Pro gradu -tutkielma
Teoreettisen fysiikan suuntautumisvaihtoehto

TOPOLOGICAL QUANTUM COMPUTATION – AN ANALYSIS OF AN ANYON MODEL BASED ON QUANTUM DOUBLE SYMMETRIES

Ville Lahtinen

08.05.2006

Ohjaaja: FT Claus Montonen

Tarkastajat: Prof. Keijo Kajantie
FT Jani Martikainen
FT Claus Montonen

HELSINGIN YLIOPISTO
FYSIKAALISTEN TIETEIDEN LAITOS

PL 64 (Gustaf Hällströmin katu 2)
00014 Helsingin yliopisto

Contents

Introduction

> "... you don't want to do it unless there is a sweet way to do it. That is sort of the way I feel about topological quantum computation, that the word topological is going to make it sweet, that we are not going to take some system and just make it more and more isolated, colder and colder and force one or two more qubits in a year out of it. We are going to do something that is beautiful and elegant and then even if we fail, we have at least pursued the right course and will probably learn something interesting about solid state physics on the way."
>
> -Michael H. Freedman, [23]

It maybe a cliché to start with a quotation, but there is hardly a better way to express the attitude for exploring the topic of this thesis. Words such as 'sweet', 'beautiful' and 'elegant' are a bit too poetic and vague to be used in a scientific context, but there are good reasons why such words of praise are not out of place, as opposed to the more conventional approaches to quantum computation, when used in connection with topological quantum computation. To fully understand these reasons, it is in place to take a quick look on the brief history of quantum computation.

The classical computer science, the study of information processing with computers, has been a crucial asset for the rise of the modern information society. The development of computers during the 20th century has been extremely rapid. This progression is maybe best captured by a variant of the famous Moore's law, which states that the number of transistors per central processing unit doubles in approximately in every 24 months [40]. Even though this is more like an observation than a rigorous law, it has been shown to hold with amazingly good accuracy since the 1960s. This progress has been made possible by the development of miniaturization techniques, which have allowed squeezing the physical size of the transistors ever smaller. However, it is natural that there will be a limit on the size of transistors. As the size diminishes, one approaches scales where the quantum effects can not be ignored anymore. This is where the quantum computer comes into play by promising to turn the physical limitation into a new resource, which allows more powerful, and even totally new kind of information processing. The introduction of this revolutionary idea could be attributed to the two seminal physicists David Deutsch and Richard Feynman, who in the mid 1980's were the first to speculate the capabilities of quantum mechanics as computation [13, 17]. However,

the motivations for considering the computational power of quantum mechanics were quite different. The first was concerned about how such new kind of computation would contrast with the Church-Turing principle, the pillar of classical information science, whereas the latter considered the complex task of simulating quantum mechanical systems with classical computers and how quantum computers would change the situation. These two perspectives can still today be used to roughly divide the study of quantum computation into two branches of study.

First, there is the abstract theoretical branch known as quantum information science, which is concerned with the information processing capacity of quantum mechanics [38]. It is a blooming interdisciplinary field of research bringing together both theoretical physicists as well as computer scientists and much progress has been made in understanding the relevance of different aspects of the quantum theory to computation. Although much of this work strives to understand the computational power of the quantum computer, there is also a more physical side involved in switching to studying quantum systems in terms of the language of computer scientists. It is a quite modern and daring idea that the concept of information, which only recently has penetrated into the realm of physics through the study of quantum computation, might actually have a role to play in the description of the physical reality [39]. Whether such speculations prove to have any relevance for a serious physicists, is a subject of further research. Yet, it is a very motivating idea, that the study of quantum computation is not only about building a new super-computer, but also about learning something relevant about fundamental physics. These speculations aside, the progress in quantum information science has been rapid and a good overview about considering quantum mechanics as computation has been obtained [40, 42]. From this purely theoretical point of view, one could even go as far as to claim that the problem has been solved and concentrate on studying what new tricks one can perform with this new toy. However, as often is the case, bridging theoretical and experimental considerations is a non-trivial and even a daunting task. This is what the second branch of study is concerned about - finding suitable physical systems to serve as quantum computers. As candidates, there exists a wide variety of suggestions ranging from NMR systems to more exotic condensed matter systems such as superconductors or quantum dots [15, 16, 40, 44]. The multitude of suggestions is a clear reflection of the fact that at the present level of knowledge, one is still uncertain which of the proposed systems, if any, would serve the best as a large-scale quantum computer. However, one is sure of few general properties, which are demanded from all candidate systems: to retain scalability and control over the system, and most importantly, at the same time cope with the arch-enemy of quantum computation - decoherence.

Decoherence is the reason why quantum mechanical effects are not observed in every day life. Since a quantum computer relies on these effects to operate properly, to promote it from a theoretical construction to a functioning macroscopic computer, one most overcome the challenge imposed by decoherence. In principle, this can be achieved by isolating the quantum computer from the environment, but in practice such isolation is never perfect and becomes

increasingly difficult with the growing size of the computer. To deal with small errors, the theory of quantum error-correcting codes was developed. These allow quantum information to be encoded in a redundant way, which tolerates errors up to some finite error rate, and thus allows quantum computation to be performed fault-tolerantly [40, 43]. Unfortunately, the level of tolerated error is still well beyond anything that can be achieved in any of the proposed physical systems. Yet, the study of quantum error-correcting codes has not been in vain, but has shed much light on how quantum information can be encoded and stored in a robust manner. As a curious offspring, it also spawned the idea of considering topological features to store quantum information [12]. In the form they were first suggested, these topological error-correcting codes were a purely theoretical construction. However, they involved considering quantum information organized on surfaces of non-trivial topology, which could be thought of as lattices. Such constructions bear an analogy with the spin models of statistical mechanics [5], and inspired Alexei Kitaev to consider condensed matter systems, where the topological degrees of freedom would be manifest as physical degrees of freedom [31]. If one could encode quantum information by using them, the information would be intrinsically protected from decoherence, because the topological properties are by definition robust in the presence of small perturbations. In principle, there would be no need for additional error-correction. Realizing a quantum computer using such topologically ordered systems would indeed be a sweet way to deal with decoherence.

