Unit 07: Quantum Computation by Braiding

Tzu-Chieh Wei

C. N. Yang Institute for Theoretical Physics and Department of Physics and Astronomy, State University of New York at Stony Brook, Stony Brook, NY 11794-3840, USA

(Dated: October 26, 2022)

In this unit, we discuss Kitaev's toric code, anyons (including Fibonacci and Ising anyons), and topological quantum computation (using e.g. Fibonacci anyons, Ising anyons implemented by Majorana zero modes of the Kitaev's chain). We will introduce graphical diagram for fusion, braiding and basis change of fusion channels.

Learning outcomes: You'll be able to say what anyons are and how they can be used for quantum computing.

I. INTRODUCTION

We discussed using quantum error correction codes in the last unit, such as the Shor's 9-qubit code, Steane's 7-qubit code, the five-qubit code, etc. In order to reach fault tolerance, we need to use concatenation i.e., many layers of such codes. There is a substantial overhead to do that. At the same time, researchers also thought about whether one could use 'topology' to passively protect against errors, which does not require concatenation.

In intrinsic topological phases, the ground-state degeneracy depends on the topology of the underlining manifold and there are excitations called anyons, whose braiding gives rise to certain set of quantum gates. Can such topological quantum computation to be made fault tolerant?

Maybe we could even ask less stringent demand about protecting quantum information. Can we have topological codes that can be used to store quantum information indefinitely?

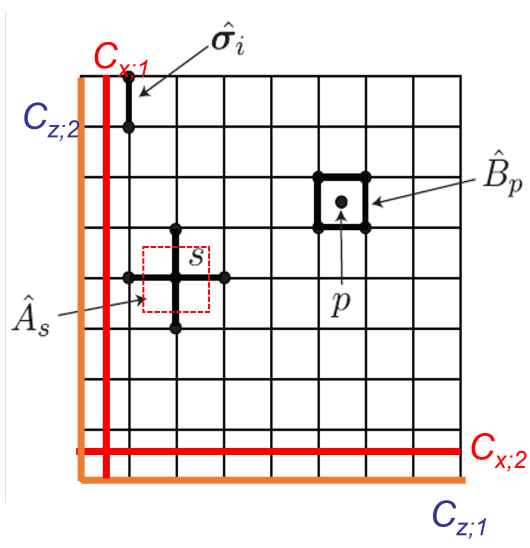


FIG. 1. Illustration of the toric code model.

The Kitaev's toric code is one of such simplest codes that illustrate many features of topological quantum computation. We will see that on the torus there are four degenerate ground states with a gap separating excited states. Local observables cannot be used to distinguish the four ground states. There are four different types of anyonic excitations: (1) vacuum: I, (2) electric charge: e, (3) magnetic flux: m, and (4) fermion: f, which is the bound state of e and m. The model is in the so-called deconfined phase, as a pair of excitations after their creation can be separated far without costing additional energy.

II. TORIC CODE: THE GROUND SPACE IN DETAIL

The toric code invented by Alexei Kitaev [1] can be defind by the following Hamiltonian, where qubits lie on edges of a lattices, such as the torus, which is the square lattice with a periodic boundary condition,

$$\hat{H} = -\sum_s A_s - \sum_p B_p,$$

where A_s is the star operator and B_p is the plaquette operators, both of which are a product of four Pauli operators,

$$A_s = \prod_{j\in s} \sigma_x^{[j]}$$

$$B_p = \prod_{j\in\partial(p)} \sigma_z^{[j]}.$$

One can easily verify that these operators commute, i.e. $[A_s, B_p] = 0$ and hence they can be simulatenously diagonalized, leading the ground states to satisfy

$$A_s|\psi_{\rm G}\rangle = |\psi_{\rm G}\rangle, \;\; B_p|\psi_{\rm G}\rangle = |\psi_{\rm G}\rangle.$$

Thus A_s's and B_p's are stabilizer generators that define the toric code stabilizer group $\mathcal{S}_{\rm TC}$. On a $N \times N$ (periodic) square lattice, see e.g. Fig. 1, there are $2N^2$ edges, and, hence, qubits. There are N^2 star operators and N^2 plaquette operators. However, these are not completely independent, as

$$\prod_s A_s = I, \;\; \prod_p B_p = I.$$

Thus, there are $2N^2 - 2$ independent generators. According to our stabilizer formalism in Unit 06, we know that there are *two* logical qubits. Moreover, this means that we can find logical operators $\bar{X}_1$, $\bar{Z}_1$, $\bar{X}_2$, and $\bar{Z}_2$, which all commute with all elements in $\mathcal{S}_{\rm TC}$ and satisfy the corresponding commutation relations among themselves, e.g. $[\bar{X}_1, \bar{Z}_2] = 0$, but $\{\bar{X}_1, \bar{Z}_1\} = 0$. We will do that later after we look at the degenerate ground states.

We know there are four orthonormal ground states, and to find one we begin with the configuration $|00\ldots0\rangle$, which satisfies all B_p, i.e. $B_p|00...0\rangle = |00...0\rangle$. How do w construct a state from this such that it also satisfies all A_s's? The action of A_s is to locally flip 0000 to 1111; see e.g. $g = A_1A_2A_3A_4A_5I\cdots I$ in Fig. 2a. If we regard 00...0 as a vacuum, then A_s's create fluctuating configurations, formed by local loops.

To statisfy all A_s's, we then apply all possible flipping and make a superposition of all fluctuating configurations, so that any A_s will not change the superposion, i.e., we consider the group G_s generated by all A_s's and the following state,

$$|G_{0,0}\rangle \equiv \frac{1}{\sqrt{|G_s|}} \sum_{g\in G_s} g|00...0\rangle.$$

We can easily see that this satisfies all A_s's and B_p's: $A_s|G_{0,0}\rangle = B_p|G_{0,0}\rangle = |G_{0,0}\rangle$. The ground state $|G_{00}\rangle$ is a equal superposition of all possible (contractible) loop configurations [0..1…10..1..1]. The ground space is effectively two qubits, but how do we get to the other three orthonormal ground states? In terms of the loop picture, there are four different types of loops: (1) no winding, (2) x winding, (3) y winding, and (4) both x and y winding. If we consider the line $C_{x;2}$ that cuts cross edges perpendicular to it and construct the following operator,

$$\bar{X}_2 \equiv \prod_{e\in C_{x;2}} X_e.$$

We can see that it commute with all B_p's operators as it either does not intersect them or intersects with exactly two edges. The action of $\bar{X}_2$ on $|G_{00}\rangle$ creates noncontractible along the x direction, as illustrated in Fig. 2b,c. Similarly, the following operator

$$\bar{X}_1 \equiv \prod_{e\in C_{x;1}} X_e$$

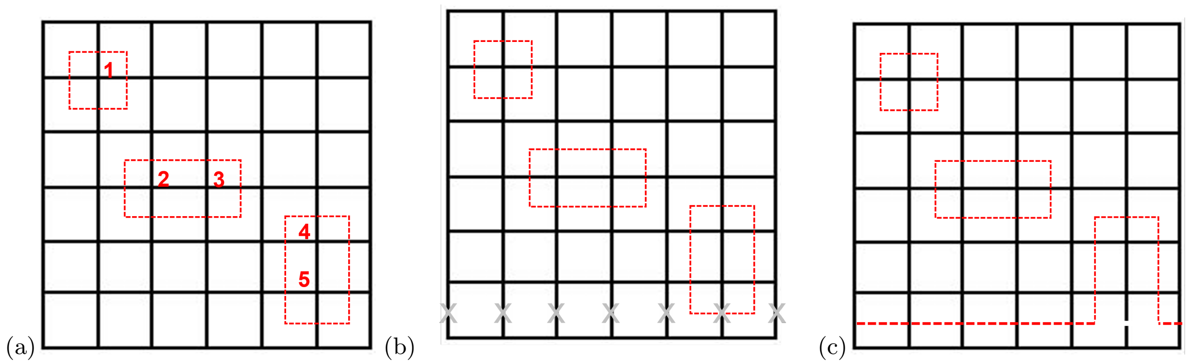


FIG. 2. Illustration of the contractible loops in the toric code model (a). (b) indicates application of a logical X operator which turns the configuration in (a) to one with a noncontractible loop.

will flip winding in the y direction. These are the two logical X operators.

