Exploring Abelian and Non-Abelian Quantum Codes

Simon David Burton

Doctor of Philosophy
University of Sydney
2016

Declaration

I declare that this thesis was composed by myself and that the work contained therein is my own, except where explicitly stated otherwise in the text.

(*Simon David Burton*)

To my friends

Abstract

Stabilizer codes... from the point of view of category theory joining stabilizer codes together comes for free once we have a suitable choice of what is meant by a homomorphism of such a code. The category of length chain complexes over Z_2 provides a natural homomorphism, namely the chain-maps. Category theory then automatically gives a definition of joining and this corresponds (partly?) to the previously discovered notion of welding of stabilizer codes. Turning to non-Abelian Hamiltonians as a possible way to construct quantum memories, we examine the eigenstructure of Hamiltonians with Pauli operator terms, from the perspective of the representation theory of the group formed by these terms. Finally, we show how to simulate an error correction scenario involving non-Abelian excitations in a two dimensional topologically ordered system.

Contents

Chapter 1

Fibered Sum of Stabilizer Codes

1.1 Introduction

1.2 Symplectic structure of stabilizer codes

We work with vector spaces over the field $\mathbb{Z}_2$.

A quantum CSS code is given by two parity check matrices S_z and S_x.

Such a code will be called *regular* when the parity checks have full rank.

Given a regular code, we can a symplectic structure is any solution to the following (block) matrix equation:

$$\begin{pmatrix} L_z \\ S_z \\ T_z \end{pmatrix} \begin{pmatrix} L_x \\ T_x \\ S_x \end{pmatrix}^{\top} = I,$$

where I denotes the appropriate identity matrix, and the small T is matrix transposition.

In general this is a non-linear equation because of the presense of the quadratic term: $T_z T_x^{\top} = 0$.

To construct solutions given S_z and S_x we proceed as follows:

(1) Find L_z. The rows of L_z lie in the kernel of S_x, chosen to be (arbitrary) elements of the cosets of $S_z^{\top}$. Ie. the rows of L_z span $\ker(S_x)/Im(S_z^t)$.

(2) Find L_x. We first repeat step *(1)* on the dual code (S_x and S_z swapped) to find

L'_x. We look for L_x such that $L_z L_x^\top = I$ knowing that the rows of L_x lie in the span of L'_x. Ie. $L_x = AL'_x$ for some A. Now solve $L_z L_x^\top A^\top = I$ for A.

(3) Find T_z. This will be a solution of the linear system:

$$\begin{aligned} (*) \quad S_x T_z^\top &= I \\ L_x T_z^\top &= 0. \end{aligned}$$

The solution space has kernel spanned by the rows of S_z.

(4) T_z is now a solution of the linear system:

$$\begin{aligned} S_z T_x^\top &= I \\ L_z T_x^\top &= 0 \\ T_z T_x^\top &= 0. \end{aligned}$$

From $(*)$ above, we know that T_z has full rank, and so this system has a unique solution T_x.

1.3 The boundary of the boundary is empty

1.3.1 Chain complexes

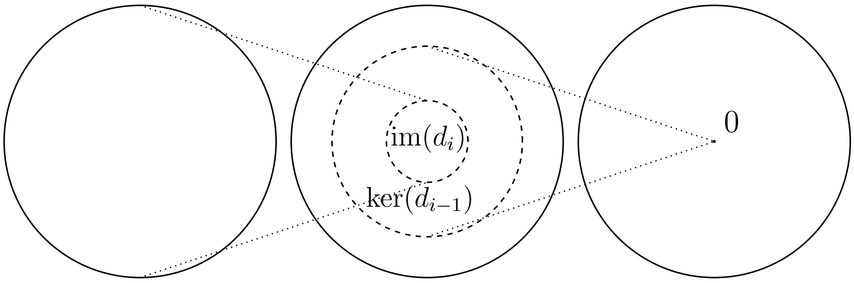
We introduce the category of chain complexes, $\widetilde{\text{Chain}}$.

A *chain complex* C is given by a sequence of vector spaces C_i and linear maps $d_i : C_i \to C_{i-1}$ such that $d_{i-1} d_i = 0$ for all i.

Here is a diagram:

$$\ldots \xrightarrow{d_{i+2}} C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \xrightarrow{d_{i-1}} \ldots$$

The condition $d_{i-1} d_i = 0$ is equivelant to requiring the image of d_i to be contained within the kernel of d_{i-1}:



$$C_i \xrightarrow{d_i} C_{i-1} \xrightarrow{d_{i-1}} C_{i-2}$$

Elements of the space $B_i := \mathrm{im}(d_{i+1})$ are known as *boundaries*, and elements of $Z_i := \ker(d_i)$ are also known as *cycles*.

We form the quotient vector space $H_i(C) := B_i(C)/Z_i(C)$, called the i'th homology group (the group operation is given by the vector space addition.)

The sequence of spaces H_i will also be denoted as simply H. It can be taken to be a chain complex with the zero boundary map.

We can always consider finite length chain complexes by appending/prepending zero vector spaces and maps, for example $A \to B \to C$ can be extended as

$$... \to 0 \to A \to B \to C \to 0 \to ...$$

1.3.2 Chain maps

A chain map $f : C \to C'$ is a sequence of linear maps $f_i : C_i \to C_i'$ that commute (intertwine) with the boundary map: $f_{i-1}d_i = d_i' f_i$. Or in diagram form:

$$\begin{tikzcd}
{} \arrow[r] & C_2 \arrow[r, "d_2"] \arrow[d, "f_2"'] & C_1 \arrow[r, "d_1"] \arrow[d, "f_1"'] & C_0 \arrow[r] \arrow[d, "f_0"'] & {} \\
... & & & & ... \\
{} \arrow[r] & C_2' \arrow[r, "d_2'"] & C_1' \arrow[r, "d_1'"] & C_0' \arrow[r] & {}
\end{tikzcd}$$

The main point about a chain map is that it induces a (linear) map of homology groups:

$$\tilde{f}_i : H_i \to H_i'.$$

1.3.3 The Hom functor

We consider the boundary operator acting by pre-composition:

$$\begin{tikzcd} C_i \arrow[r, "d_i"] \arrow[dr, "f \circ d_i"'] & C_{i-1} \arrow[d, "f"] \\ & V \end{tikzcd}$$

Given a chain complex C and an arbitrary vector space V we see that the boundary map d_i acts on maps $f : C_{i-1} \to V$ to give a map $C_i \to V$. We will fix V to be the underlying field $\mathbb{Z}_2$ then this action is "multiplying on the right", ie. the transpose operation. In this way we construct the dual cochain.

$$\cdots \longleftarrow C^{i+1} \xleftarrow{d^i} C^i \xleftarrow{d^{i+1}} C^{i-1} \longleftarrow \cdots$$

This is the familiar covector construction. In general, the so-called hom functor reverses the direction of all the arrows (of some diagram.) In our case this means simply that the transpose of a product reverses the product: $(AB)^\top = B^\top A^\top$.

1.3.4 Classical linear codes

A classical linear code may be specified as the kernel of a parity check matrix $S : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$. As a chain complex, this is the homology group at $\mathbb{Z}_2^m$.

As a notational convenience we will sometime denote a vector space by its (integer) dimension, eg. $S : n \to m$.

Chain	Cochain
$0 \longrightarrow n \xrightarrow{S} m \longrightarrow 0$	$0 \longrightarrow m \xrightarrow{S^T} n \longrightarrow 0$
$H_1 = \ker(S) =: L$	$H^0 = \ker(S^\top) =: L^\top$
$H_0 = m/\mathrm{im}(S) = \mathrm{coker}(S)$	$H^1 = n/\mathrm{im}(S^\top) = \mathrm{coker}(S^\top)$

1.3.5 Quantum stabilizer codes

A quantum (CSS) code is given by two parity check matrices $S_X : n \to m_X$ and $S_Z : n \to m_Z$, such that the chain condition $S_X S_Z^\top = 0$ is satisfied.

<u>Chain</u>

$$0 \longrightarrow m_Z \xrightarrow{S_Z^T} n \xrightarrow{S_X} m_X \longrightarrow 0$$

$$0 \longrightarrow C_2 \longrightarrow C_1 \longrightarrow C_0 \longrightarrow 0$$

$$H_2 = \ker(S_Z^\top)$$

$$H_1 = \ker(S_X)/\mathrm{im}(S_Z^\top) =: L_X$$

$$H_0 = m_X/\mathrm{im}(S_X) = \mathrm{coker}(S_X)$$

<u>Cochain</u>

$$0 \longrightarrow m_X \xrightarrow{S_X^T} n \xrightarrow{S_Z} m_Z \longrightarrow 0$$

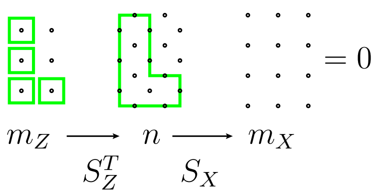
$$0 \longrightarrow C^0 \longrightarrow C^1 \longrightarrow C^2 \longrightarrow 0$$

$$H^0 = \ker(S_X^\top)$$

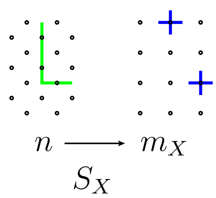
$$H^1 = \ker(S_Z)/\mathrm{im}(S_X^\top) =: L_Z$$

$$H^2 = m_Z/\mathrm{im}(S_Z) = \mathrm{coker}(S_Z)$$

In the chain we are thinking of the space m_Z as the space of “2-dimensional” objects. In the toric code this is the space of plaquettes, but more generally we can think of these as “generator labels”. The space n is associated with the physical qubits, this is where the pauli operators reside.



In the toric code n is the space of “1-dimensional” error operators. The space m_X is then the space of (X-type) syndrome measurements. In the toric code these are the “zero-dimensional” end-points of (Z-type) error operators.



1.4 Tensor product

The tensor product $C \otimes C'$ of two chain complexes (C, d) and (C', d') is given by

$$(C \otimes C')_i = \sum_{j+k=i} C_j \otimes C'_k$$

with boundary map

$$d(c \otimes c') = d(c) \otimes c' + (-1)^{deg(c)} c \otimes d'(c').$$

To motivate these formulae, consider the following two dimensional complex:

$$\begin{tikzcd}
 & {} \arrow[d, dashed] & {} \arrow[d, dashed] & {} \arrow[d, dashed] & {} \arrow[d, dashed] \\
{} \arrow[r, dashed] & C_2 \otimes C'_2 \arrow[r, "d_2 \otimes I"] \arrow[d, "I \otimes d'_2"'] & C_1 \otimes C'_2 \arrow[r, "d_1 \otimes I"] \arrow[d, "I \otimes d'_2"'] & C_0 \otimes C'_2 \arrow[d, "I \otimes d'_2"'] & C'_2 \arrow[d, "d'_2"'] \\
{} \arrow[r, dashed] & C_2 \otimes C'_1 \arrow[r, "d_2 \otimes I"] \arrow[d, "I \otimes d'_1"'] & C_1 \otimes C'_1 \arrow[r, "d_1 \otimes I"] \arrow[d, "I \otimes d'_1"'] & C_0 \otimes C'_1 \arrow[d, "I \otimes d'_1"'] & C'_1 \arrow[d, "d'_1"'] \\
{} \arrow[r, dashed] & C_2 \otimes C'_0 \arrow[r, "d_2 \otimes I"] & C_1 \otimes C'_0 \arrow[r, "d_1 \otimes I"] & C_0 \otimes C'_0 & C'_0 \\
{} \arrow[r, dashed] & C_2 \arrow[r, "d_2"] & C_1 \arrow[r, "d_1"] & C_0 &
\end{tikzcd}$$

where I indicates the appropriate identity map on each vector space.

To reduce this to a one dimensional structure we (direct) sum along the diagonals, for example:

$$(C \otimes C')_4 = C_2 \otimes C'_2$$
$$(C \otimes C')_3 = C_2 \otimes C'_1 + C_1 \otimes C'_2$$
$$(C \otimes C')_2 = C_2 \otimes C'_0 + C_1 \otimes C'_1 + C_0 \otimes C'_2$$
$$(C \otimes C')_1 = C_1 \otimes C'_0 + C_0 \otimes C'_1$$
$$(C \otimes C')_0 = C_0 \otimes C'_0$$

$$\begin{tikzcd}
C_2 \otimes C'_2 \arrow[r] \arrow[d] & C_1 \otimes C'_2 \arrow[r] \arrow[d] & C_0 \otimes C'_2 \arrow[d] \\
C_2 \otimes C'_1 \arrow[r] \arrow[d] & C_1 \otimes C'_1 \arrow[r] \arrow[d] & C_0 \otimes C'_1 \arrow[d] \\
C_2 \otimes C'_0 \arrow[r] & C_1 \otimes C'_0 \arrow[r] & C_0 \otimes C'_0
\end{tikzcd}$$

Now we add the arrows in an alternating fashion to get a boundary map. The composition of two arrows in the same direction is evidently zero, and we use an alternating weight to force the two paths around each square to cancel:

$$\begin{array}{ccccc}
C_2 \otimes C'_2 & \longrightarrow & C_1 \otimes C'_2 & \longrightarrow & C_0 \otimes C'_2 \\
+\big\downarrow & & -\big\downarrow & & +\big\downarrow \\
C_2 \otimes C'_1 & \longrightarrow & C_1 \otimes C'_1 & \longrightarrow & C_0 \otimes C'_1 \\
+\big\downarrow & & -\big\downarrow & & +\big\downarrow \\
C_2 \otimes C'_0 & \longrightarrow & C_1 \otimes C'_0 & \longrightarrow & C_0 \otimes C'_0
\end{array}$$

With this definition of tensor product the category of chain complexes becomes a monoidal category (See [4], section 2.3 for a helpful discussion of monoidal categories.)

1.4.1 The Kunneth formula

The homology group of the product inherits the same structure as the underlying chain complex. This is the import of the Kunneth formula:

$$H_i(C \otimes C') = \sum_{j+k=i} H_j(C) \otimes H_k(C')$$

We now define a homomorphism $f : H(C) \otimes H(C') \to H(C \otimes C')$ by its action on the subspaces:

$$f : H_j(C) \otimes H_k(C') \to H_{j+k}(C \otimes C').$$

defined by choosing $u_j \in \ker(d_j), u'_k \in \ker(d'_k)$ and then noting that

$$(d_j \otimes I)(u_j \otimes u'_k) = 0, \quad (I \otimes d'_k)(u_j \otimes u'_k) = 0$$

which means $u_j \otimes u'_k$ is in the kernel of the tensor product boundary map, and so represents an element of $H_{j+k}(C \otimes C')$. Next check that the choice of u_i, u'_j did not matter...

Weight of stabilizers... Weight of logops...

1.4.2 Product of two classical codes

The hypergraph product of Tillich and Zemor [30] is the product of a classical code and the dual of a classical code. We didn't define such a product above, but evidently if we follow the arrows in the same way (or alternativy, relabel the cochain) it should all work out.

$$
\begin{tikzcd}
 & & & {} \arrow[dr, "S_Z^T"] & & \\
 & & & & {} \arrow[dr, "S_X"] & \\
m_2 \arrow[d, "S_2^T"'] & n_1 \otimes m_2 \arrow[r] \arrow[d] & m_1 \otimes m_2 \arrow[d] & & & {} \\
n_2 & n_1 \otimes n_2 \arrow[r] & m_1 \otimes n_2 & & & \\
 & n_1 \arrow[r, "S_1"] & m_1 & & &
\end{tikzcd}
$$

We use the Kunneth formulae to compute the logical operators:

$$
\begin{aligned}
H_1(C_1 \otimes C_2^\top) &= \mathrm{coker}(S_1) \otimes L_2^\top + L_1 \otimes \mathrm{coker}(S_2^\top) \\
|H_1(C_1 \otimes C_2^\top)| &= (m_1 - |\mathrm{im}(S_1)|)|L_2^\top| + |L_1|(n_2 - |\mathrm{im}(S_2^\top)|) \\
&= (m_1 - |\mathrm{im}(S_1^\top)|)|L_2^\top| + |L_1|(n_2 - |\mathrm{im}(S_2)|) \\
&= |\ker(S_1^\top)||L_2^\top| + |L_1||\ker(S_2)| \\
&= |L_1^\top||L_2^\top| + |L_1||L_2|
\end{aligned}
$$

The toric code is obtained from the product of a (classical) repitition code with its dual. The important thing to note is that the parity check matrix (stabilizer generators) is the object of primary importance, not the space of logical operators. To get the toric code we must start with a degenerate parity check matrix $S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$. Then $|L| = |L^\top| = 1$ and we get the two logical qubits in the product. Using the matrix $S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$. gives $|L| = 1, |L^\top| = 0$ which gives one logical qubit in the product; this is a surface code.

1.4.3 Product of a classical and a quantum code

This results in two separate quantum codes, as indicated in the following diagram:

$$
\begin{tikzcd}
n \otimes m'_X \arrow[r] \arrow[d] & m \otimes m'_X \arrow[d] \\
n \otimes n' \arrow[r] \arrow[d] & m \otimes n' \arrow[d] \\
n \otimes m'_Z \arrow[r] & m \otimes m'_Z
\end{tikzcd}
$$

(There are also two classical codes at the endpoints.)

In this way we can generate the 3 (spatial) dimension toric code, as a product of the 2D toric code with the repitition code. Here we see the two resulting codes have sheets and lines for logical operators, one code has x-type sheets and z-type lines, the other code is x-type lines and z-type sheets.

1.4.4 Product of two quantum codes

Continueing this pattern we can generate three different quantum codes as a product of two quantum codes:

$$
\begin{tikzcd}
m_Z \otimes m'_Z \arrow[r] \arrow[d] & n \otimes m'_Z \arrow[r] \arrow[d] & m_X \otimes m'_Z \arrow[d] \\
m_Z \otimes n' \arrow[r] \arrow[d] & n \otimes n' \arrow[r] \arrow[d] & m_X \otimes n' \arrow[d] \\
m_Z \otimes m'_X \arrow[r] & n \otimes m'_X \arrow[r] & m_X \otimes m'_X
\end{tikzcd}
$$

For example, the product of the 2D toric code with itself produces the 4D toric code with x and z type sheet operators, thats the code in the middle.

Another example, the middle code of the product Stean x Stean has parameters $[67, 1, 9]$.

1.5 Sums and Pushouts

In any category the sum of two objects A and B is given by an object C and two maps $f : A \to C$ and $g : B \to C$. These maps show how to embedd A and B into their "sum". A further requirement is that C is somehow minimal: any other contender C' for the sum of A and B with "embedding" maps f' and g' must factor uniquely through C.

In the category of sets we take the disjoint union of A and B, similarly in the category of topological spaces. The embedding into the sum is the obvious inclusion map.