Remarkably enough, condensed matter systems exhibiting such topological properties had already earlier been proposed in connection with superconductors. The sweetness comes with a price though. These physical systems are available only in two spatial dimensions where the topological degrees of freedom manifest themselves as quasiparticle excitations called anyons [11, 47]. Anyons have the exotic property that they obey neither bosonic or fermionic statistics, but something in between. Clearly such genuinely two dimensional systems are hard to manufacture, but it can be done. Much pioneering work has been done related to the Quantum Hall effect and the existence of so-called abelian anyons has already been confirmed [47]. Unfortunately, to perform quantum computation with anyons, i.e. topological quantum computation, one needs non-abelian anyons [34, 42], whose existence remains to be confirmed. Though no system exhibiting them has been found yet, high hopes are placed on certain fractional Quantum Hall states [36, 37], and preliminary research has been done for utilizing them as topological quantum computer [7, 22, 45]. While the experimental search for non-abelian anyons is still in progress, the theory of topological quantum computation is well worth a closer look. The main reason is that the underlying topological and algebraic structure of non-abelian anyons is closely related to various topics in contemporary theoretical physics: topological quantum field theories [19], knot theory [27, 30, 48] as well as to Hopf algebras [3, 4, 32, 11]. Therefore, even though quantum computation with anyons using current technology might sound a bit far-fetched, there is definitely enough incentive to pursue this path. Also, as a sign that these ideas are really started to be taken seriously, the first popular article ever on topological quantum computation was recently featured on Scientific

American [10].

The outline of this thesis is as follows. Chapter 1 gives a brief introduction to the basic concepts and terminology to translate quantum mechanics into quantum computation. Chapter 2 forms the core by discussing the nature of anyons and the algebraic structure underlying them. A specific example will be given in the form of an anyon model based on the gauge group S_3. Using this model as an example, Chapter 3 pulls the two preceding chapters together by discussing how the anyons can be used to perform quantum computation with intrinsic fault-tolerance.

Chapter 1

Quantum Mechanics as Computation

The study of quantum computation can be regarded as the study of the structure of preparation, evolution and measurement of quantum systems. Since these three steps essentially form the core of quantum theory, quantum computation can be considered as quantum mechanics rephrased in the terminology of computation. Broadly speaking, the theory of computation is interested in what resources are required to perform a given computational task. Specifying these resources, which in general correspond to some initial information and some elementary operations, forms a computation, which simulates the task with some precision. To translate quantum mechanics into quantum computation, one should adopt a similar way of thinking. More precisely, one should find a way to express a given quantum system and its evolution as this kind of a computation, which could be expressed in terms of some elementary quantum mechanical objects and operations. Now, instead of considering a given task, one could ask what resources are required to perform an arbitrary task. Specifying these resources enable then one to perform *universal computation* and a systems where such resources are available are consequently referred to as *universal computers*. In direct analogue, the problem of transforming quantum mechanics into quantum computation breaks down to specifying the elementary elements and operations out of which an arbitrary quantum system and its evolution can be constructed with arbitrary precision. A system with these operations at the repertoire would then be a *universal quantum computer*. The big questions then are: what are the elementary quantum mechanical objects and operations and in which quantum systems they are available, i.e. what quantum systems are capable of *universal quantum computation*? To answer these questions, one needs the language of quantum computation. The aim of this chapter is to provide the vocabulary and way of thinking to transform quantum mechanics into quantum computation, and thereby identify the general criteria which all quantum computer candidate systems have to meet.

Before proceeding, it is useful to briefly recall the key concepts of quantum mechanics. Associated with each quantum system there is a state space, which is a Hilbert space $\mathcal{H}$. The quantum system is fully described by the state vector $|\psi\rangle \in \mathcal{H}$, $\langle\psi|\psi\rangle = 1$, a unit vector in the state space, which is a function of the system's observables M. The observables are

Hermitian operators on the state space of the system. Each observable has a spectrum of eigenvalues $\{m\}$, which are the possible outcomes when measuring M, and associated with each m there is an eigenspace $\mathcal{H}_m \subset \mathcal{H}$ of M. The quantum measurements are described by a set of measurement operators $\{M_m\}$, such that the probability that m occurs is given by

$$p_m = \langle\psi|M_m^\dagger M_m|\psi\rangle, \tag{1.1}$$

and the properly normalized state $|\psi'\rangle$ right after the measurement is given by

$$|\psi'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{1.2}$$

The evolution of the state $|\psi\rangle$ is described by unitary operators U, such that the states $|\psi\rangle$ and $|\psi'\rangle$ at two distinct times t_1 and t_2 are related by

$$|\psi'\rangle = U|\psi\rangle, \tag{1.3}$$

where U depends only on the times t_1 and t_2. Therefore, the evolution as described by such unitary operators is discrete in time. Moreover, the evolution of the state $|\psi\rangle$ in continuous time is described by the Schrödinger equation

$$H|\psi\rangle = i\hbar\frac{d|\psi\rangle}{dt}, \tag{1.4}$$

where H is the Hamiltonian of the system, which completely specifies the dynamics of the system, at least in principle [40].

1.1 Qubits and Qudits

In classical computation, the elementary indivisible unit of information is a bit, a binary valued integer. To promote the concept of the bit into quantum mechanics, the integers 0 and 1 are replaced by the orthonormal states $|0\rangle$ and $|1\rangle$ in a two dimensional vector space. Then, instead of a bit with a fixed binary value, a normalized linear combination can be defined by

$$|\phi\rangle = a|0\rangle + b|1\rangle, \qquad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1. \tag{1.5}$$

A general state of the form (1.5) is known as the *qubit*, the quantum bit, which is an object in two dimensional complex vector space with an inner product, namely the two dimensional Hilbert space $\mathcal{C}^2$. The basis spanned by the state vectors $\{|0\rangle, |1\rangle\}$ is known as the *computational basis* of the qubit.

The qubit is the basic and most widely used unit of information in quantum computation. However, also higher dimensional objects can be considered. These objects are known as *qudits* and they take the general form

$$|\phi\rangle = \sum_{i=0}^{d-1} \alpha_i|i\rangle, \qquad \alpha_i \in \mathbb{C}, \quad \sum_{i=0}^{d-1} |\alpha_i|^2 = 1, \tag{1.6}$$

where d is the dimension of the qudit. Hence, qudits are objects in a d-dimensional Hilbert space $\mathcal{C}^d$. d is assumed to be prime, because qudits of non-prime dimension can in principle always be expressed as a tensor product of qudits of smaller, but prime dimension. In this sense the qubit (1.5) is the indivisible unit of quantum information. However, the qudit (1.6) is a more general and flexible concept, which is better suited for platform-independent general discussion.

