# Topological quantum computation with anyons

– Éric Oliver Paquette (Oxford) –

**Outline:**

0. Quantum computation
1. Anyons
2. Modular tensor categories in a nutshell
3. Topological quantum computation with anyons

## 0. Quantum computation

A classical computer as a device that operates on states built from a finite number of bits, i.e. the *state* of a classical computer is an element of $\mathbb{B}^n := \{0,1\}^n$.

In contrast, a quantum computer works with a set of *Qubits* or normalized vectors $|\psi\rangle \in \mathbb{C}^2$ (read "ket-$\psi$") i.e.,

$$|\psi\rangle = \sum_{i \in \mathbb{B}} \alpha_i |i\rangle; \quad \sum_{i \in \mathbb{B}} |\alpha_i|^2 = 1.$$

where $\{|0\rangle, |1\rangle\}$ is an orthornormal basis called the *computational basis* of the *state space* $\mathbb{C}^2$.

Now, a system of $n$ qubit is a state in $\mathbb{C}^2 \otimes ... \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes n}$ i.e., a vector

$$|\psi\rangle = \sum_{x \in \mathbb{B}^n} c_x |x\rangle; \text{ with } \sum_{x \in \mathbb{B}^n} |c_x|^2 = 1.$$

While in the classical case, transformations between states are functions $\mathbb{B}^n \to \mathbb{B}^n$. In the quantum case they are unitary transformations $U : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$.

Finally, if a state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \in \mathbb{C}^2$ is measured, the probability of observing $|i\rangle \in \{|0\rangle, |1\rangle\}$ is given by

$$|\alpha_i|^2 = |\langle\psi|i\rangle|^2 = \langle\psi|i\rangle\langle i|\psi\rangle = \langle\psi|P_i|\psi\rangle$$

where

$$P_0 := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and} P_1 := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Now, as we will see later, quantum computing with anyons gives us access only to a finite set of unitary transformation one can apply on the system. Even in a ‘regular’ (or rather, non-anyonic) implementation of a quantum computer, we may not have access to all unitary transformation in the first place but only to a finite set of them.

A set of unitary transformations is said to be *universal* if any unitary transformation can be 'simulated' as a finite sequence of transformations from that set. Universal sets can be either 'exact' if we can simulate exactly any unitary transformation or 'approximated' ortherwise.

**Theorem:** The set of all 1-qubit transformations $2 \times 2$ unitaries with the controlled-**NOT** i.e.,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

is exact universal.

Now, the set of all $2 \times 2$ unitary transformations is an infinite set and, when working of anyons, we have access to only a finite number of transformations so we need to clarify the notion of 'approximated universal set'.

**Definition:** We say that a transformation $V$ *approximate* $U$ *to accuracy* $\epsilon$ if $\parallel (U - V)|\psi\rangle \parallel < \epsilon$ for all $|\psi\rangle$.

By the Solovay-Kitaev theorem, we know that if a finite $G \subset SU(2)$ containing its inverse and such that the set generated by $G$ is dense in $SU(2)$, then any 1-qubit transformation

$$U \sim g_n \circ ... \circ g_1; g_i \in G$$

up to $\epsilon$ with $n$ reasonably small.

From which such a set $G$ together with controlled-**NOT** is *approximately universal*.

## 1. Anyons

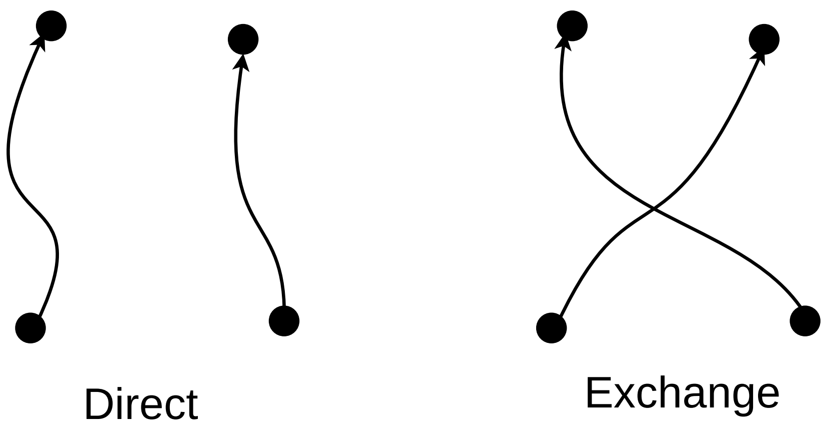
What happens when we exchange 2 undistinguishable particle in 3 dimensions?