In the category of vector spaces, we take the direct sum $A \oplus B$, together with maps $f = I \oplus 0$ and $g = 0 \oplus I$. This extends to the category of chain complexes, which gives the disjoint union of two codes.

If we would like to join objects A and B along some "sub-part", $i : R \to A$, $j : R \to B$ we play the same game but now require f and g to respect i and j, that is, $f \circ i = g \circ j$. This is known as a "pushout" (of i and j.) In the category of sets, we would take the disjoint union as before, and then identify those elements according to $(fi)(r) \sim (gj)(r), r \in R$.

This identification also works for topological spaces, but for vector spaces we project out the *subspace* defined by $fi - gj$. The notation is then $A \oplus_R B$.

Extended to chain complexes we obtain a general way to "weld" two quantum codes together [28].

TODO...

1.6 Non-CSS codes

TODO...

Chapter 2

Representations of Subsystem Code Hamiltonians

2.1 Representations

2.1.1 Motivating examples

We start our journey considering a two-dimensional state space. This space is blessed with two basis vectors $|0\rangle$ and $|1\rangle$. The Z and X operators act on these states as:

$$Z : \begin{tikzcd} |0\rangle \arrow[loop left, "+1"] & |1\rangle \arrow[loop right, "-1"] \end{tikzcd}$$

$$X : \begin{tikzcd} |0\rangle \arrow[r, bend right, "+1"'] & |1\rangle \arrow[l, bend right, "+1"'] \end{tikzcd}$$

From this picture we can see that Z acts by *stabilizing* the state $|0\rangle$ and anti-stabilizing the $|1\rangle$ state. The Z operator has been reduced to two operators each acting on a one dimensional subspace: $Z = +1 \oplus -1$. The X operator serves to "bitflip" the state between these two subspaces.

But what happens if we get confused and end up swapping the X and Z operators? We would like to see the X operator as stabilizing / anti-stabilizing two subspaces, together with the Z operator as bitflipping between these. The trick is to consider the *orbits* of the operator we hope to act as a stabilizer. In this case there is only one orbit, $|0\rangle + |1\rangle$ and indeed, the Z operator bitflips this to another state $|0\rangle - |1\rangle$ that is anti-stabilized by X.

We are going to be considering Hamiltonians built from summing operators of this form. In this paper we use a "neg-Hamiltonian" convention, to save complicating expressions with negative signs. The ground space corresponds to the *largest* eigenvalue.

Building a Hamiltonian from a single X or Z term we can find the ground space as the stabilized space using orbits. Then the adjacent operator acts to bitflip between the eigenspaces. To further elucidate this idea we turn to another example. Now we have a hamiltonian built from three commuting and independent operators

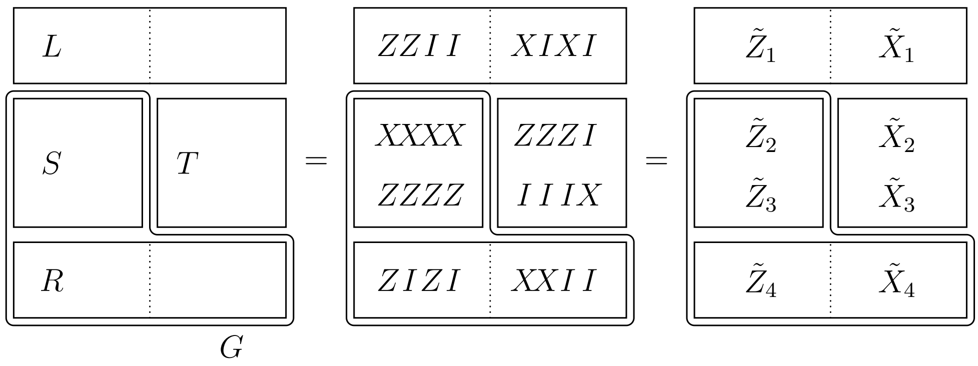
$$H = XXI + IXX + ZZZ.$$

Starting with $|000\rangle$ we compute the orbit state as $|000\rangle+|011\rangle+|110\rangle+|101\rangle$. This time we have three bitflip operators one for each of the stabilizer operators: ZII, IIZ, IXI. (We could also have chosen IZZ, ZZI, XXX.) For example, ZII sends the ground state to $|000\rangle + |011\rangle - |110\rangle - |101\rangle$ which is anti-stabilized by XXI. The bitflip operators form an abelian group of order $2^3 = 8$ and by appying each element of this group to the ground state we get a basis of our state space, which we call a *symmetry invariant basis.*

Now we consider a four qubit example:

$$H = XXII + IIXX + ZIZI + IZIZ.$$

This time the terms of the Hamiltonian do not form an abelian group. We will call the group generated by the terms in the Hamiltonian the *gauge* group, G. The stabilizers in this case will be the elements of G that commute with every other element in G. By inspection we see these are generated by $S_0 = \{XXXX, ZZZZ\}$. and we can choose the reduced gauge generators to be $R_0 = \{XXII, ZIZI\}$. The logical operators are generated by $L_0 = \{XIXI, ZZII\}$, and then the errors T_0 corresponding to S_0 will be $\{ZZZI, IIIX\}$. All of this can be summarized in a table of anti-commuting pairs:



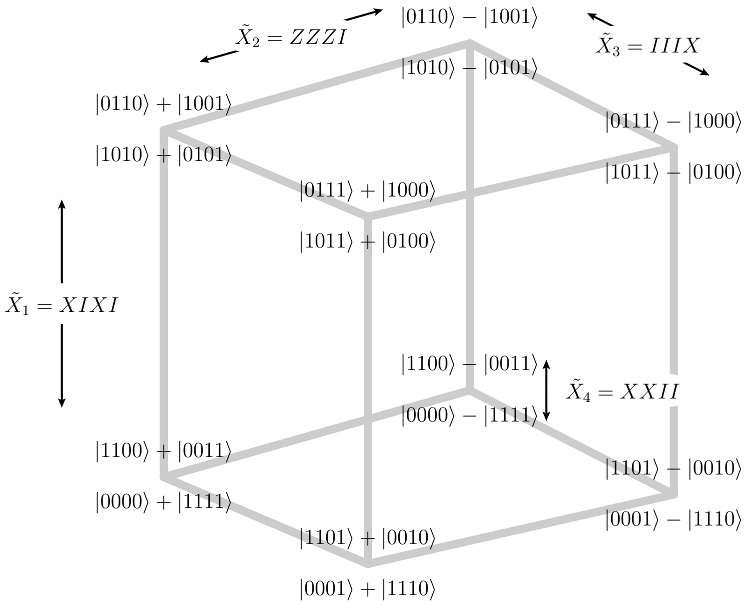
where the number of rows equals n and each entry commutes with the entries on other rows, and anticommutes with the entry on the same row. If we take all the operators in the left column we get the operators $\{ZZII, XXXX, ZZZZ, ZIZI\}$. These generate an abelian group that stabilizes the state $|\psi\rangle = |0000\rangle + |1111\rangle$. Let r be the gauge operator $XXII$ adjacent to the stabilizer $ZIZI$, The state $|\psi\rangle$ then lies in the $G-$orbit

$$\{|\psi\rangle, r|\psi\rangle\} = \{|0000\rangle + |1111\rangle, |1100\rangle + |0011\rangle\}.$$

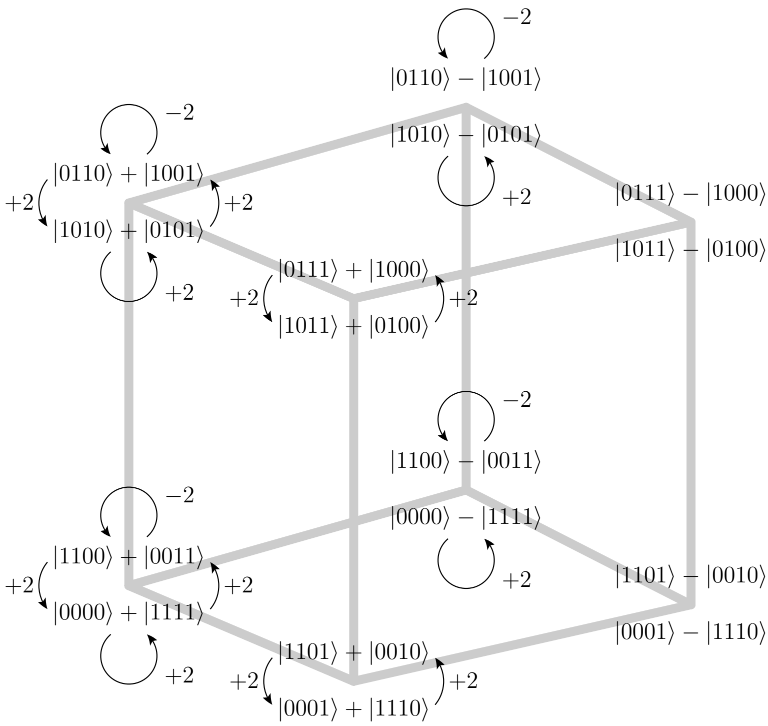
We use the T_0 operators $t_1 = ZZZI$ and $t_2 = IIIX$ to list three other $G-$orbits:

$$\{t_1|\psi\rangle, t_1 r|\psi\rangle\}, \{t_2|\psi\rangle, t_2 r|\psi\rangle\}, \{t_1 t_2|\psi\rangle, t_1 t_2 r|\psi\rangle\}.$$

Here we have sixteen vectors forming an orthogonal basis for the state space. They are arranged on the vertices of a cube. This cube is actually a four dimensional hypercube, but we suppress the last dimension in this diagram. Such an arrangement of basis vectors has a cartesian product structure which induces a tensor product decomposition of the original state space.



The Hamiltonian acts on states by left multiplication. Because this action is a sum of gauge group elements, it will decompose into blocks, one for each $G-$orbit. We depict this action as a weighted graph, where we omit edges with zero weight:



$$
\begin{aligned}
H &= XXII + IIXX + ZIZI + IZIZ \\
&= \tilde{X}_4 + \tilde{Z}_2\tilde{X}_4 + \tilde{Z}_4 + \tilde{Z}_3\tilde{Z}_4 \\
&= (I + \tilde{Z}_2)\tilde{X}_4 + (I + \tilde{Z}_3)\tilde{Z}_4.
\end{aligned}
$$

Using the symmetry invariant basis computed from the orbits we can write the matrix for the Hamiltonian in block diagonal form:

$$
H = \begin{pmatrix} 2(X+Z) & 0 & 0 & 0 \\ 0 & 2X & 0 & 0 \\ 0 & 0 & 2Z & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \otimes I
$$

2.1.2 Complex representations

The Pauli group

The Pauli group $\mathcal{P}_1$ is normally defined as a set of matrices closed under matrix multiplication, but we can define it abstractly as the group generated by the (abstract) elements $\{\omega, X, Z\}$ with relations as follows:

$$
\omega^2 = I,\ X^2 = I,\ Z^2 = I,\ \omega X \omega X = I,\ \omega Z \omega Z = I,\ \text{and}\ \omega ZXZX = I,
$$

where I is the group idenity. Actually, ω is generated by X and Z, so it is not necessary to include ω in the generating set, but here it simplifies the relations. This group has eight elements, and is isomorphic to the dihedral group D_4, the symmetry group of a square.

To define the *n-qubit Pauli group* $\mathcal{P}_n$, we use the $2n+1$ element generating set

$$
\{\omega, X_1, .., X_n, Z_1, .., Z_n\}
$$

with relation $\omega^2 = I$ as before, and

$$X_i^2 = I,\ Z_i^2 = I,\ \omega X_i \omega X_i = I,\ \omega Z_i \omega Z_i = I,\ \omega Z_i X_i Z_i X_i = I,\ \text{for } i = 1, ...n,$$
$$Z_i X_j Z_i X_j = I,\ \text{for } i, j = 1, .., n,\ i \neq j. \tag{2.1}$$

This abstract approach to the definition of a group is known as a group *presentation*. In general, this is a set of generators together with a set of relations satisfied by these generators.

Note that each of the generators squares to the identity, and of these, only ω commutes with every element of $\mathcal{P}_n$. Therefore we will write ω as $-I$, similarly $\pm I$ will denote the set $\{\omega, I\}$, and $-X$ is ωX, etc.

We write the group commutator as $[[g, h]] := ghg^{-1}h^{-1}$ and note the important commutation relation:

$$[[Z_i, X_j]] = \begin{cases} -I & \text{if } i = j, \\ I & \text{if } i \neq j. \end{cases}$$

If we take an arbitrary $g \in \mathcal{P}_n$ written as a product of the generators, it follows that we can rewrite this product uniquely as $g = \pm g_1 ... g_n$ where each g_i is one of I, Z_i, X_i or $X_i Z_i$ for $i = 1, .., n$. Therefore, the size of the Pauli group is

$$|\mathcal{P}_n| = 2^{2n+1}.$$

The subgroup of $\mathcal{P}_n$ generated by the elements $\{X_1, ..., X_n\}$ is denoted $\mathcal{P}_n^X$. These are the X-type elements. Similarly, $\{Z_1, ..., Z_n\}$ generates the subgroup of Z-type elements $\mathcal{P}_n^Z$.

Subgroups of the Pauli group

We now define an $n-$*qubit gauge group* to be any non-abelian subgroup G of $\mathcal{P}_n$, defined by a set of generators $G_0 \subset \mathcal{P}_n$,

$$G := \langle G_0 \rangle.$$

Because G is not abelian, it follows that $-I \in G$. We also restrict G_0 to only contain Hermitian operators, which is equivalent to requiring that $g^2 = I$ for all $g \in G_0$.

Now let S be the largest subgroup of G not containing $-I$. S is then an abelian subgroup, also known as the *stabilizer* subgroup. G decomposes as a direct product:

$$G = S \times R,$$

where $R \cong P_r$ for some $1 \leq r \leq n$, and $S \cong \mathbb{Z}_2^m$ for $0 \leq m < n$. Therefore,

$$|G| = |S||R| = 2^{m+2r+1}.$$

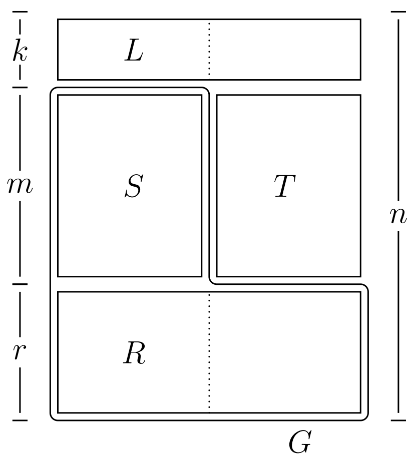
We call R the *reduced gauge group*. We consider both S and R to be subgroups of G. Let $\phi : R \to P_r$ be a group isomorphism, then $R_0 := \{\phi^{-1}(X_i), \phi^{-1}(Z_i)\}_{i=1,..,r}$ is a set of independent generators of R. We also let S_0 be a set of m independent generators of S.

To find the cosets of G in $\mathcal{P}_n$ we take the group closure of $G - \mathcal{P}_n$; when this is non-empty we only need to add I and $-I$. This is another gauge group, whose reduced gauge group is known as the *logical* operators L, and whose stabilizer subgroup is known as the *error* operators T. Now any coset of G can be written as ltG with $l \in L$ and $t \in T$. The size of T equals the size of S: $|T| = |S| = 2^m$. If we let L_0 be an independent generating set for L then we have the important formula:

$$n = \frac{1}{2}|L_0| + |S_0| + \frac{1}{2}|R_0| \tag{2.2}$$

$$= k + m + r \tag{2.3}$$

We summarize the information in this section in a table of Pauli group elements arranged in two columns and n rows:



Here we show the $2n$ generators of $\mathcal{P}_n$ arranged so that each row contains a pair of generators, where each such generator anti-commutes with the operator on the same row and commutes with all the other operators in the table. Note that this is exactly the definition of the Pauli group via a presentation given in the previous section. Furthermore, the table shows $2k$ generators of L, m generators each for S and T, and $2r$ generators of R. The gauge group G encloses R and S, and one can immediately see how L and T also form a gauge group.

Representations of the Pauli group

We now define the *Pauli representation* of the Pauli group as a group homomorphism:

$$\rho_{\text{pauli}} : \mathcal{P}_n \to \mathrm{GL}(\mathbb{C}[2^n])$$

where $\mathbb{C}[2^n]$ is the 2^n-dimensional state space of n qubits. On the independent generators $\{X_1, .., X_n, Z_1, .., Z_n\}$, ρ_{pauli} is defined as the following tensor product of 2×2 matrices:

$$\rho_{\text{pauli}}(X_i) := \bigotimes_{j=1}^{n} \begin{cases} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{for } j = i \\ \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{for } j \neq i \end{cases}$$

$$\rho_{\text{pauli}}(Z_i) := \bigotimes_{j=1}^{n} \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \text{for } j = i \\ \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{for } j \neq i \end{cases}$$

Normally the image of ρ_{pauli} is thought of as the Pauli group itself, and we are indeed free to think that way because ρ_{pauli} is a group isomorphism.

Given a group representation $\rho : G \to GL(V)$ the *character* of ρ is a function

$\chi_\rho : G \to \mathbb{C}$ given by

$$\chi_\rho(g) = \text{Tr } \rho(g).$$

Given two functions $u, v : G \to \mathbb{C}$ we define the following inner product:

$$\langle u, v \rangle := \frac{1}{|G|} \sum_{g \in G} u(g)\overline{v(g)}.$$

The character of the Pauli representation, $\chi_{pauli} : \mathcal{P}_n \to \mathbb{C}$ is given by:

$$\chi_{pauli}(g) = \sum_{v \in basis} \langle v|\rho_{pauli}(g)|v\rangle = \begin{cases} \pm 2^n & \text{if } g = \pm I \\ 0 & \text{otherwise} \end{cases}$$

Since $|P_n| = 2^{2n+1}$ it follows that $\langle \chi_{pauli}, \chi_{pauli} \rangle = 1$ and so ρ_{pauli} is an irreducible representation of $\mathcal{P}_n$.

The only other irreps of $\mathcal{P}_n$ are the 1-dimensional irreps $\rho : \mathcal{P}_n \to \mathbb{C}$ defined on the independent generators as:

$$\rho(X_i) = \pm 1, \quad \rho(Z_i) = \pm 1.$$

So we have 2^{2n} many 1-dimensional irreps, and a single 2^n-dimensional irrep. Summing the squares of the dimensions shows that we have a complete set of irreps of $\mathcal{P}_n$.

Representations of gauge groups

Although ρ_{pauli} restricted to a gauge group $G \subset \mathcal{P}_n$ serves as a representation of G it is no longer irreducible. Our aim will be to decompose ρ_{pauli} into irreps of G.