A quantum state of N qudits can be expressed as a vector in the space

$$\mathcal{C} \equiv \left(\mathcal{C}^d\right)^{\otimes N}, \qquad \dim(\mathcal{C}) = d^N. \tag{1.7}$$

This space is referred to as the *computational space* of the quantum computer. The orthornormal basis given by the tensor product of the single qudit basis states

$$\{|i_1\rangle|i_2\rangle\cdots|i_N\rangle\}_{i_1,i_2,\ldots,i_N=0,1,\ldots,d-1}, \tag{1.8}$$

where one has adopted a convention to suppress the explicit tensor product notation, $|i\rangle|j\rangle \equiv |i\rangle\otimes|j\rangle$. The normalized state vector of a general N-qudit state $|\Phi\rangle \in \mathcal{C}$ can then be expressed as

$$|\Phi\rangle = \sum_{i_1,i_2,\ldots i_N=0}^{d-1} \alpha_{i_1,i_2,\ldots i_N}|i_1\rangle|i_2\rangle\cdots|i_N\rangle, \qquad \sum_{i_1,i_2,\ldots i_N=0}^{d-1} |\alpha_{i_1,i_2,\ldots i_N}|^2 = 1, \tag{1.9}$$

where $\alpha_{i_1,i_2,\ldots i_N} \in \mathbb{C}$.

Encoding Quantum Information

When considering a quantum mechanical system in terms of quantum computation, one wants to express every quantum state $|\psi\rangle \in \mathcal{H}$ of the system as a coupled state of some n qudits $|\phi_i\rangle \in \mathcal{C}$

$$|\psi\rangle \equiv |\Phi\rangle = |\phi_1\rangle|\phi_2\rangle\cdots|\phi_n\rangle, \tag{1.10}$$

for some $|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_n\rangle$ (1.6), and the study the evolution of this $|\psi\rangle$ in terms of the evolution of the multi-qudit state $|\Phi\rangle$. The conceptual change in thought is the treatment of qudits as elementary quantum mechanical objects out of which an arbitrary quantum state, at least in principle, could be constructed.

This idea underlies one of the crucial criteria for a given quantum mechanical system to serve as a quantum computer: the computational space $\mathcal{C}$, the calculational arena of the quantum computer, should be identified somehow with the state space $\mathcal{H}$ of the system, $\mathcal{C} \subseteq \mathcal{H}$, such that the tensor product structure (1.7) exists for some $d, N \in \mathbb{R}$. In general, this criterion expresses the demand that in the quantum system there should exist some N degrees of freedom, usually meaning some N independent observables M_i, which each have d eigenspaces $\mathcal{H}_{m_i}$. Letting $\mathcal{H}_i \subset \mathcal{H}$ be the space spanned by the eigenspaces of M_i, the computational space of a single qudit would then be identified with it

$$\mathcal{C}^d \equiv \mathcal{H}_i = (\mathcal{H}_{m_i})^{\otimes d}. \tag{1.11}$$

When identifying qudits with such degrees of freedom, one talks of *encoding* the quantum information on the quantum mechanical system. For example, in nature there exists well studied physical systems, which behave as two-level systems offering natural ways of encoding qubits. Simple examples are for example the electron spin or the photon polarization, where the encoded qubits would be identified with the observables corresponding to spin or wave polarizations, respectively. These cases are also illustrative in the sense that the qubit can then be considered localized on the particle and can be thought as moving in space-time much in analogy with classical circuits. However, such simple intuitive systems are not often the most practical for large-scale implementation, and in general the exact way of encoding the quantum information always depends on the physical system in question. Hence, for a general platform-independent discussion, it is useful to treat the qudit as a purely mathematical object, an internal space identified with some subspace of the whole state space, which does not necessarily have any local physical correspondent.

1.2 Entanglement

Entanglement is maybe the most curious feature of quantum mechanics. In quantum computation it is considered as an extra resource, which can be utilized to perform computational tasks not possible with classical computers. However, it is more than just a resource. It has been proven that the ability to entangle states is required by any quantum system and therefore the concept of entanglement lies at the very heart of quantum mechanics [9] - without entanglement, there is no quantum mechanics. To better understand the role played by entanglement, the connections between quantum entanglement and topological entanglement have been studied [26, 28, 29]. These topics might have a role to play also in the theory of quantum computation, especially in topological quantum computation due to the role played by the braid group [30, 48], but since the research is still very much a work in progress, this topic will not be touched upon here.

So, entanglement is a crucial ingredient in quantum computation, but it does not appear often explicitly unless specifically looked for. As a general rule of thumb, if an N-qudit state $|\Phi\rangle$ (1.9) cannot be expressed as tensor product of single qudits,

$$|\Phi\rangle = \sum_{i_1,i_2,\ldots i_N=0}^{d-1} \alpha_{i_1,i_2,\ldots i_N} |i_1\rangle|i_2\rangle\cdots|i_N\rangle \neq |\phi_1\rangle|\phi_2\rangle\cdots|\phi_N\rangle, \tag{1.12}$$

the state is said to be entangled [40]. Similarly, an operator G is said to be entangling if

$$G|\phi_1\rangle|\phi_2\rangle\cdots|\phi_N\rangle \neq |\phi_1'\rangle|\phi_2'\rangle\cdots|\phi_N'\rangle. \tag{1.13}$$

In more casual language, to say that a state is entangled is to say that there exists non-classical correlations between the constituent states. These correlations can be non-local and may be used to gain information about the possibly spatially separated individual states. This extra information transmission channel is the resource, which enables quantum computation

to outperform classical computation on various, although currently very selected tasks. In the discussion to follow, only very little explicit attention needs to be paid to entanglement. Yet, it is an essential concept looming everywhere beneath the surface. It is responsible for most of the non-classical features and no text on quantum computation should pass on it carelessly.

1.3 The Quantum Gates and the Universal Gate Set

In classical computation, all possible logical operations, the logic *gates*, can be formed out of a small number of elementary operations. Similarly, in quantum computation one wishes to construct all possible quantum gates out of a small set of elementary quantum gates. The obvious difference to classical gate set is that instead of classical (usually irreversible) logic gates, unitary (reversible) gates are required to preserve the probability interpretation of quantum mechanics [40]. Therefore, all quantum gates G will be assumed to be unitary operators. This means that the quantum gates G are elements of the group of unitary transformations $G \in U(d^N)$ acting in the computational space (1.7) as

$$G:\ \mathcal{C} \mapsto \mathcal{C}, \qquad G \in U(d^N). \tag{1.14}$$

The unitary group is a continuous group having an infinite number of elements, and thus one can at best approximate an arbitrary gate with an arbitrary precision. To do this, one should give a set of elements

$$\mathcal{G} = \{A_1, \ldots, A_n\}, \qquad A_1, \ldots, A_n \in U(d^N), \tag{1.15}$$