Depending wether these two particles are bosons or fermions we have:

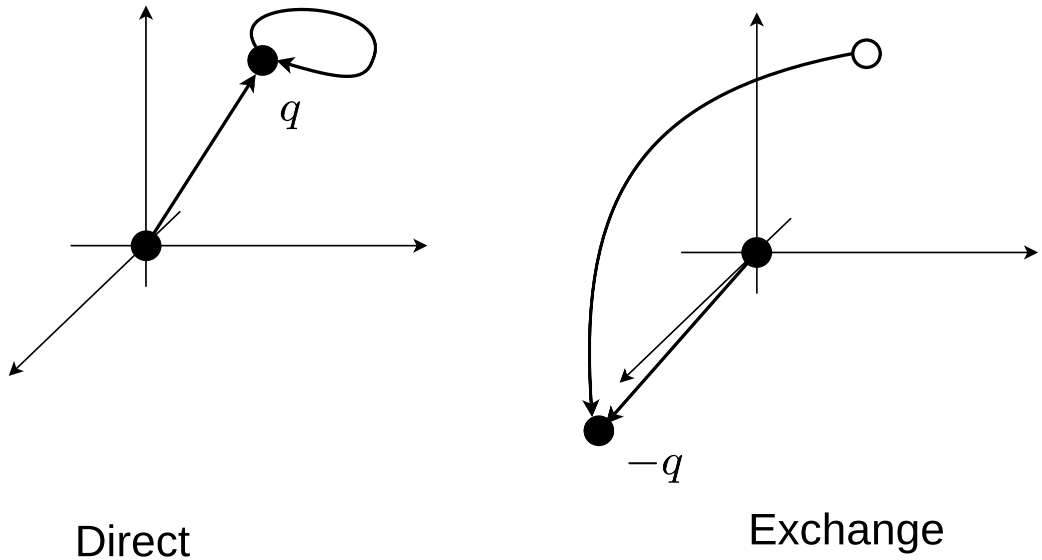
$$|\psi_1\psi_2\rangle = \pm|\psi_2\psi_1\rangle.$$

Note that in both cases, two successive exchanges lead to the identity.

Thinking in terms of paths, two particles moving from some initial configuration to some final configuration leads to two different scenarios:

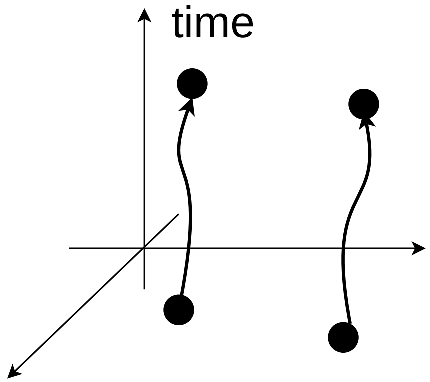


Considering the motion of one of these particle relative to the other and that the initial position is equal to the final position for both particles, these two classes of paths can be represented as

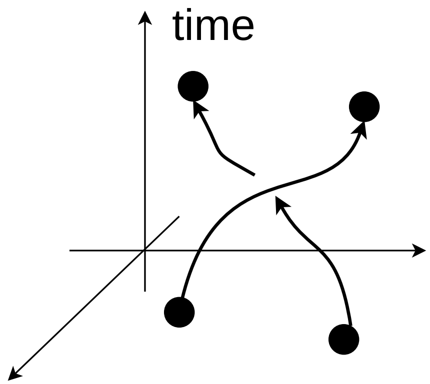



From this, we can see that a double exchange yields a path that can be contracted to the direct – or trivial – path.

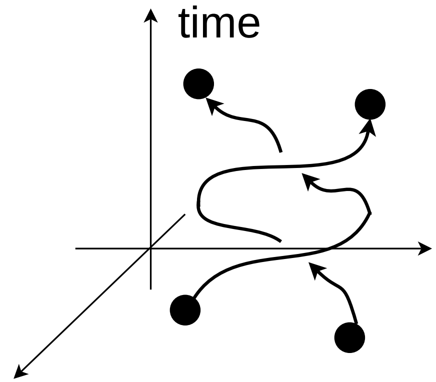
What occurs in 2 dimensions? Let us consider the following three classes of paths:




Direct

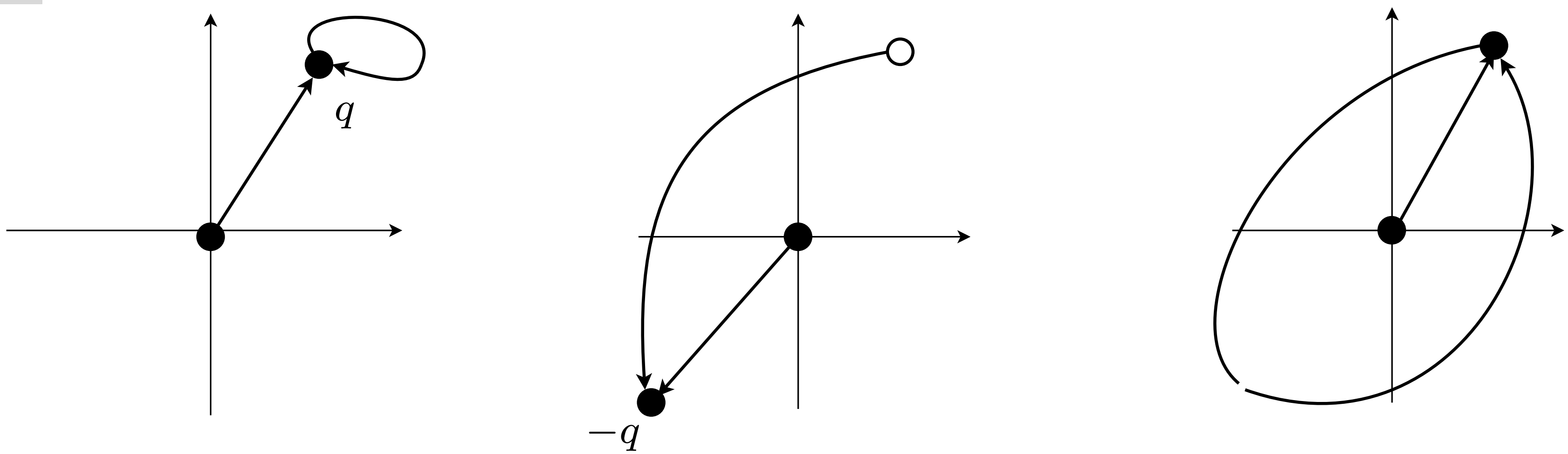



Exchange




2 exchanges

Again, we can pass to the motion of one of the two particles relative to the other:




Direct

Exchange

2 exchanges

Frow which, we see that there are no way (in general) to contract the path resulting from an exchange to the trivial path.

After some tedious calculations using path integrals, one can verify that for such quasi-particles living in 2 dimensions,

$$|\psi_1\psi_2\rangle = e^{i\theta}|\psi_2\psi_1\rangle; \theta \in [0, 2\pi).$$

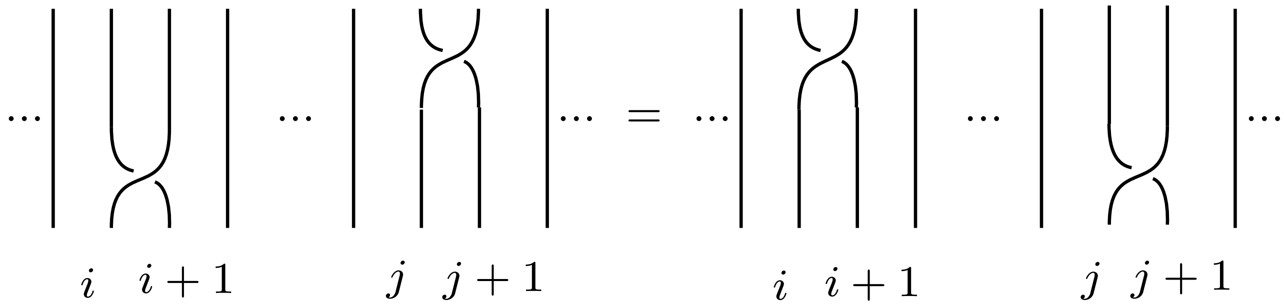
As the $e^{i\theta}$ can take ‘any’ value, such quasi-particles are called ‘any’ons.

The movement on anyons in 2+1 dimensions is encoded by the braid group which can be described by giving generators which obey the following equations:

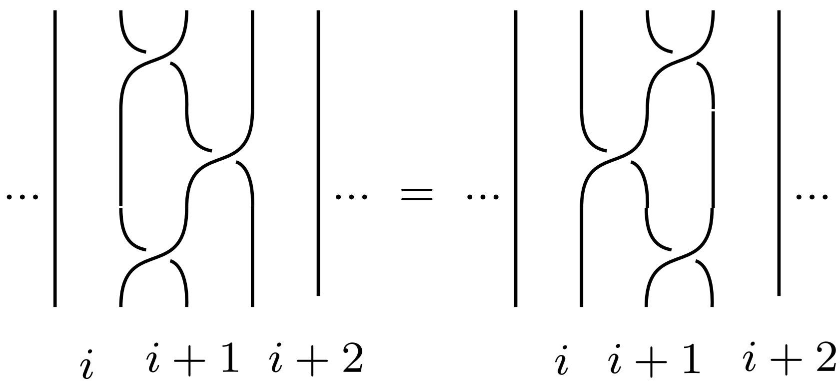
$$b_i b_j = b_j b_i \quad \text{for} \quad |i-j| \geq 2 \tag{1}$$

$$b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1} \quad \text{for} \quad 1 \leq i \leq n-1. \tag{2}$$

or, pictorially:




and



Another important point to make about anyons is that these quasi-particle arise as collective excitations of other particles. If we let them get close enough together, these anyons will fuse into another anyon.

Now, what particular algebraical structure do we need in order to describe (a system of) such quasi-particles?

**2. Modular tensor categories in a nutshell**

- First, we need a system of labels, or types, that will represent the charges of our anyons.
- We also need a way to express a compound system of anyons. This will be expressed by a monoidal (tensor) structure with the trivial charge as the tensor unit. Importantly, this category is not strict monoidal in general. This is physically important because, for instance, the bracketing of a compound system of charges will indicate in which order fusions occur.

- The worldlines of a system of anyons is described by representations of the braid group. We will require that our monoidal category has a braid structure as opposed to being symmetric
- We need a way to express the notion of conjugate charge i.e. for a given charge $A$, its conjugate charge $A^*$ is the unique charge that can fuse with $A$ to yield the trivial charge. The structure that captures these notions is called a *rigid structure*.