The upshot is that we can use the logical Pauli X operators to flip to get other ground states

$$|G_{\alpha,\beta}\rangle \equiv (\bar{X}_1)^\alpha (\bar{X}_2)^\beta |G_{0,0}\rangle$$

where

$$\bar{X}_{1/2} \equiv \prod_{j\in C_{x;1/2}} \sigma_x^{[j]},$$

and we have use $\sigma_x^{[j]}$ to denote the single Pauli X operator on edge j, as opposed to the above X_e on edge e.

It is an important property that the degenerate ground states cannot be distinguished locally; this can be understood as the X strings can be deformed (as long as the winding is not changed) and the state will not be changed, e.g.

$$|G_{0,1}\rangle = \big(\bar{X}_2 \equiv \prod_{j\in C_{x;2}} \sigma_x^{[j]}\big), |G_{0,0}\rangle$$

i.e. $\bar{X}_2$ mutiplied by any product of A_s's gives equivalent logical X operator, and the non-contractible loop with winding number=1 (odd) in horizontal direction will not be changed. If there is any local operator, one can always deform the X logical operator to avoid this region. Hence, to distinguish different ground states requires nonlocal operators.

Now that we have found the two logical X operators. What are the two logical Z operators? They are constructed as follows,

$$\bar{Z}_{1/2} \equiv \prod_{j\in C_{z;1/2}} \sigma_z^{[j]},$$

and one can easily verify the commutation relations of the four logical operators, e.g. $\{\bar{X}_1, \bar{Z}_1\} = 0$, e.g. $C_{x;1}$ and $C_{z;1}$ intersects at an single edge.

III. ANYONS

As seen in Fig. 3, a Z_e operator acting on an edge e (which happens to share the same symbol as the excitation) will create from the ground state a pair of excitations $A_{s_1} = -1 = A_{s_2}$ for neighboring s_1 and s_2 connected by e. Note that the excitations thus have an energy of $E = 4$. Further action of Z along a path moves the excitations apart but their energy remain the same. This is also referred to as a pair of e excitations. If one apply even further Z operations so that they form a contratible loop, then the two excitations annihilate and the system returns to the ground space (but it might be a different ground state than the original one).

Similarly, if one uses instead X_e operator to act on an edge e, this will create a pair of $B_p = -1 = B_{p'}$, where p and p' share the edge e. This is the magnetic flux excitations m. A contractible loop of X returns the system back to the ground state. However, a non-contractible loop of X is equivalent to a logical X operator (or product of them, if it winds in both x and y direction). This will flip one ground state, e.g. $|G_{00}\rangle$ to another one $|G_{\alpha\beta}\rangle$.

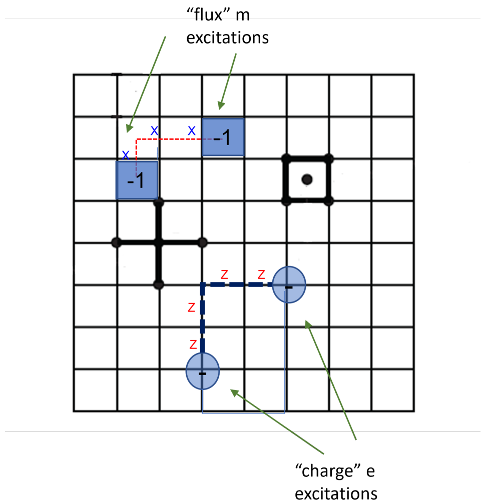


FIG. 3. Illustration of the e and m excitations in the toric code model.

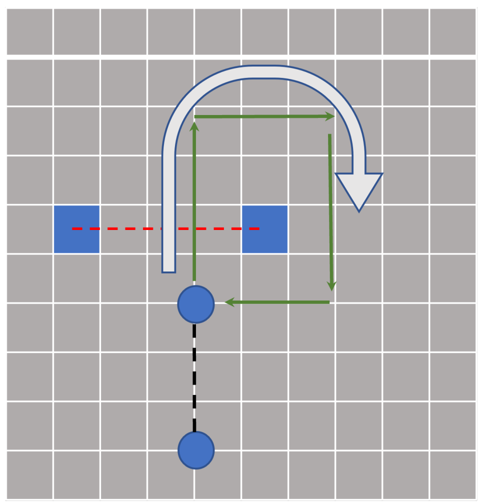


FIG. 4. Illustration of the braiding of e and m excitations in the toric code model (moving e to go around an m).

If one can move an e excitation around an m excitation, this will give a (-1) sign, which originates from the anticommutation of X and Z, as illustrated in Fig. 4. Thus e and m are call relative semions.

If one applies X and Z on neighboring edges and applies further X and Z in close proximity, this will create a two e and two m or equivalently two bound pairs of e and m, which are labelled f (fermions); see Fig. 5a. How do we understand that this is a fermion? We see this by explicitly exchanging the pair while paying attention to how the fermions were created in the first place; see Fig. 5b. We will also come back to this question later when we discuss about the modular matrices and using the braid diagrams.

From the way the cyclic properties $XY = iZ$, $YZ = iX$, and $ZX = iY$, we can see that the 'fusion' of anyons can be represented as,