The 1-dimensional irreps $\rho : G \to \mathbb{C}$, are now defined by specifying the action of ρ on the independent generators:

$$\rho(h) = \pm 1 \text{ for } h \in S_0, \quad \rho(\phi^{-1}(X_i)) = \pm 1, \quad \rho(\phi^{-1}(Z_i)) = \pm 1.$$

This gives all 2^{m+2r} of the 1-dimensional irreps.

The 2^r-dimensional irreps are given by:

$$\rho(h) = \pm I^{\otimes r} \text{ for } h \in S_0, \quad \rho(\phi^{-1}(X_i)) = X_i, \quad \rho(\phi^{-1}(Z_i)) = Z_i.$$

We are free to choose the signs of the $\rho(h)$ for each $h \in S_0$. Hence there are 2^m many of these irreps. Each such choice corresponds to the choice of a *syndrome* vector $s(h) = \pm 1$, for $h \in S_0$, or alternatively, choice of an element $t \in T$:

$$\rho_t^1(h) = \begin{cases} I^{\otimes r} & \text{if } th = ht \\ -I^{\otimes r} & \text{if } th = -ht \end{cases}$$

Because G decomposes into a direct product $G = S \times \mathcal{P}_r$ we have the following representations:

$$\rho_t(g) = \rho_t^1(h)\rho_{pauli}^r(g'),$$

where $g = hg'$, $h \in S$, $g' \in \mathcal{P}_r$ and ρ_{pauli}^r is the r-qubit Pauli representation. The character for this representation is:

$$\chi_t(hg') = \rho_t^1(h) \sum_{v \in basis} \langle v|\rho_{pauli}^r(g')|v\rangle = \begin{cases} \pm 2^r \rho_t^1(h) & \text{if } g' = \pm I \\ 0 & \text{otherwise} \end{cases}$$

We have that $|G| = 2^{2r+m+1}$ and so $\langle \chi_t, \chi_t \rangle = 1$ and ρ_t is an irreducible representation of G. We now count the occurances of this representation in ρ_{pauli}^r:

$$\begin{aligned} \langle \chi_{pauli}^r, \chi_t \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_{pauli}^r(g)\overline{\chi_t(g)} \\ &= \frac{1}{2^{2r+m+1}} \sum_{g = \pm I} 2^n 2^r = \frac{2^{n+1+r}}{2^{2r+m+1}} = 2^k \end{aligned}$$

where k is the number of logical qubits so that $n = r + m + k$.

In summary, the Pauli representation decomposes into 2^m many irreps ρ_t, each with dimension 2^r, and appearing with multiplicity 2^k :

$$\rho_{\text{pauli}} = \bigoplus_{t \in T} \rho_t \otimes I^{\otimes k}$$

Symmetry invariant basis

In general, given a representation $\rho : G \to \mathrm{GL}(V)$ and the character of some irreducible representation $\chi : G \to \mathbb{C}$ the following operator $P : V \to V$ projects onto the subspace on which this irreducible representation acts:

$$P := \frac{d}{|G|} \sum_{g \in G} \overline{\chi(g)} \rho(g).$$

where d is the dimension of the irreducible representation. We can use this to calculate projectors onto the irreps ρ_t in ρ_{pauli}:

$$\begin{aligned}
P_t &= \frac{d}{|G|} \sum_{g \in G} \overline{\chi_t(g)} \rho_{pauli}(g) \\
&= \frac{d}{|G|} \sum_{h \in S} \sum_{g \in R} \overline{\chi_t(hg)} \rho_{pauli}(hg) \\
&= \frac{d}{|G|} 2^{2r} \sum_{h \in S} \rho_t^1(h) \rho_{pauli}(h) \\
&= \frac{1}{2^m} \sum_{h \in S} \rho_t^1(h) \rho_{pauli}(h).
\end{aligned}$$

We can also write this as a product of projectors onto the ± 1 eigenspaces of stabilizers $\rho_{pauli}(h)$ for $h \in S$. Choose generators $h_1, ..., h_m$ of S and then the projectors onto the ± 1 eigenspace of $\rho_{pauli}(h_i)$ are

$$P_t^i = \frac{1}{2} \big(I^{\otimes n} \pm \rho_{pauli}(h_i) \big)$$

and we see that

$$P_t = \prod_{i=1,...,m} P_t^i = \frac{1}{2^m} \big(I^{\otimes n} \pm \rho_{pauli}(h_1) \big) ... \big(I^{\otimes n} \pm \rho_{pauli}(h_m) \big).$$

This projector will have rank 2^{k+r} and

$$U := \sum_{t \in T} P_t$$

is a unitary transformation that sends physical qubits to encoded qubits.

The Hamiltonian

The Hamiltonian of interest is an operator $H : \mathbb{C}[2^n] \to \mathbb{C}[2^n]$:

$$H := \sum_{g \in G_0} \rho_{\text{pauli}}(g).$$

Using the above decomposition we find:

$$\begin{aligned} H &= \sum_{g \in G_0} \bigoplus_{l \in L, t \in T} \rho_t(g) \\ &= \bigoplus_{l \in L, t \in T} \sum_{g \in G_0} \rho_t(g). \end{aligned}$$

We will notate each block as $H_t := \sum_{g \in G_0} \rho_t(g)$ for each irrep ρ_t appearing in H.

> **Fact 0:**
>
> The Hamiltonian is block diagonalized, with blocks indexed by operators t in the abelian group T and multiplicity 2^k :
>
> $$H = \bigoplus_{t \in T} H_t \otimes I^{\otimes k}.$$

More generally, we can assign real valued weights $J_g \in \mathbb{R}$ to each operator $g \in G_0$,

$$H = \sum_{g \in G_0} J_g \rho_{\text{pauli}}(g) = \bigoplus_{l \in L, t \in T} \sum_{g \in G_0} J_g \rho_t(g).$$

In other words, using weights does not change the block structure of H.

In the following sections we will forget the distinction between g and $\rho_{\text{pauli}}(g)$, so terms such as Z and X can be understood as the corresponding Pauli linear operators.

2.1.3 Applications

We now use the tools built so far to analyse two examples of gauge code Hamiltonians. The above procedure is not entirely automatic, it relies on extracting the isomorphism ϕ, but when this can be made to work it works surprisingly well.

2D compass model

Here we consider the two-dimensional compass model [2]. We coordinatize the qubits on a square lattice of $l \times l$ sites, (i, j) for $1 \le i, j \le l$. This gives $n = l^2$. For the single qubit Pauli operators acting on site (i, j) we coordinatize with subscripts ij, with i and j understood modulo l. The generators of the gauge group are

$$G_0 = \big\{X_{ij}X_{i,j+1},\ Z_{ij}Z_{i+1,j} \text{ for } 1 \le i, j \le l\big\}.$$

We write generators of the reduced gauge group in anti-commuting pairs:

$$R_0 = \big\{X_{i1}X_{ij},\ Z_{1j}Z_{ij} \text{ for } 2 \le i, j \le l\big\}.$$

This makes it clear the isomorphism $\phi : R \to \mathcal{P}_r$ to use, and we again use pairs i, j to coordinatize $\mathcal{P}_r$:

$$\phi(X_{i1}X_{ij}) = X_{i-1,j-1},\quad \phi(Z_{1j}Z_{ij}) = Z_{i-1,j-1},\ \text{for } 2 \le i, j \le l.$$

The generators for the stabilizers are

$$S_0 = \big\{\prod_{i=1}^{l} X_{ij}X_{i,j+1},\ \prod_{i=1}^{l} Z_{ji}Z_{j+1,i} \text{ for } 1 \le j \le l-1\big\}.$$

The logical operators are generated by $L_0 = \big\{\prod_i X_{i1}, \prod_j Z_{1j}\big\}$. These sets have cardinalities:

$$|G_0| = 2l^2,\ |R_0| = 2(l-1)^2,\ |S_0| = 2(l-1).$$

And we note that $k+m+r = n$ is satisfied. Now we write down the values of the irreps on the gauge operators. Here we define each irrep using a pair of syndrome vectors s_X

and s_Z :

$$\rho(X_{i1}X_{i2}) = X_{i-1,1} \qquad \rho(Z_{1i}Z_{2i}) = Z_{1,i-1}$$
$$\text{for } 2 \le i \le l$$
$$\rho(X_{il}X_{i1}) = X_{i-1,l-1} \qquad \rho(Z_{li}Z_{1i}) = Z_{l-1,i-1}$$
$$\text{for } 2 \le i \le l$$
$$\rho(X_{ij}X_{i,j+1}) = X_{i-1,j-1}X_{i-1,j} \qquad \rho(Z_{ji}Z_{j,i+1}) = Z_{j-1,i-1}Z_{j,i-1}$$
$$\text{for } 2 \le i \le l, 2 \le j < l$$
$$\rho(X_{1j}X_{1,j+1}) = s_X(j-1)\prod_{i=1}^{l-1} X_{i,j-1}X_{ij} \qquad \rho(Z_{j1}Z_{j+1,1}) = s_Z(j-1)\prod_{i=1}^{l-1} Z_{j-1,i}Z_{ji}$$
$$\text{for } 2 \le j < l$$
$$\rho(X_{11}X_{12}) = \prod_{j=1}^{l-1} s_X(j)\prod_{i=1}^{l-1} X_{i1} \qquad \rho(Z_{11}Z_{21}) = \prod_{j=1}^{l-1} s_Z(j)\prod_{i=1}^{l-1} Z_{1i}.$$

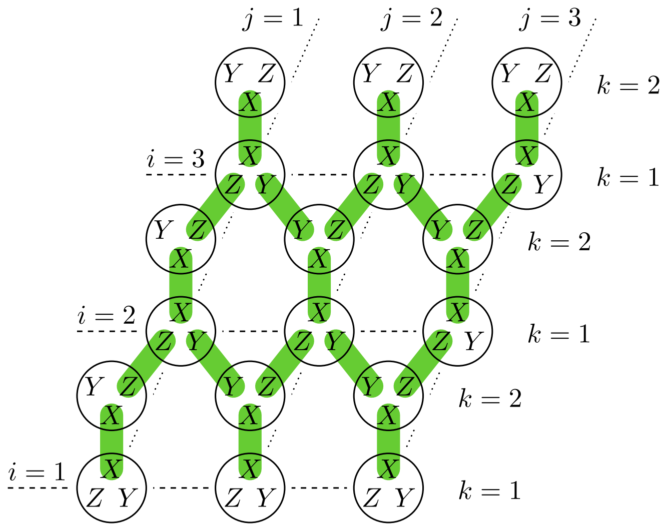
Note the transposition symmetry between the X and Z-type operators. We sum all these terms to find the form of the hamiltonian in each block:

$$H_\rho = \sum_{g \in G_0} \rho(g) = \sum_{1 \le i,j < l} \rho(X_{ij}X_{i,j+1}) + \rho(Z_{ij}Z_{i+1,j}).$$

We note that in [12], they perform a spin transformation of the compass model which also results in an $(l-1) \times (l-1)$ lattice of spins and identical Hamiltonian up to some signs.

Kitaev honeycomb model

The Kitaev honeycomb model [25] is built from spins on the sites of a hexagonal lattice. The lattice of linear size l has $n = 2l^2$ sites which we coordinatize using integer triples i, j, k with $1 \le j, k \le l$ and $k = 1, 2$. We use periodic boundary conditions so i, j are to be taken modulo l. Gauge generators have support on the edges of the honeycomb lattice, and we depict qubits here as circles:



The edges of the lattice are in one-to-one correspondence with the generators G_0:

$$G_0 := \left\{ X_{ij1}X_{ij2},\ Z_{ij2}Z_{i+1,j1},\ Y_{ij1}Y_{i-1,j+1,2} \text{ for } 1 \le i,j \le l \right\}.$$

Note that we make the definition $Y := XZ$ for each site.

Stabilizers are generated from closed strings of gauge operators. For example, each hexagon gives a stabilizer

$$\begin{aligned} h_{ij} :&= X_{ij1}X_{ij2}Z_{ij2}Z_{i+1,j1}Y_{i+1,j1}Y_{i,j+1,2}X_{i,j+1,2}X_{i,j+1,1}Z_{i,j+1,1}Z_{i-1,j+1,2}Y_{i-1,j+1,2}Y_{ij1} \\ &= Z_{ij1}Y_{ij2}X_{i+1,j1}Z_{i,j+1,2}Y_{i,j+1,1}X_{i-1,j+1,2}. \end{aligned}$$

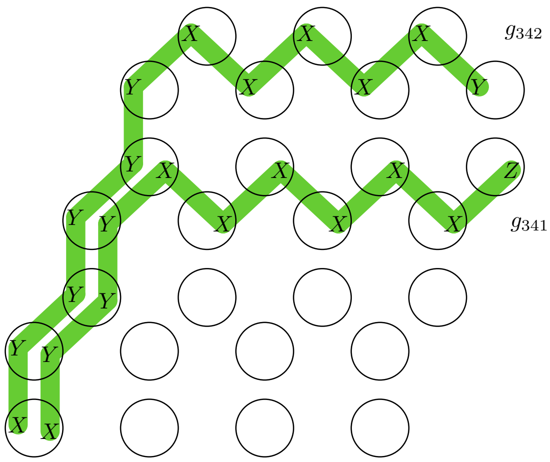
And the two homologically non-trivial loops give stabilizers:

$$h_v := \prod_{i=1}^{l} Y_{i11}Y_{i12}, \quad h_h := \prod_{j=1}^{l} X_{1j2}X_{2j1}.$$

This gives independent stabilizer generators S_0 from each hexagon, less one, as well as h_v and h_h. The number of hexagons is $\frac{1}{2}n$ and so we find $|S_0| = \frac{1}{2}n + 1$. There are no logical operators, so we must have $|R_0| = n - 2$.

Now we construct a set of string operators R_0, one for each site on the lattice, except for the two sites $(1,1,1)$ and $(1,1,2)$. Each string $g_{ijk} \in R_0$ is constructed as the product of gauge operators along a path starting at $(1,1,1)$ and terminating at (i,j,k).

Two elements of the set R_0 corresponding to $i = 3$, $j = 4$ and $k = 1, 2$.



Each such path is built from two "straight" path segments, first in the i direction and then in the j direction. The paths for operators g_{ij1} and g_{ij2} coincide along the i direction but become disjoint in the j direction: the g_{ij1} path goes around the bottom of the hexagons and the g_{ij2} path goes around the top. With periodic boundary conditions R_0 forms an independent generating set of R of size $n-2$.

We construct an isomorphism $\phi : R \to \mathcal{P}_r$ by sending elements of R_0 bijectively to the following independent generating set of $\mathcal{P}_r$:

$$\left\{c_{2j} := Z_1 ... Z_{j-1} X_j,\ c_{2j+1} := Z_1 ... Z_{j-1} Y_j \quad \text{for } 1 \leq j \leq r\right\}.$$

The bijection is constrained by setting $\phi(g_{ij1}) := c_{2j'+1}$ and $\phi(g_{ij2}) := c_{2j'}$ where j' is chosen uniquely for each i, j. The c_j are paired Majorana fermion operators [25].

We check this is a group homomorphism by showing that relations satisfied by elements of R_0 are satisfied by their images under ϕ. All such relations are either of the form $g^2 = \ \pm\ I$, $gg' = \pm\ g'g$, or products thereof. So it is sufficient to check squares of elements and commutation relations. Every element of R_0 anticommutes with every other element of R_0, and this is true also of the c_j. Also, $g_{ij1}^2 = -I$ and $g_{ij2}^2 = I$ is preserved by ϕ because $c_{2j}^2 = I$ and $c_{2j+1}^2 = -I$. Finally, ϕ is an isomorphism because it is a bijection of two independent generating sets.

The next step is to write each element of G_0 as a product of reduced gauge operators and stabilizers. The key thing to note is that the product of two operators $g_{ijk}, g_{i'j'k'} \in R_0$ gives a string operator between the sites (i, j, k) and (i', j', k'). And *any* string operator between these two sites can then be generated by using stabilizers to "deform" the string $g_{ijk}g_{i'j'k'}$. For example, taking the product of two operators from R_0 that differ by one path segment gives the following:

$$Z_{ij2}Z_{i+1,j,1} = g_{ij2}g_{i+1,j,1}$$
$$Y_{i+1,j,1}Y_{i,j+1,2} = g_{i+1,j,1}g_{i,j+1,2}$$

We need the homologically non-trivial stabilizers to get these:

$$Z_{lj2}Z_{1j1} = h_v g_{lj2}g_{1j1} \qquad \text{for } \; 2 \leq j \leq l$$

And the $X_{ij1}X_{ij2}$ gauge operators can be generated by the product of $g_{ij1}g_{ij2}$ and the enclosed hexagon stabilizers:

$$X_{ij1}X_{ij2} = g_{ij1}g_{ij2}\prod_{j'=1}^{j-1} h_{ij'}.$$

The only G_0 operators that are not quadratic in R_0 operators are the five operators that touch either of the sites $(1,1,1)$ or $(1,1,2)$.

So each block in the Hamiltonian is seen to be quadratic in the c_j plus five other Pauli operator terms which we denote as Λ_ρ:

$$H_\rho = \sum_{ij}\Gamma_{ij}(\rho)c_ic_j + \Lambda_\rho$$

The coefficients Γ_{ij} are dependant on the irrep ρ.

In [24] they introduce a similar set of mutually anti-commuting string operators R_0.

2.1.4 $\mathcal{F}_2$-linear representations

This is a way of "brute-forcing" the representations when we cannot find a way of writing them down in a closed form expression. For finite systems this yields an algorithm that is efficiently implementable.

In this section, and the remainder of this paper, we restrict our attention to gauge groups formed from terms in $\mathcal{P}_n^X \cup \mathcal{P}_n^Z$. We call these *CSS gauge codes.* We briefly review the $\mathcal{F}_2$ symplectic structure of these operators.

Both $\mathcal{P}_n^X$ and $\mathcal{P}_n^Z$ are abelian groups, and can be identified with the additive group structure of the n dimensional vector space over the finite field of two elements $\mathcal{F}_2$:

$$\mathcal{P}_n^X \cong \mathcal{F}_2^n, \quad \mathcal{P}_n^Z \cong \mathcal{F}_2^n.$$

We do this in the obvious way by sending X_i to the basis vector with 1 in the $i-$th entry, and similarly for each Z_i. We also identify the computational basis of our statespace $\mathbb{C}[2^n]$ with $\mathcal{F}_2^n$ in the obvious way:

$$\mathbb{C}[2^n] \cong \mathbb{C}[\mathcal{F}_2^n].$$

This has the potential to be very confusing, and so where appropriate we use X and Z subscripts.

