TOPOLOGICAL QUANTUM COMPUTING

KYLE EVITTS

Introduction

Quantum Computers have generated a lot of interest in the academic world, security circles, and tech companies because of their computational advantages over classical computers. However, even though we have a good understanding of the mathematical theory behind them, we still have yet to implement a quantum computer physically. One of the big obstacles to realizing a quantum computer is having a robust way to implement quantum gates. That is, a reliable way of performing quantum gates that is error free. One possible solution to this problem is to create a topological quantum computer. While this approach most likely isn't as practical as current attempts at creating quantum gates, it does theoretically guarantee essentially error free quantum computation. The goal of this paper is to describe a basic model of a topological quantum computer, and to explain how it accomplishes the task of performing accurate quantum computation.

The main sources for this paper were a paper by Louis H. Kauffman and Samuel J. Lomonaco Jr. and a video lecture series on youtube by Nick Bonesteel. They are citations [1] and [4] in the bibliography.

Background

In this section we give a quick and dirty overview of the key algebraic and topological concepts that will play a role in the future sections of this paper. We start first with the key definitions and concepts in abstract algebra. Then we will introduce the reader to the basics of topology and algebraic topology. This material is usually taught in one to two years worth of courses, so understandably this introduction will not be sufficient to have a full understanding of the material, but hopefully it will at least give the reader an idea of the necessary mathematics required for topological quantum information theory. There are of course many textbooks on these topics, as they a featured in most standard beginning graduate mathematics courses. I have listed some of these textbooks in the sources (See [2],[3]). They are most likely not the best sources, but they are the ones I am familiar with.

Groups. One of the most basic objects in abstract algebra are groups. Formally, they are a way to abstract the important properties of sets of numbers like the integers $\mathbb{Z}$, rationals $\mathbb{Q}$, or real numbers $\mathbb{R}$. Another common view point, is that groups are a way of mathematically describe symmetry. This viewpoint will become apparent in the examples that follow. For now we start with the definition.

Definition A group is a set G together with a binary operation $\cdot : G \times G \to G$ satisfying the following properties:

i) (Associativity) For every $g, h, j \in G$, we have $(g \cdot h) \cdot j = g \cdot (h \cdot j)$. This property tells us that it doesn't matter how we pair elements together to perform long sequences of multiplications. Thus the expression $g \cdot h \cdot j$ is unambiguous.
ii) (Identity) There is a element $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$. This element e is called the identity element of the group. It is commonly denoted as 1 or 0 depending on whether it is more natural to think of the group operation as an addition or multiplication.
iii) (Inverses) For every $g \in G$, there is an element $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Note that groups are not required to be commutative. Thus it may be the case that $g \cdot h \neq h \cdot g$. Commonly groups are referred to just by their underlying set G when the group operation is clear. Also, it is important to point out an important part of the definition is not explicitly stated in the axioms. This property is called closure. Closure means that the product of two group elements results in another element in the group. This is implied by the fact that the group operation is a function from $G \times G\ to\ G$.

Some of the first results ones proves in group theory is that the identity element and inverses are unique. The proof of these facts are fairly standard exercises. For details see the references. We now present some examples.

Example As suggested by the discussion proceeding the definition $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are all groups with addition as the group operation. The sum of two integers, rationals, or real numbers is again an integer, rational, or real number respectively. Thus we have closure. Addition is also associative. The identity element is 0, and the inverse of any element is its negative. This verifies all of the group axioms.

In addition to examples, it is indispensable to have good non-examples of any mathematical definition.

Non-Example The natural numbers $\mathbb{N}$ are not a group under addition, as it does not have inverses for all elements. For example, the inverse of 1 should be -1, but $-1 \notin \mathbb{N}$.

