that of braiding of d with c if the combined pair (a, b) behaves like c. Combining the above two assumptions, we derive the equality in Figure 48, which means braiding commutes with the splitting process. Graphically, this means one can always slide an edge representing a braiding process through a vertex. To see what restrictions this equality imposes on R-symbols, consider the transformations in Figure 49. Each splitting tree in the figure represents a basis in the space V_d^{bca}. To convert the basis labeled by ① to the basis labeled by ④, there are two sequences of F/R-moves: ① → ② → ③ → ④ and ① → ⑥ → ⑤ → ④. And it is natural to require these two sequences of moves produce the

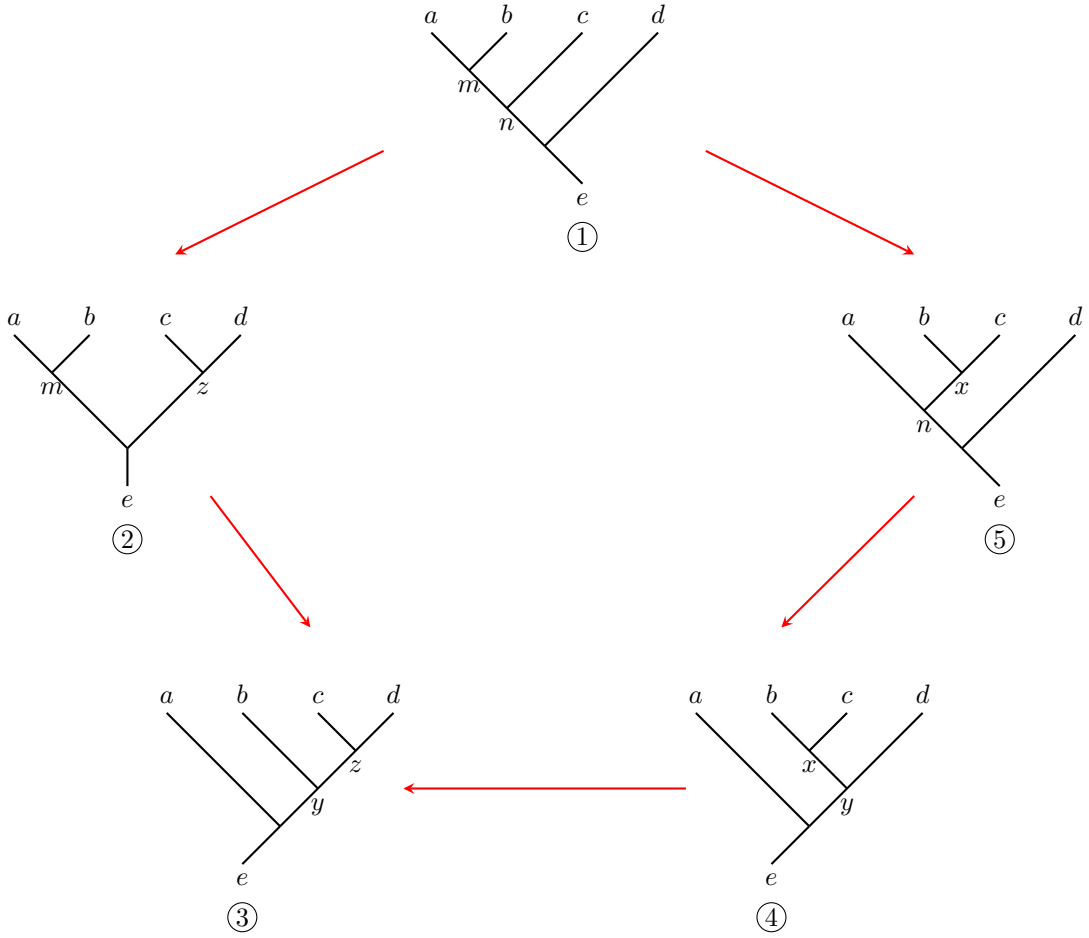


Figure 46: Consistency condition for F-moves.

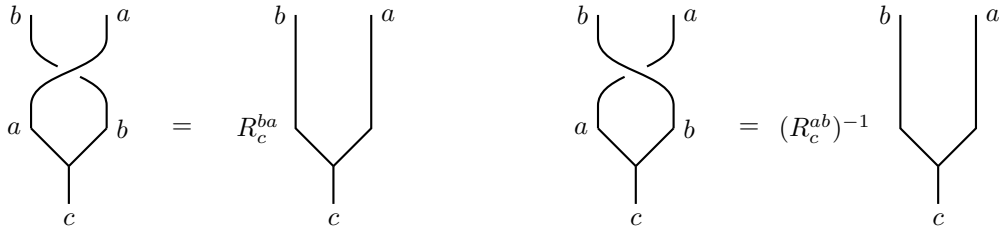


Figure 47: (Left) A counterclockwise swap (braiding) of a and b; (Right) A clockwise swap of a and b

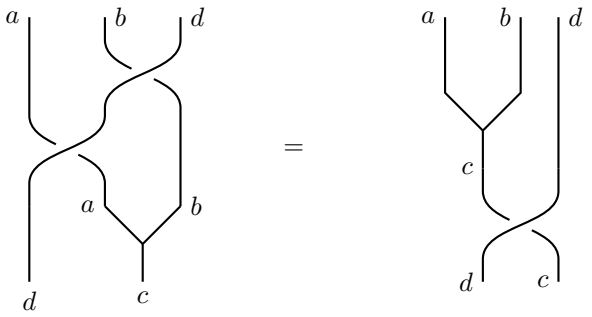


Figure 48: The equality shows that the splitting process commutes with braiding.

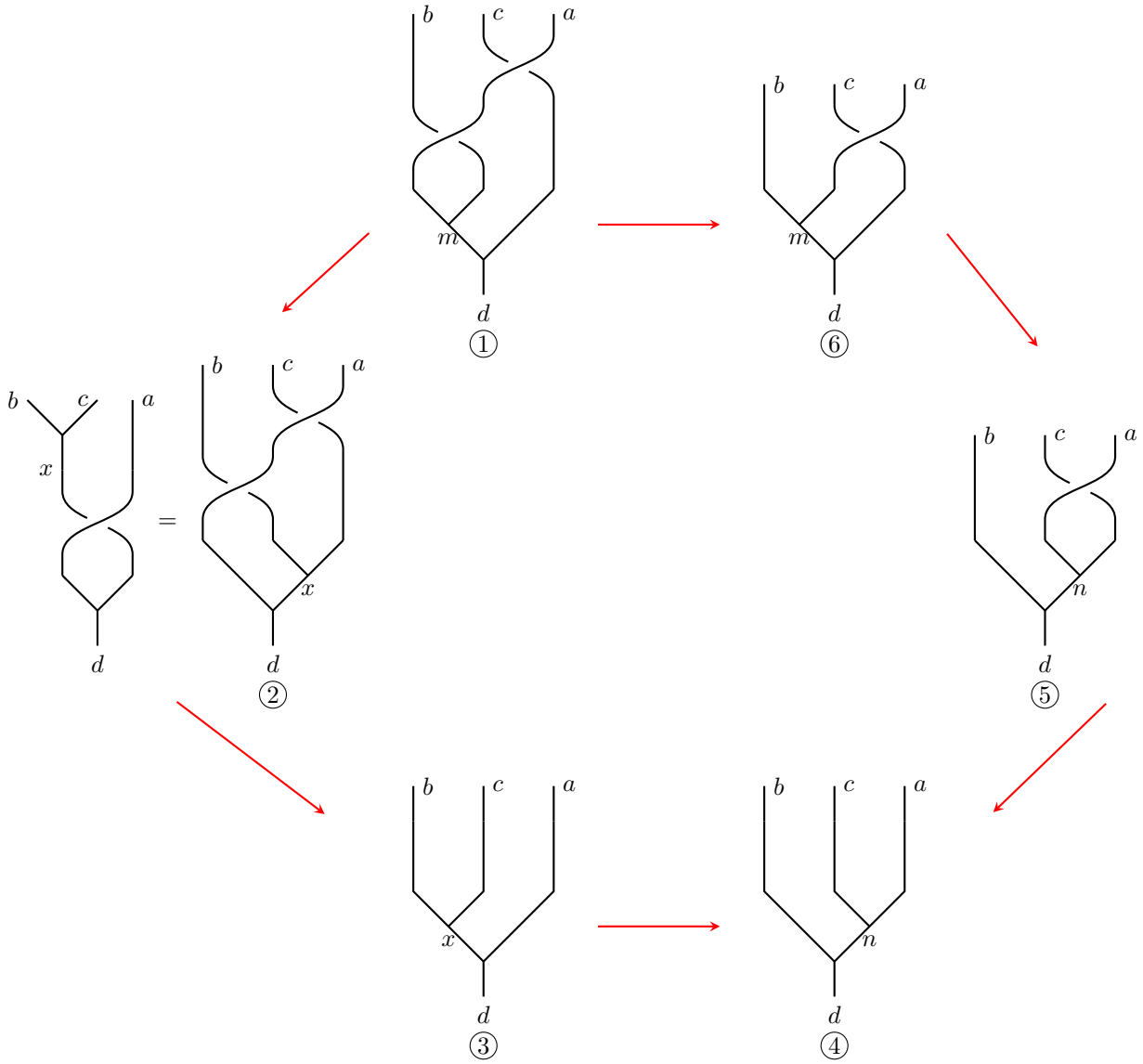


Figure 49: Consistency for R-symbols

same transformation. For the sequence ① → ② → ③ → ④, the transformation is given by,

$$\begin{aligned}|①; m\rangle &= \sum_x F^{abc}_{d;xm}|②; x\rangle \\ &= \sum_x F^{abc}_{d;xm} R^{xa}_d |③; x\rangle \\ &= \sum_x F^{abc}_{d;xm} R^{xa}_d F^{bca}_{d;nx} |④; n\rangle. \end{aligned} \tag{136}$$

For the sequence ① → ⑥ → ⑤ → ④, we have

$$\begin{aligned}|①; m\rangle &= R^{ba}_m |⑥; m\rangle \\ &= \sum_n R^{ba}_m F^{bac}_{d;nm} |⑤; n\rangle \\ &= \sum_n R^{ba}_m F^{bac}_{d;nm} R^{ca}_n |④; n\rangle \end{aligned} \tag{137}$$

Hence we arrive at the Hexagon Equation:

$$R^{ba}_m F^{bac}_{d;nm} R^{ca}_n = \sum_{x\in L} F^{abc}_{d;xm} R^{xa}_d F^{bca}_{d;nx}. \tag{138}$$

By replacing the counterclockwise braidings in Figure 49 with clockwise braidings, we obtain another Hexagon Equation:

$$(R^{ab}_m)^{-1} F^{bac}_{d;nm} (R^{ac}_n)^{-1} = \sum_{x\in L} F^{abc}_{d;xm} (R^{ax}_d)^{-1} F^{bca}_{d;nx}. \tag{139}$$

Again it is a theorem that the Hexagon Equations also guarantee the consistency of braiding one anyon with a group of anyons viewed either as a single braiding with the group or as a sequence of braidings with each member of the group.