- The fact that the objects we are looking at are extended objects – flux tubes – means that, in general, representing their movements graphically with strands in $2+1$ dimensions is not enough; the correct graphical representation is realised by using ribbons, which can be twisted, instead of strands. The algebraic axiomatization of this has been given – long before mathematicians were aware of anyons – and is called a *ribbon structure* on our category.

- A formal way to express the fusion rules and to map all the preceding algebraic formalism into the context of Hilbert space is taken care via a *semisimple* structure compatible with all the preceding structures.

In particular, semisimplicity captures the following ideas:

- The charge of an anyon is elementary i.e., it cannot be decomposed into other elementary entities. In categorical terms, the charge of an anyons has no other subobject than 0 and itself.
- The set of endomorphisms of a charge (a simple object) is isomorphic to the complex field.

Finally, this structure entails that given two different simple charges $S_1$ and $S_2$, Hom$(S_1, S_2) = \{0\}$.

- Finally, we consider a special class of semisimple ribbon categories called *modular tensor categories*. Such categories prohibit an infinite number of possible charges for an anyon of a given theory. Moreover, its defining conditions ensure that the braids are not degenerate.

A category with all these structures is called a semi-simple modular tensor categories and is fairly long to define in details. I'll skip the details and go straight to the simplest example of such a category in order to describe how to do quantum computation with anyons.

### 3. Quantum computing with Fibonacci anyons

Our intended model to illustrate quantum computation with anyons is the formal semisimple modular tensor category $\mathbf{Fib}$ which captures the rules of Fibonacci anyons.

These rules are given as follows:

- Fibonacci anyons have only two charges: $\mathbf{1}$ and $\tau$, where $\mathbf{1}$ is the trivial charge,
- Both are their own anti-charge i.e., $\tau^* = \tau$ and $\mathbf{1}^* = \mathbf{1}$,
- They satisfies the following fusion rules:

$$
\begin{aligned}
\mathbf{1} \otimes \mathbf{1} &\simeq \mathbf{1} \\
\mathbf{1} \otimes \tau &\simeq \tau \otimes \mathbf{1} \simeq \tau \\
\tau \otimes \tau &\simeq \mathbf{1} \oplus \tau
\end{aligned}
$$

Let us inspect the fusion rules. While the two first trivially hold, the third one:

$$\tau \otimes \tau \simeq \mathbf{1} \oplus \tau$$

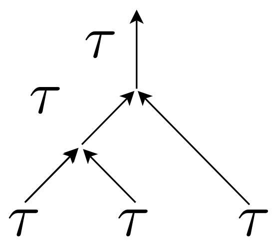
says that the charge resulting from the fusion of two anyons of charge $\tau$ is either $\mathbf{1}$ or $\tau$.

Now, back to our model, consider three anyons of charge $\tau$ all lined up $(\tau \otimes \tau) \otimes \tau$ and let them fuse in the order fixed by the bracketing. Such a process is algebraically described by:

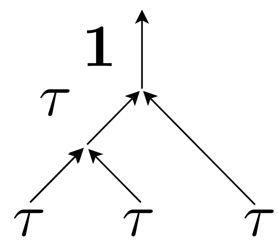
$$
\begin{aligned}
(\tau \otimes \tau) \otimes \tau &\simeq (\mathbf{1} \oplus \tau) \otimes \tau \\
&\simeq (\mathbf{1} \otimes \tau) \oplus (\tau \otimes \tau) \\
&\simeq \tau \oplus (\mathbf{1} \oplus \tau) \\
&\simeq \mathbf{1} \oplus 2 \cdot \tau.
\end{aligned}
$$

Hence, the fusion process for three $\tau$ anyons yields a final charge $\tau$ in 2 different ways or $\mathbf{1}$ in a single way.

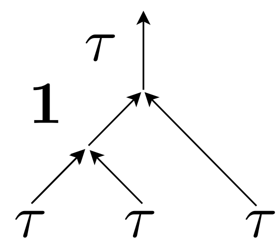
These three scenarios depict as




or




or



We now pass to the context of finite-dimensional complex vector spaces via the splitting spaces. Consider

$$\begin{aligned} \textit{Hom}(b, (\tau \otimes \tau) \otimes \tau) &\simeq \textit{Hom}(b, \mathbf{1} \oplus 2 \cdot \tau) \\ &\simeq \textit{Hom}(b, \mathbf{1}) \oplus \textit{Hom}(b, 2 \cdot \tau) \text{ and as } 2 \cdot \tau := \tau \oplus \tau, \\ &\simeq \textit{Hom}(b, \mathbf{1}) \oplus 2 \cdot \textit{Hom}(b, \tau). \end{aligned}$$

Now, since for different charges $S_1$ and $S_2$ we have Hom$(S_1, S_2) = \{0\}$ and since for any $S \in \{\mathbf{1}, \tau\}$, End$(S) \simeq \mathbb{C}$; if we set $S = \mathbf{1}$, then the last expression is isomorphic to $\mathbb{C} \oplus 2 \cdot 0$. Conversely if $S = \tau$, then it is isomorphic to $0 \oplus 2 \cdot \mathbb{C}$.