$$e \times m = f, \; e \times f = m, \; m \times f = e.$$

The vacuum I is the identity,

$$I \times e = e, \; I \times m = m, \; I \times f = f.$$

Moreover, two of the same type of anyons fuse to the vacuum,

$$e \times e = I, \; m \times m = I, \; f \times f = I.$$

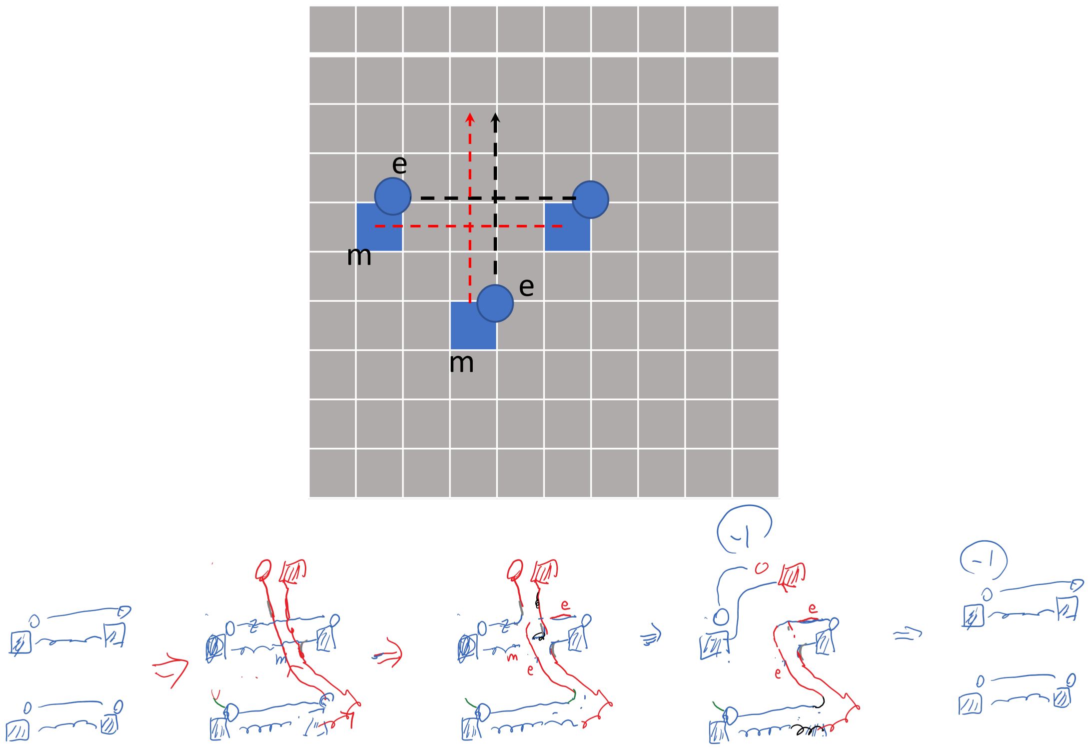


FIG. 5. (a) [Top] Illustration of the fermions f, which are e and m bound pairs in the toric code model. (b) [Bottom] Illustration of exchanging two pairs of $(e, m) = f$ excitations in the toric code model, which gives a -1 sign. Note that in the second step, the two strings of e are recombined and the two strings of m are recombined as the two different ways commute. The curves going over and under in the third step are used to keep track which operators have applied first and which have applied later, i.e. the ordering of operators. In the fourth step, we have used results in Fig. 4 to break the action of winding around, which gives a (-1) sign. In the last step, we have moved anyons to a configuration like the original one. Note that this explanation here does not explicitly use the braid diagram, but suggests its convenience in understanding the braiding of two composite fermions.

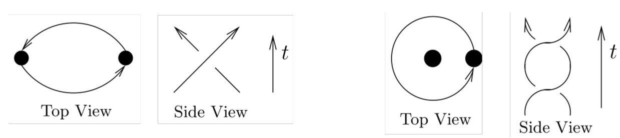


FIG. 6. Illustration of the exchange or braiding (on the left) and rotation (on the right).

So there are their own anti-particles.

In general, the fusion rule for two anyons a and b can result in multiple types of other anyons c,

$$a \times b = \sum_c N_{ab}^c c.$$

When there is only one $N_{ab} \neq 0$, there is only one fusion channel and these anyons are called Abelian. On the other hand, if there exists multiple $N \neq 0$, then the anyon model is non-Abelian. The toric code represents one of the (non-chiral) Z_2 topological phases; the other is exmplified by the so-called double semion [2], which we will not discuss in this course.

IV. MUTUAL AND SELF-STATISTICS

The ground-space basis $|G_{\alpha\beta}\rangle$ is useful for considering logical operations. In terms of the physics of anyons and their exchange statistics, there is a special basis called the opological charge basis, e.g. horizontal loops defined by

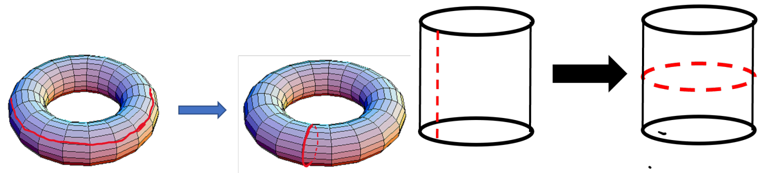


FIG. 7. Illustration of the 90° rotation, S, which also gives the mutual statistics in the topological basis.

$\bar{Z}_1$ and $\bar{X}_2$ of $C_{z;1}$ and $C_{x;2}$ respectively,

$$Z_1 \otimes X_2|0/1, \pm\rangle = (-1)^{0/1} \cdot (\pm 1)|0/1, \pm\rangle.$$

This corresponds to a mixed basis and the four basis states are

$$|0, \pm\rangle \equiv \frac{1}{\sqrt{2}}(|G_{0,0}\rangle \pm G_{0,1}\rangle), \qquad |1, \pm\rangle \equiv \frac{1}{\sqrt{2}}(|G_{1,0}\rangle \pm G_{1,1}\rangle).$$

The topological charges along the loops are well defined, and hence a cut that is along the loop direction to make the system into two halves will result in a minimal of the subsystem entropy. Hence, it is also called the minimally entangled basis (MEB).

Modular S transformation. One can also choose the topological charge in the perpendicular loop direction. The two such bases are related by a 90° rotation (see Fig. 7) and the overlap between the two bases gives rise to the so-called modular S matrix, i.e. $S_{ij} = \langle \Pi_i | \Pi_j^{\perp} \rangle$, up to some phases, where $|\Pi_j\rangle$ represents the corresponding basis state and $\hat{S}$ is the action of the rotation. This approach is useful as one can compute numerically the entanglement entropy for small system sizes and obtains the S matrix.

We can also calculate $\hat{S}$ in the $|G_{\alpha\beta}\rangle$ basis and it is obvious that the rotation takes $|G_{\alpha\beta}\rangle \to |G_{\beta\alpha}\rangle$, and thus we have

$$\langle G'|\hat{S}|G\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

From here we can transform it to the topological basis, and we obtain that the basis under S is mapped to

$$\begin{pmatrix} |0,+\rangle \\ |0,-\rangle \\ |1,+\rangle \\ |1,-\rangle \end{pmatrix} \longrightarrow \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} |0,+\rangle \\ |0,-\rangle \\ |1,+\rangle \\ |1,-\rangle \end{pmatrix}.$$

Modular T transformation. There is an operation on the torus by first cutting it to a cylinder, rotating or twisiting one end of the circle by 360°, and then gluing the two ends back; see Fig. 8. This is called the Dehn twist. This means that the winding in one specific direction will be 'added' to the other direction (depending on the choice of which big circle to cut and twist). This takes for example,

$$|G_{\alpha,\beta}\rangle \longrightarrow |G_{\alpha,\beta+\alpha}\rangle.$$

In the $|G\rangle$ basis, the T matrix is

$$\langle G'|\hat{T}|G\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

But the transformation in the topological basis is

$$\begin{pmatrix} |0,+\rangle \\ |0,-\rangle \\ |1,+\rangle \\ |1,-\rangle \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} |0,+\rangle \\ |0,-\rangle \\ |1,+\rangle \\ |1,-\rangle \end{pmatrix}.$$

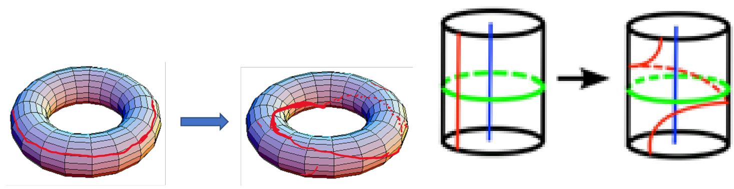


FIG. 8. Illustration of the exchange or braiding, which gives the modular T matrix, representing the self-statistics.

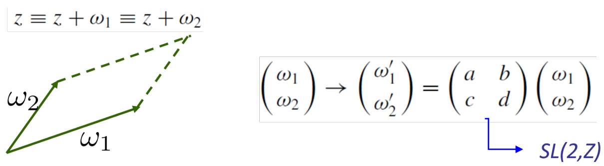
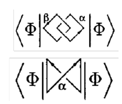


FIG. 9. Illustration of the modular trasnformation $SL(2, Z)$.