Rigidity and quantum dimension. We introduce a convention that if in a splitting/fusion tree an edge is labeled by the vacuum $\mathbf{1}$, then we can also erase that edge (together with its label.) For example, see Figure 50 and 51. However, the trees in Figure 50 can also be related by F-moves. To make the convention consistent, the involved F-moves have to equal the identity transformation. It is not hard to see that this is equivalent to the condition,

$$F^{abc}_d = (1)\,, \text{ whenever } a, b, \text{ or } c \text{ is } \mathbf{1}. \tag{140}$$

Note that if one of a, b, c is $\mathbf{1}$, then the rest two together with d need to be admissible. A similar argument on braidings requires the condition,

$$R^{\mathbf{1}a}_a = R^{a\mathbf{1}}_a = 1. \tag{141}$$

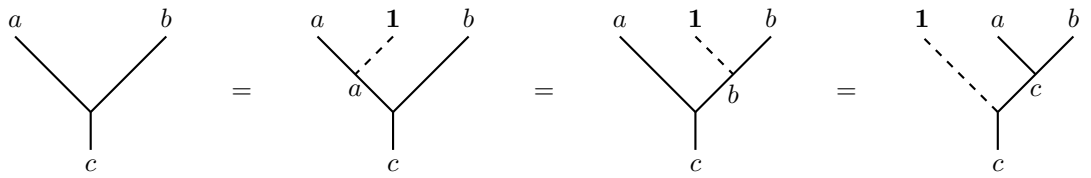


Figure 50: Conventions for erasing edges with label **1**

Figure 51: Conventions for erasing edges with label **1**

Now consider the two processes shown in Figure 52. The first process starts with an anyon a, creates a pair $(a, \bar{a})$ on the left, and fuses $\bar{a}$ with the original a. The amplitude of this process is given by $F^{a\bar{a}a}_{a;\mathbf{11}}$. The second process has a similar interpretation but starts with the anyon $\bar{a}$, the amplitude of which is $G^{\bar{a}a\bar{a}}_{\bar{a};\mathbf{11}}$, where $G^{\bar{a}a\bar{a}}_{\bar{a}}$ denotes the matrix $(F^{\bar{a}a\bar{a}}_{\bar{a}})^{-1}$. We require the two processes to have the same nonzero amplitude:

$$F^{a\bar{a}a}_{a;\mathbf{11}} = G^{\bar{a}a\bar{a}}_{\bar{a};\mathbf{11}} \neq 0. \tag{142}$$

Remark 8.2. In fact, it suffices to require $F^{a\bar{a}a}_{a;\mathbf{11}} \neq 0$. In [9], it is shown that the equality $F^{a\bar{a}a}_{a;\mathbf{11}} = G^{\bar{a}a\bar{a}}_{\bar{a};\mathbf{11}}$ can be derived as a consequence.

Note that each F-matrix is a unitary matrix, hence $G^{\bar{a}a\bar{a}}_{\bar{a}} = (F^{\bar{a}a\bar{a}}_{\bar{a}})^{\dagger}$. Let $\phi_a := (F^{a\bar{a}a}_{a;\mathbf{11}})^{-1}$, then we have

$$\overline{\phi_a} = \phi_{\bar{a}}, \tag{143}$$

where the first $\bar{(\cdot)}$ in the above equation means complex conjugation, while the second means taking the dual. Define

$$d_a := |\phi_a|, \tag{144}$$

where d_a is called quantum dimension of a whose meaning is to be justified later. Clear we have $d_{\mathbf{1}} = 1$ and $d_a = d_{\bar{a}}$. We further introduce some notations as shown in Figure 53. Roughly, we scale the creation process from the vacuum and the fusion process to the vacuum. For the creation process (as well as the fusion process), there are two versions of scaling depending on the arrow. One can think of the arrow as specifying a direction on the arc. The rule for interpreting the labels at the two ends of an arc is as follows. *If the arc itself is labeled by a as the ones in Figure 53, then the end of the arc is labeled by a if the direction near the end is pointing downwards, and is labeled by $\bar{a}$ if the direction is pointing upwards.* These scalings are chosen so that the equalities in Figure 54 and 55 hold. That is, a circle labeled by a with either direction is equal to d_a. The equalities in Figure 55 are

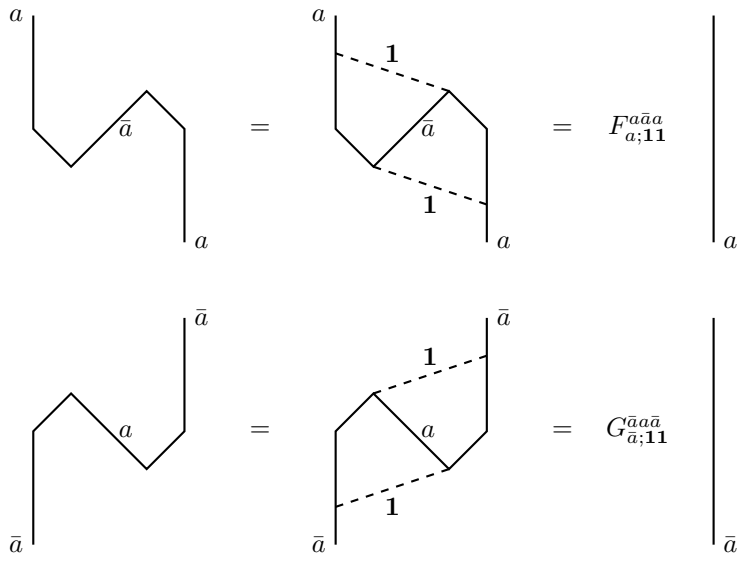


Figure 52: Two proceses both starting and ending with a single anyon a. Here $G^{\bar{a}a\bar{a}}_{\bar{a}}$ denotes $(F^{\bar{a}a\bar{a}}_{\bar{a}})^{-1}$.

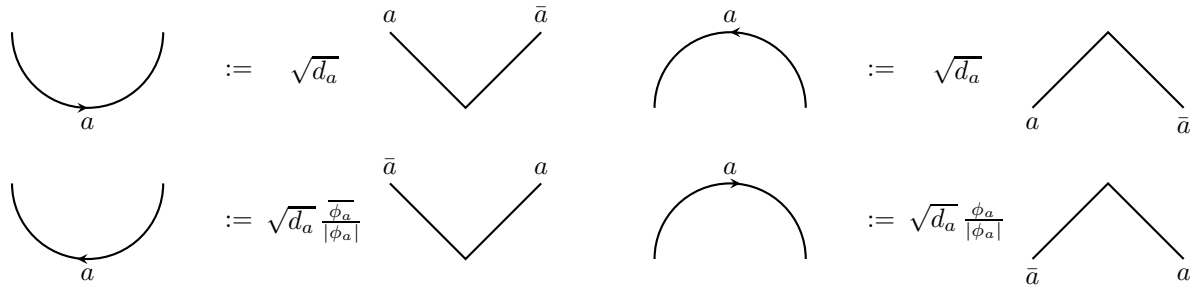


Figure 53: Some notations

known as rigidity properties. Note that a vertical string with upward direction labeled by a represents the identity process on $\bar{a}$. The rigidity properties mean that the identity process is 'topological'; one can isotope the trajectory as long as the arrow on the trajectory does not change direction.

We now give an interpretation of the quantum dimension d_a. For $a \in L$, define a $|L| \times |L|$ matrix N_a whose (b, c)-entry $(N_a)_{bc}$ is N^c_{ab}. Hence the entries of N_a are either 0 or 1. By the Perron-Frobenius theorem, N_a has an eigenvalue d'_a which is greater than or equal to, in absolute value, any other eigenvalues. We call d'_a the Frobenius-Perron dimension of a. It

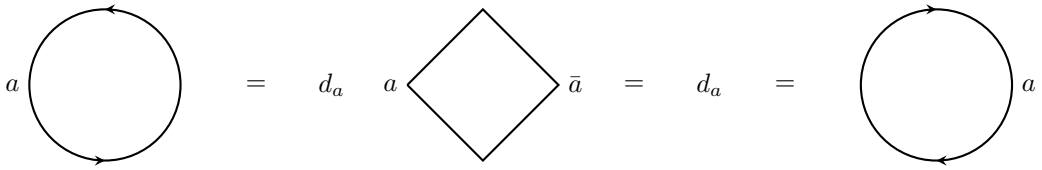


Figure 54: A circle labeled by a with either direction is equal to d_a.

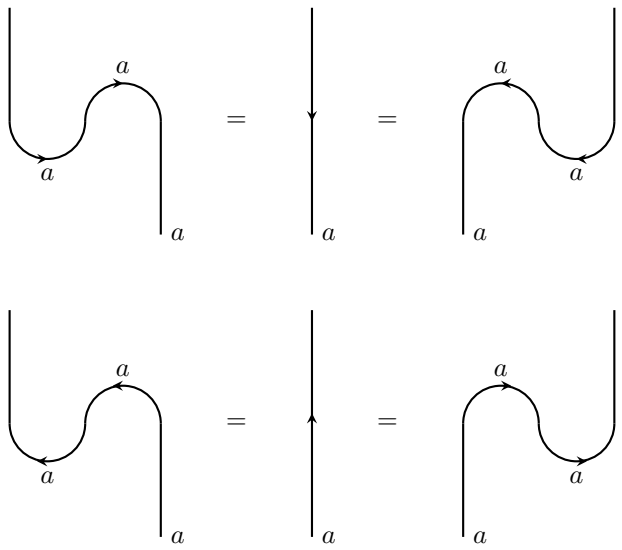


Figure 55: Rigidity proerties.

can be shown that $d_a = d'_a$. The dimension of $V_{\mathbf{1}}^{a^{\otimes n}}$ is (see Figure 44 (Left))

$$\sum_{b_1,\cdots,b_{n-2}} N_{aa}^{b_1} N_{b_1 a}^{b_2} \cdots N_{b_{n-3}a}^{b_{n-2}} N_{b_{n-2}a}^{\mathbf{1}} = \sum_{b_1,\cdots,b_{n-3}} N_{aa}^{b_1} N_{b_1 a}^{b_2} \cdots N_{b_{n-3}a}^{\bar{a}} \tag{145}$$

$$= \left((N_a)^{n-2}\right)_{a\bar{a}} \overset{n\to\infty}{\sim} d_a^{n-2}. \tag{146}$$

Thus, d_a measures the asymptotic size of the space of n type-a anyons with total charge trivial. d_a does not have to be an integer and generalizes the usual notion of dimension of a Hilbert space. In fact, it can be shown that for the anyons in the quantum double model of a group G, the quantum dimension of an anyon is indeed the dimension of the irrep of DG corresponding to that anyon. Here are some further properties of quantum dimension.