Example Other common examples of groups that illustrate how general of a concept groups can be are dihedral groups. Consider a regular polygon like a triangle whose vertices are colored with distinct colors. There are 6 different ways we can move the triangle around and return it to its original location (the vertices are allowed to change positions, but without the colors you would not be able to tell the difference between the starting position of the triangle and its final position). You can flip the triangle around one of three axis, you can rotate the triangle clockwise by 120 degrees, or 240 degrees. These are all symmetries of a triangle. What is the sixth symmetry? The sixth symmetry is the symmetry where you do not move the triangle at all. It is quite a stupid symmetry, but, as you will see in a moment, it plays an indispensable role. Now you may have the objection that you can come up with more than 6 symmetries of a triangle. For instance you can rotate the triangle by 480 degrees. However, this gives the same final result as rotating the triangle by 120 degrees. Thus we consider these rotations as representing the same symmetry of the triangle.

There is also a very natural way to combine symmetries of a triangle. You perform one symmetry on the triangle and then follow it with another symmetry to create a composite symmetry. For example, you can do a 120 degree rotation followed by another 120 degree rotation resulting in a 240 degree rotation. Or you can preform a reflection and then a rotation to get a reflection through another axis. It turns out that symmetries of a regular polygon form a group with this composition of symmetries as the group operation. The identity element is the stupid symmetry. The inverse of a rotation through angle θ is a rotation through angle $2\pi - \theta$. The inverse of a reflection is itself. If we think of each symmetry as a function from the triangle to itself, associativity of symmetry composition follows from the fact that function composition is associative. The symmetry group of a regular n-gon is typically denoted as D_n. These groups are called dihedral groups, which is where the D comes from. Dihedral groups are good examples of non-commutative groups.

Example There are four important groups that will play a role in this paper. They are the general linear group $GL_n(\mathbb{C})$, the unitary group $U(n)$, the quaternions Q_8, and the braid group B_n. The group $GL_n(\mathbb{C})$ is the group of invertible $n \times n$ matrices with coefficients in $\mathbb{C}$. The unitary group $U(n)$ is the set of all $n \times n$ unitary matrices over $\mathbb{C}$ with matrix multiplication as the group operation. Thus $U(n)$ is a subgroup of $GL_n(\mathbb{C})$ (a subset that is also a group with the same operation). The quaternions are the set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with the group multiplication given by the table below.

$\times$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

We leave it as an exercise to the reader to check that $GL_n(\mathbb{C})$, $U(n)$, and Q_8 satisfy the group axioms. We will wait to give a definition of the braid group until the background section on topology.

Group Homomorphisms and Group Representations.

Definition A group homomorphism is a structure preserving map between two groups. Specifically it is a function $f : G \to H$ between two groups G and H such that $f(g_1 \cdot_G g_2) = f(g_1) \cdot_H f(g_2)$, where $\cdot_G$ is the product in G and $\cdot_H$ is the product in the group H. Typically this is just written as $f(g_1 g_2) = f(g_1)f(g_2)$. Thus such a function f respects the important multiplication structure of the group G. If such an f is bijective, then it is called a group isomorphism. Intuitively an isomorphism between two groups G and H tells us that the groups G and H can be thought of as the same group. They have the same multiplication structure, but the elements are just labeled differently. The isomorphism gives a way of converting the labels in G to the labels in H and vice versa.

Example The multiplication by 2 map sending $x \mapsto 2x$ is a group homomorphism from $\mathbb{Z}$ to itself. The fact that it is a homomorphism follows from the distributive property; i.e. $2(x+y) = 2x + 2y$ for all $x, y \in \mathbb{Z}$.

We now list some basic properties of group homomorphisms.

Proposition 0.1. *Let G and H be groups and $f : G \to H$, be a group homomorphism. Then*

- *$f(e_G) = e_H$ (a homomorphism takes the identity in G to the identity in H),*
- *$f(g^{-1}) = (f(g))^{-1}$ for all $g \in G$ (homomorphisms take inverses to inverses),*
- *f is injective if and only if $\ker f = \{e_G\}$ ($\ker f = \{g \in G \mid f(g) = e_H\}$).*

The concept of a group representation will be a critical idea in this paper. A group representation is basically a way of encoding a group using matrices and matrix multiplication. The way this is formalized is by using group homomorphisms.

Definition A representation of a group G is a homomorphism $\rho : G \to GL_n(\mathbb{C})$. More generally, one can have ρ map to $GL_n(K)$ for any field K, or $GL(V)$ for any vector space V. However, working over $\mathbb{C}$ vector spaces is sufficient for this paper, as this is the natural setting for quantum information theory.