such that every $G \in U(d^N)$ can be expressed as

$$G \approx A_{i_1}^{m_1} \cdots A_{i_k}^{m_k}, \tag{1.16}$$

for some k, $m_1, \ldots, m_k \in \mathbb{Z}$ and $i_1, \ldots, i_k = 1, \ldots, n$. Then, the elements $A_1, \ldots, A_n$ would be the generators of the group and the set $\mathcal{G}$ would form the *universal gate set* for quantum computation. In direct analogy with qudits, which in quantum computation are taken as the elementary quantum mechanical objects (1.10), the elements of the universal gate set $\mathcal{G}$ are to be treated as the most elementary unitary transformations out of which, at least principle, an arbitrary unitary transformation G could be constructed. This idea gives the second criterion for given system to be able to execute universal quantum computation: the qudits must be encoded on the system such that by performing some unitary transformations U_i (1.3) on the systems state space $\mathcal{H}$, one should be able to apply the universal gate set $\mathcal{G}$ in the computational space $\mathcal{C}$. In practice this breaks down to specifying a set of physical operations $\{U_1, U_2, \ldots, U_n\}$ on the state space $\mathcal{H}$ such that

$$U_i:\ |\phi\rangle \mapsto A_i|\phi\rangle, \qquad \forall A_i \in \mathcal{G}, \tag{1.17}$$

or to put the criterion in more general form, the set $\{U_1, U_2, \ldots, U_N\}$ should generate $U(d^N)$ in $\mathcal{C}$.

In order to specify the U_i, which can be used to implement the universal gate set, one should know which A_i constitute $\mathcal{G}$. There is flexibility, since the choice for $\mathcal{G}$ (1.15) is not unique and various suggestions have been considered [40]. Different choices arise naturally in different experimental platforms, and the implementational efficiency varies from one platform to another. Still, as already anticipated in connection with entanglement, all the valid universal gate sets have to share one common feature: at least one of the gates has to be entangling (1.13). A general theorem proven in [9] states that a single entangling gate, when appended with all the possible single qudit gates, is universal for quantum computation. Usually all universal gate sets are structured in this way. Hence, choosing a universal gate set breaks down to choosing a set elementary single qudit gates

$$A_i : \mathcal{C}^d \mapsto \mathcal{C}^d, \qquad A_i \in \mathcal{G}, \tag{1.18}$$

which generate in the sense of (1.16) all unitary mappings from $\mathcal{C}^d$ to itself, and a single entangling two-qudit gate

$$A : \mathcal{C}^d \otimes \mathcal{C}^d \mapsto \mathcal{C}^{d^2}, \qquad A \in \mathcal{G}. \tag{1.19}$$

By forming tensor products of these elementary elements, one can extend the action of $\mathcal{G}$ to the whole computational space and thereby approximate an arbitrary $G \in U(d^n)$ gate.

Only a few simple and illustrative universal gate sets have been explicitly constructed. Their main function is to serve as a basis for theoretical considerations, and it is a rare occasion that one could actually implement these most elementary gate sets on a given quantum mechanical system [40, 42]. In a realistic setting the available unitary transformations are determined by the dynamics of the system, and in practice, one has to resort to studying case-wise whether the given unitary operations allow universal quantum computation. Yet, as an example of the presented abstract discussion, it is illustrative to briefly consider one particular universal gate set for qubits ($d = 2$), which, surprisinly enough, will be partially encountered later on. For a more rigorous discussion about the universality, gate sets for qubits have been discussed in more detail in [14, 42, 40], and gate sets for qudits of arbitrary d in [8, 25, 46].

The universal gate set in question consists of the unitary gates

$$\mathcal{G} = \{H, T, \textsc{cnot}\ \}, \tag{1.20}$$

whose action on the qubit basis $|j\rangle \in \mathcal{C}^2, j \in \{0, 1\}$, is defined by

$$H|j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^j|1\rangle\right), \tag{1.21}$$

$$T|j\rangle = (e^{i\frac{\pi}{4}})^j|j\rangle, \tag{1.22}$$

$$\textsc{cnot}\ |j\rangle|k\rangle = |j\rangle|j + k \pmod 2\rangle. \tag{1.23}$$

In literature, H is known as the Hadamard gate, T is known as the $\frac{\pi}{8}$-phase gate and CNOT as the controlled-not. It has been explicitly proven in [40], that modulo the relations

$$HT^4 = T^4H, \qquad H^2 = \mathbf{1}, \qquad T^8 = \mathbf{1}, \tag{1.24}$$

where $\mathbf{1}$ is an identity gate, H and T freely generate $U(2)$ to an arbitrary accuracy. Hence, when appended with an entangling CNOT gate, they form a universal gate set. Consequently, the elements of $U(4)$ are freely generated, modulo some further relations, by CNOT together with the tensor products $\mathbf{1} \otimes H^m$, $\mathbf{1} \otimes T^n$, $T^k \otimes \mathbf{1}$ and $H^l \otimes \mathbf{1}$ for all $m, l \in \{0, 1\}$ and $n, k \in \{0, \ldots, 7\}$.

1.4 Quantum Measurements

The qudit $|\phi\rangle$ as the elementary unit of information and the universal gate set $\mathcal{G}$ as the toolkit for quantum computation are direct generalizations of their classical correspondents. However, having access to a computational space (1.7) and a universal gate set (1.15) is still not enough to execute quantum computation. One needs an extra piece of structure, which is the quantum measurement (1.1). Classical computation is deterministic in the sense that given an input and a a set of logical operations, the outcome of the computation is always uniquely defined. Also quantum computation is deterministic in the sense that given an input state $|\Psi\rangle \in \mathcal{C}$ and a computation C, a set of unitary transformations performed in fixed order $C = G_1 \cdots G_n \in U(d^N)$, the output state $|\Psi'\rangle = C|\Psi\rangle$ is uniquely defined (1.3). However, the difference is that whereas the output of the classical computation is a fixed string of bits, in general the output $C|\Psi\rangle$ is now an entangled superposition, and to extract any information from it, one must project it onto the computational basis. The real outcome of the computation is then the probability p_i for projecting onto the computational basis state $|i\rangle$. Therefore, the quantum measurement to be performed at the end of the computation is an as essential ingredient of quantum computation as are the computational space and universal gate set. A criterion for quantum computer candidates is then that the encoding of quantum information must be allowed in such a way that by performing measurements $\{M_m\}$ (1.2) on the quantum system, one can apply projectors P_i in the computational space,

$$M_m : \ |\Phi\rangle \mapsto P_i|\Phi\rangle. \tag{1.25}$$

That is, performing a measurement described by M_m and observing the outcome m with the probability p_m (1.1) should in the computational space $\mathcal{C}$ uniquely correspond to projecting onto $|i\rangle$ with the probability $p_i = p_m$.