X-type operators act on the $\mathbb{C}[\mathcal{F}_2^n]$ basis vectors using $\mathcal{F}_2$ addition:

$$g_X \in \mathcal{P}_n^X \cong \mathcal{F}_2^n, \quad g_X : v \longmapsto g_X + v$$

Z-type operators act on the $\mathbb{C}[\mathcal{F}_2^n]$ basis vectors using $\mathcal{F}_2$ inner product:

$$g_Z \in \mathcal{P}_n^Z \cong \mathcal{F}_2^n, \quad g_Z : v^\top \longmapsto g_Z v^\top$$

This is an $\mathcal{F}_2$ scalar, just zero or one. We think of this as a "syndrome". This suggests that actually these Z-type operators live in the dual vector space $\mathcal{F}_2^{n*}$. Because of the underlying symmetry (and notational confusion) between the X and Z-type operators, we make the convenction that by default all our $\mathcal{F}_2$ vectors come as row vectors (ie. dual vectors). This means we use the transpose operator $^\top$ to indicate a primal (column) vector.

It doesn't make sense to add an X-type operator and a Z-type operator:

$$g_Z + g_X \quad \textit{no no!!!}$$

but it does make sense to take the inner product:

$$g_Z g_X^\top = g_X g_Z^\top.$$

This is an $\mathcal{F}_2$ scalar which gives the commutator of the two operators.

A $\mathcal{F}_2$-linear operator such as $A : \mathcal{F}_2^n \to \mathcal{F}_2^m$ acts on the left as $u^\top \mapsto Au^\top$. It also acts on dual vectors as $A : \mathcal{F}_2^{m*} \to \mathcal{F}_2^{n*}$ which corresponds to acting on the right: $v \mapsto vA$. We call the rowspace of A the *span* and denote it as

$$\langle A \rangle = \{vA | v \in \mathcal{F}_2^{m*}\}$$

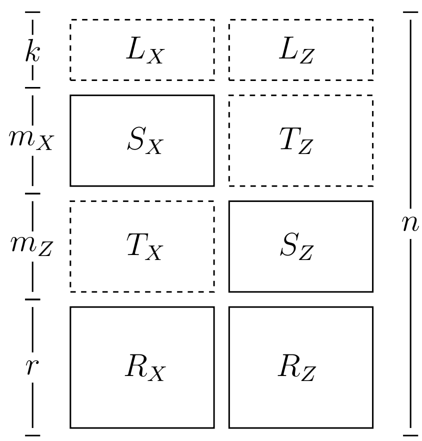
The kernel of A is defined as

$$\ker(A) = \{u^\top | u^\top \in \mathcal{F}_2^n, \quad Au^\top = 0\}.$$

We wish to use this language to decompose a CSS gauge group G. First we write the gauge group generators in terms of X-type and Z-type operators:

$$G_0 = G_X \cup G_Z.$$

Following the theory from the previous section, we are going to rewrite the gauge group generators as a union of stabilizer generators $S_0 = S_X \cup S_Z$ and reduced gauge generators $R_0 = R_X \cup R_Z$. Similarly, the error operators will be split into X and Z type operators T_X and T_Z and finally the logical operators L_X and L_Z. We summarize all of these sets in the following table:



The solid rectangles indicate operators that span the X and Z parts of the gauge group, and the dashed rectangles indicate operators that do not live inside the guage group.

We consider each of these blocks $L_X, L_Z, S_X, T_Z, T_X, S_Z, R_X, R_Z$, as well as G_X, G_Z, as either a set of $\mathcal{F}_2^{n*}$ vectors (the rows) or as an $\mathcal{F}_2$-linear operator. For example, we write $u \in R_X$ to mean u is a row of the matrix R_X.

We first find the stabilizers S_Z. These are built out of $\mathcal{F}_2^{n*}$ vectors from the span of G_Z that commute with the rows of G_X :

$$
\begin{aligned}
\langle S_Z \rangle &= \{ \ vG_Z \mid vG_Z G_X^\top = 0, \quad v \in F_2^{|G_Z|*} \ \} \\
&= \{ \ vG_Z \mid v^\top \in \ker(G_X G_Z^\top) \ \}.
\end{aligned}
$$

The generators (rows of S_Z) are then extracted from this span by row reduction. We swap the role of X and Z to find S_X.

Once we have the stabilizers, in order to complete the above table as a presentation of the Pauli group we solve the following $\mathcal{F}_2$ block matrix equation,

$$
\begin{pmatrix} L_X \\ S_X \\ T_X \\ R_X \end{pmatrix} \begin{pmatrix} L_Z \\ T_Z \\ S_Z \\ R_Z \end{pmatrix}^\top = I,
$$

subject to the restriction that the rows of R_X lie in the span of G_X and the rows of L_X do not. Similarly for R_Z and L_Z. This set of 16 equations is quadratic in the unknown variables and so it is not obvious how to proceed, but it turns out a systematic way can be found.

We begin by finding L_Z. These operators satisfy the following *homology* condition:

$$
l_Z \in L_Z \ \text{ is given by } \ l_Z^\top \in \ker(G_X) \mod \langle S_Z \rangle.
$$

In other words, L_Z is formed from a basis for the kernel of G_X row-reduced using S_Z.

To be more specific we take any direct sum decomposition

$$\mathcal{F}_2^{n*} = \langle S_Z \rangle \oplus V$$

then the operation of mod $\langle S_Z \rangle$ is the projection onto V. We can explicitly write such a projector as the $n \times n$ matrix given by

$$P_Z = I + A^\top S_Z$$

where the matrix A is the $m_Z \times n$ matrix consisting of the leading 1's in any row-reduction of S_Z. We define P_X similarly for the operation of mod $\langle S_X \rangle$.

To find L_X we solve the following $\mathcal{F}_2$-linear system:

$$\begin{pmatrix} L_Z \\ G_Z \end{pmatrix} L_X^\top = \begin{pmatrix} I \\ 0 \end{pmatrix}$$

The reduced gauge group matrix R_X is found as a row-reduction of $G_X P_X$. We cannot merely set R_Z to be $G_Z P_Z$ because we also require $R_X R_Z^\top = I$. Instead we define the auxiliary matrix $\widetilde{R}_Z$ to be a row-reduction of $G_Z P_Z$.

The error operators T_X are then found as the solution to the $\mathcal{F}_2$-linear system:

$$\begin{pmatrix} L_Z \\ S_Z \\ \widetilde{R}_Z \end{pmatrix} T_X^\top = \begin{pmatrix} 0 \\ I \\ 0 \end{pmatrix}$$

And then the operators T_Z solve the $\mathcal{F}_2$-linear system:

$$\begin{pmatrix} L_X \\ S_X \\ T_X \\ R_X \end{pmatrix} T_Z^\top = \begin{pmatrix} 0 \\ I \\ 0 \\ 0 \end{pmatrix}$$

Finally at this point R_Z is given as the solution to

$$\begin{pmatrix} L_X \\ S_X \\ T_X \\ R_X \end{pmatrix} R_Z^\top = \begin{pmatrix} 0 \\ 0 \\ 0 \\ I \end{pmatrix}$$

Note that R_Z and $\widetilde{R}_Z$ have identicle span and so we have $R_Z T_X^\top = 0$.

We call this array of eight $\mathcal{F}_2$-linear matrices an (L, S, T, R)-decomposition of the gauge group. In general this will not be unique for any given gauge group.

The Hamiltonian

The complex Hilbert state space of our Hamiltonian has 2^n dimensions and we write this space as $\mathbb{C}[2^n]$. This notation is meant to suggest that we are forming a $\mathbb{C}$ vector space using 2^n "points" as basis vectors. Working in the computational basis, we do indeed have 2^n such points; these are the elements of $\mathcal{F}_2^{n*}$. And so we make the identification

$$\mathbb{C}[2^n] \cong \mathbb{C}[\mathcal{F}_2^{n*}].$$

In other words, we are labeling our basis vectors with elements of $\mathcal{F}_2^{n*}$ and therefore such notation as

$$\langle u|H|v\rangle$$

with $u, v \in \mathcal{F}_2^{n*}$ makes sense. We will make further use of this below, by writing $\mathcal{F}_2$-vector space computations inside the Dirac brakets.

Returning to the code (L, S, T, R)-decomposition above, given the Pauli operator $t \in T$ such that $t = t_X t_Z$ (in $\mathcal{P}_n$) we get a basis for the irrep ρ_t:

$$\{|vR_X + t_X\rangle \text{ such that } v \in \mathcal{F}_2^{r*}\}.$$

In other words, the basis of the irrep ρ_t is an affine subspace of $\mathcal{F}_2^{n*}$. Each such affine subspace is indexed by an element of $\mathcal{F}_2^{r*}$ and all of these are translates of each other, so we make the following identification:

$$\mathbb{C}[\{vR_X + t_X\}_{v\in\mathcal{F}_2^{r*}}] \cong \mathbb{C}[\mathcal{F}_2^{r*}].$$

This will allow us to write the components of each block H_t of the Hamiltonian as $\langle u|H_t|v\rangle$ for $u, v \in \mathcal{F}_2^{r*}$. We make this identification of affine subspaces not out of laziness but because it will help us to compare each of the Hamiltonian blocks H_t below.

> **Important:** The computational basis identifies basis vectors of $\mathbb{C}[2^n]$ with elements of a finite vector space $\mathcal{F}_2^{n*}$:
>
> $$\mathbb{C}[2^n] \cong \mathbb{C}[\mathcal{F}_2^{n*}].$$
>
> The (L, S, T, R)-decomposition naturally splits $\mathcal{F}_2^{n*}$ into 2^{m_Z+k} affine subspaces:
>
> $$\{vR_X + t_X + l_X\}_{v\in\mathcal{F}_2^{r*}}$$
>
> for each $t_X \in \langle T_X\rangle, l_X \in \langle L_X\rangle$. Each such affine subspace forms a basis for the irreducible blocks H_{t_X,t_Z} of H, and can be naturally identified with $\mathcal{F}_2^{r*}$:
>
> $$H_{t_X,t_Z} : \mathbb{C}[\mathcal{F}_2^{r*}] \to \mathbb{C}[\mathcal{F}_2^{r*}].$$

We now wish to understand the action of the gauge group on each of its irreps. Starting with the $t_X, t_Z = 0, 0$ irrep, this is where each of the stabilizers has a trivial action. In $\mathcal{F}_2^n$ this corresponds to the additive action of the zero vector.

States $u \in \langle R_X\rangle$ can be built from a vector matrix product

$$u = vR_X$$

with $v \in \mathcal{F}_2^{r*}$. Since $R_X R_Z^\top = I$ we can write $v = uR_Z^\top$. Each $g_X \in G_X$ acts on u to give

$$
\begin{aligned}
u_1 &= (u + g_X) \bmod \langle S_X \rangle \\
&= (u + g_X) P_X \\
&= (vR_X + g_X) P_X.
\end{aligned}
$$

writing $u_1 = v_1 R_X$ we then have

$$
\begin{aligned}
v_1 &= (vR_X + g_X) P_X R_Z^\top \\
&= v + g_X R_Z^\top.
\end{aligned}
$$

So we have that working in the computational basis, the action of the X part of the gauge group in the $t_X, t_Z = 0, 0$ irrep is to send $v \in \mathcal{F}_2^{r*}$ to $v + g_X R_Z^\top$. In summary, we have the following contributions from the G_X terms of the Hamiltonian:

$$
\langle v | H_{0,0} | v + g_X R_Z^\top \rangle \mathrel{+}= 1, \quad \text{for } g_X \in G_X, v \in \mathcal{F}_2^{r*}
$$

where we use the += notation because there may be other contributions to the same component. These terms will always be off the diagonal unless g_X is a stabilizer.

The action of the G_Z gauge group contributes to the diagonal of H. These diagonal terms apply a kind of "potential energy" penalty to the basis states that depends on the *syndrome* vector:

$$
\text{syndrome}(u) = G_Z u^\top
$$

for $u^\top \in \mathcal{F}_2^n$. This is an $\mathcal{F}_2$ vector that has one component for each row of G_Z. Writing $|G_Z|$ for the number of these rows, and using a *weight* function w that just counts the number of non-zero entries in any $\mathcal{F}_2$ vector we have the following contributions to the Hamiltonian:

$$
\langle v | H_{0,0} | v \rangle \mathrel{+}= |G_Z| - 2w(G_Z R_X^\top v^\top),
$$

for $v \in \mathcal{F}_2^{r*}$.

Adding up all of the above we have in summary,

$$H_{0,0} = \sum_{\substack{v \in \mathcal{F}_2^{r*} \\ g_X \in G_X}} |v + g_X R_Z^\top\rangle\langle v| + \sum_{v \in \mathcal{F}_2^{r*}} \big(|G_Z| - 2w(G_Z R_X^\top v^\top)\big)\ |v\rangle\langle v|.$$

For any $t_X \in \langle T_X \rangle$ the Hamiltonian block $H_{t_X,0}$ has components indexed by basis vectors:

$$u = vR_X + t_X$$

this means that the G_X gauge terms have the same effect on $H_{t_X,0}$ as $H_{0,0}$ and only the diagonal has changed:

$$H_{t_X,0} = \sum_{\substack{v \in \mathcal{F}_2^{r*} \\ g_X \in G_X}} |v + g_X R_Z^\top\rangle\langle v| + \sum_{v \in \mathcal{F}_2^{r*}} \big(|G_Z| - 2w(G_Z R_X^\top v^\top + G_Z t_X^\top)\big)\ |v\rangle\langle v|.$$

Writing the difference explicitly:

$$H_{0,0} - H_{t_X,0} = \sum_{v \in \mathcal{F}_2^{r*}} 2\big(w(G_Z R_X^\top v^\top + G_Z t_X^\top) - w(G_Z R_X^\top v^\top)\big)\ |v\rangle\langle v|.$$

The general form of each the Hamiltonian block is:

$$\begin{aligned} H_{t_X,t_Z} = &\sum_{\substack{v \in \mathcal{F}_2^{r*} \\ g_X \in G_X}} \eta(t_Z g_X^\top)\ |v + g_X R_Z^\top\rangle\langle v| \\ &+ \sum_{v \in \mathcal{F}_2^{r*}} \big(|G_Z| - 2w(G_Z R_X^\top v^\top + G_Z t_X^\top)\big)\ |v\rangle\langle v|. \end{aligned}$$

Here we use η to send $t_Z g_X^\top$ which is an $\mathcal{F}_2$ value to the multiplicative subgroup $\{\pm 1\}$ of $\mathbb{C}$:

$$\eta(0) = 1,\ \eta(1) = -1.$$

The $\eta(t_Z g_X^\top)$ term is a kind of parity check that picks up one phase flip for (some of) the X type stabilizers found in g_X. This works because T_Z is a left inverse of $S_X^\top$. The $t_Z \in \langle T_Z \rangle$ selects which X type stabilizers act as -1 in this irrep.

In summary, we have the complete representation theory for CSS gauge code Hamiltonians.

2.1.5 Lie algebra representations

We now turn to a finer notion of representation theory, being the representation theory of semi-simple Lie algebras.

Recall [18] that an abstract *Lie algebra* $\mathfrak{g}$ is a vector space with a bracket operation:

$$[\ ,\ ] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$$

such that $[A, B] = -[B, A]$ and $[A, [B, C] + [B, [C, A]] + [C, [A, B]] = 0$.

A *representation* of a Lie algebra $\mathfrak{g}$ on a vector space V is a linear map

$$\rho : \mathfrak{g} \to \mathrm{GL}(V)$$

that sends the abstract bracket to the concrete one:

$$\rho([A, B]) = \rho(A)\rho(B) - \rho(B)\rho(A).$$

A Lie algebra requires us to "forget" about multiplication of operators, and only allow taking brackets (and linear combinations.) This is not as crazy as it may seem. The fundamental calculation in the theory of quantum stabilizer codes is actually a Lie algebra calculation. Consider a state $|\psi\rangle$ that is stabilized by some operator $s \in S$:

$$s|\psi\rangle = |\psi\rangle,$$

We wish to understand the effect of an error operator $t \in T$ on our state $|\psi\rangle$, where we have $st = -ts$:

$$st|\psi\rangle = ts|\psi\rangle + [s, t]|\psi\rangle = -ts|\psi\rangle = -t|\psi\rangle,$$

which shows that $t|\psi\rangle$ is a -1 eigenvalue of s. The key point here is that nowhere did we need to multiply (compose) two operators, it was all done using the bracket.

We continue the analysis of CSS gauge code Hamiltonians. The terms of the Hamiltonian block H_{t_X,t_Z} form a Lie algebra which we denote $\mathfrak{g}_{t_X,t_Z}$. The basis for this Lie algebra is formed from all iterated brackets of terms in H_{t_X,t_Z}.

The simplest such example of this is the one qubit Lie algebra which is generated by X and Z. This will have basis $\{X, Z, XZ = \frac{1}{2}[X, Z]\}$ and so is a three dimensional Lie algebra. In fact, it is isomorphic to $sl_2(\mathbb{C})$ the Lie algebra of traceless two by two matrices. Notice that we do not include I in these algebras as this is associated to the multiplicative (group) structure of the operators, and moreover we never need consider Hamiltonians with such terms as these just shift the spectrum by a constant. Notice also that if we try to build a larger Lie algebra from taking iterated brackets of the n-qubit operators $\{X_i, Z_i\}$ we still only get a direct sum of n copies of $sl_2(\mathbb{C})$.

An *ideal* of a Lie algebra $\mathfrak{g}$ is a Lie subalgebra $\mathfrak{h} \subset \mathfrak{g}$ that "eats" all the other elements of $\mathfrak{g}$:

$$[A, B] \in \mathfrak{h}, \quad \text{for all} \quad A \in \mathfrak{h}, B \in \mathfrak{g}.$$

In general the structure of the Lie algebra $\mathfrak{g}_{t_X,t_Z}$ will be more complicated than the corresponding group structure. But we do have the following:

> The Lie algebra $\mathfrak{g}_{t_X,t_Z}$ is a semi-simple subalgebra of $\mathfrak{sl}_{2^n}(\mathbb{C})$.

This follows from the characterization of semi-simple Lie algebras as those having no nonzero abelian ideals.

We also have a ready made *Cartan subalgebra* of $\mathfrak{g}_{t_X,t_Z}$. This is the algebra $\mathfrak{h}_{t_X,t_Z}$ generated by the $Z-$type terms of H_{t_X,t_Z}. The *weight spaces* are the simultaneous eigenspaces of the operators in the Cartan subalgebra. These eigenspaces are labeled by what we called syndromes previously, and these are all one dimensional because the span of R_X does not intersect the kernel of R_Z. Therefore the representation of $\mathfrak{g}_{t_X,t_Z}$ on $\mathbb{C}[\mathcal{F}_2^{r*}]$ is irreducible.

Note that a decomposition of a Lie algebra into disjoint ideals will give a direct sum decomposition of the Lie algebra. Also, any irreducible representation of a direct sum of Lie algebras can be considered as the tensor product of irreducible representations of the individual summands. This is key to the numerical algorithms below: we examine the ideals generated by the terms in the Hamiltonian block H_{t_X,t_Z}. Each such ideal corresponds to a direct summand of $\mathfrak{g}_{t_X,t_Z}$ and so the spectrum of H_{t_X,t_Z} can be written as a sum over spectra of smaller gauge code Hamiltonians corresponding to each ideal.