From this, we conclude that considering the space of states with global charge $S \in \{\mathbf{1}, \tau\}$ is the same as considering

$$\text{Hom}(S, (\tau \otimes \tau) \otimes \tau).$$

In its turn, such a consideration fixes either of the splitting spaces $\mathbb{C}$ or $2 \cdot \mathbb{C} := \mathbb{C}^2$ as orthogonal subspaces of $\mathbb{C}^3$, the topological space representing our triple of anyons.

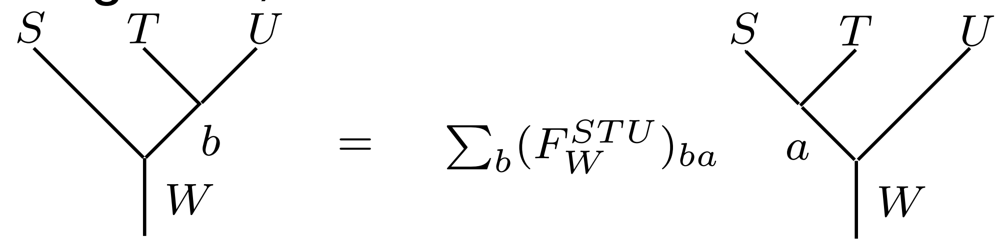
It is within the two-dimensional complex vector space (i.e. with $S = \tau$ as global charge) that we will simulate our qubit. Indeed, with this global charge, we are left with two degrees of freedom which are the two possible outputs of the second splitting. Of course, such a space is spanned by the two possible scenarios of the splitting.

**Remark:** It is worth stressing that it takes *three* anyons of charge $\tau$ to simulate a *single* qubit. Moreover, we shall see later that braiding these anyons together simulates a unitary transformation on such a simulated qubit.

In order to ensure consistency of the model $\mathbf{Fib}$, splitting has to be associative as expressed categorically via an incarnation of the pentagon axiom from the monoidal structure.

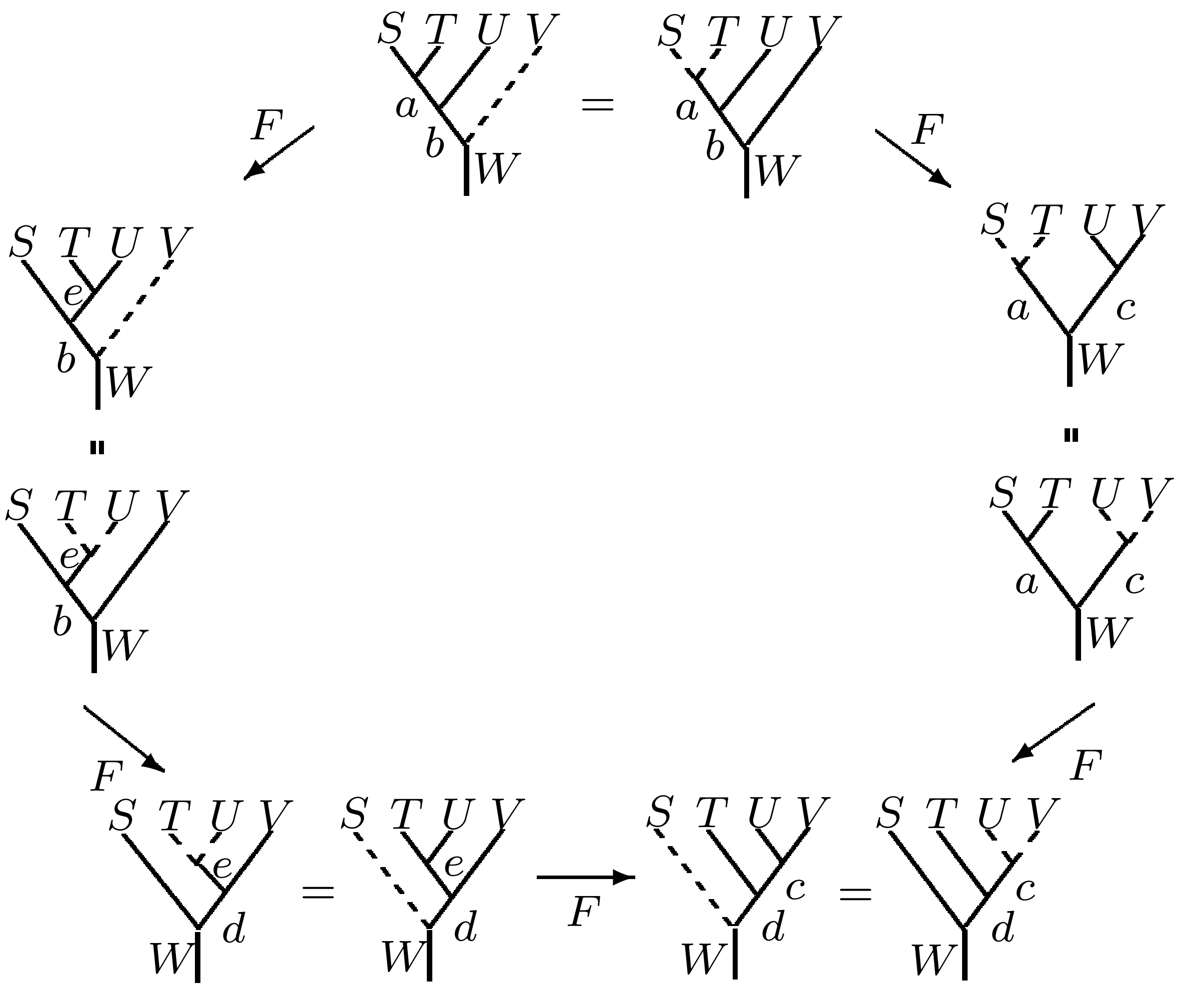
There are two distinct splitting spaces that can be obtained from a triple of anyons i.e.: $(\tau \otimes \tau) \otimes \tau$ and $\tau \otimes (\tau \otimes \tau)$.