- $$d_a d_b = \sum_{c\in L} N_{ab}^c d_c. \tag{147}$$

- $d_a \geq 1$, and $d_a = 1$ if and only if a is Abelian, namely, $a \otimes \bar{a} = 1$.

T-matrix. For each $a \in L$, we define a scalar θ_a as shown in Figure 56(Left). Namely, $\frac{\theta_a}{d_a}$ is the amplitude the following process. Start with an anyon a, create a pair of anyons a and $\bar{a}$ from the vacuum on the right(this step is assumed to be deterministic.), braid the two type-a anyons counterclockwise, and finally fuse a and $\bar{a}$ into vacuum. θ_a is called the topological spin of a. Define T to be the $|L| \times |L|$ diagonal matrix with the (a, a)-entry to be θ_a. This is called the T-matrix. By closing up the process in Figure 56(Left) to a circle, we obtain the equality as shown on the right of that figure, which can also be viewed as a definition of θ_a (, which is also why the it is called θ).

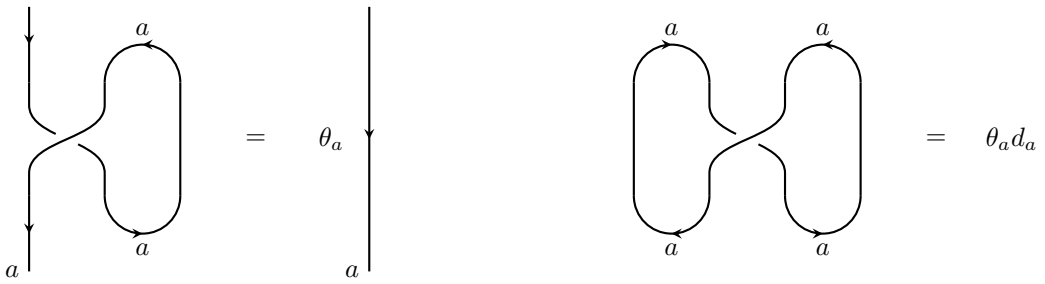


Figure 56: The definition of θ_a.

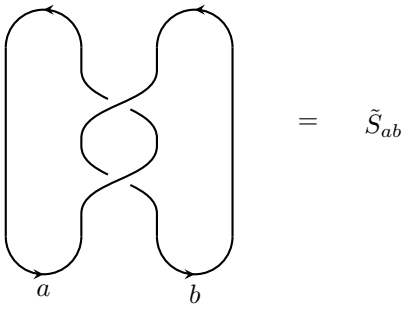


Figure 57: The definition of $\tilde{S}_{ab}$.

S-matrix. Similarly, for $a, b \in L$, define $\tilde{S}_{ab}$ to be amplitude shown in Figure 57. Let $\tilde{S}$ be the $|L| \times |L|$ matrix whose (a, b)-entry is given by $\tilde{S}_{ab}$. Also denote by $D = \sqrt{\sum_{a \in L} d_a^2}$. D is called the total dimension of the theory. Let $S = \frac{1}{D}\tilde{S}$, which we call the S-matrix. We require that,

$$\det(S) \neq 0. \tag{148}$$

To summarize, a UMTC is defined to be a set consisting of a label set L, the fusion rules, the F-symbols, and the R-symbols, satisfying rules we have given above. Specifically, the rules are classified in Table 6.

The S and T matrices are very important data of a UMTC. They satisfy very constraint conditions. We list some properties of them. See [20, 2] for their proof.

Theorem 8.3. 1. (Vafa) The T matrix has finite order, hence every θ_a is a root of unity.

Data	Rules
Label set with a convolution	Equation 122
Fusion rules	Equations 124 - 128.
F-symbols	Equations 135, 140, 142.
R-symbols	Equations 138, 139, 141.
S-matrix	Equation 148

Table 6: Rules defining a UMTC.

2. (Verlinde formula):

$$N_{ij}^k = \sum_r \frac{S_{ir} S_{jr} S_{\bar{k}r}}{S_{\mathbf{1}r}}. \tag{149}$$

3. $S^4 = id$, $(ST)^3 = \lambda S^2$, for some scalar λ. Hence S and T defines a projective representation of $\mathrm{SL}_2(\mathbb{Z})$.

9 Unitary Modular Tensor Category(UMTC) II

We have defined a UMTC in terms of a set of discrete data satisfying certain rules. Now we look at some examples of UMTCs and examine their power in terms of topological quantum computing.

We first set up some conventions. In any anyon theory, there is a particular type $\mathbf{1}$, the vacuum. The total charge of $\mathbf{1}$ with any anyon a is still a. So we will not mention this rule explicitly. Also, since $a \otimes b = b \otimes a$, only one of them will be listed for each example below. We call an F-symbol or an R-symbol trivial if it is defined[2] and is equal to 1. All the trivial F-symbols and trivial R-symbols will be omitted.

Toric code. The first anyon system we encountered is the toric code, which corresponds to the quantum double model for the group $\mathbb{Z}_2$.

- Label set $L = \{\mathbf{1}, e, m, em\} \longleftrightarrow \{(0,0),(1,0),(0,1),(1,1)\} = \mathbb{Z}_2 \times \mathbb{Z}_2$; $\bar{a} = a$.
- Fusion rules $a \otimes b = (a+b) \mod 2$.
- All F-symbols are trivial.
- Quantum dimension: for any a, $d_a = 1$; total quantum dimension $D = 2$.
- R-symbols $R_{a+b}^{a,b} = (-1)^{a_1 b_2}$, $a = (a_1, a_2), b = (b_1, b_2) \in \mathbb{Z}_2 \times \mathbb{Z}_2$.
- $\theta_a = (-1)^{a_1 a_2}$, $S_{ab} = \frac{1}{2}(-1)^{a_1 b_2 + a_2 b_1}$.

Thus all the anyons in toric code are Abelian as we have seen before. Note that $R_{\mathbf{1}}^{ee} = R_{\mathbf{1}}^{mm} = -R_{\mathbf{1}}^{em,em} = 1$, hence e and m are both bosons while em is a fermion.

Ising theory. There are several related but slightly different UMTCs that are called Ising theory. The following list of data corresponds to one of them.

- Label set $L = \{\mathbf{1}, \sigma, \psi\}$; $\bar{x} = x$.
- Fusion rules: $\psi \otimes \psi = \mathbf{1}$, $\psi \otimes \sigma = \sigma \otimes \psi = \sigma$, $\sigma \otimes \sigma = \mathbf{1} \oplus \psi$.
- The F-symbols are given in terms of F-matrices.

$$F_\sigma^{\psi\sigma\psi} = F_\psi^{\sigma\psi\sigma} = (-1), \quad F_\sigma^{\sigma\sigma\sigma} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{150}$$

[2]This means all involved triples (a, b, c) are admissible.

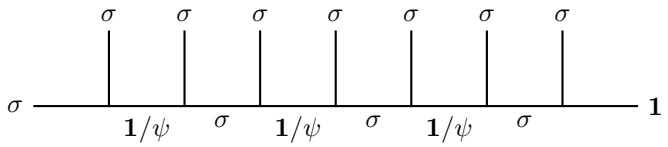


Figure 58: A splitting tree basis for $V_{\mathbf{1}}^{\sigma^{\otimes n}}$

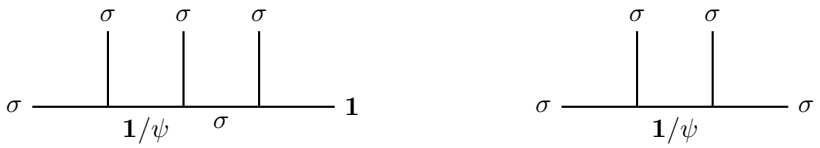


Figure 59: (Left) a splitting tree basis for $V_{\mathbf{1}}^{\sigma^{\otimes 4}}$;(Left) a splitting tree basis for $V_{\sigma}^{\sigma^{\otimes 3}}$.

- Quantum dimension $d_{\mathbf{1}} = d_\psi = 1$, $d_\sigma = \sqrt{2}$; $D = 2$.
- R-symbols: $R_{\mathbf{1}}^{\psi\psi} = -1$, $R_\sigma^{\psi\sigma} = R_\sigma^{\sigma\psi} = -i$, $R_{\mathbf{1}}^{\sigma\sigma} = e^{-\frac{\pi i}{8}}$, $R_\psi^{\sigma\sigma} = e^{\frac{3\pi i}{8}}$.
- $\theta_{\mathbf{1}} = 1$, $\theta_\psi = -1$, $\theta_\sigma = e^{\frac{2\pi i}{16}}$.

$$S = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix} \tag{151}$$

From the above list, we see that ψ is self dual and $R_{\mathbf{1}}^{\psi\psi} = -1$ means that swapping two ψ's change the state by a minus sign. Hence ψ is called a Majorana fermion. The σ particle is an non-Abelian anyon, called Ising anyon.

Let's look at some properties of the Ising anyon in terms of quantum computing. Consider the space $V_{\mathbf{1}}^{\sigma^{\otimes n}}$, namely, the space of n σ-anyons with total charge trivial. We choose a splitting tree for the space as shown in Figure 58, where, in contrast to the usual vertical alignment we draw the tree horizontally and the right end labeled by $\mathbf{1}$ is the root of the tree. From the fusion rules, it is direct to see that all possible labels for internal edges of the tree are the ones shown in Figure 58. That is, a $\mathbf{1}$ or ψ label and a σ label always alternate. Hence the dimension of $V_{\mathbf{1}}^{\sigma^{\otimes n}}$ is 0 if n is odd, and is $2^{\frac{n-2}{2}}$ if n is even. This means if n is even, $V_{\mathbf{1}}^{\sigma^{\otimes n}}$ has a natural tensor product structure to encode $\frac{n-2}{2}$ qubits. Each edge labeled by a $\mathbf{1}/\psi$ corresponds to a qubit. This tensor product structure is very rare in other anyon systems.