2.1.6 Applications

Self-dual codes

We make the following definitions. A CSS gauge code is *self-dual* when the X and Z type gauge generators are equal:

$$G_X = G_Z.$$

A CSS gauge code is *weakly self-dual* when there is a permutation P on the set of n qubits that induces equality of the gauge generators:

$$G_X P = G_Z,$$

where we write P as an $n \times n$ permutation matrix. The compass model is then weakly self-dual when we transpose the square lattice of $l \times l$ qubits.

The gauge color code

The three dimensional gauge color code [9, 10] is a self-dual CSS gauge code. It is based on the following geometric construction known as a *colex* [11]. We begin with a tetrahedron and subdivide it into finitely many convex 3-dimensional polytopes, or *balls.* Each ball has a boundary consisting of 0-dimensional cells which we call *vertices*, 1-dimensional cells called *edges* and 2-dimensional cells called *faces.* By a *cell* we mean any of these 0,1,2 or 3-dimensional convex polytopes. Any two balls in this tetrahedral subdivision will have either empty intersection or otherwise intersect on a common vertex, edge or face. When the intersection is on a face these two balls are called *adjacent.* Two vertices in the same edge will also be called adjacent. Each ball is colored by one of four *colors*, either taken to be red, green, blue, yellow or otherwise an element of the set $\{1, 2, 3, 4\}$. The four exterior triangular faces of the bounding tetrahedron are called *regions,* the intersection of two regions is called a *border* and the intersection of three regions is called a *corner.* A cell not contained within any region is called an interior cell.

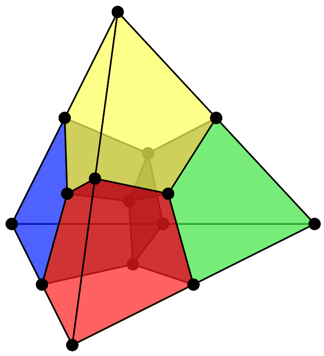
This colored cellulation is required to have the following further properties:

1. Adjacent balls have different colors.

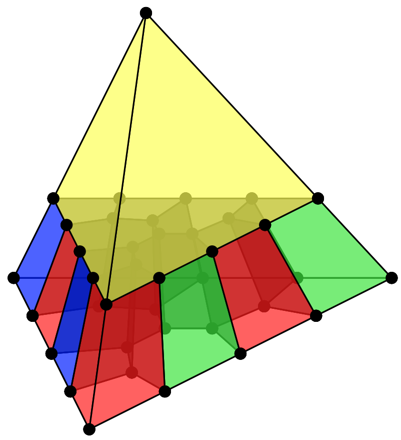
2. Each region has a unique color such that no balls intersecting that region has that color.

3. All vertices are adjacent to four other vertices, except for the corner vertices which are adjacent to three other vertices.

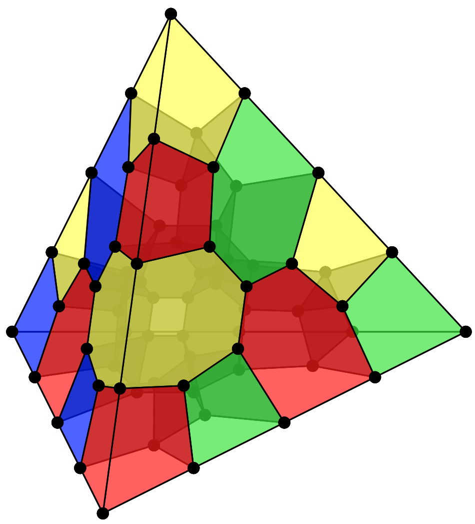
Here we show some instances of this construction, along with the colors of the unobscured balls. Each instance is labeled by the number of vertices n.



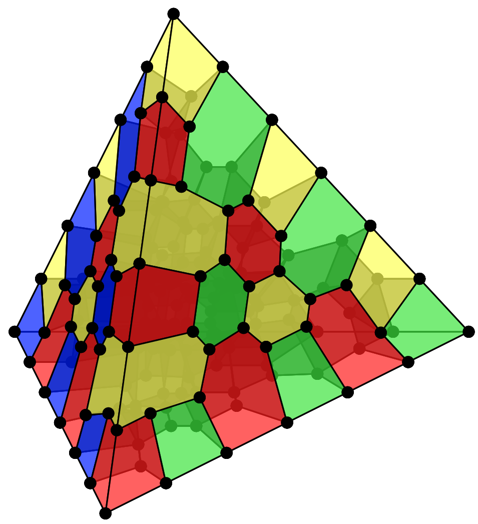
$n = 15$



$n = 39$



$n = 65$

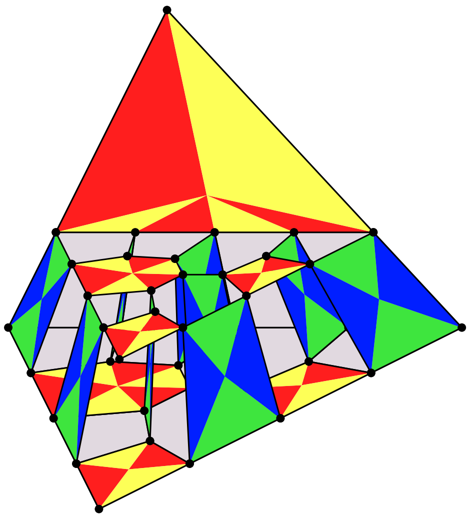


$n = 175$

We note the following consequences of the above conditions. Every face supports an even number of vertices. We now think of each region as corresponding to a “missing” ball. Each edge is then contained in the boundary of three balls. This means we can associate a unique color to each edge, which is also the color of two balls intersecting a vertex of the edge. That is, each edge joins two balls of the same color. Each face bounds two balls, and so we color each face with the two colors of these balls.

Using this cellulation we now construct the gauge code. Qubits are associated with the n vertices. We associate operators to other cells, or union of cells, by using the contained vertices as support. Because this is a self-dual code, the same goes for both the X and Z type operators. The $X/Z-$type gauge group is generated by $X/Z-$type operators supported on each face. The $X/Z-$type stabilizer group is generated by $X/Z-$type operators supported on each ball. There is one $X/Z-$type logical operator and these are generated by $X/Z-$type operators supported on any region.

We next examine the Lie algebra ideal structure. Two faces operators, of X and Z type, will anti-commute only when they intersect on a single vertex. This only happens when such faces have disjoint coloring. Here we show an example of this in the $n = 39$ model:



There are three of these arrangements, each corresponding to the three ways of partitioning the set of colors into two sets of two. It follows that $\mathfrak{g}_{t_X,t_Z}$ is the direct sum of 6 disjoint ideals, and specifically, that each Hamiltonian term in H_{t_X,t_Z} lies in a single one of these ideals. This result is crucial for obtaining the exact diagonalization numerical results below.

2.2 Spectra

2.2.1 Perron-Frobenius structure theory

We now turn to a coarser notion of reducibility. The easiest way to understand this is via graph theory. Given a CSS gauge code Hamiltonian H, we see that the diagonal terms (working in the computational basis) come from the Z operators and the off-diagonal terms come from X type operators. This suggests the following definition. We define a graph Γ with vertices the 2^n computational basis elements, and edges:

$$|v\rangle \mapsto g_X|v\rangle, \quad \text{for all} \quad v \in \mathcal{F}_2^{n*}, g_X \in G_X.$$

These are undirected edges because $g_X^2 = I$. We also add weighted loops corresponding to the Z-type gauge operators:

$$|v\rangle \mapsto \sum_{g_Z \in G_Z} g_Z|v\rangle, \quad \text{for all} \quad v \in \mathcal{F}_2^{n*}.$$

In this way we can consider H and Γ interchangeably, as either a matrix or a graph. An irreducible matrix is one whose corresponding graph is connected. Using the $\mathcal{F}_2$-linear (L, S, T, R)-decomposition of the gauge group we then have the following:

> In the computational basis, any CSS gauge code Hamiltonian H is the direct sum of 2^{m_Z} irreducible matrices Γ_{t_X} indexed by $t_X \in \langle T_X\rangle$ with multiplicity 2^k:
>
> $$H = \bigoplus_{\substack{t_X \in \langle T_X\rangle \\ l_X \in \langle L_X\rangle}} \Gamma_{t_X}.$$

A basis for each Γ_{t_X} is given by a coset of G_X in $\mathcal{F}_2^{n*}$:

$$\{vS_X + uR_X + t_X\}_{v\in\mathcal{F}_2^{m_X*}, u\in\mathcal{F}_2^{r*}}.$$

The off-diagonal entries of H are all positive. If we use a spectral shift operator, a constant multiple of the identity $+cI$, we find that $H + cI$ is a non-negative matrix. We call such a matrix *Perron-Frobenius.* Each of the blocks Γ_{t_X} is also Perron-Frobenius and in combination with their irreducibility this means the following:

For each $t_X \in \langle T_X \rangle$ the largest eigenvalue of Γ_{t_X},

$$\lambda_1(\Gamma_{t_X})$$

is non-degenerate, and is associated with an eigenvector

$$v_1(\Gamma_{t_X})$$

with positive components.

Now we make the restriction that H comes from a weakly self-dual gauge code. Our goal will be to show that the groundspace of H is spanned by vectors which are stabilized. This will imply that $\lambda_1(H) = \lambda_1(H_{0,0})$. To begin, let v_1 be the top eigenvector of Γ_{t_X} with $t_X \in \langle T_X \rangle$. Because v_1 has all positive components it will be fixed by any operator $s \in \langle S_Z \rangle$. To show that the X type stabilizers also fix v_1 we use weak self-duality and see that by change of basis we can swap the roles of the X and Z type operators.

Fact 1:

For any weakly self-dual gauge code Hamiltonian H every groundstate is stabilized and so

$$\lambda_1(H) = \lambda_1(H_{0,0})$$

and for $t_X \in \langle T_X \rangle, t_Z \in \langle T_Z \rangle$ with $t_X \neq 0$ or $t_Z \neq 0$

$$\lambda_1(H) > \lambda_1(H_{t_X,t_Z}).$$

Notice that $H_{0,0}$ is also Perron-Frobenius (in the computational basis) and so has non-degenerate groundspace, but it appears with multiplicity 2^k within the Hamiltonian H and this accounts for the degeneracy of the groundspace of H.

The next goal is to search for the second eigenvalue of H, $\lambda_2(H)$. Using a basis change and the above equation for $H_{t_X,0}$ we have

> **Fact 2:**
>
> Given a weakly self-dual gauge code Hamiltonian H and $t_X \in \langle T_X \rangle$, $t_X \in \langle T_Z \rangle$ the blocks $H_{t_X,0}$ and H_{0,t_Z} are Perron-Frobenius.

We extend the above argument:

> For a weakly self-dual gauge code Hamiltonian, and $t_X \neq 0$, $t_Z \neq 0$
>
> $$\lambda_1(H_{t_X,0}) < \lambda_1(H_{t_X,t_Z}) \quad \text{and}$$
> $$\lambda_1(H_{0,t_Z}) < \lambda_1(H_{t_X,t_Z}).$$

In summary, to find the spectral gap of a weakly self-dual Hamiltonian, which is the difference of the top two eigenvalues of the Hamiltonian, we need only examine the top two eigenvalues of $H_{0,0}$ and the top eigenvalue of $H_{t_X,0}$ for each $t_X \in T_X$.

2.2.2 Numerics

Here we show tables for the first and second eigenvalues of the compass and gauge color code models. These results are obtained using exact diagonalization methods. For each instance we indicate the groundspace eigenvalue λ_1 which is obtained from $H_{0,0}$. Then we list the second eigenvalue of $H_{0,0}$ as well as the first eigenvalue of $H_{t_X,0}$ and the weight of the corresponding frustrated stabilizer $w(s_X)$. The eigenvalue closest to $\lambda_1(H_{0,0})$ is marked with a tick, along with the value of the gap. We only show the results for a single frustrated stabilizer generator, as it was confirmed numerically that adding further frustrated stabilizers never produces a better candidate for λ_2. Also, we only consider non-isomorphic stabilizer generators, under the lattice symmetry of the model. We use the iterative solvers in software library `SLEPc` [20] to find these eigenvalues.

model	n	t_X	$w(s_X)$	λ_1	λ_2 ?		gap
compass $l = 4$	16	0		19.012903	16.335705		
			8		18.369300	✓	0.643603
compass $l = 5$	25	0		29.076200	27.597280		
			10		28.624004	✓	0.452196
compass $l = 6$	36	0		41.410454	40.585673		
			12		41.094532	✓	0.315922

The numerics for the compass model have been previously found [12] using similar methods.

model	n	t_X	$w(s_X)$	λ_1	λ_2 ?		gap
gauge color	15	0		25.455844	16.970563		
			8		22.214755	✓	3.24108
gauge color	39	0		64.476081	58.137233		
			8		60.706477		
			8		60.357053		
			12		61.366348		
			20		63.495916	✓	0.98016
gauge color	65	0		104.076026	99.014097		
			8		100.429340		
			12		100.585413		
			12		101.602340		
			18		102.382483	✓	1.69354
gauge color	175	0		267.197576	264.250644		
			8		263.171190		
			8		263.324858		
			8		263.340832		
			12		264.269635		
			12		264.617135		
			12		264.745548		
			18		264.843629		
			18		265.413935		
			18		265.754772		
			24		266.148188	✓	1.0493

There are two main points to make about these numerics. The first is that the gap of the compass model is decreasing much faster than the gap in the gauge color model. In fact, there is strong evidence [14] that the gap of the compass model tends to zero as the lattice size grows. The second point to make is that the gap always corresponds to frustrating the stabilizer (generator) of largest weight. This is a crucial connection to make because the stabilizers of the compass model grow with the linear size of the model[1], while those of the gauge color model do not need to grow beyond a constant bound. This would suggest that if this is the mechanism for gapless behaviour that the gauge color model may be gapped.

2.2.3 Cheeger cuts

In this final section we give some heuristic arguments for how the size of stabilizers is related to the gap of the code. Unfortunately, this does not lead to definitive conclusions; it appears that new ideas are required.

The Perron-Frobenius structure theory places strong constraints on the first and second eigenvectors of Γ_{t_X} : the first eigenvector has all positive entries, and therefore all vectors orthogonal to the first eigenvector will have both positive and negative entries. In general, the set of edges of Γ_{t_X} where such a vector changes sign we call a Cheeger cut. (We ignore the possibility that this vector may have zero entries.) The Cheeger cut associated to the second eigenvector is particularly important, and we next show an example of how this cut relates to the gap.

The double well model is gapless

We consider a linear graph Hamiltonian with a "double-well" potential. This does not correspond to any gauge code Hamiltonian. The state space will be d dimensional with basis vectors numbered $|1\rangle, ..., |d\rangle$. We take $H = A + U$ with

$$A_{ij} = \begin{cases} 1 & \text{if } |i-j| = 1, \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad U_{ij} = \begin{cases} 2 & \text{if } i = j = 1 \ \text{ or } \ i = j = n, \\ 0 & \text{otherwise.} \end{cases}$$

A here is a kind of transition matrix, and U is a diagonal potential energy term.

For $d \gg 1$, the largest eigenvalue is $\lambda_1 \cong \frac{5}{2}$. The corresponding eigenvector $|v_1\rangle$ has all positive components that decay exponentially away from the well sites at $|1\rangle$ and $|d\rangle$:

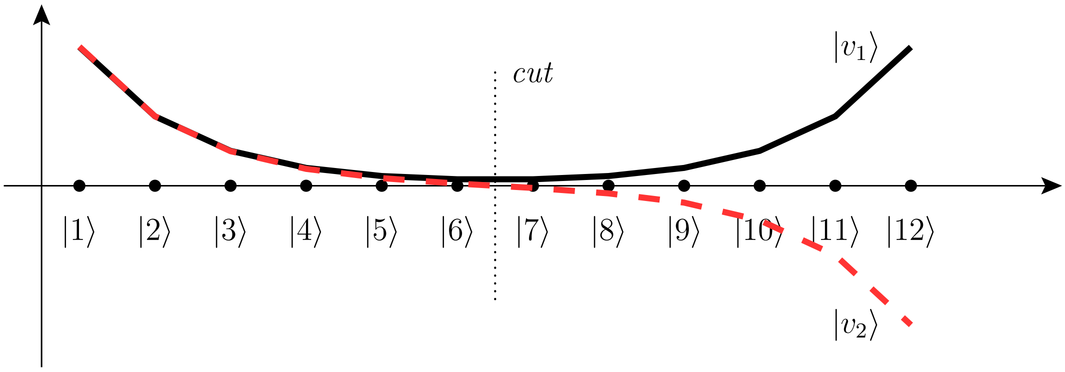
$$\langle i|v_1\rangle \cong 2^{i-1}\langle 1|v_1\rangle \ \text{ for } \ i \ll \frac{d}{2}.$$

For the second eigenvalue, λ_2 we also have $\lambda_2 \cong \frac{5}{2}$ and indeed, as d grows the gap

[1]Note the similar behaviour of the 1-dimensional XY-model and transverse field ising model.

$\lambda_1 - \lambda_2 \to 0$ and so this model is gapless.

Here we depict the wavefunctions for the first two eigenvectors for a system with $d = 12$:



The simplest way to show this model is gapless is using a variational argument. Any another vector $|u\rangle$ that is orthogonal to the groundspace vector will have $\langle u|H|u\rangle \leq \lambda_2$. To construct a candidate for $|u\rangle$ partition the basis vectors into two parts:

$$\Gamma = \Gamma_A \cup \Gamma_B$$

and write $|v_1\rangle = |v_A\rangle \oplus |v_B\rangle$ as well as Hamiltonian with this decomposition as

$$H = \begin{pmatrix} H_{AA} & H_{AB} \\ H_{BA} & H_{BB} \end{pmatrix}.$$

Now let

$$|u\rangle = |v_A\rangle \oplus -|v_B\rangle$$

And then

$$\begin{aligned} \lambda_2 \geq \langle u|H|u\rangle &= \langle v_A|H_{AA}|v_A\rangle + \langle v_B|H_{BB}|v_B\rangle - \langle v_B|H_{BA}|v_A\rangle - \langle v_A|H_{AB}|v_B\rangle \\ &= \lambda_1 - 4\langle v_B|H_{BA}|v_A\rangle. \end{aligned}$$

So if we can show that $\langle v_B|H_{BA}|v_A\rangle$ tends to zero we are done. This term involves the dynamical coupling between the groundstate wavefunction along the cut between A and B. To succeed we must find such a cut where the wavefunction is small. In general this appears to be quite difficult, even though in the models we are considering numerics show that not only is the wavefunction small away from potential wells but it is exponentially small.