Using splitting diagrams, we have:




Considering the splitting diagram for fixed $a$ and $W$ as a basis vector, this is nothing but the matrix expression of $F$. In order to obtain a solution for the $F$-matrix, we need to recast the pentagon axiom from the monoidal structure in this context in such a way that we obtain a matrix equation.

Consider



Now, equating both sides of the diagram yields

$$(F_W^{STc})_{da}(F_W^{aUV})_{cb} = \sum_e (F_d^{TUV})_{ce}(F_W^{SeV})_{db}(F_b^{STU})_{ea}. \tag{3}$$

Solving this in conjunction with a given set of fusion rules yields the $F$-matrix. To solve such an equation, one has to fix the labels for all the possible states in the splitting basis and solve the resulting system of equations.

In $\mathbf{Fib}$, for a triple of anyons of charge $\tau$, the trivial charge can split into such a triple in only one way. In this particular case, the $F$-matrix is

$$F_{\mathbf{1}}^{\tau\tau\tau} = [1]$$

as the first splitting must yields $\tau \otimes \tau$.

Conversely, if the initial charge is $\tau$ then, the splitting process can occur in two distinct manners. In order to get the $F$-matrix, we must use the previous matrix equation. For instance, a possible splitting scenario occurs when one fixes $a = \mathbf{1} = c$ and $d = \tau = b$. Using this with the matrix equation gives:

$$(F_{\mathbf{1}}^{\tau\tau\mathbf{1}})_{\tau\mathbf{1}}(F_{\mathbf{1}}^{\mathbf{1}\tau\tau})_{\mathbf{1}\tau} \quad = \quad \sum_{e\in\{\mathbf{1},\tau\}} (F_{\tau}^{\tau\tau\tau})_{\mathbf{1}e}(F_{\mathbf{1}}^{\tau e\tau})_{\tau\tau}(F_{\tau}^{\tau\tau\tau})_{e\mathbf{1}}$$

Using this, the other consistency relations and the fact that $F$ is unitary, we find:

$$F_{\tau}^{\tau\tau\tau} = \begin{bmatrix} F_{\mathbf{11}} & F_{\mathbf{1}\tau} \\ F_{\tau\mathbf{1}} & F_{\tau\tau} \end{bmatrix} = \begin{bmatrix} \phi^{-1} & \sqrt{\phi^{-1}} \\ \sqrt{\phi^{-1}} & -\phi^{-1} \end{bmatrix}$$

where $\phi$ is the golden ratio.

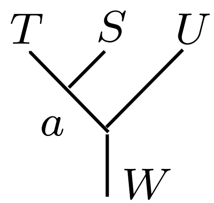
Finally, combining the results for $F_{\tau}^{\tau\tau\tau}$ and $F_{\mathbf{1}}^{\tau\tau\tau}$ yields

$$F = \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \phi^{-1} & \sqrt{\phi^{-1}} \\ 0 & \sqrt{\phi^{-1}} & -\phi^{-1} \end{array}\right]$$

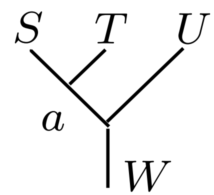
which is also unitary. The lower-right block induces a change of basis on the 2-dimensional splitting space while the upper-left block is the trivial transformation on the one-dimensional splitting space.

We now express what will be the consequence of exchanging two anyons on the splitting space. As such an exchange is represented categorically by a braiding, this will yield a representation of the braid group in the splitting space.