This kind of correspondence arises naturally when qudits are encoded in the physical degrees of freedom of some observable M (1.11), which consequently leads to the computational basis being identified with the eigenspaces $\mathcal{H}_m$ of M, i.e. one can define $|i\rangle \equiv |m\rangle$. The measurement of M can be formulated as projective measurements, meaning that the Hermitian operators $\{M_m\}$ describing the measurement are orthogonal projectors, $M_m \equiv P_m$, which satisfy the projector algebra

$$P_m P_n = P_m \delta_{m,n}, \quad \sum_m P_m = I. \tag{1.26}$$

The observable M has then a spectral decomposition

$$M = \sum_m m P_m, \tag{1.27}$$

where P_m are the projectors onto eigenspaces $\mathcal{H}_m$ of M corresponding to the eigenvalue m. Then, performing a measurement of M and observing the outcome m is equivalent in the computational space to projecting the associated qudit onto the computational basis state $|m\rangle$.

Given a computation C, the output of a quantum computation, i.e. the probability p_m to project onto the state $|m\rangle$, is then given by the expression

$$p_m = \langle \Psi | C^\dagger P_m C | \Psi \rangle, \tag{1.28}$$

which nicely summarizes a single run of the quantum computer as the expectation value of the operator $C^\dagger P_m C$ in the initial state $|\Psi\rangle$. Of course, with the single run of a quantum computer one can only infer the information whether the projection onto the state $|m\rangle$ succeeds or not, which is a binary yes-no information. Whether this piece of information is sufficient to deduce the result depends on the architecture of computation. In same cases, it is also worth considering measurements, if such are available, which in the computational space translate to projections onto some other orthogonal basis than the computational basis. This freedom offers much flexibility when designing quantum computations, and with clever designs one can enhance the information gained from single projective measurements.

One might also ponder whether performing intermediate measurements and conditioning the computation on them would improve the computation. However, according to the *principle of deferred measurement*, without any loss of generality, all measurements can be postponed till the end of computation [40]. No computation requires intermediate measurements and nothing is gained by using them. This means that the state of the system after the measurement plays no role, since all the information lies in the probabilities to obtain the different outcomes at the end of the computation. It is in the measurement statistics where all the information resides.

1.5 The Framework for a Quantum Computer

One is now ready to present the very general theoretical framework for the quantum computer. In order for a given quantum system to serve as a universal quantum computer, the necessary requirements for encoding quantum information are:

1. The computational space $\mathcal{C}$ has a tensor product decomposition in terms of d-dimensional subspaces (qudits) (1.7).

2. By performing unitary transformations on the system, one can, to an arbitrary precision, generate an arbitrary element of $U(d^N)$ on $\mathcal{C}$, which is equivalent to showing that one can implement some universal quantum gate set (1.15).

3. By performing measurements on the system, one can perform projective measurements in $\mathcal{C}$.

These are the structures, which one sets out to look for in the anyonic system to be presented in the next chapter. The aim is to try to discover some physical degrees of freedom, which exhibit the promised intrinsic fault-tolerance and which at the same time allow the implementation of the properties listed above.

Chapter 2

Non-Abelian Anyons and the Algebraic Structure

To make a long story short, *anyons* are identical particles which do not obey the usual Fermi-Dirac or Bose-Einstein statistics, but something in between. Hence, the term fractional statistics is also often used in connection with anyons. The aim of this chapter is to give a compact account of classification of different anyons and describe their exotic interactions. The relevant aspects to performing quantum computation will be made transparent when encountered, but the discussion on performing quantum computation with anyons, that is *topological quantum computation*, will have to wait till the next chapter.

There exist two prominent approaches to tackle the anyonic behavior. The first incorporates the fractional statistics through fictitious Chern-Simons gauge fields, which transmute the statistics into the particular topological interactions [18, 35, 47]. The second one makes use of quantum symmetries as described by Hopf algebras, which offer a unified description of the particle properties [2, 11, 31, 32, 42]. Of course, both capture the same physics, but the argumentation leading to the existence of anyons and the emphasis on different features vary. From the point of view of the applicability of anyons to quantum computation, it is the latter approach which provides more insight to the problem. However, before proceeding to the abstract algebraic treatment, motivation will be derived from physical considerations, which will provide the grounds for the rather abstract mathematical framework.

The defining property of anyons arises when one considers the symmetry properties of an N-particle system of varying spatial dimension. Under the action of S_N, the permutation group of N particles, the Hamiltonian of the system remains invariant, but the eigenstates $|\psi_j\rangle$ are transformed according to an irreducible representation. Letting $\psi_j(1,2,\ldots,N) = \langle 1,2,\ldots,N|\psi_j\rangle$ denote an N-particle wave function and $U(\pi)$ an operator implementing a particular permutation π, this can be expressed as the transformation

$$U(\pi)\psi_j(1,2,\ldots,N) = \sum_k \psi_k(\pi(1),\pi(2),\ldots,\pi(N))D_{kj}(\pi), \tag{2.1}$$

where $D_{kj}(\pi)$ are the matrices representing the permutation π. In most quantum mechanical

systems the Fermi-Dirac and Bose-Einstein statistics are sufficient to describe the symmetry properties of the wave function. These two cases are the two one-dimensional representations: the trivial representation $D(\pi) = 1$ and the alternating representation $D(\pi) = (-1)^{|\pi|}$, with $|\pi|$ the number of interchanges in π [35]. These correspond to bosons and fermions, respectively.

Anyons correspond to irreducible representations taking other forms than the two aforementioned ones. They come about when one considers particles on manifolds of varying spatial dimension. The symmetry group to which the permutation π belongs to depends on the topology of the configuration space M_N^D of the D-dimensional N-particle system, and especially on the structure of the fundamental group $\pi_1(M_N^D)$. The configuration space M_N^D is not simply connected, because indistinguishable particles are not allowed to coincide, and thus the fundamental group is non-trivial [11, 35]. This is reflected in the structure of the first homotopy group, which now depends on the dimension D of the space. Namely, in two spatial dimensions it is known to be isomorphic to the *N-string braid group*,

$$\pi_1(M_N^2) \simeq B_N, \tag{2.2}$$

whereas for $D \geq 3$ it is isomorphic to the permutation group of N-objects,

$$\pi_1(M_N^D) \simeq S_N, \qquad D \geq 3. \tag{2.3}$$

The one-dimensional irreducible representations of S_N correspond to the aforementioned trivial and alternating representations, but it is known that there are also higher dimensional irreducible representations. However, these would correspond to so called parastatistics, which are not observed and, at the present knowledge, are not assumed to exist in nature [35]. On the other hand, there are no such constraints on the dimensionality of the representations of the braid group. Therefore, it follows that the anyonic behavior is manifest only in two spatial dimensions and the symmetry properties of the N-anyon wavefunction are described by the braid group B_N. If the wave function transforms in some one-dimensional irreducible representation of B_N, one talks of *abelian anyons*. Wavefunctions transforming in some higher dimensional irreducible representation are said to describe *non-abelian anyons*.