It represents the 'self-statistics' of anyons, and the diagonal elements are of the form $e^{i\theta}$; if $e^{i\theta} = 1$, it represents a self-boson, whereas $e^{i\theta} = -1$ represents a self-fermion.

Diagrammatically, the meaning of S and T are given as follows,

$$S_{\beta\alpha} = \langle \Xi_\beta^{//} | \hat{R}(90^\circ) | \Xi_\alpha^{//} \rangle$$
$$T_{\beta\alpha} = \langle \Xi_\beta^{//} | \text{Dehn Twist} | \Xi_\alpha^{//} \rangle$$



For the S, two pairs of anyons, respectively of types α and β, are created. One α and one β anyons rotate around one another (two braids) and then the anyons annihilate in pairs. It is obvious that this gives mutual statistics. For the T, two pairs of anyons of the same type α are created. Two of them exchange and the all anyons annihilate in pairs. It is obvious that this gives self-statistics.

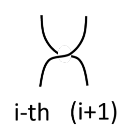
$SL(2, Z)$. In fact, the above two transformations are two special cases (actually generators) of the modular transformation, $SL(2, Z)$; see Fig. 9. The group is generated by the two matrices $\hat{s}$ and $\hat{t}$,

$$\hat{s} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; \hat{t} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

V. EXCHANGE (BRAIDING) AND FULL ROTATION

We refer to the references: Kitaev 2006 [1], Kitaev & Laumann, arXiv:0904.2771 [3], Lahtinen & Pachos, arxiv:1705.04103 [4], Nayak et al. Rev. Mod. Phys. 80, 1083 (2008) [5].

In Unit 03, we mentioned the braid group and used T_i to represent braiding of i-th and (i+1)-th threads:



.

They form a group but there is some constraint:

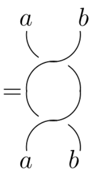
$$T_i T_{i+1} T_i = T_{i+1} T_i T_{i+1},$$

which a kind of the so-called Yang-Baxter equation. Here, we consider braiding of anyons.

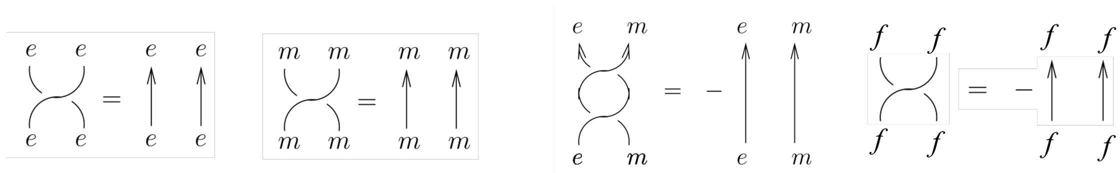
Their rotation and exchanges can be illustrated as braids that evolve in time; see e.g. Fig. 6. It is convenient to introduce the notation R_{ab} to denote the braiding between a and b anyons,

$R_{ab} =$ 

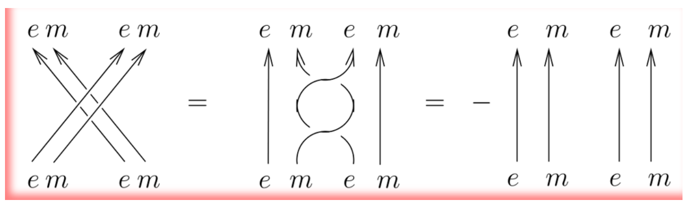
In general, it is an arbitrary phase (for Abelian anyons) unless $a = b$. However, $R_{ba}R_{ab}$ represents a rotation and will be a topological invariant

$R_{ba} \cdot R_{ab} =$ 

From our earlier discussion of the toric code, we have



How do we understand the last equality about the fermion exchange? It comes from the mutual statistics of e and m, as seen below,



In the first equality, we have used the identity of braiding e with e and of m with m and in the second equality, we have used the braiding of e with m.

VI. UNITARY F MOVE OR BASIS TRANSFORMATION

More about fusion. Before we move on to discuss the F operation, we spend some time to study more detail in fusion. If a and b fuse to several types of anyons $c, d, \ldots$, we can define orthonormal states $|a, b; c\rangle$ (in fusion space) that satisfy $\langle a, b; d|a, b; c\rangle = \delta_{cd}$. If we only two anyons: a and b, as different c fused outcomes are distinct, they cannot be superposed to form basis to encode quantum information. This means that we need a third anyon. With fixed a, b, c and d anyons, we have two orderings in the choice of fusing these three anyons, (1) a and b fuse to e, then e fuses with c to d (where e and c can have multiple choices), which is denoted by $|(ab)c; ec; d\rangle$, and (2) b and c fuse to f, then a and f fuse to d, which is denoted by $|a(bc); af; d\rangle$. In case (1), different possibilities of e can be used to encode information, $\sum q_e|(ab)c; ec; d\rangle$. In case (2), different possibilities of f can be used to encode information, $\sum_f r_f|a(bc); af; d\rangle$. That two different ways of fusion ending up the same outcome d means that the two bases are related by a unitary matrix, denoted by F,

$$|(ab)c; ec; d\rangle = \sum_e (F^d_{abc})_{ef}|a(bc); af; d\rangle,$$

which is the convention used in many places, such as in Ref. [6]. However, the opposite convention is also used,

$$|a(bc); af; d\rangle = \sum_e (F^d_{abc})_{fe}|(ab)c; ec; d\rangle,$$

e.g., in Ref. [5].

This relation is illustrated in Fig. 10. We have introduced R earlier. Together with F, there are several constraints (self-consistency relations), such as the so-called pentagon (among F's) and hexagon (between F's and R's) equations; see Fig. 11 from Ref. [1]. These equations are very hard to solve in general. But for simple anyon models, such as the Fibonacci and Ising anyons, their F's and R's can solved and are well-known.

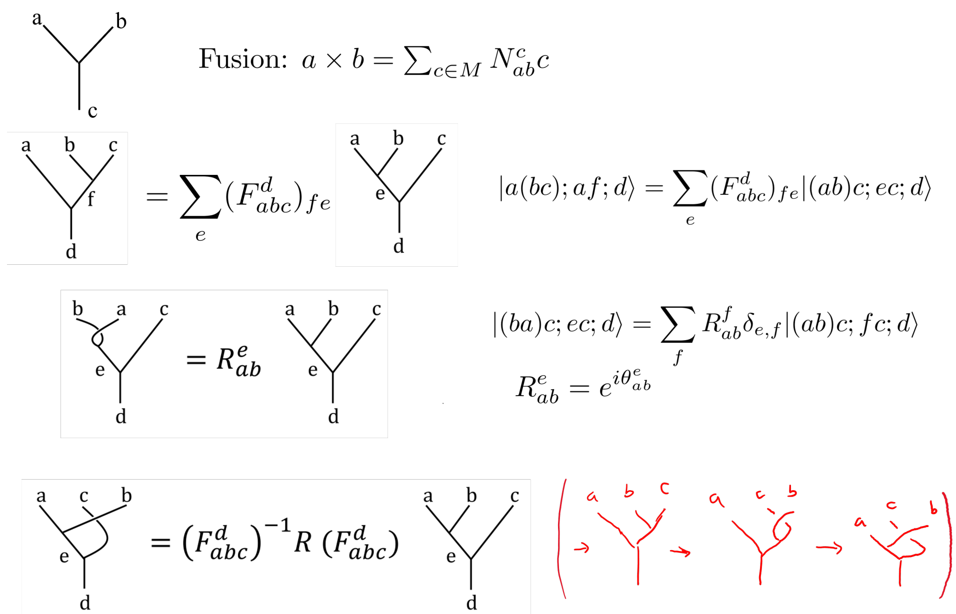


FIG. 10. Illustration of the anyon model defined by several graphs.