The cut and symmetry

We now study the cut associated to the second eigenvector of a weakly self-dual gauge Hamiltonian H, and relate this to the stabilizers of the code. The key realization is that Γ_{t_X} is like the double well potential above, but now we have 2^{m_X} such wells, that is, one for every $s_X \in \langle S_X \rangle$. This is clear from examining the basis vectors for Γ_{t_X}. These are

$$vS_X + uR_X + t_X, \quad \text{where } \; v \in \mathcal{F}_2^{m_X *}, u \in \mathcal{F}_2^{r*}$$

and those that satisfy the most G_Z terms are precisely those with $u = 0$.

We already know this is either the second eigenvector of $H_{0,0}$ or otherwise the first eigenvector of $H_{t_X,0}$ for some $t_X \neq 0$. To relate this to the Perron-Frobenius theory we note the decomposition:

$$\Gamma_{t_X} = \bigoplus_{t_Z \in \langle T_Z \rangle} H_{t_X, t_Z}.$$

This gives the spectral decomposition of each graph Γ_{t_X} in terms of "momenta" t_Z.

We focus on Γ_0. This must contain the second eigenvector of H by weak self-duality of the code. X type stabilizers $s_X \in S_X$ act on the $0, t_Z$ irreps in Γ_0 by ± 1 according to the commutator $[[s_X, t_Z]]$. Suppose the second eigenvector of H lives in H_{0,t_Z} for $t_Z \neq 0$. Let $s_X \in S_X$ with $[[s_X, t_Z]] = -1$. Then we must have an odd number of Cheeger cuts on every Γ_0 path between $|v\rangle$ and $s_X|v\rangle$ for all basis vectors $|v\rangle$, that is, $v \in \langle S_X \rangle \oplus \langle R_X \rangle$.

In a similar vein, if the second eigenvector of H lives in $H_{0,0}$ then we must have an even number of Cheeger cuts on every Γ_0 path between $|v\rangle$ and $s_X|v\rangle$ for all stabilizers $s_X \in S_X$ and basis vectors $|v\rangle$.

In summary, the idea is that large stabilizers lead to widely separated well potentials and hense gapless behaviour, while stabilizers of bounded weight force the cuts to appear close to the wells and hense maintain a gap. Making these arguments rigorous appears to be difficult.

Finally, we suspect that $H_{0,0}$ will not be gapped in the generic case. Numerics show that these stabilizer-less Hamiltonians can be constructed with small gap. It appears that double well behaviour can still be imitated even without stabilizers: merely having a large region of almost-stabilizer behaviour (large shallow well) could be enough to send the gap to zero.

Chapter 3

Error Correction in a Non-Abelian Topologically Ordered System

In this work we describe the theory of two-dimensional topologically ordered systems with anyonic excitations. There are two main approaches to defining these, one being more algebraic and the other more topological.

The algebraic side is known to mathematicians as the study of braided fusion tensor categories, or more specifically, modular tensor categories. This algebraic language appears to be more commonly used in the physics literature, such as the well cited Appendix E of Kitaev [25]. Such algebraic calculations can be interpreted as manipulations of string diagrams [3], or *skeins.* These strings encode connections in the algebra, for example the Einstein summation convention. But they also faithfully encode the twisting that occurs when anyons are re-ordered or braided around each other. And these kinds of spatial relationships are fruitfully studied using topological methods.

Working from the other direction, one starts with a topological space (of low dimension) and attempts to extract a combinatorial or algebraic description of how this space can be built from joining smaller (simpler) pieces together. These topologically rooted constructs are known as modular functors, or the closely related topological quantum field theories (TQFT's).

That these two approaches – algebraic versus topological – meet is one of the great surprises of modern mathematics and physics.

Modular functors can be constructed from skein theory. In the physics literature, this appears as skeins growing out of manifolds [29], or as motivated by renormalization group considerations [27]. A further physical motivation is this: if a skein is supposed to correspond to the $(2+1)$-dimensional world-lines of particles as in the Schrödinger picture, modular functors would correspond to the algebra of observables, as in a Heisenberg picture.

In the physics literature, modular functors are explicitly used in Refs. [17, 16]. Also, Refs. [7] and [26] use the language of modular functors but they call them TQFT's. This is in fact reasonable because a modular functor can be seen as part of a TQFT, but is quite confusing to the novice who attempts to delve into the mathematical literature.

The definition of a modular functor appears to be well motivated physically. Unfortunately, there are many such definitions in the mathematical literature [33, 32, 5, 31]. According to [6] section 1.2 and 1.3, there are several open questions involved in rigorously establishing the connection between these different axiomatizations. In particular, what physicists call anyon theory, and mathematicians call a modular tensor category, has not been established to correspond exactly (bijectively) to any of these modular functor variants. We try not to concern ourselves too much with these details, but merely note these facts as a warning to the reader who may go searching for the "one true formulation" of topological quantum field theory.

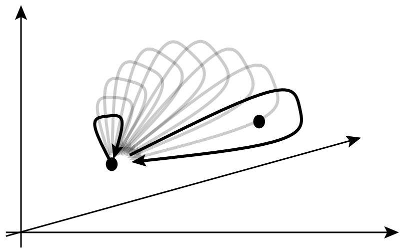
Of the many variants of modular functor found in the literature, one important distinction to be made is the way anyons are labeled. In the mathematical works [32, 5, 31] we see that anyons are allowed to have superpositions of charge states. However, in this work we restrict anyons to have definite charge states, as in [33, 16, 7]. This seems to be motivated physically as such configurations would be more stable.

The main goal of the present work is to sketch how a braided fusion tensor category arises from a modular functor. In the mathematical literature, this is covered in [32, 31, 5] but as we just noted they use a different formulation for a modular functor.

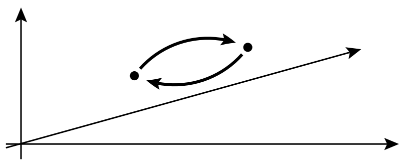
3.0.4 Topological Exchange Statistics

In this section we begin with the familiar question of particle exchange statistics in three dimensions, whose answer is bosons and fermions. We then show how in restricting the particles to two dimensions many more possibilities arise. Our focus will be on the close connection between the algebraic and the topological viewpoints, aiming to motivate the definition of a modular functor given in the next section.

In three spatial dimensions, the process of winding one particle around another, a *monodromy*, is topologically trivial. This is because the path can be deformed back to the identity; there is no obstruction:



The square root of this operation is a swap:



For identical particles this is a *symmetry* of the system. Continuing with this line of thought leads to consideration of the *symmetric group* on n letters, S_n. This group is generated by the $n-1$ swap operations $s_1, ..., s_{n-1}$ that obey the relations

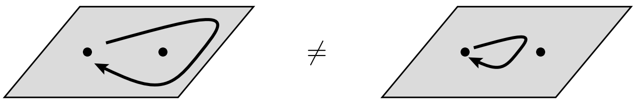
$$\begin{aligned} s_i^2 &= 1, \\ s_i s_j &= s_j s_i \quad \text{for} \quad |i-j|>1, \\ s_i s_{i+1} s_i &= s_{i+1} s_i s_{i+1} \quad \text{for} \quad 1 \le i \le n-2. \end{aligned}$$

Writing the Hilbert space of the system as V we would then expect S_n to act on this space via unitary transformations $U(V)$:

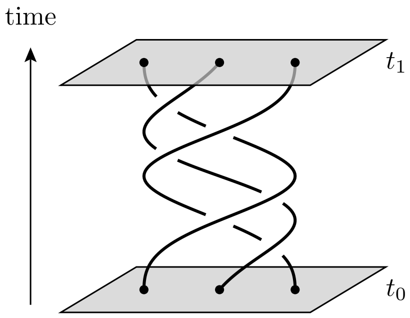
$$\mathscr{H} : S_n \to U(V).$$

This is the first example of the kind of functor we will be talking about. In this case it is a group representation; $\mathscr{H}$ is a homomorphism between two groups.

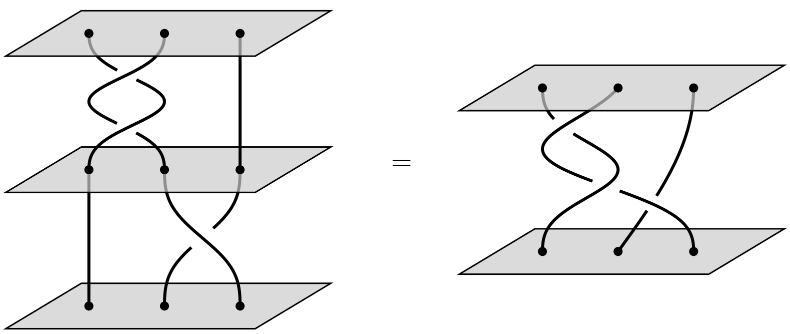
When the above monodromy is constrained to two dimensions we can no longer deform this process to the identity:



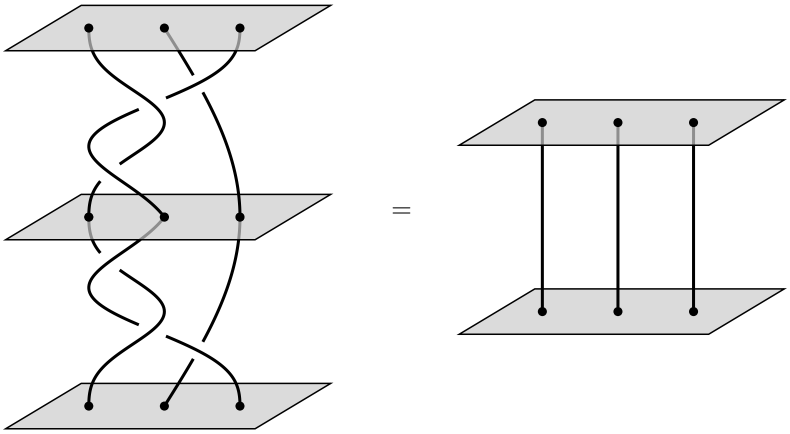
and so in two dimensions we cannot expect a swap to square to the identity. To see this more clearly, we must examine the entire (2+1)-dimensional *world-lines* of these particles. For an example, here we show the world-lines of three particles undergoing an exchange and then returning to their original positions:



Note that if we allow the particles to move in one extra dimension then we can untangle these braided world lines. The question is now, what is the group that acts on the state space from t_0 to t_1? Examining the structure of these processes more closely, we see that we can compose them by sequentially performing two such braids, one after the other:



And, by "reversing time", we can undo the effect of any braid:



This shows that these processes do form a group, known as the *braid group.* For n particle world-lines we denote this group as B_n. For identical particles this group acts as symmetries of the state space:

$$\mathscr{H} : B_n \to U(V).$$

What we have given is a topological description of the group B_n. More formally, we can describe these braid world lines as paths in the *configuration space* of n points. This space is defined as the product of a two dimensional space M for each point, minus the subspace where points overlap:

$$\mathcal{C}_n = \Big(\prod_1^n M\Big) - \Delta, \quad \Delta = \{(x_1, ..., x_n) | x_i = x_j \text{ for some } i \neq j\}.$$

Because we are considering identical particles (so far) we use the *unlabelled configuration space* $\mathcal{UC}_n$ which is the quotient of $\mathcal{C}_n$ by the natural action of the permutation group S_n :

$$\mathcal{UC}_n = \mathcal{C}_n / S_n.$$

The *geometric braid group* as we have so far informally described it can now be rigorously defined as the fundamental group:

$$B_n = \pi_1(\mathcal{UC}_n, x)$$

where x is some reference configuration in $\mathcal{UC}_n$. See Ref. [19] for further discussion.

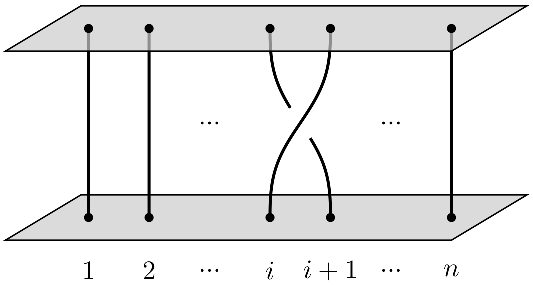
This group also has a purely algebraic description via generators and relations, as was shown by Artin in 1947, [1, 8]. In this description, B_n is generated by $n-1$ elements $\sigma_1, .., \sigma_{n-1}$ that satisfy the following relations:

$$\sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{for} \quad |i-j| > 1,$$
$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \quad \text{for} \quad 1 \leq i \leq n-2.$$

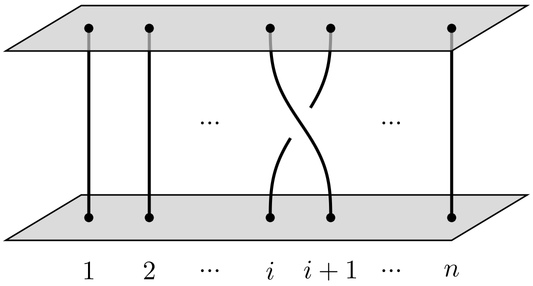
These relations are the same as for S_n above, except we do not require $\sigma_i^2 = 1$.

It is easy to see that the geometric braid group satisfies these relations. Here we show the braids corresponding to the generators σ_i :

$\sigma_i =$

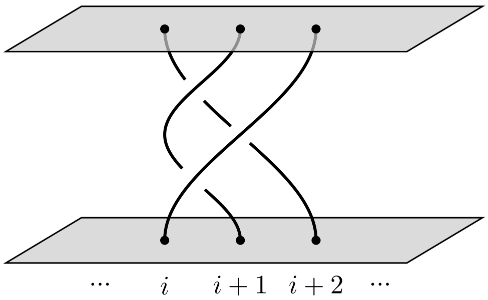


$\sigma_i^{-1} =$

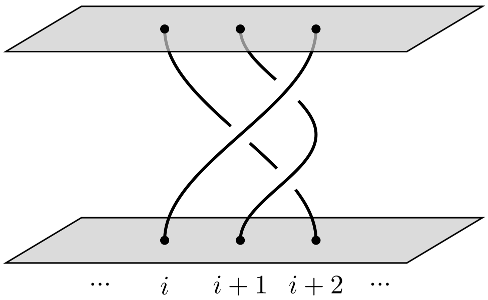


So that $\sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{for} \quad |i-j| > 1$ because the two braids are operating on disjoint world-lines. The second relation is also easy to see:

$\sigma_i \sigma_{i+1} \sigma_i =$



$=$

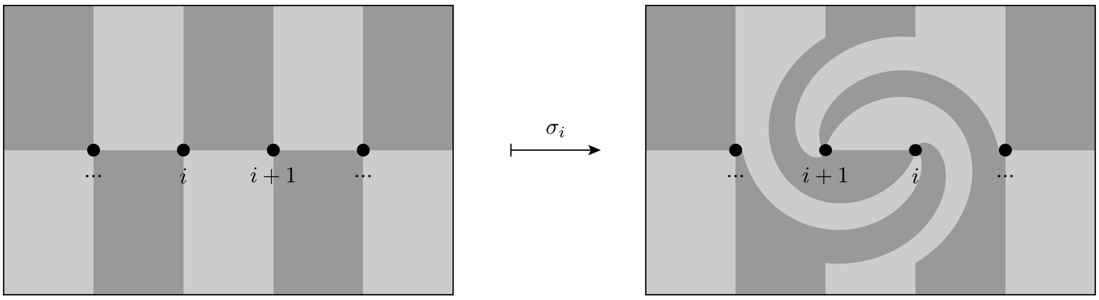


$= \sigma_{i+1} \sigma_i \sigma_{i+1}$

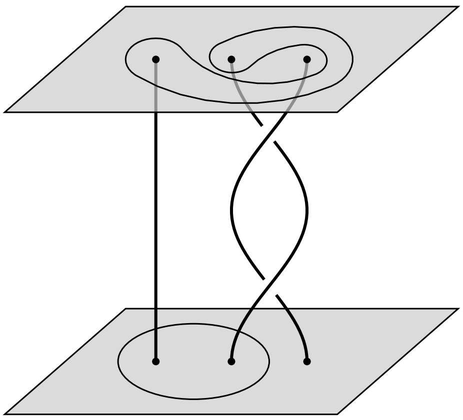
There is another important geometric representation of the braid group which is purely two-dimensional. We pick an n-point finite subset $Q_n \subset M$ and consider diffeomorphisms $f : M \to M$ that map Q_n to itself. The *mapping class group* of M relative to Q_n is the set of all such diffeomorphisms up to an equivalence relation $\sim_{\text{iso}}$:

$$MCG(M, Q_n) = \{f : M \to M \;\; \text{such that} \;\; f(Q_n) = Q_n\} / \sim_{\text{iso}}$$

The equivalence relation $\sim_{\text{iso}}$ is called *isotopy* which allows for any continuous deformation of $f : M \to M$ that fixes each point in Q_n. Each generator σ_i of the braid group is found in $MCG(M, Q_n)$ as a *half-twist* that swaps two points $i, i+1 \in Q_n$:



In order to show the action of this half-twist we have decorated the manifold with a a checkered pattern, but there is a more important object that lives on the manifold itself. An *observable* is a simple closed curve in M that does not intersect Q_n. Such a closed curve is called an observable because these will be associated to measurements of the total anyonic charge on the interior of the curve. The importance of understanding the braid group as identical to the mapping class group is now manifest: whereas geometric braids act on states as in a Schrödinger picture, elements of the mapping class group act on the observables as in a Heisenberg picture.



This diagram should give the reader some idea as to why these two definitions of the braid group are equivalent, but the actual proof of this is somewhat involved. We cite Ref. [23] for an excellent contemporary account that fills in these gaps.

The definition given above for the geometric braid group and the mapping class group make sense for any two dimensional manifold M but for concreteness we consider M to be a flat disc. The corresponding algebraic definition of the braid group will in general be altered depending on the underlying manifold M.