Example The mapping below defines a group representation of Q_8. In fact it is an isomorphism. Thus we could use the matrices below to completely describe Q_8 instead of the clunky multiplication table description we had above. In particular, it is not hard to check that $i^2 = j^2 = k^2 = -1$, $ij = k$, and that i, j, and k anticommute.

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Categories. The last bit of algebra we need in order to describe a topological quantum computer is the concept of a category.

Definition A category $\mathscr{C}$ is a collection of objects $\text{ob}(\mathscr{C})$ with the following properties:

1) For every $A, B \in \text{ob}(\mathscr{C})$ there is a collection of morphisms or arrows from A to B denoted $\text{Hom}_{\mathscr{C}}(A, B)$. Typically these morphisms are particular types of functions.
2) For every three objects $A, B, C \in \text{ob}(\mathscr{C})$ there is a binary operation $\circ : Hom_{\mathscr{C}}(A, B) \times Hom_{\mathscr{C}}(B, C) \to Hom_{\mathscr{C}}(A, C)$, which tells you how to compose morphisms. Typically this operation is standard function composition.
3) Furthermore, we require that morphism composition is associative; i.e. for every $f : A \to B$, $g : B \to C$, and $h : C \to D$ we have $f \circ (g \circ h) = (f \circ g) \circ h$.
4) We also require that for every object A there is an identity morphsim $id_A \in Hom_{\mathscr{C}}(A, A)$ such that for every morphism $f : X \to A$ and $g : A \to Y$, $id_A \circ f = f$ and $g \circ id_A = g$.

Example A good example of a category is the category **Groups**, which, as one might guess, has groups as its objects and group homomorphisms as its morphisms. Other examples in the same vein include: $\mathbf{Vect}_{\mathbb{R}}$ vector spaces over $\mathbb{R}$ with linear maps as the morphisms, and **Sets** whose objects are sets and whose morphisms are arbitrary functions between sets.

This last example might set off some alarm bells though. In particular, it violates the axioms of set theory to have a set of all sets, so then how could make sense of ob(**Sets**)? This points out one vague part of the definition above. I only said that a category is a *collection* of objects. I have not specified what i mean by *collection*. A fully mathematically rigorous definition of a category would replace all instances of the word "collection" with "class" in the definition above. A class is similar to a set, however, they have slightly different axioms that allow for a class of all sets. It not necessary to have a detailed description of classes to accomplish the goals of this paper, so I have opted to leave out a description of them. In the interest of transparency, however, I have decided that I should at least point out this small ambiguity in this definition of a category.

As with most other mathematical objects, it is useful to have a notion of a structure preserving map between categories. Such a map is called a functor.

Definition A functor $F : \mathscr{C} \to \mathscr{D}$ is a mapping that associates to each object $A \in \mathrm{ob}(\mathscr{C})$ an object $F(A) \in \mathrm{ob}(\mathscr{D})$ and to each morphism $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ a morphism $F(f) \in \mathrm{Hom}_{\mathscr{D}}(F(A), F(B))$ such that

1) $F(id_A) = id_{F(A)}$ for all $A \in \mathrm{ob}(\mathscr{C})$,
2) $F(g \circ f) = F(g) \circ F(f)$ for all morphisms $f : A \to B$, $g : B \to C$.

The reason why mathematicians care about categories and functors is that they summarize over arching themes common in many areas of mathematics. Almost every area of mathematics can be formulated completely abstractly as a collection of objects with arrows between, without having to know much about what the objects and arrows represent. In particular, many important theories and results that connect two seemingly disparate areas of mathematics essentially boil down to having a functor between two categories. So functors are incredibly useful tools for examining relationships between many areas of mathematics.

Topology. Now that we have covered all of the algebra that is required for this paper, we can move on to the background of topology.Topology is basically a study of one category called **Top**, which is the category of topological spaces with continuous maps as morphisms. To start with we must define these terms.