We can encode one qubit in either the space $V_{\mathbf{1}}^{\sigma^{\otimes 4}}$ or the space $V_{\sigma}^{\sigma^{\otimes 3}}$ (see Figure 59), which are isomorphic. We take the latter as example. The braiding matrices turn out to be the same to the two spaces. A label of $\mathbf{1}$ or $\mathbf{1}$ of the internal edge gives a basis. The set of quantum gates obtained from braiding are generated by two generators σ_1 and σ_2, where σ_i corresponds to braiding the i-th anyon with the $(i+1)$-th counterclockwise. Note that here the notation for the braiding σ_i has nothing to do with the particle σ. Apparently, the matrix for σ_1 is the diagonal matrix

$$\sigma_1 = \begin{pmatrix} R_{\mathbf{1}}^{\sigma\sigma} & 0 \\ 0 & R_\psi^{\sigma\sigma} \end{pmatrix} = e^{-\frac{\pi i}{8}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{152}$$

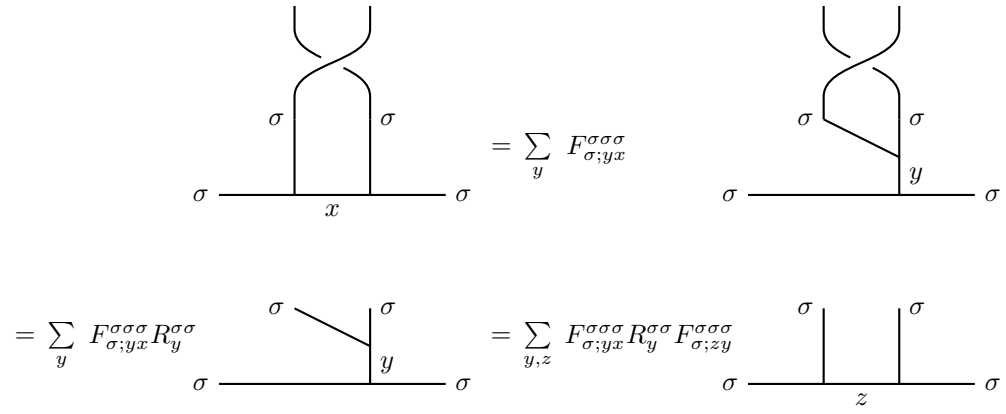


Figure 60: Caculation of the matrix of σ_2. Note that in the last step, an inverse F-move is performed. Thus we should apply the inverse of $F_\sigma^{\sigma\sigma\sigma}$. However, in this case $F_\sigma^{\sigma\sigma\sigma}$ is equal to its inverse.

Thus up to an unimportant scalar, σ_1 is the so-called phase gate. To compute σ_2, we need to first apply an F-move. See Figure 60 for the calculation. Let $F = F_\sigma^{\sigma\sigma\sigma}$ be the Hadamard matrix, then we have

$$\sigma_2 = F\sigma_1 F. \tag{153}$$

By direct calculations, we see that up to a global phase,

$$F = \sigma_1\sigma_2\sigma_1. \tag{154}$$

Hence the 1-qubit gates from braiding are generated by the phase gate σ_1 and the Hadamard gate F. It is well known that these two gates generate the 1-qubit Clifford group, which is stabilizer of the Pauli group. In fact, it is not hard to check that all n-qubit quantum gates obtained from braiding on $V_{\mathbf{1}}^{\sigma\otimes(2n+2)}$ form precisely the n-qubit Clifford group, which, as a group, is generated by the phase gate, the Hadamard gate, and the control-NOT gate. By Gottesman-Knill theorem [16], a quantum circuit only consisting of gates from the Clifford group can be efficiently simulated classically. Hence, the Ising anyon is not braiding universal.

Fibonacci theory. Let $\phi = \frac{1+\sqrt{5}}{2}$ be the golden ratio.

- Label set $L = \{\mathbf{1}, \tau\}$; $\bar{x} = x$.
- Fusion rules: $\tau \otimes \tau = \mathbf{1} \oplus \tau$.
- F-symbols:

$$F_\tau^{\tau\tau\tau} = \begin{pmatrix} \phi^{-1} & \sqrt{\phi^{-1}} \\ \sqrt{\phi^{-1}} & -\phi^{-1}. \end{pmatrix} \tag{155}$$

- Quantum dimension $d_{\mathbf{1}} = 1$, $d_\tau = \phi$; $D = \sqrt{1+\phi^2}$.
- R-symbols: $R_{\mathbf{1}}^{\tau\tau} = e^{-\frac{4\pi i}{5}}$, $R_\tau^{\tau\tau} = e^{\frac{3\pi i}{5}}$.

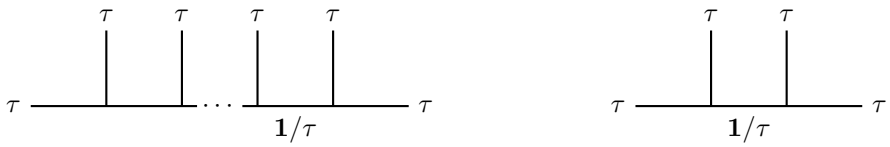


Figure 61: A splitting tree for $V_\tau^{\tau^{\otimes n}}$

- $\theta_{\mathbf{1}} = 1$, $\theta_\tau = e^{\frac{4\pi i}{5}}$.

$$S = \frac{1}{\sqrt{1+\phi^2}} \begin{pmatrix} 1 & \phi \\ \phi & 1 \end{pmatrix}. \tag{156}$$

Remark 9.1. In some references, the R-symbols are defined as the inverse of the ones given here. Changing R-symbols to their inverses corresponds to a "mirror image" of the theory, i.e., positive braiding is changes to negative braiding. Apparently, the group generated by all braiding matrices remain the same under such a change.

The theory contains only one nontrivial anyon τ which is non-Abelian. In this case, one can actually solve the Pentagon Equation and the Hexagon Equations fairly easily to find the solution [17]. Again let's check the properties of the τ anyon in the aspect of quantum computing.

First of all, let

$$a_n = \dim V_\tau^{\tau^{\otimes n}}, \quad b_n = \dim V_{\mathbf{1}}^{\tau^{\otimes n}}. \tag{157}$$

Clearly, $a_1 = 1, a_2 = 1$ and $b_n = a_{n-1}$. Choose the splitting tree as shown in Figure 61 as the basis for $V_\tau^{\tau^{\otimes n}}$. If the internal edge most close to the root is labeled by $\mathbf{1}$, then the number of possible labels of all other internal edges is equal to b_{n-1}. If that edge is labeled by τ instead, then the number of possible labels of all other internal edges is equal to a_{n-1}. Hence we have the recursion relation:

$$a_n = a_{n-1} + a_{n-2}, \tag{158}$$

and thus a_n is equal to the n-th Fibonacci number:

$$a_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n. \tag{159}$$

This explains the name of theory. Note that a_n is rarely a power of 2 and the space $V_\tau^{\tau^{\otimes n}}$ or $V_{\mathbf{1}}^{\tau^{\otimes n}}$ usually does not have a natural tensor product structure. We can encode one qubit in the space $V_\tau^{\tau^{\otimes 3}}$ with the basis given by the splitting tree shown in Figure 61. Then similar to the calculations in Ising theory, the 1-qubit gates are generated by

$$\sigma_1 = \begin{pmatrix} R_{\mathbf{1}}^{\tau\tau} & 0 \\ 0 & R_\tau^{\tau\tau} \end{pmatrix} = \begin{pmatrix} e^{-\frac{4\pi i}{5}} & 0 \\ 0 & e^{\frac{3\pi i}{5}} \end{pmatrix}, \text{ and } \sigma_2 = F\sigma_1 F, \tag{160}$$

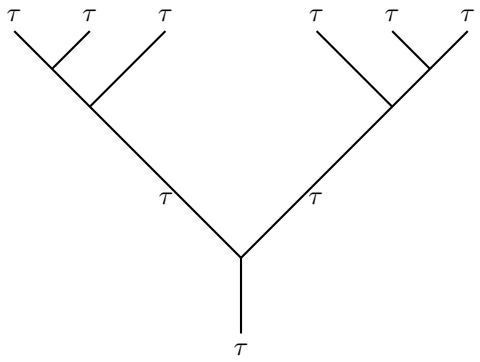


Figure 62: A sparse encoding of two qubits in the space of six τ-anyons.

where F is the only non-trivial $F_\tau^{\tau\tau\tau}$. Note that $\sigma_1^{10} = \sigma_2^{10} = id$, and σ_1, σ_2 generate a representation of the 3-strand braid group B_3. It can be shown that the image of this representation is a dense subgroup of $U(2)$, hence one can approximate any single qubit gate with a braid. More generally, it is a theorem of [11] that for arbitrary number n, the braidings on the space of n anyons of type τ with total charge $\mathbf{1}$ or τ generate a dense subgroup. Thus the Fibonacci theory is braiding universal.

There is not a natural way to encode several qubits, say k qubits, in the space of n τ anyons, since the dimension of the latter is usually not a power of 2. In practice, we have two encoding schemes, the dense encoding and the sparse encoding. For the dense encoding, one simply chooses some n large enough so that $2^k < \dim V_{\mathbf{1}}^{\tau^{\otimes n}}$, and takes any 2^k-dimensional subspace as the space of k-qubits. Since braidings can approximate arbitrary unitaries in the larger space, they can also approximate arbitrary unitaries of the k-qubit subspace. However, during the intermediate state, each individual braid may not preserve the k-qubit subspace, and one needs to think about the issues of information leakage. For the sparse encoding, we take $k = 2$ as an illustration. We encode one qubit in the space $V_\tau^{\tau^{\otimes 3}}$. Then there is a natural embedding

$$V_\tau^{\tau^{\otimes 3}} \otimes V_\tau^{\tau^{\otimes 3}} \subset V_\tau^{\tau^{\otimes 6}}, \tag{161}$$

shown in Figure 62. So the six τ anyons are partitioned into two groups, each group with three anyons. The first group encodes the first qubit, and the second group encodes the second qubit. In this way, this is a natural tensor product structure, and one can perform a single qubit braiding within each group. The problem now is that the space $V_\tau^{\tau^{\otimes 6}}$ is strictly larger than two qubits. Therefore, an arbitrary braiding, such as braiding the third with the fourth anyon, may not preserve the 2-qubit subspace. The issue of information leakage still needs to concerned.

10 $\mathbf{SU}(2)_k$ and Jones Polynomial

In this section, we study a family of anyon theories called $\mathbf{SU}(2)_k$ for k a positive integer. It turns out this theory is closely related with the Jones polynomial evaluated at certain root of unity. So let's start with the definition of the Jones polynomial.

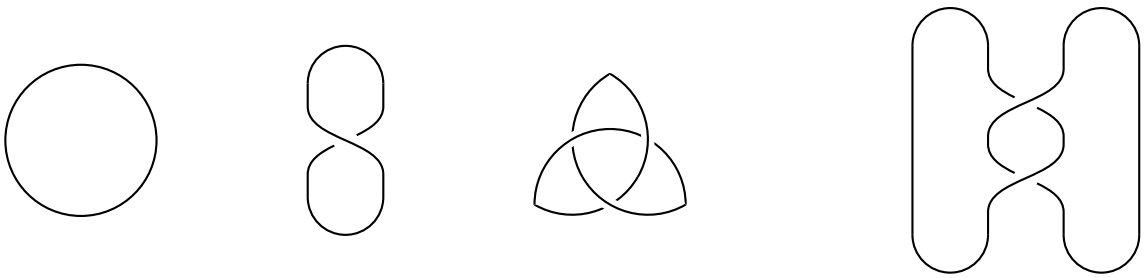


Figure 63: Some examples of knot diagrams.