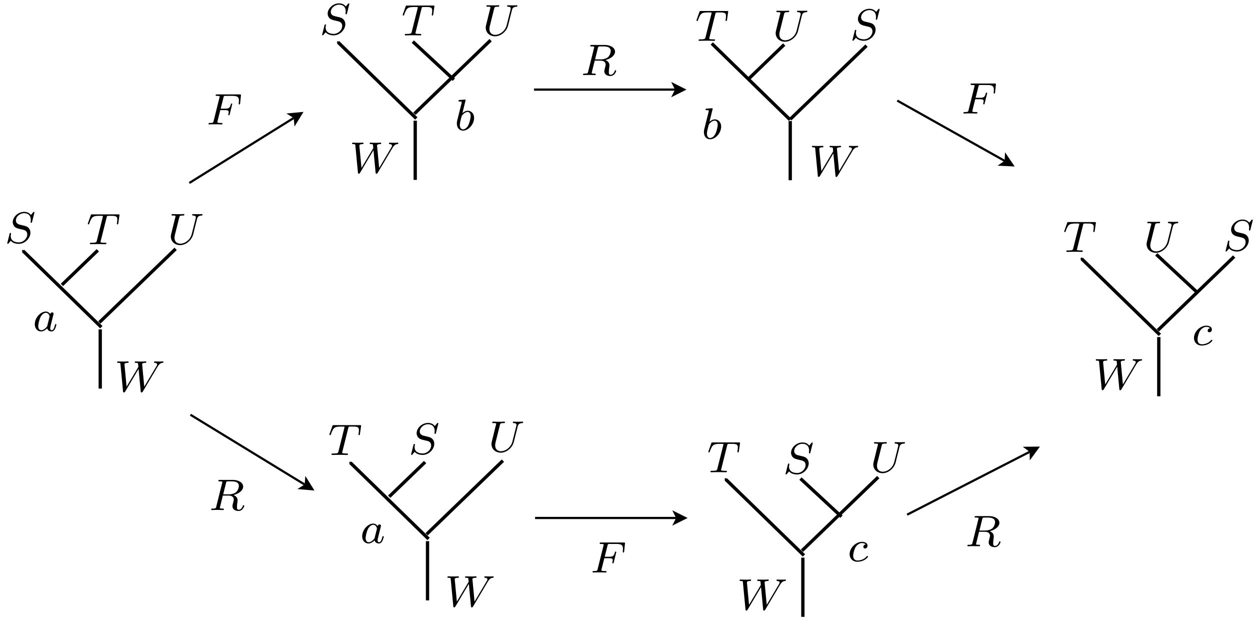
The game here is very similar to the one for the $F$-matrix except that we use the hexagon axiom from the braided monoidal structure instead. The $R$ matrix is described, using splitting diagrams:




$$= [R_a^{ST}]_{aa}$$



We already have the $F$-matrix thus, the hexagon needs to be solved only for the $R$-matrix. Recasted with splitting diagrams, the hexagon axiom from the braided structure becomes:



Writing it as a matrix equation yields

$$R_c^{SU}(F_W^{TSU})_{ca}R_a^{ST} = \sum_b (F_W^{TUS})_{bc}R_W^{Sb}(F_W^{STU})_{ba}.$$

For a triple of anyons with charge $\tau$, explicit calculations of the R-matrix yields:

$$\left[\begin{array}{c|cc} -e^{-2i\pi/5} & 0 & 0 \\ \hline 0 & e^{-4i\pi/5} & 0 \\ 0 & 0 & -e^{-2i\pi/5} \end{array}\right]$$

Such a diagonal form is not surprising: whether the global charge of a couple is $\mathbf{1}$ (resp. $\tau$), it must remain so even if we exchange the two components of the pair.

The $R$-matrix provided in the previous section give us a way to exchange the two leftmost anyons in a set of three. We now need a way to find the matrix that exchanges the two rightmost anyons, this will be the $B$-matrix and defined as:

$$B := F^{-1}RF$$

Now, we have described a way to initialise a qubit as the two-dimensional subspace of the topological space of a triple of anyons and we have both the $R$- and $B$-matrices as unitaries acting on such a subspace. The goal now is to show that this is enough to describe a universal set of gates.

The basic idea to simulate quantum computation with anyons is given by the following steps:

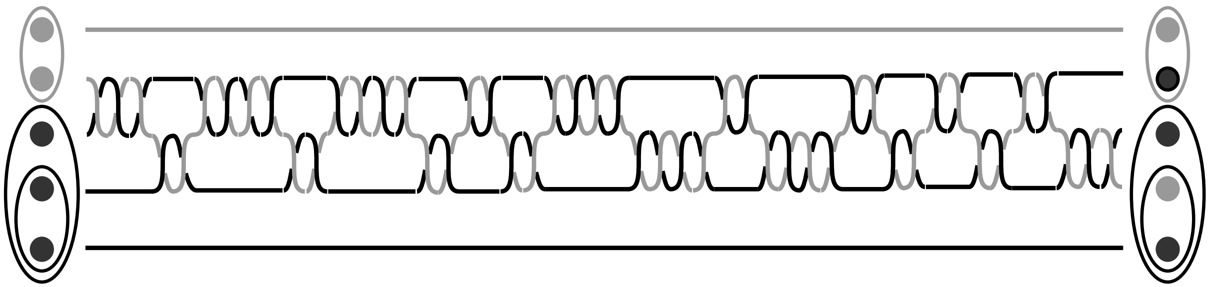
1. Consider a compound system of anyons. We initialise a state in the splitting space by fixing the charges of subsets of anyons according to the way they will fuse. This determines the basis state in which the computation starts.
2. We braid the anyons together, it will induce a unitary action on the chosen splitting space.
3. Finally, we let the anyons fuse together and the way they fuse determines which state is measured and this constitutes the output of our computation.

In fact, we are lucky. The set of $R$- and $B$-matrices and their inverses (the representation of the inverse braiding) is dense in $SU(2)$ thus satisfies the condition of Sovolay-Kitaev theorem. Thus, to get an approximate universal set of gates, it just remains to construct a controlled-**NOT** gate. We will do so by following the works of Bonesteel et al.