Definition A topological space $(X, \mathscr{T})$ is a set X together with a set $\mathscr{T} \subseteq \mathscr{P}(X)$ with the following properties

1) $\emptyset, X \in \mathscr{T}$.
2) If $\{U_\alpha\}_{\alpha \in I}$ is any arbitrary collection of sets in $\mathscr{T}$ (The index set I could be infinite or even uncoutable), then $\cup_{\alpha \in I} U_\alpha \in \mathscr{T}$. This property says that $\mathscr{T}$ is closed under arbitrary unions.
3) If $U, V \in \mathscr{T}$, then $U \cap V \in \mathscr{T}$. Note that this implies that $\mathscr{T}$ is closed under any finite intersection.

The elements of $\mathscr{T}$ are called open subsets of X and $\mathscr{T}$ is called a topology on X.

Example The topological spaces the reader is probably most familiar with are euclidean spaces $\mathbb{R}^n$. The open sets in $\mathbb{R}^n$ are any set that can be expressed as an arbitrary union of open balls. This is the standard definition of an open set in most beginning analysis classes. Note that $\mathbb{C}^n$ is essentially the same as $\mathbb{R}^{2n}$ since we are not considering the algebraic structure of these sets.

Example Given any set X there are two somewhat trivial topologies on X. One is called the discrete topology, in which all subsets of X are open (i.e. $\mathscr{T} = \mathscr{P}(X)$). The other is called the indiscrete topology, where the only open sets are $\emptyset$ and X.

Now that we have described the objects in **Top** we can move on to describing the morphisms (continuous functions).

Definition A continuous function $f : X \to Y$ from a topological space $(X, \mathscr{T}_X)$ to another topological space $(Y, \mathscr{T}_Y)$ is function such that the pre-image $f^{-1}(V)$ of any open set $V \in \mathscr{T}_Y$ is an open set in X; i.e. $f^{-1}(V) \in \mathscr{T}_X$.

Example Using euclidean spaces as an example again, it is possible to show that this definition completely matches up with the ε, δ definition of a continuous function given in most analysis classes. For example $f(x) = 2x$, $g(x) = x^2$, $h(x) = |x|$ are all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ under this definition.

Example If X is a topological space with the discrete topology one it, then any function $f : X \to Y$ is continuous.

Definition If a function $f : X \to Y$ is a continuous function between topological spaces X and Y that is bijective (so f^{-1} exists), such that f^{-1} is also a continuous function, then f is called a homeomorphism. We say that X and Y are homeomorphic ($X \cong Y$).

A homeomorphism is similar to a group isomorphism. If two spaces are homeomorphic, then really they can be thought of as the same space. The homeomorphism gives a way of identifying the open sets in each space, so their topologies are essentially indistinguishable.

In general, many topological spaces can be viewed as geometric objects such as a sphere or a torus (surface of a doughnut). These sorts of spaces are called manifolds. The intuition behind continuous functions is that they can stretch, compress, bend, or kink a space, but ripping or tearing the space is not continuous.

Definition A manifold of dimension n is a topological space M such that every point $x \in M$ has an open neighborhood U containing x such that $U \cong B_1(0) \subseteq \mathbb{R}^n$ where $B_1(0)$ is the open unit ball around $0 \in \mathbb{R}^n$.

Thus a manifold is a space that locally looks like euclidean space, and as stated above they can often be thought of as geometric objects.

Example The surface of a sphere and a cube are manifolds that are homeomorphic (any point in either space has an open neighborhood that looks like an open ball in $\mathbb{R}^2$, so they are both manifolds of dimension 2). One can think of patting in the corners of a cube to create a sphere. However, a sphere and a torus are non-homeomorphic 2-manifolds. We will explain why shortly.

In general, it is fairly easy to show that two topological spaces are homeomorphic. You just have to exhibit a homeomorphism between them. However, showing two spaces are not homeomorphic is much more difficult. Just because you can not think of a homeomorphism between two spaces doesn't mean one doesn't exist. This is where one of the main brilliant ideas of algebraic topology comes into play. One of the biggest tools in algebraic topology is that there are a number of functors from **Top** to **Groups**. These functors associate the same group to homeomorphic topological spaces, which gives an invariant of a topological space. Thus if two spaces have different associated groups, then they must be distinct spaces (not homeomorphic).