So far we have been studying the exchange statistics for n identical particles. Without this restriction, one needs to constrain the allowed exchange processes so as to preserve particle type. For example, if all particles are different we would use the *pure braid group* PB_n. The geometric description of this group is as the fundamental group of the labelled configuration space

$$PB_n = \pi_1(\mathcal{C}_n, x).$$

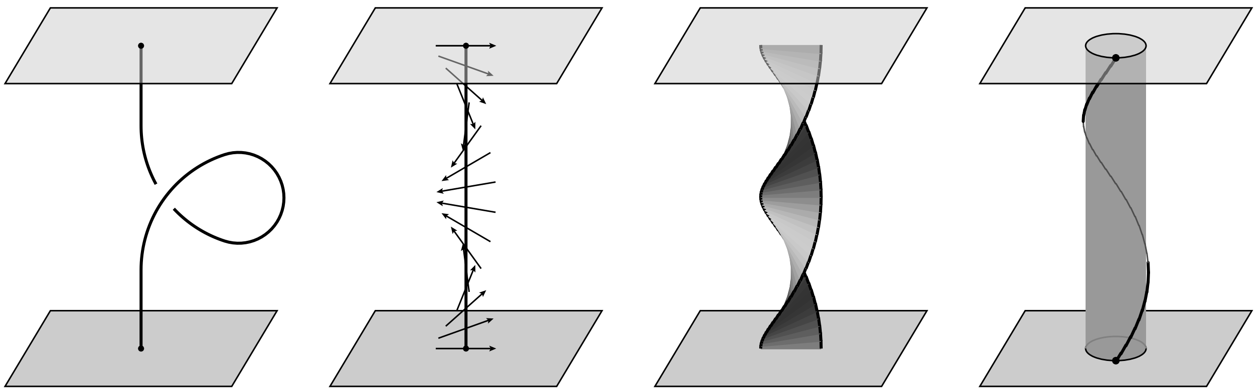
Loops in $\mathcal{C}_n$ correspond to braids where each world-line returns to the point it started from. The algebraic description of this group is somewhat complicated and we omit this. In terms of the mapping class group, we can describe PB_n as the *pure mapping class group*:

$$PMCG(M, Q_n) = \{f : M \to M \text{ such that } f(x) = x \text{ for } x \in Q_n\}/ \sim_{\text{iso}} .$$

One further complication arises when particles have a rotational degree of freedom: ie., they can be rotated by 2π in-place and this effects the state of the system. To capture this action, we use the *framed braid group* FB_n. This group can be presented algebraically using the same generators and relations as for the braid group B_n, along with "twist" generators θ_i for $i = 1, .., n$. These must satisfy the further relations

$$\begin{aligned} \theta_i\theta_j &= \theta_j\theta_i \\ \theta_i\sigma_j &= \sigma_j\theta_i \text{ if } i < j \text{ or } i \geq j+2 \\ \theta_{i+1}\sigma_i &= \sigma_i\theta_i \\ \theta_i\sigma_i &= \sigma_i\theta_{i+1}. \end{aligned}$$

Here we show four geometric approaches to representing a twist. Any person that has struggled to untangle their headphone cable will immediately see what is going on here.



On the left we have a loop; it is not a braid because it travels backwards in time. If we pull on this loop to make it straight, we introduce a twist. This is shown in the next figure, where we show a *framing* which is a non-degenerate vector field along the world-lines of a braid. The initial and final vectors in the vector field must be the same. By non-degenerate we mean that the vector field is everywhere non-zero and non-tangent to the world-line. In the next figure we show a *ribbon*: instead of point particles we have short one-dimensional curves in M. On the right the particle is represented as a boundary component (a hole) of M with a distinguished point. In this picture the world-line looks like a tube.

All these representations of twists carry essentially the same information. In the sequel we will stick to thinking of particles as boundary components because this fits well with the way we are formulating observables as simple closed curves in M.

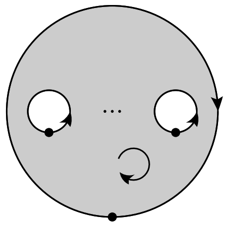
At this point in the narrative we are close to our next destination. All of these considerations, of framed or unframed, labelled or not, with possibly different underlying manifolds, together with observables, is mean to be captured by the formalism of a modular functor which we turn to next.

3.0.5 Modular Functors

We list the axioms for a *2-dimensional unitary topological modular functor*.

For our purposes a *surface* will be a compact oriented 2-dimensional differentiable manifold with boundary. We will not require surfaces to be connected. By a *hole* of M we mean a connected component of its boundary. Each hole will inherit the manifold orientation, contain a distinguished *base point*, and be labeled with an element from a fixed finite set $\mathcal{A}$. This is the set of "anyon labels", and comes equipped with a vacuum element $\mathbb{I}$ and an involution $\widehat{\ }$ such that $\widehat{\mathbb{I}} = \mathbb{I}$. The involution maps an anyon label to the "antiparticle" label.

We will mostly be concerned with planar such surfaces, that is, a *disc* with holes removed from the interior. Such surfaces will be given a clockwise orientation, which induces a counterclockwise orientation on any *interior* hole and a clockwise orientation on the *exterior* hole.



Although it helps to draw such a surface as a disc with holes, we stress that there is no real distinction to be made between interior holes and the exterior hole. That is, a disc with n interior holes is (equivalent to) a sphere with $n+1$ holes. We merely take advantage of the fact that a sphere with at least one hole can be flattened onto the page by "choosing" one of the holes to serve as the exterior hole.

By a *map of surfaces* $f : M \to N$ we mean a diffeomorphism that preserves manifold orientation, hole labels, and base points. Note that we also deal with maps of various other objects (vector spaces, sets, etc.) but a map of surfaces will have these specific requirements.

Two maps of surfaces $f : M \to N$ and $f' : M \to N$ will be called *isotopic* when one is a continuous deformation of the other. In detail, we have a continuously parametrized family of maps $f_t : M \to N$ for $t \in [0, 1]$ such that $f_0 = f,\ f_1 = f'$ and the restriction of f_t to the set of marked points $X \subset \partial M$ is constant: $f_t|_X = f|_X$ for $t \in [0, 1]$. Such a family $\{f_t\}_{t\in[0,1]}$ is called an *isotopy* of f. This is an equivalence relation on maps $M \to N$, and the equivalence class of f under isotopy is called the *isotopy class* of f. The weaker notion of homotopy of maps will not be used here, but for the maps we use it turns out that homotopy is equivalent to isotopy. Furthermore, we can weaken the requirement that maps be differentiable, because every continuous map $f : M \to N$ is (continuously) isotopic to a differentiable map [15].

A *modular functor* $\mathscr{H}$ associates to every surface M a finite dimensional complex vector space $\mathscr{H}(M)$, called the *fusion space* of M. For each map $f : M \to N$ the modular functor associates a unitary transformation $\mathscr{H}(f) : \mathscr{H}(M) \to \mathscr{H}(N)$ that only depends on the isotopy class of f. Functoriality requires that $\mathscr{H}$ respect composition of maps.

We have the following axioms for $\mathscr{H}$.

Unit axioms. The fusion space of an empty surface is one dimensional, $\mathscr{H}(\phi) \cong \mathbb{C}$. For M_a a disc with boundary label a we have $\mathscr{H}(M_{\mathbb{I}}) \cong \mathbb{C}$ and $\mathscr{H}(M_a) \cong 0$ for $a \neq \mathbb{I}$. For an annulus $M_{a,b}$ with boundary labels a, b we have $\mathscr{H}(M_{a,\widehat{a}}) \cong \mathbb{C}$ and $\mathscr{H}(M_{a,b}) \cong 0$ for $a \neq \widehat{b}$.

Monoidal axiom. The disjoint union of two surfaces M and N is associated with the tensor product of fusion spaces:

$$\mathscr{H}(M \amalg N) \cong \mathscr{H}(M) \otimes \mathscr{H}(N).$$

This is natural from the point of view of quantum physics, where the Hilbert space of two disjoint systems is the tensor product of the space for each system.

Gluing axiom. Denote a surface M with (at least) two holes labeled a, b as $M_{a,b}$. If we constrain $b = \widehat{a}$ then we may *glue* these two holes together to form a new surface N. To construct N we choose a diffeomorphism from one hole to the other that maps base point to base point and reverses orientation. Identifying the two holes along this diffeomorphism gives the glued surface N. (There is a slight technicality in ensuring that N is then differentiable, but we will gloss over this detail.) The image of these holes in N we call a *seam*. The fusion space of $M_{a,\widehat{a}}$ then embeds unitarily in the fusion space of N. Moreover, there is an isomorphism called a *gluing map*:

$$\bigoplus_{a \in \mathcal{A}} \mathscr{H}(M_{a,\widehat{a}}) \xrightarrow{\cong} \mathscr{H}(N)$$

and this isomorphism depends only on the isotopy class of the seam in N.

Unitarity axiom. Reversing the orientation of the surface M to form $\overline{M}$ we get the dual of the fusion space: $\mathscr{H}(\overline{M}) = \mathscr{H}(M)^*$.

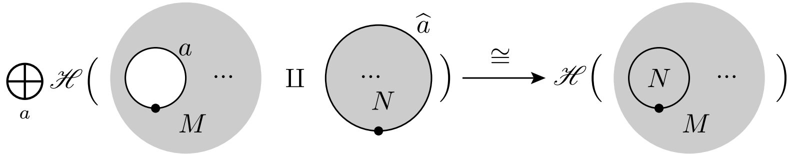
Compatibility axioms. Loosely put, we require that the above operations play nicely together, and commute with maps of surfaces. For example, a sequence of gluing operations applied to a surface can be performed regardless of the order (gluing is associative) and we require the various gluing maps for these operations to similarly agree. For another example, we require $\mathscr{H}$ to respect that gluing commutes with disjoint union.

Observables. The seam along which gluing occurs can be associated with an observable as follows. We take a gluing map g and projectors P_a onto the summands in the above direct sum:

$$P_a : \bigoplus_{b \in \mathcal{A}} \mathscr{H}(M_{b,\widehat{b}}) \to \mathscr{H}(M_{a,\widehat{a}}).$$

then the observable will be the set of operators $\{P_a g^{-1}\}_{a \in \mathcal{A}}$. For each $a \in A$ we call the image of P_a a *charge sector* for that observable. Note that in the glued surface N the seam has no preferred orientation (or base point). If we choose an orientation for the seam this corresponds to choosing one of the two boundary components in the original surface $M_{a,\widehat{a}}$. If these boundary components come from disconnected components of $M_{a,\widehat{a}}$ the seam cuts N into two pieces and the orientation chooses an *interior:* following the orientation around the seam presents the interior to the left. We intentionally confuse the distinction between an observable as a set of operators, and the associated seam along which gluing occurs.

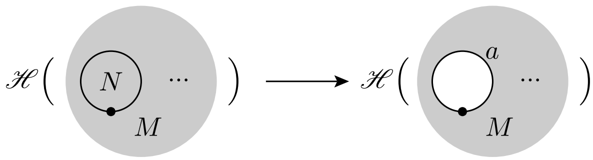
Consequences of axioms. A common operation is to glue two separate surfaces. We can do this by first taking disjoint union (tensoring the fusion spaces) and then gluing. Here we show this process applied to two surfaces M and N.



We display the surface N with the $\widehat{a}$ boundary on the outside, to show more clearly how N fits into M. In the glued surface we indicate the placement of M and N and the seam along which gluing occurred, as well as the identification of base points.

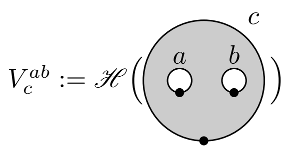
We note two other consequences of the axioms. A hole of M labeled with $\mathbb{I}$ can be replaced with a disk (by gluing) and this does not change the fusion space of M. That is, a hole that carries no charge can be "filled-in". And, the dimensionality of the fusion space of a torus is the cardinality of $\mathcal{A}$. This can be seen by gluing one end of an annulus (cylinder) to the other.

Fusion. When a surface can be presented as the gluing of two separate surfaces, we have projectors onto the fusion space of either glued surface:

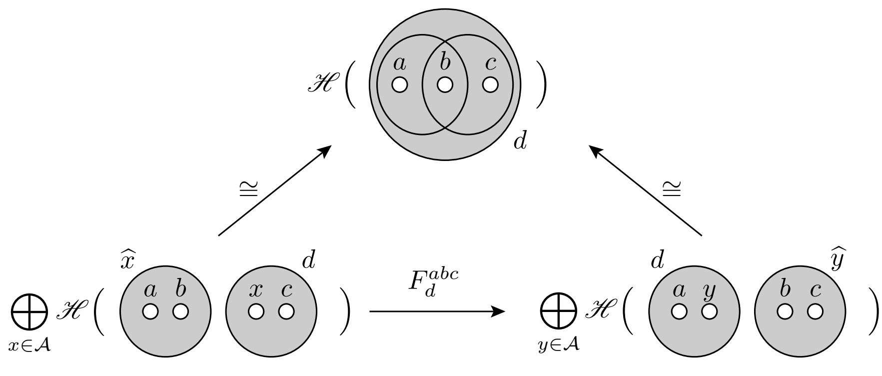


In this case, we define the operation of *fusion* to replace the interior of an observable by a single hole. This is an operation on the manifold itself, and we will only do this when the interior piece is a disc with zero or more holes.

F-move. The fusion space of the disc and annulus are specified by the axioms, and we define the fusion space of the disc with two holes, or *pair-of-pants* as:



The *F-move* is constructed from two applications of a gluing map (one in reverse) as the following commutative diagram shows:

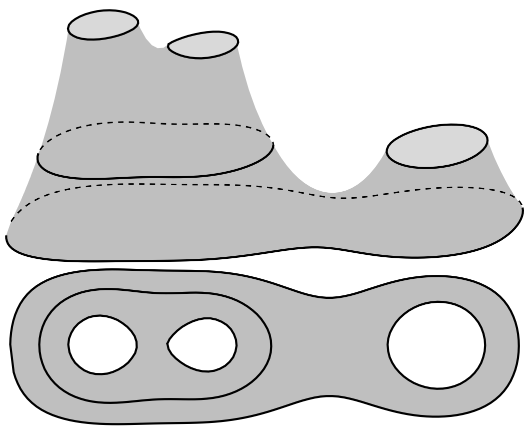


Here we have a surface M_d^{abc} with four labeled boundary components, as well as two separate ways of gluing pairs-of-pants to get M_d^{abc}. We can also write this out in terms of the fusion spaces of pair-of-pants:

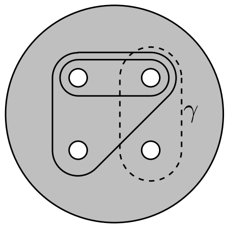
$$F_d^{abc} : \bigoplus_{x\in\mathcal{A}} V_{\widehat{x}}^{ab} \otimes V_d^{xc} \to \bigoplus_{y\in\mathcal{A}} V_d^{ay} \otimes V_{\widehat{y}}^{bc}.$$

By using gluing, and summing over charge sectors, we can extend this operation to apply where any of the boundary components a, b, c or d are merely seams in a larger manifold.

POP decomposition. Given a manifold M which is a disc with two or more holes, we show how to present M as the gluing of various pair-of-pants. Such an arrangement will be termed a *POP decomposition.* (We refer to Ref. [21] for more details on this construction, and Ref. [19] for a leisurely description of Morse theory.) This will yield a decomposition of $\mathscr{H}(M)$ into a direct sum of fusion spaces of pair-of-pants. The key idea is to choose a "height" function $h : M \to \mathbb{R}$ with some specific properties that allow us to cut the manifold up along level sets of h. First, we need that critical points of h are isolated. This is the defining condition for h to be a *Morse function.* Also, we need that h is constant on ∂M, and the values of h at different critical points are distinct. Now choose a sequence of non-critical values $a_1 < a_2 < ... < a_n$ in $\mathbb{R}$ such that every interval $[a_{i-1}, a_i]$ contains exactly one critical value of h and the image of h lies within $[a_1, a_n]$. Each component of $h^{-1}([a_{i-1}, a_i])$ is then either an annulus, a disc, or a pair-of-pants depending on the index of (any) critical point it contains. We then re-glue any annuli or discs until there are no more of these and we have only pair-of-pants.

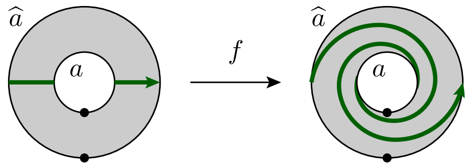


Clearly such a POP decomposition is not unique, and the goal here is to understand how to switch between decompositions, and in particular, given an observable γ, and a given POP decomposition, find a sequence of "moves" such that γ is in the resulting POP decomposition:



One way to achieve this is via Cerf theory, which is the theory of how one may deform Morse functions into other Morse functions and the kind of transitions involved in their critical point structure. This was the approach used in Ref. [16]. In this work we use a simpler method, which is essentially the same as skein theory. This is the refactoring theorem that we describe below.

Dehn twist. Consider a surface $M_{a,\widehat{a}}$ with two boundary components, a and $\widehat{a}$. Let f be a map $M_{a,\widehat{a}} \to M_{a,\widehat{a}}$ which performs a clockwise 2π full-twist or *Dehn twist*. Here we show the action of f by highlighting the equator of the annulus:



We define the induced map on fusion spaces as $\theta_a := \mathscr{H}(f)$. Because $\mathscr{H}(M_{a,\widehat{a}})$ is one-dimensional this will be multiplication by a complex number which we also write as θ_a.

If we now take M to be an arbitrary surface, and γ an observable on M, we can consider a neighbourhood of γ which will be an annulus, and perform a Dehn twist there, which we denote as $f_\gamma : M \to M$. Writing M as a gluing along γ of another manifold $N_{a,\widehat{a}}$, the action of $\mathscr{H}(f_\gamma)$ will decompose as a direct sum over charge sectors:

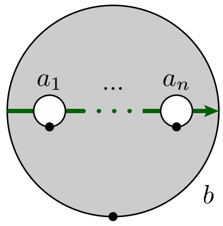
$$\bigoplus_{a \in \mathcal{A}} \theta_a \mathscr{H}(N_{a,\widehat{a}}).$$

Standard surfaces. For each $n = 0, 1, ...$ and every ordered sequence of anyon labels $a_1, ..., a_n, b$ we choose a *standard surface.* This is a surface with $n + 1$ boundary components labeled $a_1, ..., a_n, b$ which we denote $M_b^{a_1 \dots a_n}$.