The Emergence of Anyons

The emergence of anyons in only 2+1 dimensions, the additional dimension being time, greatly restricts the possible quantum mechanical systems where they could be found. Currently the most promising systems involve the fractional Quantum Hall states [36, 37, 47], but there are also proposals for engineering suitable systems [15, 16]. Constructing and controlling such systems will be a great challenge to experimentalists, but the exact details are not the item of interest here. The existence of anyons will be taken for granted and one will settle with a toy model to discuss their properties. Yet, to put the model in a physical context, a very brief overview of one theory underlying the emergence of anyons will be presented also here. A comprehensive review of these so called discrete gauge theories can be found in [11].

As usually with gauge theories, one starts with a Lagrangian, which is invariant under a continuous symmetry group G and which involves Higgs fields, which may be coupled to some external matter fields. By performing spontaneous symmetry breaking in a suitable manner, one finds a set of degenerate ground states, which are invariant only under some discrete subgroup $H \subset G$. Consequently, the ground state manifold is assumed to be isomorphic to G/H. The broken phase supports topological defects which are fingerprints of the broken symmetry, and which can be classified by the fundamental group π_1 of the ground state manifold. For a discrete and finite H, and for a continuous and simply connected G, the fundamental group is isomorphic to the residual symmetry group

$$\pi_1(G/H) \simeq H. \tag{2.4}$$

The topological defects can be treated as quasiparticles, which by (2.4) are classified by the elements $h \in H$. In addition, when one includes also matter fields coupled to the Higgs field, the broken phase supports also excitations, which, as usual with theories involving symmetry breaking, are labeled by the unitary irreducible representations Γ of the residual symmetry group H. These two seemingly different types of excitations can be treated on equal footing by considering them both to be in accordance with the irreducible representations of a larger symmetry group, namely a *quantum group*. This unified approach will be discussed in a while.

It is a feature of the broken phase that all the physical charges of the unbroken phase, both magnetic and electric, are screened and therefore there are no electromagnetic long-range interactions [11]. However, the peculiar statistics of the anyons can be interpreted as a kind of interaction, which is of topological nature. In the physics literature, these topological interactions are usually known as the famous *Aharonov-Bohm interactions* taking place between between magnetic flux and electric charge [1]. It derives from this analogy, that the h and Γ are often referred to as flux and charge, respectively, carried by the quasiparticles. The topological excitations can be treated as particles on the plane, but the way they are to be understood as physical objects is very much model dependent. For example the flux-charge analogy may in some cases be an accurate description, since in some superconductor-like systems the fluxes are magnetic vortices carrying quantized magnetic flux, and the charges are condensates of matter fields carrying some quantized electric charge as their collective property. On the other hand, in other models the quasiparticles may manifest themselves as collective excitations bearing no direct correspondence to the elementary magnetic and/or electric charge. The topological interactions still exist as if the quasiparticles were carrying some flux and charge, but these are to be regarded merely as fictitious properties having nothing to do with ordinary electromagnetism [47].

The Toy Anyon Model

For the purposes of the theory of topological quantum computation, the exact nature of the anyonic quasiparticles is not of importance. The theory of topological quantum computation is only interested in which residual gauge groups H give anyons, which are suited for quantum

computation. It has been shown that universal quantum computation is possible only with non-abelian groups [34] and hence it will be assumed that H is non-abelian. To study the properties of these non-abelian anyons, it suffices to use a toy model, which consists of N point like particles on a two-dimensional surface. The symmetry properties of the wavefunction of the N particles are described by the braid group B_N. This is not to be confused with symmetry group of the system, which is some finite discrete group H. The different particles are labeled by the elements $h \in H$ and/or the irreducible representations Γ of H. The particles carry also conserved quantum numbers, which depending on the group H, may or may not be in accordance with the labels h and Γ. This will be studied in detail in the sections to come. All the long-range interactions of the model are of Aharonov-Bohm type and there are no other long-range interaction mechanisms. Finally, when two particles are brought together, they can fuse to yield a new particle, which carries new quantum numbers, such that the total quantum numbers are conserved in the process.

2.1 The Braid Group and the Topological Interactions

The topological interactions come about when a multi-particle wavefunction undergoes a permutation (2.1), which in two spatial dimensions is described by the action of the braid group (2.2). Physically this corresponds to moving the particles around each other. The most elementary of such permutations would be the interchange of the relative positions of two particles, which would correspond to the action of a generator of the B_N. Finding how these generators act on the states appearing in the model would then be equivalent to specifying how two particles interact. Generalizing this observation, finding the irreducible representation of B_N, in which the wavefunction of multi-anyon system transforms, fully captures all the long-range interactions in the model.

Before proceeding, it is useful to adopt suitable notation and conventions for describing the quasiparticles. The notations $|h\rangle$, $|q\rangle$ and $|h, q\rangle$ will be used to denote particles carrying flux h, charge q and a combination of both, respectively. The state vector form is taken into use, because it will later be shown that the particles will carry an internal vector space with a basis given by the different flux/charge eigenstates. However, for the time being, this state vector notation is to be regarded merely as labels for different particles. Also, it is useful to adopt a gauge convention that a system of N particles is organized on a line, the x-axis for example, on the (x, y)-plane so that the spatial location and the placement on the tensor product describing the whole system are in one-to-one correspondence. That is, if $x_1 < x_2 < \ldots < x_N$ denote the positions on the line, the direct product of the labels expresses also the relative positions by

$$|a_1, x_1\rangle \otimes |a_2, x_2\rangle \otimes \cdots \otimes |a_N, x_N\rangle \equiv |a_1\rangle|a_2\rangle \cdots |a_N\rangle. \tag{2.5}$$

Further, interchanges are only allowed between particles occupying adjacent positions. These conventions are sufficient to describe the nature of the topological interactions.

The Aharonov-Bohm Interactions

The Aharonov-Bohm effect is a purely quantum mechanical effect which is of topological nature. What is commonly meant by it, following the classic paper [1], is that when an electric charge q encircles a magnetic flux h, the wave function of the charge picks up a quantum phase e^{iqhw} with w the winding number. The topological nature has several peculiar consequences. First, it is a non-local effect, because there is no particle mediating the interaction. This means that it persists, regardless of the spatial separation of the charge and flux, even at very large distances. Second, the phase picked up by the wave function is indifferent to variations of the path travelled, but depends only on the number of times the path winds around the flux [47].