One of these functors is called the fundamental group. The fundamental group of a topological space X is denoted by $\pi_1(X)$. One way to show that a sphere and a torus are not homeomorphic is to show that their fundamental groups are different. In particular, the fundamental group of a sphere is the trivial group that has only an identity element ($\pi_1(S^2) \cong 0$), however, the fundamental group of a torus is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ ($\pi_1(T^2) \cong \mathbb{Z} \times \mathbb{Z}$).

The notion of a manifold can also be extended slightly to a manifold with boundary.

Definition A n-manifold with boundary M is a topological space M such that every point $x \in M$ has an open neighborhood U containing x such that either $U \cong B_1(0) \subseteq \mathbb{R}^n$ or $U \cong B_1^+(0) \subseteq \mathbb{R}^n$ where $B_1^+(0) = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_1 \geq 0 \text{ and } \sum_i x_i^2 \leq 1\}$ is the upper half of an open ball. If $x \in U \cong B_1^+(0)$, then we say x belongs to the boundary of M, which is denoted ∂M.

Manifolds without boundary (the previous definition) are commonly called closed manifolds. It is important to point out here that the boundary of an $n+1$ manifold is a closed n manifold

Example An example of a manifold with boundary is a closed disk in $\mathbb{R}^2$. Namely $D^2 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$

Cobordism Categories. Cobordism categories play a role in defining a topological quantum field theory used later in this paper. We take the opportunity to define them now.

Definition The n^{th} cobordism category is denoted Cob$[n]$. The objects of Cob$[n]$ are smooth closed n manifolds. If L and R are objects in Cob$[n]$, then a morphism between L and R is a smooth $n+1$ manifold M with boundary ∂M such that the boundary is partitioned into two closed n manifolds a left hand boundary and a right hand one. The left hand boundary is L and the right hand boundary is R. M is regarded as a morphism from L to R.

Example The standard example of a morphism in Cob[1] is a pair of pants, which is a morphism from a pair of circles to one circle pictured in figure 1 below.

Braid groups. Another key family of groups for this paper are the braid groups. The best mathematically formal definition of a braid group is as the fundamental group of a special topological space called a configuration space. However, this has two disadvantages. The first is that it would require me to define a quotient spaces, which would take a rather lengthy discussion. The second is that it wouldn't really give a good intuitive understanding of the group. Fortunately, there is a good physical description of what the elements of braid groups look like and how they multiply together.

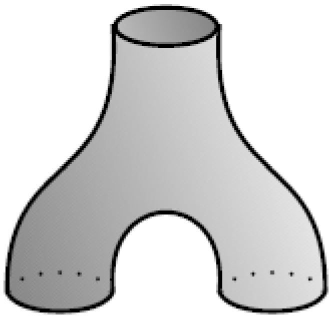

Figure 1. A morphism in Cob[1] (source: http://math.ucr.edu/home/baez/comultiplication.jpg)

The braid group on n strands is denoted Br(n). The elements of Br(n) consist of two rows of n points, with n pieces of string pairing points in the first row with points in the second row. The pieces of string can weave around each other in complicated braiding patterns (hence the name of the group).

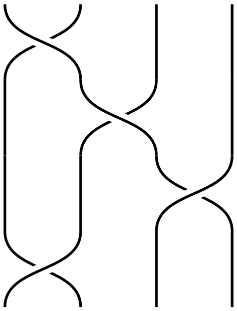

Figure 2. An element of Br(4)

If you can deform one braid in a continuous manner into another braid, then they are considered to be the same braid and represent the same element in the group. An example is given in figure 3 below. The group operation on braids is concatenation. That is gluing the top row of the first braid to the bottom row of the second braid (see figure 4). There is also a simple way to describe the braid group algebraically using generators and relations. Every braid can be expressed as a sequence of transposing adjacent strands. These transpositions are denoted by σ_i for $i = 1, \ldots, n-1$ in Br(n). The generators for Br(3) and their inverses are shown in figure 5. The fact that some braids are equivalent is expressed by relations among the generators. Namely $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for $i < n-1$ and $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| > 1$. This first relation was pictured in figure 3, the second is