Figure 64: The skein relation.

10.1 Jones Polynomial

A knot (or more precisely, a link) is a collection of circles embedded in $\mathbb{R}^3$. There are several ways to present a knot, one of which is by projecting it to a plane to get a knot diagram. See Figure 63 for some examples of knot diagrams. Two knots are defined to be equivalent if they can be deformed into each other. A knot is called trivial or unknot if it is equivalent to the one on the left of Figure 63, namely if it is equivalent to an unknotted circle. It is not hard to see the second knot from the left in Figure 63 is an unknot. A classic hard question is how to distinguish non-equivalent knots. One approach is to define a function on the set of knots such that it takes the same value on equivalent knots. So if the function has different values on two knots, then the two knots are not equivalent. Note that the converse to the above statement is not necessarily true. Namely, if the function has the same value on two knots, then they are not necessarily equivalent. The weakest function is a constant function which does not distinguish any knot at all, while the strongest function can distinguish all different knots. Ideally, we want to construct the latter function. But for practical applications, the function should also be algorithmically computable (efficiently or not). With this restriction, one wish to construct a function as strong as possible in terms of distinguishing different knots. We call any such function an invariant of knots. One of the most well known knot invariants is the Jones polynomial.

Let A be an indeterminate and let $\mathbb{Z}[A, A^{-1}]$ be the ring of Laurent polynomials over the integers. So elements of $\mathbb{Z}[A, A^{-1}]$ are of the form

$$\sum_{n=-\infty}^{+\infty} a_n A^n, \quad a_n \in \mathbb{Z}, a_n = 0 \text{ for all but finitely many } n\text{'s}. \tag{162}$$

Define $d := -A^2 - A^{-2}$.

For a knot or rather a knot diagram K, we define its bracket polynomial $\langle K \rangle \in \mathbb{Z}[A, A^{-1}]$ as follows. If K is a disjoint union of k unknots and any one of them is not linked with the rest, then $\langle K \rangle := d^k$. Such a K is called an unlink. In general, we define $\langle K \rangle$ with the so called skein relation as shown in Figure 64. The three knot diagrams involved in the equation

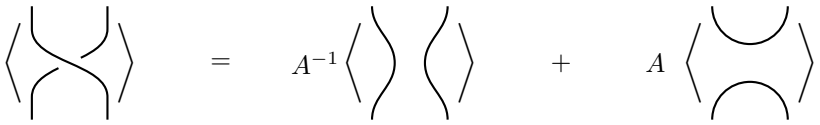


Figure 65: An equivalent skein relation.

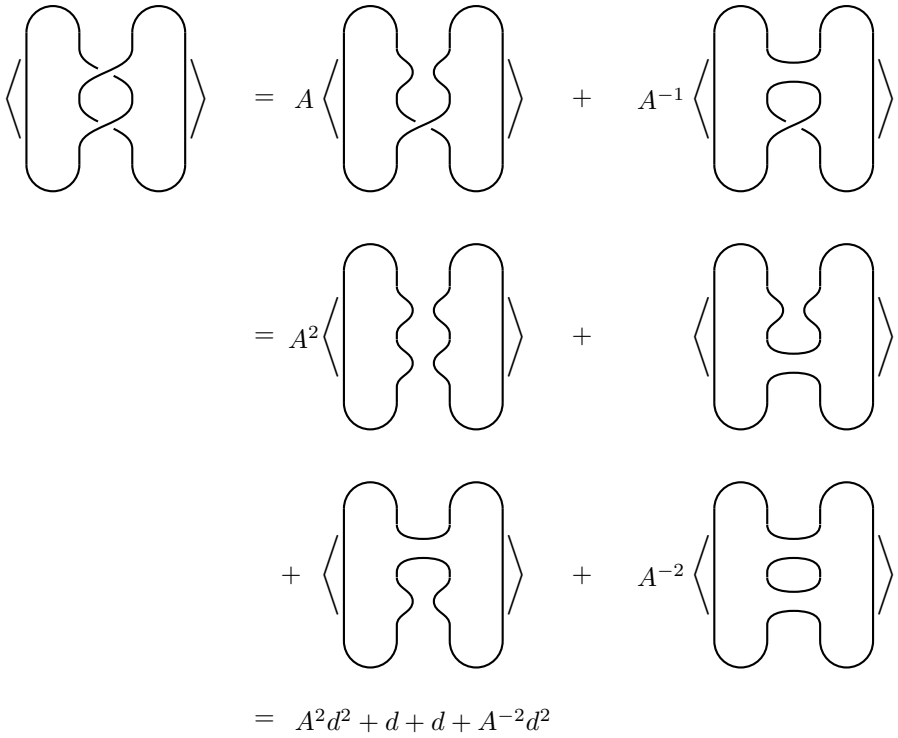


Figure 66: Computing the bracket polynomial for the Hopf link.

of that figure are interpreted as follows. They differ only locally in the portion that is drawn in the figure and are exactly the same elsewhere. From the skein relation, one can also derive an equivalent one as shown in Figure 65 by rotating the original one by 90 degrees. Since the knot diagrams on the RHS have one crossing fewer that the one on the LHS, by applying the skein relation recursively at all crossings, one can write $\langle K \rangle$ in the form

$$\langle K \rangle = \sum_i A^{n_i} \langle K_i \rangle, \tag{163}$$

where each K_i is an unlink. Since the bracket polynomial for unlinks is defined, the skein relation defines the bracket polynomial for all knot diagrams. See Figure 66 for an illustration of computing the bracket polynomial for the Hopf link.

It can be checked that the bracket polynomial is invariant under Reidemeister moves of type II and III (see Figure 67). But it is not invariant under Reidemeister moves of type I. Specifically,there are two cases of type-I move corresponding to a positive crossing and a negative crossing (see Figure 68). By Performing a type-I move of the first case, namely twisting a segment of the knot diagram to the one on the left in Figure 68, the bracket polynomial obtains a factor of $-A^3$. Similarly by performing a type-I move of the

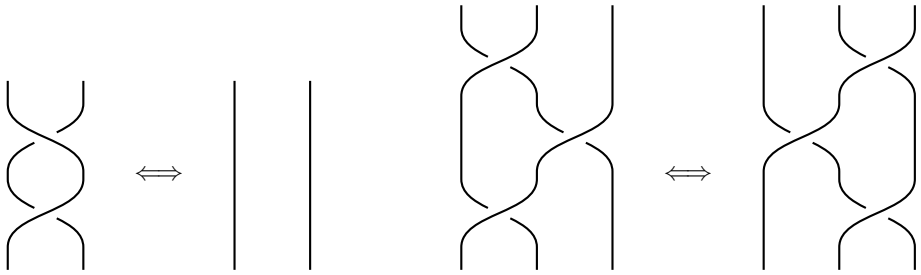


Figure 67: Reidemeister move of type II (Left) and type III (Right)

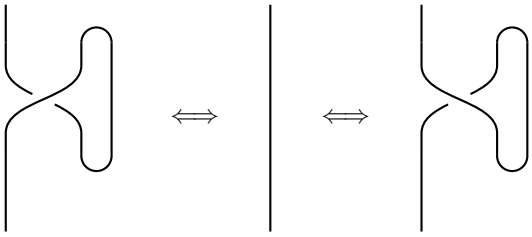


Figure 68: Reidemeister move of type I

second case, the bracket polynomial obtains a factor of $-A^{-3}$. It is possible to normalize the bracket polynomial so that it becomes invariant under type-I moves as well. To introduce the normalization, we have to orient each component of the knot. That is, we need to consider oriented knots. For each crossing c of the knot, define $\omega(c)$ to be 1 if the strand going under the crossing crosses the other strand from right to left, and define it to be -1 otherwise. See Figure 69. The crossing c is called positive if $\omega(c) = 1$, and negative if $\omega(c) = -1$. Define $\omega(K)$ to be the sum of $\omega(c)$ over all crossings c. Then we define

$$J(K; A) := (-A^3)^{-\omega(K)} \langle K \rangle. \tag{164}$$

$J(K; A)$ is invariant under all three types of Reidemeister moves and hence is an invariant of oriented knots. Note however that if K consists of only one component, then $\omega(K)$ actually does not depend on its orientation. Indeed, simultaneously reversing the arrows of all strands does not change $\omega(c)$. Therefore, $J(K; A)$ is defined for unoriented knots with one component and for oriented knots for arbitrary number of components. We also introduce a new variable $q := A^{-4}$ and let $J'(K; q) := J(K; A)$. Then $J'(K; q)$ is the well known Jones polynomial (up to a normalization factor independent of K).

Now we specialize to the case where A is a root of unity. Then $J'(K; q)$ becomes a complex number and it equals $\langle K \rangle$ up to a phase. Hence we also call the latter the evaluation of the Jones polynomial at q. Note that $\langle K \rangle$ is defined for unoriented knots.

Figure 69: (Left) a positive crossing; (Right) a negative crossing.

By the results in [19], if $q = e^{\frac{2\pi i}{r}}$, then evaluating $J'(K;q)$ is $\#P$-hard if $r \neq 1, 2, 3, 4, 6$. What about the complexity on a quantum computer? We will address this problem below.

10.2 $\mathbf{SU}(2)_k$

For each positive integer k, there is an anyon system denoted by $\mathbf{SU}(2)_k$. Strictly speaking, there are two versions of $\mathbf{SU}(2)_k$, one corresponding to the Wess-Zumino-Witten conformal field theory and the other corresponding to the Kauffman-Jones theory. These two theories are similar and many people do not distinguish them, but they are different in subtle ways. Nonetheless, these subtleties will not matter much to us, and below we give the data for the Kauffman-Jones version. Let $A = ie^{-\frac{2\pi i}{4(k+2)}}$, $d = -A^2 - A^{-2}$, and $q = A^{-4}$. As a UMTC, part of the data for $\mathbf{SU}(2)_k$ is given as follows.