All the long-range interactions of the considered anyon model are of this type. Recall that the fluxes and charges are labeled by the elements h and irreducible representations Γ of the gauge group H, respectively. Then, in general, the charges Γ carry a charge vector spaces V^Γ, which has the dimension of the representation Γ, and the state vector in V^Γ is given by $|q\rangle$. When a charge encircles a flux, the Aharonov-Bohm effect in the present formalism is then the rotation of this state vector by the matrix $\Gamma(h)$ assigned to the group element h in the representation Γ. In general, this is the transformation

$$|h\rangle|q\rangle \to |h\rangle|\Gamma(h)q\rangle, \tag{2.6}$$

which in the case of one dimensional representations boils down to the aforementioned quantum phase.

The classic Aharonov-Bohm interaction takes place between a flux and a charge. In the case of non-abelian gauge group H, there exists also an effect called the non-abelian Aharonov-Bohm effect or the *flux metamorphosis* [42, 11]. Consider a two-particle state with two fluxes $a, b \in H$ with total flux given by $ab \in H$. Since both a and b are elements of a non-abelian group, they do not in general commute. However, the long-range properties of the combined system, the total flux, should not be altered if the positions of the particles carrying flux were interchanged. This means that under the interchange of the fluxes, b should be conjugated by a. The flux metamorphosis is thus equivalent to the transformation

$$|a\rangle|b\rangle \to |aba^{-1}\rangle|a\rangle. \tag{2.7}$$

After the interchange, the total flux is $(aba^{-1})(a) = ab$ and is conserved. Both (2.6) and (2.7) can be captured in a unified way via the action of the braid group.

The Braid Group

The braid group of N particles, B_N, is generated by the abstract relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i, \quad |i-j| \geq 2, \quad i,j = 1,\ldots,N-1, \tag{2.8}$$

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \quad i = 1,\ldots,N-2. \tag{2.9}$$

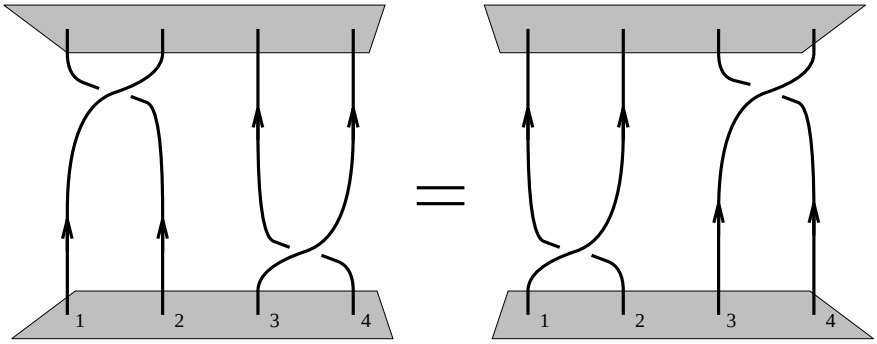

Figure 2.1: Pictorial presentation of (2.8) [11]

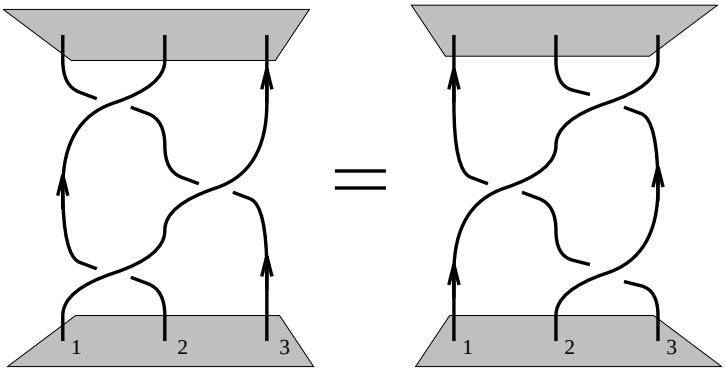

Figure 2.2: Pictorial presentation of (2.9) [11]

Altogether there are $N-1$ generators σ_i. Their inverses σ_i^{-1} are given by

$$\sigma_i \sigma_i^{-1} = \sigma_i^{-1} \sigma_i = e,$$

where e denotes the unit element. Each of the N particles can be thought as moving on a trajectory in the 2+1 dimensional space-time. Since in two spatial dimensions the counterclockwise and clockwise rotations can be distinguished, the generators σ_i and σ_i^{-1} can be thought as generating the interchange of the positions of i^{th} and $(i+1)^{\text{th}}$ particle by a rotation in a counterclockwise and clockwise direction, respectively. The choice for the direction of rotations is arbitrary, but this particular choice is commonly used in the literature and will also be adopted here. With these conventions, the relations (2.8) and (2.9) are most vividly illustrated by the Figures 2.2 and 2.1. In mathematical language, the trajectories are considered as *strands* which are *braided* by applying the generators. The elements $b \in B_N$, the *braids*, are generated by taking all possible products of all possible powers, positive or negative, of the generators. Therefore, B_N is a group of infinite order with each element b corresponding to a certain braiding.

The abstract generators σ_i can be represented in an N-particle space by the braid operators

$$\sigma_i \mapsto R_i = I^{\otimes(i-1)} \otimes R \otimes I^{\otimes(N-i-1)}, \tag{2.10}$$

where I is the identity operator and R the braid operator interchanging the positions of

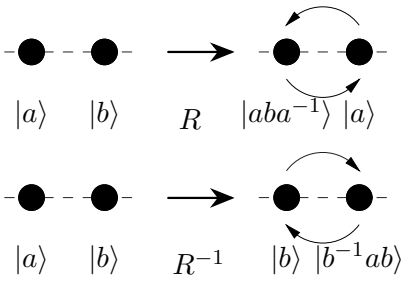

Figure 2.3: The transformation convention

adjacent particles occupying places i and $i+1$ in a counterclockwise manner. Because the representations have to respect the group properties (2.8) and (2.9), the braid operators have to satisfy

$$\begin{aligned} R_i R_j &= R_j R_i, \qquad |i-j| \geq 2, \\ R_i R_{i+1} R_i &= R_{i+1} R_i R_{i+1}, \qquad i = 1, \ldots, N-2. \end{aligned} \tag{2.11}$$

Of particular importance is the latter relation, which is known as the *Yang-Baxter equation*, which serves as a consistency condition for all possible matrix representations of braiding operators. From the point of view of quantum computation, the interest will be lying particularly on the unitary solutions of (2.11), because as will be shown later, unitary braidings can be utilized as unitary quantum gates.