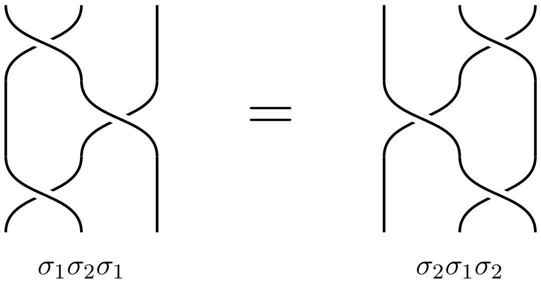

FIGURE 3. Two equivalent braids

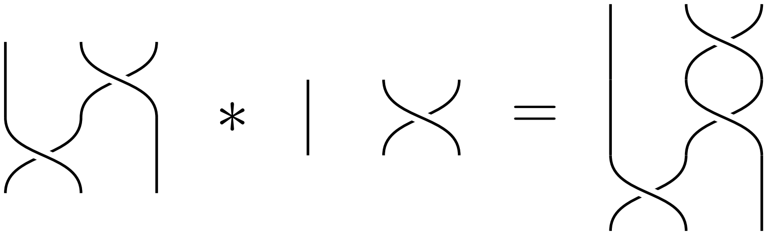

FIGURE 4. Concatenation of braids

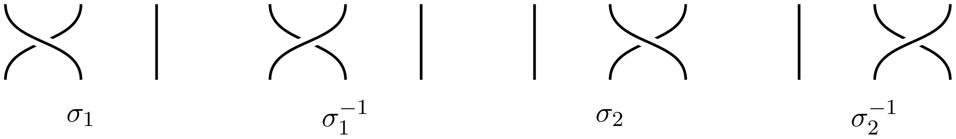

FIGURE 5. The generators of Br(3) and their inverses

pictured in figure 6 below. The first relation is commonly called the braid relation. It is also know as the Yang-Baxter equation.

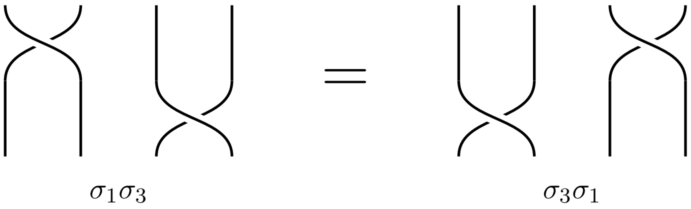

FIGURE 6. The second braid relation

What is a topological quantum computer?

Now we are ready to describe the idea behind a topological quantum computer. In order to describe how to carry out a quantum computation, we need to explain how to initialize a state, perform a quantum gate, and they finally how to measure the outcome.

We will start with how to perform a quantum gate. The main idea is that there is a group representation of the braid group in the unitary group. For the braid group $\mathrm{Br}(3)$, one such representation is $\rho_f : \mathrm{Br}(3) \to U(2)$ defined by

$$\sigma_1 \mapsto R = \begin{pmatrix} e^{-4\pi i/5} & 0 \\ 0 & e^{3\pi i/5} \end{pmatrix} \qquad \sigma_2 \mapsto FRF = \begin{pmatrix} -\tau e^{-\pi i/5} & \sqrt{\tau} e^{-3\pi i/5} \\ \sqrt{\tau} e^{-3\pi i/5} & -\tau \end{pmatrix},$$

where F is the matrix

$$F = \begin{pmatrix} \tau & \sqrt{\tau} \\ \sqrt{\tau} & -\tau \end{pmatrix},$$

and τ is the reciprocal of the golden ratio. The golden ratio is $\varphi = \frac{1+\sqrt{5}}{2}$, and thus $\tau = 1/\varphi = \frac{\sqrt{5}-1}{2}$. A nice property of φ and τ is that they satisfy the relations $\varphi^2 - \varphi = 1$ and $\tau^2 + \tau = 1$. Using these relations it is not hard to check that both R and F are unitary matrices, and that F is its own inverse. Thus we can think of σ_2 as a conjugate of σ_1.