- Label set: $L = \{0, 1, 2, \cdots, k\}$; $\bar{x} = x$.
- Fusion rules: $N_{ab}^c = 1$ if and only if

$$|a - b| \leq c \leq |a + b|, \tag{165}$$

$$a + b + c \text{ even and } \leq 2k. \tag{166}$$

- Quantum dimension: $d_0 = 1, d_1 = d$, $d_i = dd_{i-1} - d_{i-2}$.
- R-symbols:

$$R_c^{ab} = (-1)^{\frac{a+b+c}{2}} A^{\frac{c(c+2)-a(a+2)-b(b+2)}{2}}. \tag{167}$$

In this theory, the vacuum is $\mathbf{1} = 0$ and all types of anyons are self dual. Some examples of fusion rules and R-symbols are as follows.

$$1 \otimes 1 = 0 \oplus 2, \text{ if } k \geq 2 \tag{168}$$

$$R_0^{11} = -A^{-3}, \quad R_2^{11} = A. \tag{169}$$

The F-symbols, S- and T-matrices are omitted since they will not be used here. We will only use the fact that for any $a \in L$, $F_{a;00}^{aaa} = d_a^{-1} > 0$[3].

Recall that we have introduced the notations in Figure 70. In the theory $\mathbf{SU}(2)_k$, since $a = \bar{a}$ and $\phi_a = (F_{a;00}^{aaa})^{-1} > 0$, the arrows in the figure do not make a difference and hence we will simply drop the arrows. Moreover, we adopt the notation that an edge without an label means the label is 1. Hence we have the equality as shown in Figure 71. An unknotted circle (with arbitrarily deformed shape) has evaluation equal to d. Also note that we have a decomposition of the identity process on $a \otimes b$. See Figure 72. To verify the identity, precompose the splitting channel ϕ_c^{ab} with the channel on either side of the equality.

Now consider the following process. Create n pairs of anyons all of which have type 1, arbitrarily braid these anyons, and finally fuse the n pairs back to vacuum. See Figure 73

[3]The property actually only holds in the Kauffman-Jones version, but not in the WZW CFT; this is also the original of subtle differences between the two theories.

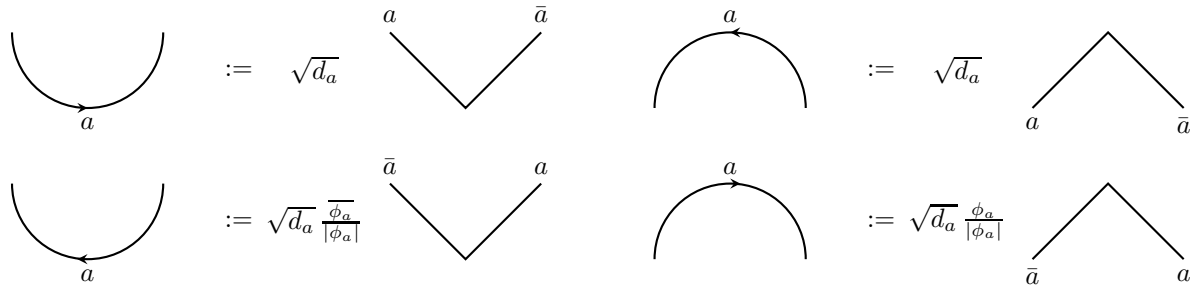


Figure 70: Some notations

Figure 71: The edges are implicitly assumed to labeled by 1.

for an illustration. Denote the state before braiding by $|0\rangle \in V_0^{1^{\otimes 2n}}$, the braid diagram implementing the braiding by σ, and the knot diagram representing the whole process by $\hat{\sigma}$. Also, denote by $U(\sigma)$ the action of σ on the space $V_0^{1^{\otimes 2n}}$. $U(\sigma)$ is a quantum circuit that we can realize via braiding. Then the amplitude corresponding to $\hat{\sigma}$ is given by $d^n\langle 0|U(\sigma)|0\rangle$. The factor d^n comes from the notation in Figure 71.

On the other hand, we show another way of computing the amplitude. At each crossing of the knot diagram, perform the procedure shown in Figure 74. This means that the amplitude of a knot diagram satisfies the skein relation. Combining with the fact that an unknotted circle has evaluation d, we obtain the conclusion that the amplitude of a knot is exactly equal to its bracket polynomial with A taken to be the specific root of unity mentioned at the beginning the subsection. Hence we have the equality:

$$\langle 0|U(\sigma)|0\rangle = \frac{J(\hat{\sigma}; A)}{d^n}(-A)^{3\omega(\hat{\sigma})}. \tag{170}$$

Therefore we have an efficient quantum circuit to approximate $|\frac{J(\hat{\sigma};A)}{d^n}|^2$. Specifically, we initialize the system at the state $|0\rangle$, braid the anyons according to the braid σ, and finally fuse all anyons pair by pair back to vacuum. Each run of the circuit returns a random variable $Z(\sigma)$ which takes the value 1 if the fusion results in the state $|0\rangle$ and the value 0 otherwise. The expectation value of $Z(\sigma)$ is hence $|\frac{J(\hat{\sigma};A)}{d^n}|^2$. Given a precision δ, it suffices to run the circuit $O(\text{poly}(\frac{1}{\delta}))$ times to get a good approximation.

Furthermore, it is a theorem of [12] that for $k \neq 1, 2, 4$, the braiding of $2n$ anyons of type 1 generate a dense subgroup of $\mathbf{U}(V_0^{1^{\otimes 2n}})$. The following theorem is proved in a number of

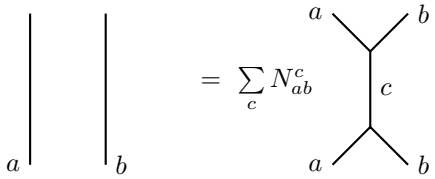


Figure 72: Decomposition of the identity channel on $a \otimes b$.

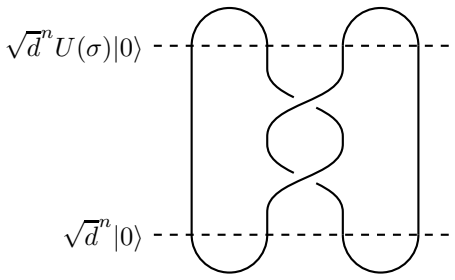


Figure 73: A quantum circuit.

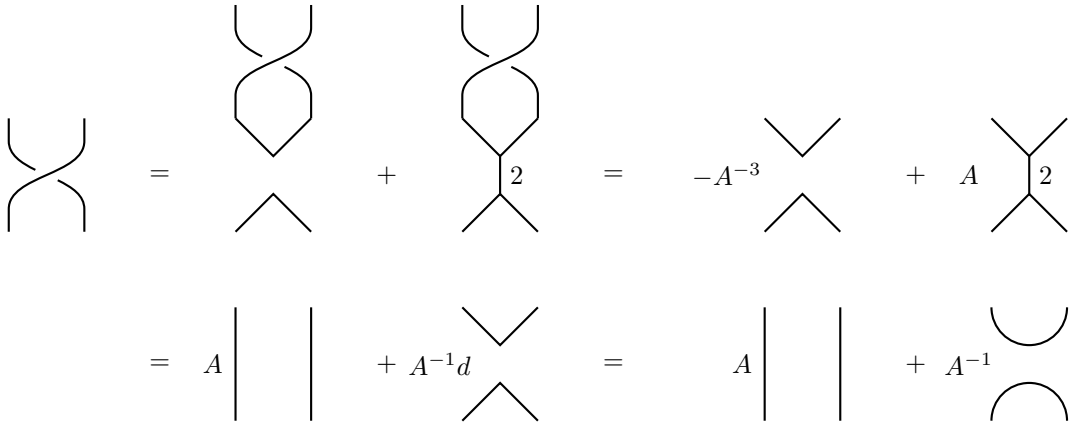


Figure 74: A derivation of the skein relation.

references, such as in [11, 1], et. al.

Theorem 10.1. Approximating $|J(K; ie^{-\frac{2\pi i}{4(k+2)}})|$ is BQP-complete for $k \neq 1, 2, 4$.

A Appendix

A.1 Homework 1

1. (Logical operators in toric code.) In class, we studied string operators $S^Z(t)$ and $S^X(t')$ where t and t' are strings in the lattice and dual lattice, respectively. By definition, $S^Z(t)$ acts by Pauli Z on each edge of t and by identity on other edges. Similarly, $S^X(t')$ acts by Pauli X on each edge crossed by t' and by identity otherwise. Now we consider the case where both t and t' are closed strings (paths). See Figure 75. Let V_{gs} be the ground state space.

- Show that $S^Z(t)$ and $S^X(t')$ preserve V_{gs} for arbitrary closed strings t and t'. Moreover, show that the action of these operators on V_{gs} only depends on the isotopy class of the strings. In particular, this means if a closed string is contractible, the corresponding string operator acts by identity on ground states.

- By the previous result, there are four string operators of Z-type which are $\{S^Z(\emptyset), S^Z(m), S^Z(l), S^Z(m \cup l)\}$, where $\emptyset$ is the empty string or any contractible

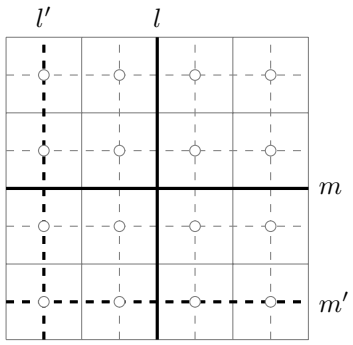


Figure 75: closed strings in the lattice and dual lattice

string, m is a loop along the horizontal direction, and l is a loop along the vertical direction. (See Figure 75). Similarly, there are four string operators of X-type, $\{S^Z(\emptyset), S^X(m'), S^X(l'), S^X(m' \cup l')\}$. See Figure 75. Let

$$\hat{Z}_1 = S^Z(m), \qquad \hat{Z}_2 = S^Z(l),$$
$$\hat{X}_1 = S^X(l'), \qquad \hat{X}_2 = S^X(m').$$

Show that on the ground states the communication relations between the operators $\{\hat{Z}_1, \hat{Z}_2, \hat{X}_1, \hat{X}_2\}$ behave like the usual Pauli operators on two qubits $\{Z_1, Z_2, X_1, X_2\}$. These operators are the logical operators.

- (*optional*) Show that the space of logical operators, i.e., those preserving V_{gs}, is generated as an algebra by $\{\hat{Z}_1, \hat{Z}_2, \hat{X}_1, \hat{X}_2\}$. (Hint: the space of all operators on a physical qubit has a basis given by $\{Id, X, Z, XZ\}$.)