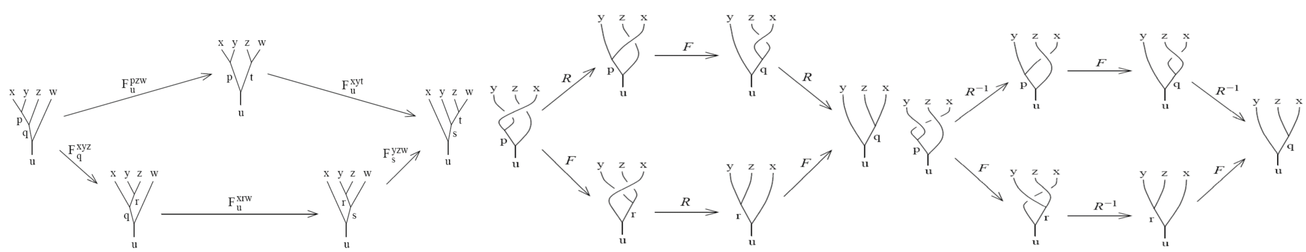


FIG. 11. Illustration of the pentagon and hexagon (two of them) self-consistent relations.

VII. FIBONACCI ANYONS

In this anyon model, there is only one type of nontrivial anyon, denoted by τ. The fusion rule is very simple,

$$\tau \times \tau = 1 + \tau,$$

which can be represented graphically,

$$(\bullet,\bullet)_0 \qquad (\bullet,\bullet)_1$$

with the subscript 0 representing the identity and 1 representing the anyon τ (which may be confusing as 1 is also used as the vacuum). Let us fuse three or more τ's,

$$\tau \times \tau \times \tau = (1+\tau) \times \tau = \tau \times \tau + \tau = 1 + 2\tau$$

$$\tau \times \tau \times \tau \times \tau = 2 \cdot 1 + 3\tau$$

$$\tau \times \tau \times \tau \times \tau \times \tau = 3 \cdot 1 + 5\tau$$

$$\tau \times \tau \times \tau \times \tau \times \tau \times \tau = 5 \cdot 1 + 8\tau$$

We observe the multiplicity numbers, e.g. in front of 1 or τ: 1,1,2,3,5,8, ..., forming the Fibonacci sequence. We also see that dimensions form a Fibonacci series and thus the vector space does not form a tensor-product structure.

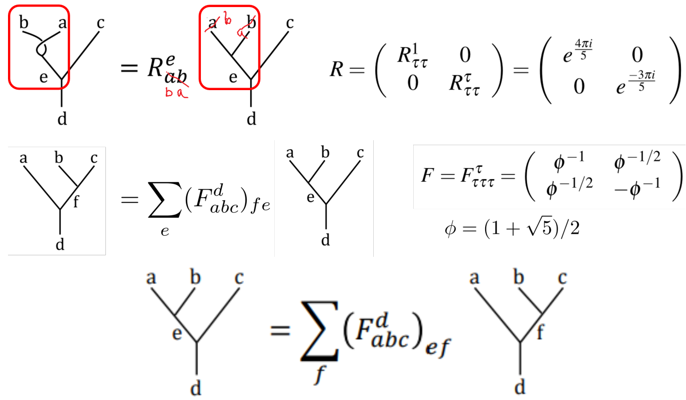


FIG. 12. Illustration of the exchange and basis change for Fibonacci anyons. We list two different versions of convention for the F move.

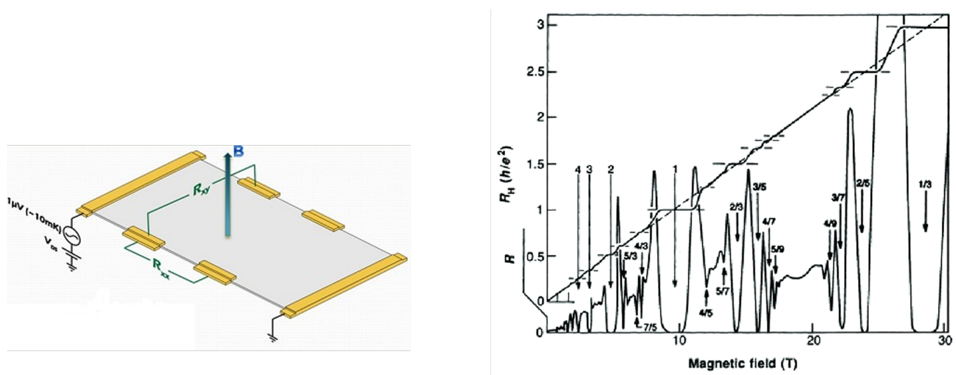
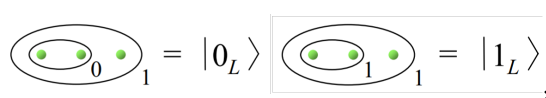


FIG. 13. Illustration of the Hall and resistance measurement as well as some experimental data.

How do we encode a quantum bit? Let us take, e.g., the case that has 3 τ's fused to a τ in two ways,

$$|(\tau\tau)\tau;1\tau;\tau\rangle,\ |(\tau\tau)\tau;\tau\tau;\tau\rangle,$$

which form the basis of a qubit and are also represented graphically as follow,

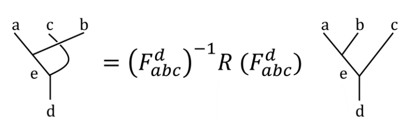


where 0 denotes indentity 1 and 1 denotes the anyon τ.

In this case, the exchange of two τ anyons gives,

$$R = \begin{pmatrix} R^{1}_{\tau\tau} & 0 \\ 0 & R^{\tau}_{\tau\tau} \end{pmatrix} = \begin{pmatrix} e^{\frac{4\pi i}{5}} & 0 \\ 0 & e^{\frac{-3\pi i}{5}} \end{pmatrix}$$

In Fig. 12, we show the exchange and basis change. To exchange b and c, we can use basis change to bring them to the position of a and b and do the exchange before bring them back to the original order, as illustrated below,



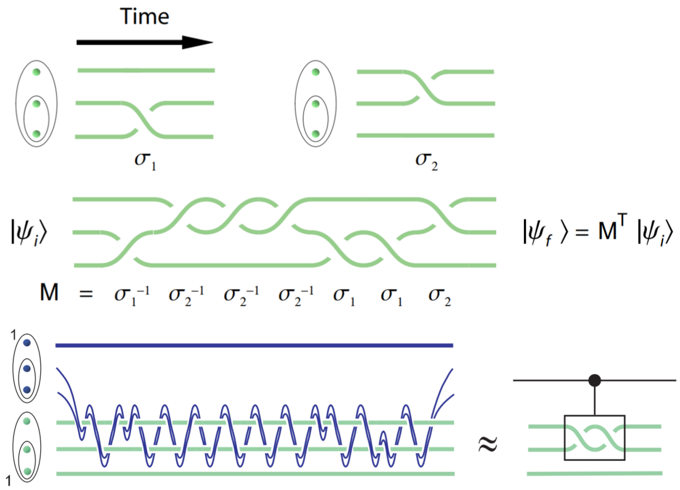
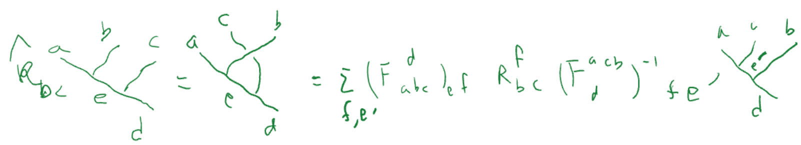


FIG. 14. Illustration of quantum gates in the Fibonacci model.