In order to check that this mapping does indeed define a group homomorphism, one only needs to verify that $\rho_f(\sigma_1)$ and $\rho_f(\sigma_2)$ statisfy the same relations that define the braid group. It this case, we only need to check that the braid relation holds. Namely, $\rho_f(\sigma_1)\rho_f(\sigma_2)\rho_f(\sigma_1) = \rho_f(\sigma_2)\rho_f(\sigma_1)\rho_f(\sigma_2)$.

One particularly nice fact about this representation is that its image is dense in $U(2)$. This means that we can approximate a unitary matrix to any degree of accuracy by $\rho_f(b)$ where b is a braid in $\mathrm{Br}(3)$. In order to increase the accuracy of this approximation, the braid b must become more and more complicated and twisted.

Since unitary matrices are how we represent quantum gates mathematically, this gives us a way of encoding quantum gates topologically. So how would we use this representation to perform a quantum computation? The idea is encapsulated in the picture below. First we spawn two pairs of particles called anyons. This corresponds to the initialization of the quantum computer. Then we rotate the particles around each other in a flat plane, which creates a braiding of their world lines. This carries out some some unitary operation given by the representation above. Finally, we fuse the pairs of anyons back together to make a measurement on the state. Either the particles annihilate each other (corresponding to a measurement of 0), or they don't (corresponding to a measurement of 1).

So how does this create an low error implementation of a quantum gate? The answer is that braids are the same up to deformation. Thus even if the braids we are trying to perform are perturbed by the environment in some way, they still represent the same braid group element, and so the intended quantum gate will still be performed.

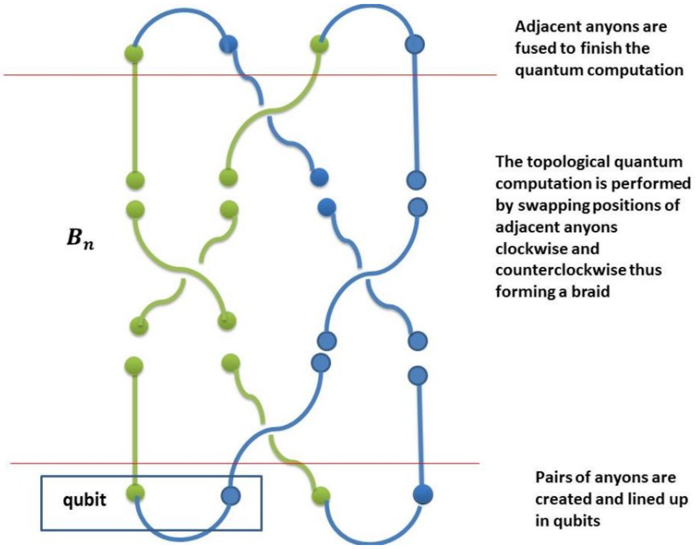
Adjacent anyons are fused to finish the quantum computation
The topological quantum computation is performed by swapping positions of adjacent anyons clockwise and counterclockwise thus forming a braid
B_n
qubit
Pairs of anyons are created and lined up in qubits

Figure 7. Topological quantum computing (source: https://media.licdn.com/mpr/mpr/p/4/005/06a/2b3/142d0d2.jpg)

What are Anyons?

The only somewhat mysterious part of the explanation above is that it is not clear what exactly the anyons are. Anyons are theorized quasiparticles that could result from something called the fractional quantum hall effect. However, I am not a physicist, so most of that just sounds like funny jargon to me. It is possible to describe the particle interactions of these anyons though something called a topological quantum field theory. I originally wanted to present the details of that description in this paper, but I think that it would take too many pages to do so effectively. Instead, I have decided to give a basic overview of what a topological quantum field theory (TQFT) is, and how it is used to create the representation given above.

Definition A topological quantum field theory in dimension n is a functor $Z : \text{Cob}[n] \to \mathbf{Vect}_{\mathbb{C}}$ that associates

1) to each closed, oriented n-manifold $\Sigma \in \text{Cob}[n]$ a finite dimensional $\mathbb{C}$-vectorspace $Z(\Sigma) \in \mathbf{Vect}_{\mathbb{C}}$,
2) a vector $Z(M) \in Z(\Sigma)$ to every compact, oriented $n+1$-manifold M with boundary Σ,
3) and a linear mapping $Z(Y) : Z(\Sigma_1) \to Z(\Sigma_2)$, if Y is a cobordism from Σ_1 to Σ_2.