2. (V_{gs} is an error correcting code.) Let the square lattice $\mathcal{L}$ in the definition of toric code have size $L \times L$, namely, there are L edges in the shortest non-contractible loop both along the horizontal direction and along the vertical direction. Let

$$P := \prod_{v \in V} \frac{Id + A_v}{2} \prod_{p \in F} \frac{Id + B_p}{2}.$$

Namely, P is the projector onto the ground space V_{gs}. Let $\mathcal{O}$ be any operator acting on less than L qubits, namely, $\mathcal{O}$ acts non-trivially on at most $L-1$ qubits (edges). Show that

$$P\mathcal{O}P = \alpha_{\mathcal{O}} P, \tag{171}$$

for some scalar $\alpha_{\mathcal{O}}$. By Theorem Theorem 10.1 of [16], V_{gs} is an error correcting code which corrects errors on arbitrary $\lfloor \frac{L-1}{2} \rfloor$ qubits. (Hint: it suffices to show Equation 171 for a basis of the space of operators acting on at most $L-1$ qubits. A basis for this space is given by

$$\left\{ \prod_{e \in E} \mathcal{P}_e : \mathcal{P}_e \in \{Id, X, Z, XZ\}, \text{ and at most } L-1 \quad \mathcal{P}_e's \text{ are not trivial} \right\}.$$

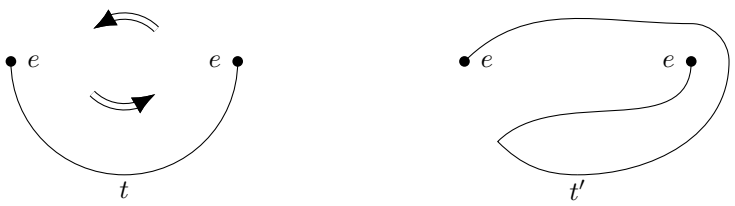


Figure 76: A pair of electric charges before the braiding (Left) and after the braiding (Right).

Any basis element is collection of string operators.)

3. (Braiding statistics of quasi-particles in toric code.) In class, we have shown that there are four types of quasi-particles, the vacuum **1**, the electric charge e, the magnetic charge m, and the composite em of an electric charge with a magnetic charge. Consider a pair of electric charges e, (See Figure 76, where the background lattice and dual lattice are ignored.), denote the state of such configuration by

$$|\psi_{in}\rangle = S^Z(t)|\mathcal{E}\rangle,$$

where $|\mathcal{E}\rangle$ is some ground state. If we swap the two particles in counterclockwise direction, then the state becomes

$$|\psi_{fi}\rangle = S^Z(t')|\mathcal{E}\rangle.$$

But since, t and t' can be deformed to each other, we have $|\psi_{in}\rangle = |\psi_{fi}\rangle$. Hence the electric charge e is a boson. Similarly, the magnatic charge m is also a boson. However, show that the composite em is a fermion.

A.2 Homework 2

Choose n problems, $2 \leq n \leq 5$.

1. (Single-particle excitation on a torus) Single-particle state can not exist on the sphere, but it can on a surface with non-trivial topology. Consider a square lattice on the torus (See Figure 77), where the edges on the top are identified with those on the bottom and the edges on the left are identified with those on the right. *All horizontal edges are oriented to the right and all vertical edges are oriented upwards.* Let G be a finite group and let $a, b \in G$ be two group elements which do not commute. (obviously, this is only possible if G is not Abelian.) Let $r := ab\bar{a}\bar{b}$. Then r is not the identity element. Recall that on each edge lives a Hilbert space with the basis $\{|g\rangle : g \in G\}$ and the total Hilbert space is the tensor product of the Hilbert spaces on all edges. Let $|\psi\rangle$ be the basis state in the total Hilbert space whose value at each edge is shown in Figure 77, where any edge without a label on it means the label is the identity element e. Namely, the five horizontal edges on the far right are each

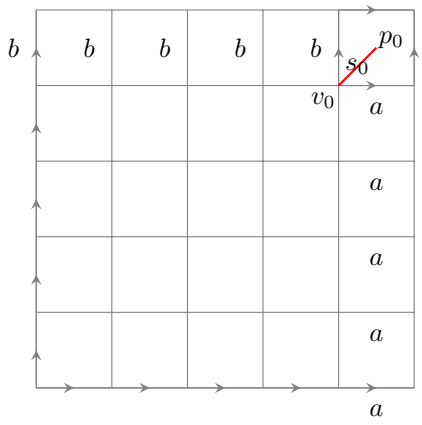


Figure 77: A lattice on the torus.

labeled by a, the five vertical edges on the top are each labeled by b, and all other edges are labeled by e. Define

$$|\psi_{a,b}\rangle := \prod_{v \in V} A(v)|\psi\rangle. \tag{172}$$

- By definition, $|\psi_{a,b}\rangle$ is stabilized by all $A(v)$'s. Let p_0 be the plaquette on the top right corner of the lattice. Show that

$$B(p)|\psi_{a,b}\rangle = |\psi_{a,b}\rangle, \quad \forall p \neq p_0, \tag{173}$$
$$B(p_0)|\psi_{a,b}\rangle = 0. \tag{174}$$

  Thus $|\psi_{a,b}\rangle$ is a state which violates only one constraint. (By the way, it should be clear, and also important, that $|\psi_{a,b}\rangle$ is not the zero vector.)

- Let C be the conjugacy class containing r. Let v_0 be a vertex on the boundary of p_0 and $s_0 = (v_0, p_0)$ be a site (See Figure 77). For each $c \in C$, define

$$|c\rangle := B_c(s_0)|\psi_{a,b}\rangle, \tag{175}$$

  and let $V = \text{span}\{|c\rangle : c \in C\}$. Show that the states $\{|c\rangle : c \in C\}$ form a basis of V.

- It is not hard to see that any state in V is stabilized by all $A(v)$ and $B(p)$ for which $v \neq v_0, p \neq p_0$. (Verify the statement if you are not comfortable with it.) What is the action of the operators $A_g(s_0)$ and $B_h(s_0)$ on V? Write it out under the basis $\{|c\rangle : c \in C\}$. Conclude which irrep V corresponds to. A state in V represents an excitation on the single site s_0.

2. (Local operators interpreted as ribbon operators.) Let $s = (v, p)$ be any site on a lattice. We show the local operators $A_g(s)$ and $B_h(s)$, $h, g \in G$ can be interpreted as ribbon operators for certain ribbons. We start with $B_h(s)$. Let t_s be a ribbon contained in the plaquette p,

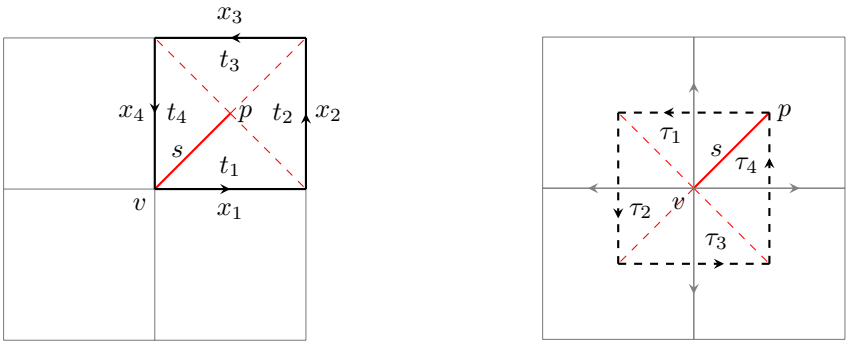


Figure 78: (Left) a closed ribbon t_s; (Right) a closed ribbon τ_s

starting and ending both at s. See Figure 78(Left). It consists of four triangles of type-II (direct triangles) t_1, t_2, t_3, t_4, and is directed in the order the triangles are listed. Assume the edges on the boundary of p are directed as shown in Figure 78(Left) and a basis state $|x_1, x_2, x_3, x_4\rangle$ is given. Then

$$F^{(h,g)}(t_i)|x_i\rangle = \delta_{g,x_i}|x_i\rangle. \tag{176}$$

By the inductive formula for ribbon operators

$$F^{(h,g)}(t_1 t_2) := \sum_{k\in G} F^{(h,k)}(t_1) F^{(\bar{k}hk,\bar{k}g)}(t_2), \tag{177}$$

we have

$$\begin{aligned} F^{(h,g)}(t_1t_2)|x_1,x_2\rangle &= \sum_{k\in G} F^{(h,k)}(t_1)|x_1\rangle \otimes F^{(\bar{k}hk,\bar{k}g)}(t_2)|x_2\rangle \\ &= \sum_{k\in G} \delta_{k,x_1}\delta_{\bar{k}g,x_2}|x_1,x_2\rangle \\ &= \delta_{g,x_1x_2}|x_1,x_2\rangle. \end{aligned} \tag{178}$$

Inductively, it is not hard to see that

$$F^{(h,g)}(t_s)|x_1,x_2,x_3,x_4\rangle = \delta_{g,x_1x_2x_3x_4}|x_1,x_2,x_3,x_4\rangle = B_g(s). \tag{179}$$

Similarly, let τ_s be a ribbon around the vertex v, starting and ending at s. It has four triangles of type-I (dual triangles) $\tau_1, \tau_2, \tau_3, \tau_4$, and is also directed in the order the triangles are listed. See Figure 78(Right). Prove that

$$F^{(h,g)}(\tau_s) = \delta_{g,e}A_h(s). \tag{180}$$

Note that $A_h(s)$ actually only depends on v, hence the ribbon operator $F^{(h,g)}(\tau_s)$ does not depend on the choice of the initial site.

3. (Excitation types can be locally measured.) We know that an excitation in general occupies a site $s = (v, p)$ and the types of excitations are in one-to-one correspondence with

irreps of DG. Recall that the irreps $\mathrm{Irr}(DG)$ are characterized by the pairs (C, χ), where C is a conjugacy class with a pre-selected element $r \in C$ and χ is an irrep of $Z(r)$, the centralizer of r. For each $c \in C$, arbitrarily choose $q_c \in G$ such that $q_c r \bar{q}_c = c$. See Lecture note 3 for more details and conventions. Also recall that DG acts on the total Hilbert space by the local operators $D(s)$. We wish to find a set of elements

$$\{P_{(C,\chi)} \in DG : (C, \chi) \in \mathrm{Irr}(DG)\} \tag{181}$$

which satisfy the following properties.

$$P_{(C,\chi)} P_{(C',\chi')} = \delta_{C,C'} \delta_{\chi,\chi'}, \tag{182}$$

$$\sum_{(C,\chi) \in \mathrm{Irr}(DG)} P_{(C,\chi)} = 1, \tag{183}$$

$$P_{(C,\chi)} \text{ acts on } V_{(C,\chi)} \text{ by } \delta_{C,C'} \delta_{\chi,\chi'}. \tag{184}$$

If we have such a set of elements, then their corresponding operators $\{P_{(C,\chi)}(s)\}$ in $D(s)$ form a complete set of orthogonal projectors and hence can be used to construct a measurement. Moreover, the projector $P_{(C,\chi)}(s)$ precisely projects states to the irrep $V_{(C,\chi)}$. Verify Equation 185 gives the desired elements.