In our convention, this is



$$= \sum_{f,e'} (F^d_{abc})_{ef} \, R^f_{bc} \, (F^{acb}_d)^{-1}_{fe'}$$

How do we get two qubits? Naively, we can use two groups of three τ anyons. Alternatively, one could use 6 τ anyons fuse to vacuum: there are 5 different ways (slightly more than two-qubit dimension).

Where do we get Fibonacci anyons? One possibility is the Fractional Quantum Hall state with the filling factor $\nu = 12/5$; see Fig. 13. The corresponding quantum state is described by the Read-Rezayi wave function, which has a filling fraction $\nu = N + k/(Mk+2)$ with M odd and which generalizes the Moore-Read wave functions, including one that is likely to be the candidate for $\nu = 5/2$; see the review [5]. The quasiparticle excitations in these systems give rise to the corresponding anyons.

Gates using Fibonacci anyons braiding were studied previously, see e.g. Bonesteel, Hormozi, Zikos & Simon, PRL95, 140503 (2005) [7]; Hormozi, Zikos, Bonesteel & Simon, PRB 75, 165310 (2007) [8]. These are illustrated in Fig. 14. It was shown that the Fibonacci anyon model provides a universal set of gates for quantum computing.

A. F's and R's for the Fibonacci anyons [9]

Here we follow Ref. [10] and sketch how F's and R's can be obtained for the Fibonacci anyons; see Fig. 15 for the explicit diagrams and labels used. First, we note that if any of a, b, c, d contains identity 1, then the element $F^d_{abc} = 1$, which is due to that there is only one unique fusion path in the tree. Thus the only nontrivial matrix if $F^\tau_{\tau,\tau,\tau}$, which is 2×2, as there are two allowed intermediate anyons 1 and τ in the fusion tree. Using the pentagon equation, we have

$$(F^\tau_{\tau,\tau,c})_{ad}(F^\tau_{a,\tau,\tau})_{bc} = (F^d_{\tau,\tau,\tau})_{ec}(F^\tau_{\tau,e,\tau})_{bd}(F^b_{\tau,\tau,\tau})_{ae}. \tag{1}$$

The only nontrivial case is when $b = c = 1$, we simplify the above equation to

$$(F^\tau_{\tau,\tau,\tau})_{11} = (F^\tau_{\tau,\tau,\tau})_{\tau,1}(F^\tau_{\tau,\tau,\tau})_{1,\tau}. \tag{2}$$

Using further that $F^\tau_{\tau,\tau,\tau}$ is unitary, we can obtain F as shown in Fig. 12.

Next, we use the hexagon equation to find R, which reads

$$R^c_{\tau,\tau}(F^\tau_{\tau,\tau,\tau})_{ac}R^a_{\tau,\tau} = \sum_b (F^\tau_{\tau,\tau,\tau})_{bc}R^\tau_{\tau,b}(F^\tau_{\tau,\tau,\tau})_{ab}. \tag{3}$$

Using also the trivial effect by braiding around 1: $R^\tau_{\tau,1} = R^\tau_{1,\tau} = 1$, we can plug in the explicit expression for F, and find that $R^1_{\tau,\tau} = e^{4\pi i/5}$ and $R^\tau_{\tau,\tau} = e^{-3\pi i/5}$. See Ref. [10] for more details.

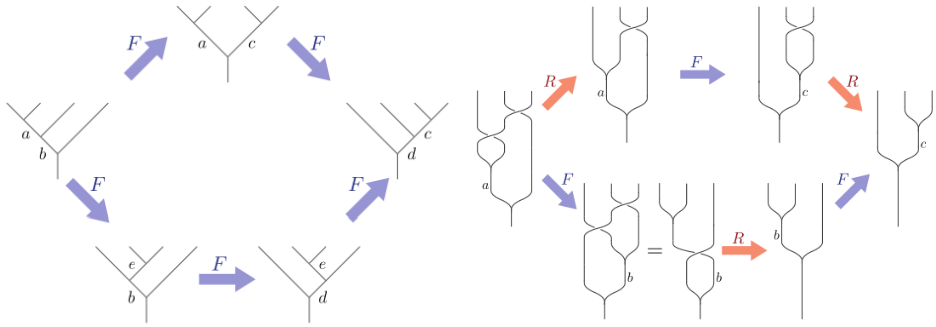


FIG. 15. The diagrams for the pentagon and hexagon equations used in Ref. [10] for the derivation of F's and R's.

VIII. ISING ANYONS

There are three anyons (two nontrivial ones): 1, ψ, and σ. Their fusion rules are,

$$1 \times 1 = 1,\ 1 \times \psi = \psi,\ 1 \times \sigma = \sigma$$

$$\psi \times \psi = 1,\ \psi \times \sigma = \sigma,\ \sigma \times \sigma = 1 + \psi$$

The physical picture is that 1 is the condensate of Cooper pairs, ψ is a Bogoliubov fermion, and σ is the Majorana zero mode bound to a vortex. These anyons can arise from the excitations in the fractional quantum Hall system. The corresponding quantum state is described by the Moore-Read Phaffian wave function

$$\Psi_{\text{Pf}} = \text{Pf}\left(\frac{1}{z_i - z_j}\right) \prod_{i<j} (z_i - z_j)^m e^{-\sum_i |z_i|^2/(4l_0^2)}, \tag{4}$$

with m being even and $\nu = 1/m$; note Pf denotes the Phaffian of an even dimensional antisymmetric matrix. For further details, see the review [5].

How do we get qubits? From the fusion of three σ's,

$$\sigma \times \sigma \times \sigma = (1 + \psi) \times \sigma = 2 \cdot \sigma$$

we have

$$\{|(\boldsymbol{\sigma\sigma})\boldsymbol{\sigma}; \mathbf{1}\boldsymbol{\sigma}; \boldsymbol{\sigma}\rangle, |(\boldsymbol{\sigma\sigma})\boldsymbol{\sigma}; \boldsymbol{\psi\sigma}; \boldsymbol{\sigma}\rangle\}$$

We can also have four σ's,

$$\sigma \times \sigma \times \sigma \times \sigma = 2 \cdot 1 + 2 \cdot \psi,$$

which also allow encoding of a single qubit. We can also use five σ's,

$$\sigma \times \sigma \times \sigma \times \sigma \times \sigma = 4 \cdot \sigma.$$

In fact, if we continue to fuse more σ's, we find that $2n$ σ's can encode $n-1$ qubits (assuming they fuse to vacuum). In Fig. 16, we illustrate a few potential physical implementations for the Majorana zero modes, which host the σ anyons.

We note that one could derive the F's and R's in a similar way to what we have illustrated for the Fibonacci anyon before. The key equation for the F's is

$$(F^1_{\sigma,\sigma,c})_{ad} (F^1_{a,\sigma,\sigma})_{bc} = \sum_e (F^d_{\sigma,\sigma,\sigma})_{ec} (F^1_{\sigma,e,\sigma})_{bd} (F^b_{\sigma,\sigma,\sigma})_{ae}. \tag{5}$$

From this we find that $F_{\sigma,\sigma,\sigma}$ is a 2×2 matrix (labelled by 1 and ψ) is identical to the Hadamard matrix. The derivation for R is left as an exercise.