This functor must satisfy the following properties

1) $Z(\Sigma^\dagger) = Z(\Sigma)^\dagger$, where $\Sigma^\dagger$ represents the manifold with the opposite orientation, and $Z(\Sigma)^\dagger$ is the dual vector space.
2) $Z(\Sigma_1 \sqcup \Sigma_2) = Z(\Sigma_1) \otimes Z(\Sigma_2)$, where $\sqcup$ denotes disjoint union.
3) $Z(\emptyset) = \mathbb{C}$, where $\emptyset$ is the empty manifold.
4) Since $\Sigma \times [0,1]$ is the indentity morphism on Σ in $\text{Cob}[n]$, $Z(\Sigma \times [0,1]) = id_{Z(\Sigma)}$

Anyons are described by a 1-dimensional quantum field theory. This theory consists of one type of particle that can have a "topological charge" of either 0 or 1. The particles can interact by fusing together. The rules for this fusion are that fusing any particle of charge 0 with another particle p results in a particle with the same charge as p. However, if two particles of charge 1 fuse, then they can produce either a particle of charge 1 or of charge 0. The way we get a TQFT out of these abstract particle interactions, is by satisfying some relations on how the charge of the particles are measured. These relations are called the pentagon and hexagon identities in the literature. Solving some matrix equations expressing these relations gives exactly the representation of Br(3) given above. For a more detailed description of how this works see Louis Kauffman's paper [4].

Further Questions

One concern the reader may have is that, in order to perform universal quantum computation, we need a way of performing entangling gates such as CNOT. However, these are two qubit gates, and the representation given above only allows us to carry out single qubit gates. There is a way of generalizing the representation of Br(3) to Br(n) using different TQFT's. Under these representations of Br(n), a two qubit quantum gate corresponds to braiding two pairs of anyons around each other.

Another issue is that the representation outlined above sort of goes in the wrong direction. In order to use a topological quantum computer we would want to know what braid to perform in order to carryout a specific quantum gate. The representation only tells us which unitary a braid carries out, not the other way around. However, other authors have created algorithms for answering this question. There are even algorithms that give a systematic way of improving the accuracy of approximating a specific quantum gate by increasing the complexity of the braid.

Another question is whether any of this is practical. Has anyone built a topological quantum gate? I did find a news article that suggests that an individual working at bell labs is close to creating a limited topological quantum gate (see [5]). It is limited in the sense that it would not provide universal quantum computation, but would allow some quantum gates to be implemented topologically.

One interesting result of the theory behind topological quantum computing is that it suggests that quantum computers could deal with knots in a very natural way. This indicates that quantum computers could be useful in computing invariants of knots. For example there are many authors who have written about quantum algorithms for computing the jones polynomial, which a particular knot invariant. This is interesting as computation of the jones polynomial is known to be NP-hard classically.

Bibliography

1 Bonesteel, N. (2014). Topological Quantum Computation, Lectures 1 to 3 of 3. YouTube. YouTube. https://www.youtube.com/watch?v=sb5agbk5z4y. Accessed 8 June 2016

2 Brundan, J., & Kleshchev, A. A Graduate Course in Algebra. University of Oregon. http://pages.uoregon.edu/vaintrob/classes/brun_klesh_600alg15.pdf. Accessed 8 June 2016

3 Hatcher, A. (2002). Algebraic topology. Cambridge: Cambridge University Press.

4 Kauffman, L. H., & Lomonaco, S. J. Topological Quantum Information Theory. AMS Meetings. AMS. http://www.ams.org/meetings/short-courses/kauffman_notes.pdf. Accessed 8 June 2016

5 Wolchover, N. Forging a Qubit to Rule Them All — Quanta Magazine. Quanta Magazine. https://www.quantamagazine.org/20140515-forging-a-qubit-to-rule-them-all/. Accessed 8 June 2016