The idea is relatively simple: We start with two triplets of anyons. We need to intertwine a pair of quasi-particles from the first triplet – the control pair – with the target triplet *without disturbing it*; as the braid operators are dense in $SU(2)$, we will arrange such an intertwining so that its representation in $SU(2)$ is close enough to the identity. The next thing is to implement a $\mathbf{NOT}$ – actually a $i \cdot \mathbf{NOT}$ – by braiding our two anyons of the control pair with those of the target triple. Finally, we extract the control pair from the second triplet – again – without disturbing it.

The key point is the following: a braiding involving the trivial charge $\mathbf{1}$ with an anyon of arbitrary charge does not change anything. Thus, when measuring the control pair, the $i \cdot \mathbf{NOT}$ will occur if and only if the two anyons from the control pair fuse as an anyon of charge $\tau$; otherwise the control pair only induces a trivial change on the system.

Consider the following braiding:



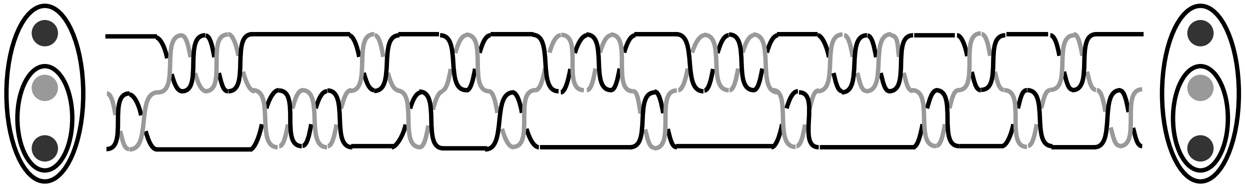
As an action on the splitting space of the three anyons involved, this is, in the same order as depicted in the picture:

$$B^3R^{-2}B^{-4}R^2B^4R^2B^{-2}R^{-2}B^{-4}R^{-4}B^{-2}R^4B^2R^{-2}B^2R^2B^{-2}R^3 \sim \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$$

This tells us how the given braid insert an anyon within a triplet without disturbing it.

In fact, this stresses the distinction between the dynamics of the anyons and the consequences on the splitting space. Indeed, even if we disturbed the initial configuration of anyons via multiple braidings, the effect on the splitting space is approximately the identity.

Now, we implement an $i \cdot \mathbf{NOT}$ as the following braid:

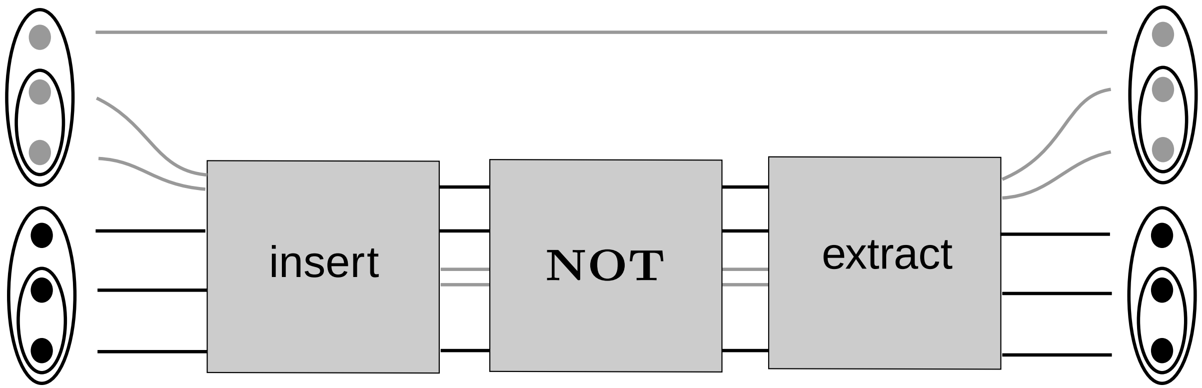


The unitary acting on the splitting space of the initial triple is given by:

$$R^{-2}B^{-4}R^{4}B^{-2}R^{2}B^{2}R^{-2}B^{4}R^{-2}B^{4}R^{2}B^{-4}R^{2}B^{-2}R^{2}B^{-2}R^{-2} \sim \left(\begin{array}{cc|c} 0 & i & 0 \\ i & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$$

This combination of braids tells us how to implements a $i \cdot \mathbf{NOT}$ gate on the two dimensional fusion space of our triple of anyons. Again, this gate is approximated.

Finally, the $i \cdot \mathbf{CNOT}$ gate acting on two topological qubits is realised as follows:




Note that instead of inserting 1 anyon, we insert a couple that will be used as a test couple.

We claim that this implements a $\mathbf{CNOT}$. Indeed, the test couple can fuse in two ways. If it fuse as $\mathbf{1}$, then nothing happens as $\mathbf{1}$ is the trivial charge. If it fuse as $\tau$, then we effectively apply the $i \cdot \mathbf{NOT}$ gate.

Thus, this indeed implements a controlled-*NOT* which, together with our four braiding operations define an approximate universal set of transformations.

In conclusion, using a set of anyons we can:

- Simulate a qubit,
- Approximate any unitary tranformation on a set of qubits and
- Measure the system using fusion,

from which we can simulate quantum computation with anyons.