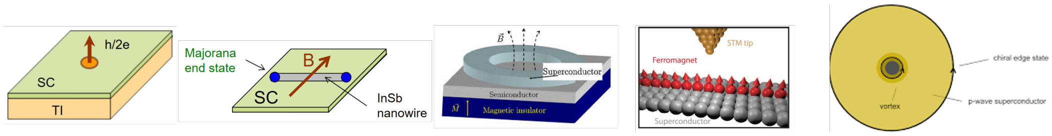
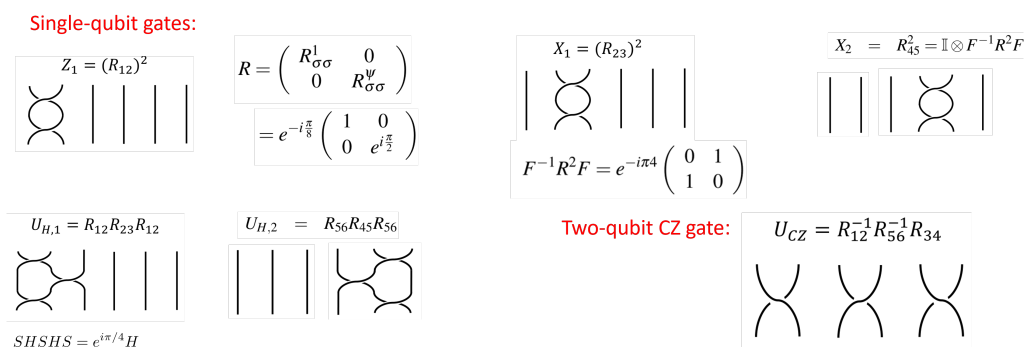


FIG. 16. Illustration of possible realizations of Majorana zero modes.

Let us consider six Ising anyons σ's that fuse to the vacuum 1, as shown in Fig. 17. Some example single qubits are shown here,

$$\begin{aligned} X_1 &= R_{23}^2 = F^{-1}R^2F\otimes\mathbb{I}, \quad & Z_1 = R_{12}^2 = R^2\otimes\mathbb{I}, \quad & U_{H,1} = R_{12}R_{23}R_{12} = RF^{-1}RFR\otimes\mathbb{I}, \\ X_2 &= R_{45}^2 = \mathbb{I}\otimes F^{-1}R^2F, \quad & Z_2 = R_{56}^2 = \mathbb{I}\otimes R^2 \quad & U_{H,2} = R_{56}R_{45}R_{56} = \mathbb{I}\otimes RF^{-1}RFR, \end{aligned}$$

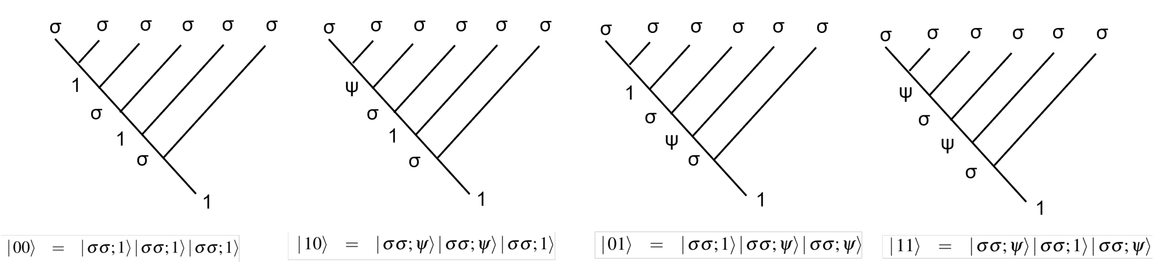
We show some examples in terms of braiding,



We can also implement the two-qubit Controlled-Z gate, as shown in the last gate above,

$$U_{\rm CZ} = R_{12}^{-1}R_{34}R_{56}^{-1}.$$

To understand the encoding above, we know that we can relate the basis states to the standard fusion trees,



which we will verify in a homework problem.

As a brief summary, the Ising anyon model, unfortunately, does not provide a universal set of quantum gates; only Clifford gates are achieved and topologically protected. We shall see in the next unit, additional procedure is needed, in particular, the magic state distillation, in order to 'inject' a protected non-Clifford gate, such as the T gate.

One naive solution, which is non-topological, is to bring two anyons closer to induce interaction and energy shift,

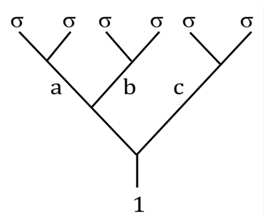
$$U = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\Delta E t} \end{pmatrix}$$

but this is physical-system dependent.

Initialization and Readout. For example, we would like to prepare a two-qubit state $|00\rangle$. Assume that σ anyons are created pairwise from the vacuum with no other anyons present, this will give $|00\rangle$. Other computational basis states can be obtained by applying corresponding X gates.

To read out via the Z-basis measurement, e.g. of the first qubit: we can detect the fusion outcome of anyons 1 and 2. If no change in energy is detected, then it is the 0 state; if we observe change in energy, then it is the 1 state. To measure in the Z-basis of the 2nd qubit: we detect the fusion outcome of anyons 5 and 6 similarly.

To read out in the X basis, for example wof qubit 1: we detect the fusion outcome of anyons 2 and 3. To read out the X-basis measurement of qubit 2, we detect the fusion outcome of anyons 4 and 5. Alternatively, one can apply appropriate Hadamard gate before Z measurement.



➔ Basis states:

$$
\begin{aligned}
|00\rangle &= |\sigma\sigma;1\rangle|\sigma\sigma;1\rangle|\sigma\sigma;1\rangle, \\
|10\rangle &= |\sigma\sigma;\psi\rangle|\sigma\sigma;\psi\rangle|\sigma\sigma;1\rangle, \\
|01\rangle &= |\sigma\sigma;1\rangle|\sigma\sigma;\psi\rangle|\sigma\sigma;\psi\rangle, \\
|11\rangle &= |\sigma\sigma;\psi\rangle|\sigma\sigma;1\rangle|\sigma\sigma;\psi\rangle,
\end{aligned}
$$

$$
\boxed{
\begin{aligned}
R &= \begin{pmatrix} R^1_{\sigma\sigma} & 0 \\ 0 & R^\psi_{\sigma\sigma} \end{pmatrix} \\
&= e^{-i\frac{\pi}{8}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix} \\
F &= F^\sigma_{\sigma\sigma\sigma} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\
F^{-1}R^2F &= e^{-i\pi/4} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\end{aligned}
}
$$

FIG. 17. Illustration of fusing of six Ising anyons and choice of two qubit basis states, as well as R and F. For R's, in addition to what is shown in the diagram, we also have two nontrivial ones: $R^1_{\psi,\psi} = -1$ (for two fermions) and $R^\sigma_{\sigma,\psi} = i$.