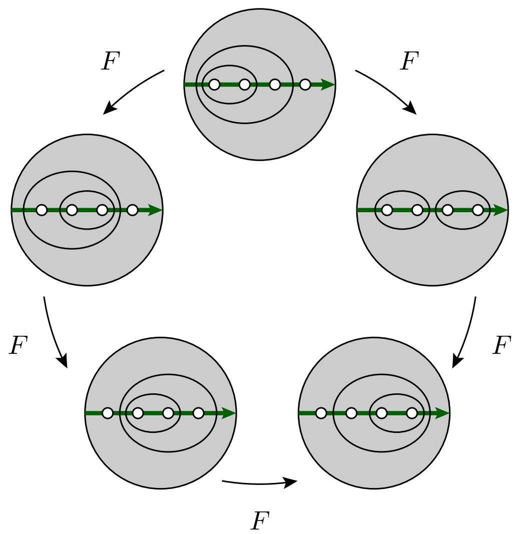
For concreteness we define this surface using the following expression for a closed disc less n open discs:

$$\left\{(x,y)\in\mathbb{R}^2 \text{ st. } \left|(x,y)-\left(\frac{1}{2},0\right)\right|\leq\frac{1}{2}\right\}-\left\{(x,y)\in\mathbb{R}^2 \text{ st. } \left|(x,y)-\left(\frac{2i-1}{2n},0\right)\right|<\frac{1}{4n}\right\}_{i=1,\ldots n}.$$

We then label the interior holes $a_1,\ldots,a_n$ in order of increasing x coordinate, and the exterior hole is labeled b. The base points are placed in the direction of negative y coordinate. As a notational convenience we highlight the *equator* of the surface which is the intersection of the x axis with the surface:



Each standard surface comes with a collection of *standard POP decompositions*: these will be POP decompositions where we require each observable to cross the equator twice and have counterclockwise orientation. Up to isotopy, a given standard surface will have only finitely many of these. On a standard surface with three interior holes there are two standard POP decompositions, and one F-move that relates these. On a standard surface with four interior holes there are five standard POP decompositions and five F-moves that relate these. In this case the F-moves themselves satisfy an equation that is an immediate consequence of the way we have defined F-moves. This is known as the pentagon equation, which we depict as the following commutative diagram:



We are now starting to confuse the notation for the topological space M and the fusion space $\mathscr{H}(M)$. Also, each of these F-moves is referring to an isomorphism that is block decomposed according to the charge sectors of the indicated observables.

We define the vector spaces $V_b^{a_1 \dots a_n} := \mathscr{H}(M_b^{a_1 \dots a_n})$. We now choose a basis for each of the $V_b^{a_1 a_2}$ to be $\{v_{b,\mu}^{a_1 a_2}\}_\mu$. For every standard POP decomposition of $M_b^{a_1 \dots a_n}$, we get a decomposition of $V_b^{a_1 \dots a_n}$ into direct sums of various $V_{b'}^{a'_1 a'_2}$. This then gives a *standard basis* of $V_b^{a_1 \dots a_n}$ relative to this standard POP decomposition using the corresponding $\{v_{b',\mu}^{a'_1 a'_2}\}_\mu$ for each of the $V_{b'}^{a'_1 a'_2}$.

Note that for any standard surface $M_b^{a_1 \dots a_n}$ and any choice of k contiguous holes $a_j, \dots, a_{j+k-1}$ we can find an observable that encloses exactly these holes in at least one of the standard POP decompositions of $M_b^{a_1 \dots a_n}$.

We next show how to glue the exterior hole of a standard surface M to an interior hole of another standard surface N. To do this within $\mathbb{R}^2$ we rescale and translate the two surfaces so that the exterior hole of M coincides with the interior hole of N. At this point the union is not in general going to produce another standard surface, and so we remedy this by applying any isotopy within $\mathbb{R}^2$ that fixes the x-axis while moving the surface to a standard surface.

Curve diagram. We next study maps from standard surfaces to arbitrary surfaces. The reader should think of this as akin to choosing a basis for a vector space. The set of all maps from $M_b^{a_1 \dots a_n}$ to a surface N will be denoted as $\mathrm{Hom}(M_b^{a_1 \dots a_n}, N)$. We call each such map a *curve diagram*, or more specifically, a curve diagram on N. The reason for this terminology is that we can reconstruct (up to isotopy) any map $f : M_b^{a_1 \dots a_n} \to N$ from the restriction of f to the equator of $M_b^{a_1 \dots a_n}$. In other words, we can uniquely specify any map $f : M_b^{a_1 \dots a_n} \to N$ by indicating the action of f on the equator. (This reconstruction works because a simple closed curve on a sphere cuts the sphere into two discs.) We take full advantage of this fact in our notation: any figure of a surface with a "green line" drawn therein is actually notating a diffeomorphism, not a surface!

Any curve diagram will act on a standard POP decomposition of $M_b^{a_1 \dots a_n}$ sending it to a POP decomposition of N. Surprisingly, the converse of this statement also holds: any POP decomposition of N (a disc with holes) comes from some curve diagram acting on a standard POP decomposition. The proof of this is constructive, and we call this the refactoring theorem below.

The operation of gluing of surfaces can be extended to gluing of curve diagrams as long as we are careful with the way we identify along the seam: the identification map needs to respect the equator of the curve diagram. (Keep in mind that a curve diagram is really a map of surfaces, and so gluing two such maps involves two separate gluing operations.)

We note in passing two connections to the mathematical literature. Such curve diagrams have been used in the study of braid groups [13], and this is where the name comes from, although our curve diagrams respect the base points and so could be further qualified as "framed" curve diagrams. And, we note the similarity of curve diagrams and associated modular functor to the definition of a planar algebra [22], the main difference being that planar algebras allow for not just two but any even number of curve intersections at each hole.

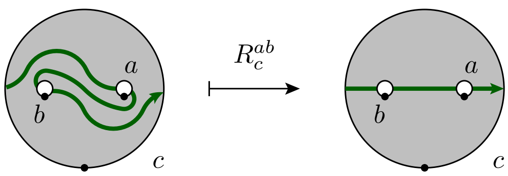
Z-move. We let z be a diffeomorphism of standard surfaces $z : M_b^{a_1 \dots a_n} \to M_{a_1}^{a_2 \dots a_n b}$ that preserves the equator. (Considering the standard surface as a sphere with holes placed uniformly around a great circle, z is seen to be a "rotation".) This acts by pre-composition to send a curve diagram $f \in \mathrm{Hom}(M_b^{a_1 \dots a_n}, N)$ to $fz \in \mathrm{Hom}(M_{a_1}^{a_2 \dots a_n b}, N)$. This we call a Z-move of f.

In this way, any curve diagram can be seen as another curve diagram that has a cyclic permutation of the labels of the underlying standard surface.

R-move. Given anyon labels a, b and c, and arbitrary surface N, we now define the following map of curve diagrams on N :

$$R_c^{ab} : \mathrm{Hom}(M_c^{ab}, N) \to \mathrm{Hom}(M_c^{ba}, N).$$

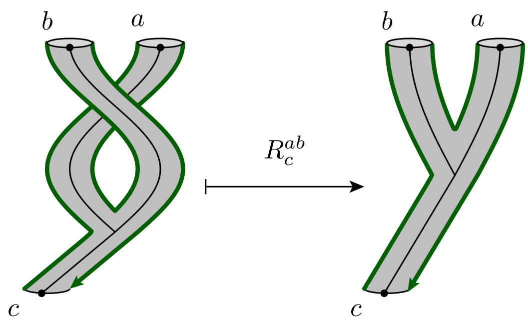
This map works by taking a curve diagram $f : M_c^{ab} \to N$ to the composition $f\sigma$ where $\sigma : M_c^{ba} \to M_c^{ab}$ is a counterclockwise "half-twist" map that exchanges the a and b holes. Here we show the action of R_c^{ab} on one particular curve diagram:



Such an application of R^{ab}_c to a particular curve diagram we call an *R-move.* As noted above, a curve diagram serves to pick out a basis for the fusion space, and the point of this R-move is to switch between different curve diagrams for the same surface. This is highlighted to draw the readers attention to the fact that the R-move does not swap the labels on the holes: the surface itself stays the same.

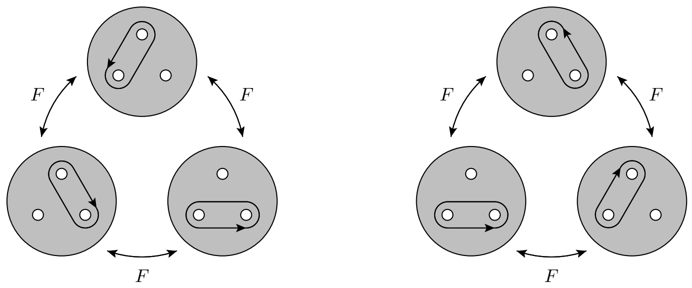
As we extended Dehn twists under gluing, and F-moves under gluing, we also do this for R-moves.

Skeins. The previous figure can be seen as a "top-down" view of the following three dimensional arrangement:

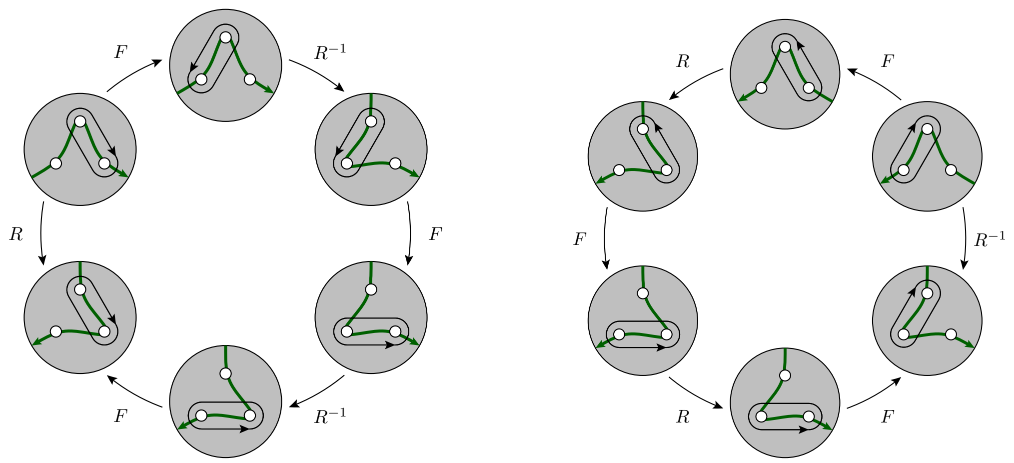


This figure is intended to be topologically the same as the previous flat figure, with the addition of a third dimension, and the c boundary has been shrunk. Also note thin black lines connecting the base points. The black lines do not add any extra structure, they can be seen as a part of the hexagon cut out by the green line and boundary components. But notice this: the black lines are "framed" by the green lines. These are the ribbons used in skein theory! Note that all the holes are created equal: there is no distinction between "input" holes and "output" holes (as there is with cobordisms or string diagrams.)

Hexagon equation. For a surface with three interior holes there are infinitely many POP decompositions (up to isotopy). These are all made by choosing an observable that encloses two holes. The F-moves allow us to switch between these POP decompositions, and the axioms for the modular functor make these consistent. Here we show two such triangle consistency requirements (they are reflections of each other):



Given a POP decomposition of a surface N there are various curve diagrams on N that produce this decomposition from a standard POP decomposition, and there are certain R-moves that will map between these. Once again, these moves must be consistent, and here we note the two "hexagon equations" corresponding to the above two triangles:



Note that we have neglected to indicate the base points here. Given a curve diagram, we can agree that base points occur "to the right" of the image of the equator. But in notating diagrams such as these, there is still an ambiguity: the position of the base points should be the same in each surface in the diagram. If we try to correct for this post-hoc by rotating individual holes, we will then be correct only up to possible Dehn twist(s) around each hole. We can certainly track these twists if we wanted to, but in the interests of simplicity we do not. This introduces a global phase ambiguity into the calculations.

The reason why we mention the pentagon and hexagon equations is that these become important in an algebraic description of the theory. Because we have defined everything in terms of a modular functor we get these equations "for free".

3.0.6 Refactoring theorem

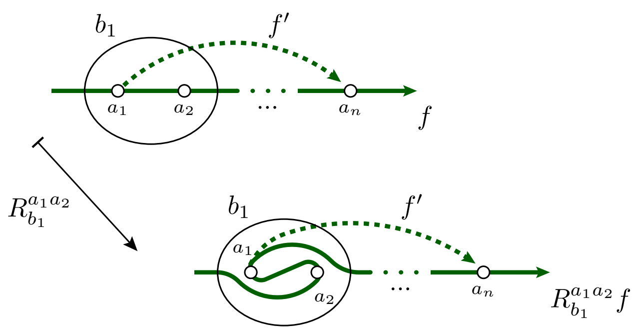
In this section we specialize to considering planar surfaces only. The theorem we are building towards shows that the R-moves act transitively on curve diagrams. By transitive we mean that given two curve diagrams f and f' on N we can find a sequence of R-moves that transform f to f'. The key idea is to consider the (directed) image of the equator under these curve diagrams. As mentioned previously, this image is sufficient to define the entire diffeomorphism (up to isotopy) and so we are free to work with just this image, or *curve*, and we confuse the distinction between a curve diagram (a diffeomorphism) and its curve.

The construction proceeds by considering adjacent pairs of holes along f' and then acting on the portion of f between these same two holes so that they then become adjacent on the resulting curve. Continuing this process for each two adjacent holes of f' will then show a sequence of R-moves that sends f to f'.

To this end, consider a sequence of holes $a_1, ..., a_n$ appearing sequentially along f such that a_1 and a_n appear sequentially on f'. We may need to apply some Z-moves to f to ensure that a_1 appears sequentially before a_n. Now consider the case such that along f' between these two holes there is no intersection with f. We form a closed path ξ by following the f' curve between a_1 and a_n and then following the f curve in reverse from a_n back to a_1. (Note that to be completely rigorous here we would need to include segments of path contained within boundary components.) The resulting closed path bounds a disc. If ξ has clockwise orientation we apply the following sequence of R-moves to f:

$$R^{a_1 a_2}_{b_1}, R^{a_1 a_3}_{b_2}, ..., R^{a_1 a_{n-1}}_{b_{n-1}}.$$

Depicted here is the first such move:



After each of these R-moves the closed path formed by following the f' curve between a_1 and a_n and then following the R-moved f curve back to a_1 will traverse one less hole, and still bound a disc. After all of the R-moves this path will only touch a_1 and a_n, and bound a disc. Therefore, we have acted on the f curve so that the resulting curve has a_1 and a_n adjacent and the bounded disc gives an isotopy for that segment of the curve.

When the closed curve ξ has anti-clockwise orientation we use the same sequence of R-moves but with R replaced by R^{-1}.

Generalizing further, when the f' curve between a_1 and a_n has (transverse) intersections with f we use every such intersection to indicate a switch between using R and R^{-1}.

We continue in this way moving backwards (from head to tail) sequentially applying this procedure.

Bibliography

[1] E. Artin. Theory of braids. *Annals of Mathematics*, pages 101–126, 1947.

[2] D. Bacon. Operator quantum error-correcting subsystems for self-correcting quantum memories. *Phys. Rev. A*, 73:012340, Jan 2006.

[3] J. Baez and M. Stay. *Physics, topology, logic and computation: a Rosetta Stone*. Springer, 2010.

[4] J. C. Baez and M. Stay. Physics, topology, logic and computation: A rosetta stone. Physics, topology, logic and comp In New Structures for Physics, ed. Bob Coecke, Lecture Notes in Physics vol. 813, Springer, Berlin, 2011, pp. 95-174, 2009.

[5] B. Bakalov and A. A. Kirillov. *Lectures on tensor categories and modular functors*, volume 21. American Mathematical Society Providence, 2001.

[6] B. Bartlett, C. L. Douglas, C. J. Schommer-Pries, and J. Vicary. Modular categories as representations of the 3-dimensional bordism 2-category. *arXiv preprint arXiv:1509.06811*, 2015.

[7] M. E. Beverland, R. König, F. Pastawski, J. Preskill, and S. Sijher. Protected gates for topological quantum field theories. *arXiv preprint arXiv:1409.3898*, 2014.

[8] J. Birman. Braids, links and mapping class groups. *Annals of Math. Studies*, 82, 1974.

[9] H. Bombín. Gauge color codes: optimal transversal gates and gauge fixing in topological stabilizer codes. *New Journal of Physics*, 17(8):083002, 2015.

[10] H. Bombín. Single-shot fault-tolerant quantum error correction. *Physical Review X*, 5(3):031043, 2015.

[11] H. Bombin and M. Martin-Delgado. Exact topological quantum order in d= 3 and beyond: Branyons and brane-net condensates. *Physical Review B*, 75(7):075103, 2007.

[12] W. Brzezicki and A. M. Oleś. Symmetry properties and spectra of the two-dimensional quantum compass model. *Phys. Rev. B*, 87:214421, Jun 2013.

[13] P. Dehornoy. *Why are braids orderable?* Panoramas et synthèses - Société mathématique de France. Société Mathématique de France, 2002.

[14] J. Dorier, F. Becca, and F. Mila. Quantum compass model on the square lattice. *Physical Review B*, 72(2):024448, 2005.

[15] B. Farb and D. Margalit. *A Primer on Mapping Class Groups (PMS-49)*. Princeton University Press, 2011.

[16] M. H. Freedman, A. Kitaev, and Z. Wang. Simulation of topological field theories by quantum computers. *Communications in Mathematical Physics*, 227(3):587–603, 2002.

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

[18] W. Fulton and J. Harris. *Representation theory: a first course*, volume 129. Springer Science & Business Media, 2013.

[19] R. Ghrist. *Elementary applied topology*. Createspace, 2014.

[20] V. Hernandez, J. E. Roman, and V. Vidal. SLEPc: A scalable and flexible toolkit for the solution of eigenvalue problems. *ACM Trans. Math. Software*, 31(3):351–362, 2005.

[21] N. V. Ivanov. Mapping class groups. In R. Sher and R. Daverman, editors, *Handbook of Geometric Topology*, pages 523–633. Elsevier Science, 2001.

[22] V. F. Jones. Planar algebras, i. *arXiv preprint math/9909027*, 1999.

[23] C. Kassel, O. Dodane, and V. Turaev. *Braid Groups*. Graduate Texts in Mathematics. Springer New York, 2010.

[24] G. Kells, J. K. Slingerland, and J. Vala. Description of kitaev's honeycomb model with toric-code stabilizers. *Phys. Rev. B*, 80:125415, Sep 2009.

[25] A. Kitaev. Anyons in an exactly solved model and beyond. *Annals of Physics*, 321(1):2 – 111, 2006. January Special Issue.

[26] A. Kitaev and J. Preskill. Topological entanglement entropy. *Physical review letters*, 96(11):110404, 2006.

[27] M. A. Levin and X.-G. Wen. String-net condensation: A physical mechanism for topological phases. *Phys. Rev. B*, 71:045110, Jan 2005.

[28] K. Michnicki. 3-d quantum stabilizer codes with a power law energy barrier, 2012.

[29] R. N. C. Pfeifer, O. Buerschaper, S. Trebst, A. W. W. Ludwig, M. Troyer, and G. Vidal. Translation invariance, topology, and protection of criticality in chains of interacting anyons. *Phys. Rev. B*, 86:155111, Oct 2012.

[30] J.-P. Tillich and G. Zemor. Quantum ldpc codes with positive rate and minimum distance proportional to $n^{1/2}$, 2009.

[31] U. Tillmann. S-structures for k-linear categories and the definition of a modular functor. *Journal of the London Mathematical Society*, 58(1):208–228, 1998.

[32] V. G. Turaev. *Quantum invariants of knots and 3-manifolds*, volume 18. Walter de Gruyter, 1994.

[33] K. Walker. On wittens 3-manifold invariants. *preprint*, 1991.