$$P_{(C,\chi)} := \frac{|\chi|}{Z(r)} \sum_{c \in C} \sum_{z \in Z(r)} \overline{\mathrm{Tr}(\chi(z))} B_c A_{q_c z \bar{q}_c}. \tag{185}$$

4. (Non-Abelian Aharonov-Bohm effect.) We consider two special types of excitations. An anyon of type $(C, \mathbf{1})$ is called a magnetic charge and an anyon of type $(\{e\}, \chi)$ is called an electric charge, where $\mathbf{1}$ means the trivial irrep of the corresponding centralizer and $\{e\}$ is the conjugacy class containing only the identity element. In the latter case, χ is an irrep of G. For a magnetic charge $(C, \mathbf{1})$, a basis for the irrep is given by

$$\{|c\rangle : c \in C\}, \tag{186}$$

and the action of the double DG is

$$\begin{aligned} A_g |c\rangle &= |g c \bar{g}\rangle \\ B_h |c\rangle &= \delta_{h,c} |c\rangle. \end{aligned} \tag{187}$$

For an electric charge $(\{e\}, \chi)$, a basis for the irrep is given by

$$\{|j\rangle : j = 1, \cdots, |\chi|\}, \tag{188}$$

and the action is

$$\begin{aligned} A_g |j\rangle &= \chi(g) |j\rangle \\ B_h |j\rangle &= \delta_{h,e} |j\rangle. \end{aligned} \tag{189}$$

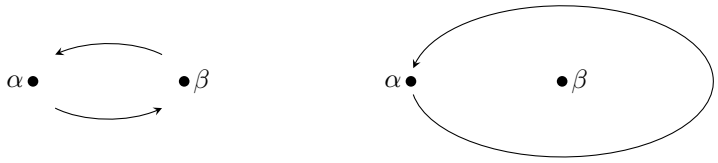


Figure 79: (Left) Swap of α and β in counterclockwise direction. (Right) Drag α around β in counterclockwise direction. This is equivalent to two counterclockwise swaps.

Note that the actions above can all be derived from the general formula on irreps of DG. If we swap an anyon of type α with an anyon of type β in the counterclockwise direction (see Figure 79 (Left)), then this induces the transformation $c_{\alpha,\beta}$ given by:

$$\alpha \otimes \beta \xrightarrow{R} \alpha \otimes \beta \xrightarrow{\text{Flip}} \beta \otimes \alpha, \tag{190}$$

where $R = \sum_g A_g \otimes B_g$, and the first factor of R acts on α and the second factor acts on β.

- If $\alpha = (\{e\}, \chi), \beta = (C, \mathbf{1})$, a basis for $\alpha \otimes \beta$ and $\beta \otimes \alpha$ are given, respectively, by

$$\{|j, c\rangle : j = 1, \cdots, |\chi|, c \in C\} \text{ and } \{|c, j\rangle : j = 1, \cdots, |\chi|, c \in C\}. \tag{191}$$

  Write out the transformation $c_{\alpha,\beta}$ under the bases above. Do the same for $c_{\beta,\alpha}$. Swapping α and β followed by another swap of β and α is the same as dragging α along some closed path around β (see Figure 79 (Right)). The net result is a unitary transformation on $\alpha \otimes \beta$ given by

$$\alpha \otimes \beta \xrightarrow{c_{\alpha,\beta}} \beta \otimes \alpha \xrightarrow{c_{\beta,\alpha}} \alpha \otimes \beta. \tag{192}$$

  If you have worked out $c_{\alpha,\beta}$ and $c_{\beta,\alpha}$, then you will see that

$$c_{\beta,\alpha} \circ c_{\alpha,\beta}|j, c\rangle = \chi(c)|j\rangle \otimes |c\rangle. \tag{193}$$

  This is the non-Abelian Aharonov-Bohm effect for anyons.

- Work out the formula for $c_{\beta,\alpha} \circ c_{\alpha,\beta}$ in Case I where α, β are two magnetic charges and in Case II where α, β are two electric charges.

5. (Quantum double model for $\mathbb{Z}_2$.) The quantum double based on $G = \mathbb{Z}_2 = \{0, 1\}$ recovers the toric code. In this case, at each edge in the lattice lives a qubit with the standard basis $\{|0\rangle, |1\rangle\}$. There is no need to orient the edges since all group elements are their own inverse and the group is Abelian. Let X and Z be the Pauli matrices.

- Work out the formula for the vertex operator $A(v)$ and plaquette operator $B(p)$. These will not be exactly the same as the ones defined originally in toric code, but only differ in a simple way. The two Hamiltonians are equivalent, up to an energy shift.

Figure 80: The action of $F^{(i,j)}(\tau)$ for two types of triangles.

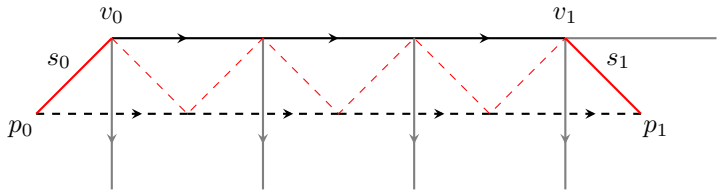


Figure 81: A general ribbon t

- Let's look at ribbon operators. Let $(i,j) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ be a pair of group elements. If t is a type-I triangle(resp. type-II triangle) (see Figure 80), then $F^{(i,j)}(t)$ acts as $\delta_{j,0}X^i$ (resp. $|j\rangle\langle j|$) on the corresponding edge. The inductive formula for spliting ribbons is given by

$$F^{(i,j)}(t_1 t_2) := \sum_{k\in\mathbb{Z}_2} F^{(i,k)}(t_1)F^{(i,j+k)}(t_2). \tag{194}$$

  Note that arithmetic is performed modulo 2. Work out an explicit expression for the ribbon operator $F^{(i,j)}(t)$ where t is shown in Figure 81. (I already gave the formula in class for a general G.)

- To continue, we need to study irreps of $D\mathbb{Z}_2$. Each element of $\mathbb{Z}_2$ represents a conjugacy class, and the centralizer is always $\mathbb{Z}_2$ itself since the group is Abelian. An irrep of $\mathbb{Z}_2$ is 1-dimensional and is given by a group element, 0 or 1, corresponding to the trivial and non-trivial irrep. To avoid confusion, let's denote them by [0] and [1]. The [0] irrep maps everything to 1 and the [1] irrep maps a group element i to $(-1)^i$. Therefore, irreps of $D\mathbb{Z}_2$ correspond to

$$\{(i,[j]) : i,j \in \mathbb{Z}_2\}. \tag{195}$$

  All of them are 1-dimensional. Show that the matrix element of $D_{(k,l)} = B_k A_l$ in the irrep $(i,[j])$ is given by

$$\Gamma_{11}^{(i,[j])}(D_{(k,l)}) = \delta_{k,i}(-1)^{jl}. \tag{196}$$

- In general case, the ribbon operator in the representation basis is given by

$$F^{(C,\chi;u,u')}(t) = \frac{|(C,\chi)|}{|G|}\sum_{h,g}\Gamma_{u,u'}^{(C,\chi)}\left(D_{(h,g)}\right)F^{(h,g)}(t). \tag{197}$$

In our case, this formula can be simplified as

$$F^{(i,[j])}(t) = \frac{1}{2}\sum_{l=0}^{1}(-1)^{jl}F^{(i,l)}(t). \tag{198}$$

What is the explicit formula of $F^{(i,[j])}(t)$ for the ribbon t in Figure 81? You will recover the string operators.

Acknowledgment I would like to thank Patrick Hayden who made it possible for this course to be opened. I would also like to thank Zhenghan Wang for answering various questions on topics related to the course. I acknowledge the support from the Simons Foundation.

References

[1] Dorit Aharonov and Itai Arad. The BQP-hardness of approximating the Jones polynomial. *New Journal of Physics*, 13(3):035019, 2011.

[2] Bojko Bakalov and Alexander A Kirillov. *Lectures on tensor categories and modular functors*, volume 21. American Mathematical Soc., 2001.

[3] Maissam Barkeshli, Parsa Bonderson, Meng Cheng, and Zhenghan Wang. Symmetry, defects, and gauging of topological phases. *arXiv preprint arXiv:1410.4540*, 2014.

[4] Hector Bombin and MA Martin-Delgado. Family of non-Abelian Kitaev models on a lattice: Topological condensation and confinement. *Physical Review B*, 78(11):115421, 2008.

[5] Parsa Hassan Bonderson. *Non-Abelian Anyons and Interferometry*. PhD thesis, California Institute of Technology, 2007.

[6] Oliver Buerschaper, Juan Martín Mombelli, Matthias Christandl, and Miguel Aguado. A hierarchy of topological tensor network states. *Journal of Mathematical Physics*, 54(1):012201, 2013.

[7] Liang Chang. Kitaev models based on unitary quantum groupoids. *Journal of Mathematical Physics*, 55(4):041703, 2014.

[8] Shawn X Cui, Seung-Moon Hong, and Zhenghan Wang. Universal quantum computation with weakly integral anyons. *Quantum Information Processing*, 14(8):2687–2727, 2015.

[9] Orit Davidovich, Tobias Hagge, and Zhenghan Wang. On arithmetic modular categories. *arXiv preprint arXiv:1305.2229*, 2013.

[10] Pavel Etingof, Eric Rowell, and Sarah Witherspoon. Braid group representations from twisted quantum doubles of finite groups. *Pacific journal of mathematics*, 234(1):33–41, 2008.

[11] Michael H Freedman, Michael Larsen, and Zhenghan Wang. A modular functor which is universal for quantum computation. *Communications in Mathematical Physics*, 227(3):605–622, 2002.

[12] Michael H Freedman, Michael J Larsen, and Zhenghan Wang. The two-eigenvalue problem and density of Jones representation of braid groups. *Communications in mathematical physics*, 228(1):177–199, 2002.

[13] Christian Kassel and Vladimir Turaev. *Braid groups*, volume 247. Springer Science & Business Media, 2008.

[14] A Yu Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, 2003.

[15] Chetan Nayak, Steven H Simon, Ady Stern, Michael Freedman, and Sankar Das Sarma. Non-abelian anyons and topological quantum computation. *Reviews of Modern Physics*, 80(3):1083, 2008.

[16] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[17] John Preskill. Lecture notes for Physics 219: Quantum computation. *Caltech Lecture Notes*, 1999.

[18] Vladimir G Turaev. *Quantum invariants of knots and 3-manifolds*, volume 18. Walter de Gruyter GmbH & Co KG, 2016.

[19] Dirk Vertigan. The computational complexity of Tutte invariants for planar graphs. *SIAM Journal on Computing*, 35(3):690–712, 2005.

[20] Zhenghan Wang. *Topological quantum computation*. Number 112. American Mathematical Soc., 2010.