A. Kitaev's Majorana chain

The Kitaev chain has the following Hamiltonian [11],

$$H = \sum_{x=1}^{N-1} -t(\hat{c}_x^\dagger \hat{c}_{x+1} + \hat{c}_{x+1}^\dagger \hat{c}_x) + \Delta(\hat{c}_x \hat{c}_{x+1} + \hat{c}_{x+1}^\dagger \hat{c}_x^\dagger) - \mu\, c_x^\dagger c_x,$$

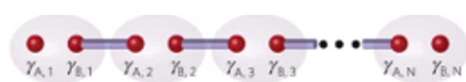
where t is the hopping strength for electrons to hop from one site to the next, Δ is the p-wave Cooper pairing between electrons, and μ is the chemical potential (that controls the tendency of how many electrons will occupy the whole chain and can be implemented by an electric gate). We have seen in homework 3 for the special case $\Delta = -t = -1$ and $\mu = 0$, the chain has two Majorana zero modes at the ends,

$$H = -\sum_{x=1}^{N-1} (\hat{c}_x^\dagger \hat{c}_{x+1} + \hat{c}_x \hat{c}_{x+1} + \hat{c}_{x+1}^\dagger \hat{c}_x + \hat{c}_{x+1}^\dagger \hat{c}_x^\dagger) = -i \sum_{x=1}^{N-1} \hat{\gamma}_{B,x} \hat{\gamma}_{A,x+1},$$

where

$$\hat{c}_x = (\hat{\gamma}_{B,x} + i\hat{\gamma}_{A,x})/2, \;\; \hat{c}_x^\dagger = (\hat{\gamma}_{B,x} - i\hat{\gamma}_{A,x})/2.$$

This is an example of non-trivial topological phase and the following illustrates this,



We can define a fermion operator from these two zero modes:

$$\hat{d} = (\gamma_1 + i\gamma_{2L})/2,$$

and a fermion parity operator

$$P_f = (1 - 2\hat{d}^\dagger \hat{d}) = -i\gamma_1\gamma_{2L}.$$

For the naive two-σ encoding, we have

$$i\gamma_1\gamma_{2L}|\sigma\sigma;1\rangle = -|\sigma\sigma;1\rangle, \qquad i\gamma_1\gamma_{2L}|\sigma\sigma;\psi\rangle = +|\sigma\sigma;\psi\rangle$$

Because the two basis states have different parities, they cannot be used to encode a quantum bit.

In a different regime, $t = \Delta = 0$ but $\mu > 0$,

$$H = \sum_{x=1}^{N-1} -\mu\,(c_x^\dagger c_x - \frac{1}{2}),$$

represents a trivial phase, as it will have $\langle c_x^\dagger c_x \rangle = 1$, i.e. each site having a fermion, i.e. the "bonds" in the above are now within sites and there are no unpaired Majorana zero modes.

In general, the model has two phases.

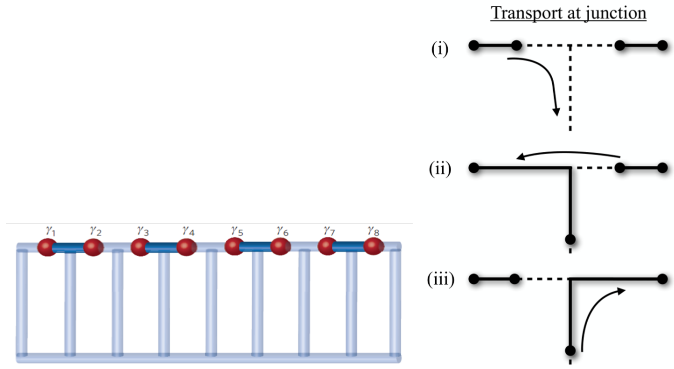


FIG. 18. Illustration of segments of Kitaev chain and braiding via the T junction; figures taken from Ref. [12].

- Topological, when ($|2t| > |\mu|$). The localized modes decay exponentially into the bulk from the boundary.
- Trivial, when $|2t| < |\mu|$. There is no localized mode.

We remark that one can local gates to break a Kitaev chain into several segments of topological chains so that there are several pairs of Majorana zero modes, which can then be used for (multiple-) qubit encoding. To perform braiding, one can use a T junction to shuffle particles, as proposed by Alicea et al., Nat Phys (2011) [12] and the review by Lahtinen & Pachos, arxiv:1705.04103 [4]; see Fig. 18.

In Fig. 16, we illustrate a few potential physical implementations for the Majorana zero modes. For some, it has been demonstrated that there is a zero bias conductance, but there has not been any verification of Majorana zero modes yet, let alone their braiding.

IX. CONCLUDING REMARKS

In this unit, we have discussed Kitaev's toric code, anyons (including Fibonacci and Ising anyons), and topological quantum computation (using e.g. Fibonacci anyons, Ising anyons implemented by Majorana zero modes of the Kitaev's chain). We introduced graphical diagram for fusion, braiding and basis change of fusion channels. The physics of topological quantum computation originates from topological phases of matter and its mathematics is described by topological quantum field theory and modular tensor category, which is beyond the scope of this course. But the fault tolerance using TQC originates from the nonlocal encoding using anyons and gates are achieved by braiding these quasiparticles. The Ising anyons, however, do not achieve a universal set of gates, which can be remedied by the so-called magic state distillation (to be discussed in the next unit). The Fibonacci anyon model does offer construction of quantum gates which are universal.

It is a good time to check whether you have achieved the following Learning Outcomes:
After this Unit, you'll be able to say what anyons are and how they can be used for quantum computing.

Suggested reading: See also the paper by Bombin on topological quantum codes [13]. Majorana zero modes and topological quantum computation, Sankar Das Sarma, Michael Freedman & Chetan Nayak, npj Quantum Information volume 1, Article number: 15001 (2015) [14]. Dan Browne has a short lecture series on "Topological Codes and Quantum Computation" at
`https://sites.google.com/site/danbrowneucl/teaching/lectures-on-topological-codes-and-quantum-computation`.

---

[1] A. Kitaev, Anyons in an exactly solved model and beyond, Annals of Physics **321**, 2 (2006).
[2] A. Y. Kitaev, Fault-tolerant quantum computation by anyons, Annals of Physics **303**, 2 (2003).
[3] A. Kitaev and C. Laumann, Topological phases and quantum computation, Exact methods in low-dimensional statistical physics and quantum computing, Lecture Notes of the Les Houches Summer School , 101 (2010).
[4] V. Lahtinen and J. K. Pachos, A Short Introduction to Topological Quantum Computation, SciPost Phys. **3**, 021 (2017).
[5] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. D. Sarma, Non-abelian anyons and topological quantum computation, Reviews of Modern Physics **80**, 1083 (2008).

[6] J. K. Pachos, *Introduction to topological quantum computation* (Cambridge University Press, 2012).
[7] N. E. Bonesteel, L. Hormozi, G. Zikos, and S. H. Simon, Braid topologies for quantum computation, Phys. Rev. Lett. **95**, 140503 (2005).
[8] L. Hormozi, G. Zikos, N. E. Bonesteel, and S. H. Simon, Topological quantum compiling, Phys. Rev. B **75**, 165310 (2007).
[9] This can be skipped.
[10] S. Trebst, M. Troyer, Z. Wang, and A. W. Ludwig, A short introduction to fibonacci anyon models, Progress of Theoretical Physics Supplement **176**, 384 (2008).
[11] A. Y. Kitaev, Unpaired majorana fermions in quantum wires, Physics-uspekhi **44**, 131 (2001).
[12] J. Alicea, Y. Oreg, G. Refael, F. Von Oppen, and M. Fisher, Non-abelian statistics and topological quantum information processing in 1d wire networks, Nature Physics **7**, 412 (2011).
[13] H. Bombín, An introduction to topological quantum codes, arXiv preprint arXiv:1311.0277 (2013).
[14] S. Das Sarma, M. Freedman, and C. Nayak, Majorana zero modes and topological quantum computation, npj Quantum Information **1**, 1 (2015).