Before proceeding, it is useful to adopt a further gauge convention. Recall that the particles were organized in a line in x-direction (2.5) and that interchanges were allowed only between neighboring particles. The topological interactions take place when the particles encircle each other, but to allow a consistent description of the phenomena, one should specify when exactly do the transformations (2.6) and (2.7) occur. Since the braiding in clockwise and counterclockwise direction are inverse operations of each other, they should also correspond to inverse transformations. A convention to be adopted here is illustrated by two fluxes in Figure 2.3. When particles a and b, a being to the left of b, are braided counterclockwise, the state of b is transformed by a. On the other hand, under clockwise braiding the state of a is transformed by b^{-1}, the inverse of b. Then, in terms of the braid operator R implementing a counterclockwise interchange, the non-abelian Aharonov-Bohm effect (2.7) between two fluxes $|a\rangle$ and $|b\rangle$ can be summarized by

$$\begin{gathered} R|a\rangle|b\rangle = |aba^{-1}\rangle|a\rangle, \qquad R^{-1}|a\rangle|b\rangle = |b\rangle|b^{-1}ab\rangle, \\ R^2|a\rangle|b\rangle = |(aba^{-1})a(aba^{-1})^{-1}\rangle|aba^{-1}\rangle = |(ab)a(ab)^{-1}\rangle|aba^{-1}\rangle. \end{gathered} \tag{2.12}$$

Similarly the abelian Aharonov-Bohm interaction between a pure flux $|h\rangle$ and pure charge $|q\rangle$ can be summarized by

$$\begin{aligned} R|h\rangle|q\rangle &= |\Gamma(h)q\rangle|h\rangle, & R^{-1}|h\rangle|q\rangle &= |q\rangle|h\rangle, \\ R|q\rangle|h\rangle &= |h\rangle|q\rangle, & R^{-1}|q\rangle|h\rangle &= |h\rangle|\Gamma^{-1}(h)q\rangle, \\ R^2|h\rangle|q\rangle &= |h\rangle|\Gamma(h)q\rangle. \end{aligned} \tag{2.13}$$

Two pure charges $|q\rangle$ and $|p\rangle$ do not interact topologically and hence the action of braiding is trivial

$$R|q\rangle|p\rangle = R^{-1}|q\rangle|p\rangle = |p\rangle|q\rangle. \tag{2.14}$$

These formal, but simple expressions capture all the long-range interactions of particles carrying only either flux or charge. The treatment of particles carrying both flux and charge is slightly trickier and it will be discussed in a while.

2.2 The Quasiparticle Spectrum

It has been illustrated above how would the particles carrying only the elements $h \in H$ or the representations Γ of H as their quantum numbers transform under the action of the braid group. If these were the good quantum numbers, the given expressions would capture all the topological interactions. However, they are not good quantum numbers, because one has not yet accounted for the existence of the residual non-abelian symmetry group H, which implies that the physics should remain invariant under all global $g \in H$ transformations

$$g \in H: \quad |h\rangle \mapsto |ghg^{-1}\rangle, \qquad |q\rangle \mapsto |\Gamma(g)q\rangle. \tag{2.15}$$

This is equivalent to demanding that the good quantum numbers, the particle labels, remain unchanged and that g commutes with the braiding operator R,

$$gR = Rg, \qquad \forall\ g \in H. \tag{2.16}$$

As can clearly be seen from (2.15), unless h and g commute and the representation Γ is trivial for all $g \in H$, the $|h\rangle, |q\rangle$ labeling is not in general invariant under global symmetry transformations and does not therefore bear a gauge-invariant meaning. To find the physically meaningful particles of a non-abelian anyon model, some other labeling should be used. Still, because of (2.4), this new labeling should account somehow for the fact that $h \in H$ labels the distinct topological excitations. Most insight to the problem is obtained when each of the three general particle types are considered separately.

The Pure Fluxes

The pure fluxes are particles, which were originally assumed to be labeled with some $h \in H$. To find the good quantum numbers for pure fluxes, one should find the the invariant features of H under conjugation (2.15). By definition, these are the *conjugacy classes*

$$C(h) = \{ghg^{-1}|g \in H\}, \tag{2.17}$$

Therefore, the pure fluxes manifest in a non-abelian model should be labeled by the conjugacy classes C of H. This means that the particles are organized into degenerate multiplets labeled by the conjugacy classes C, and for a given conjugacy class, there are altogether $|C|$ different

representatives of the same physical particle [11, 42]. Therefore, a particle labeled by C can be thought as carrying a $|C|$-dimensional internal flux vector space V^C. The basis in this internal space is given by the flux eigenstates

$$\{|h\rangle\}_{h\in C}, \qquad \langle h'|h\rangle = \delta_{h',h} \qquad \forall\ h', h \in C. \tag{2.18}$$

A general state can be expressed as a superposition of the form

$$|a\rangle = \sum_{h\in C} a_h |h\rangle. \tag{2.19}$$

Although the emergence of the internal spaces V^C is a consequence of the topological degeneracy of the system, they are not the protected subspaces one is looking for. Even though no small local perturbation can affect the state in this internal space, global transformations (2.15) become rotations in V^C, and thus states of the form (2.19) are not in general invariant under $g \in H$ transformations. The topologically protected subspace, which is the major motivation for studying anyons, still awaits to reveal itself.

The Pure Charges

The pure charges of an anyon model were assumed to be labeled by the unitary irreducible representations Γ of H. Depending on the dimensions of the representations Γ, there is an internal $|\Gamma|$-dimensional charge vector space V^Γ associated with each particle carrying charge. A basis in this space is given by some set of charge eigenvectors

$$\{|i\rangle\}, \quad \langle i|j\rangle = \delta_{i,j}, \qquad i,j = 1,\ldots,|\Gamma|, \tag{2.20}$$

and a general state is a superposition of the form

$$|q\rangle = \sum_{i=1}^{|\Gamma|} a_i |i\rangle. \tag{2.21}$$

Unlike with the fluxes, the existence of the residual gauge group does not introduce any modification in the labeling, i.e. the pure charges are still labeled by the different irreducible unitary representations Γ of H. For the same reasoning as with the pure fluxes, states in the internal space V^Γ carried by a pure charges are resistant to small local perturbations, but not conserved under global transformations (2.15).

The Dyons

In addition to the pure fluxes and charges, there exists also particles carrying both flux and charge. These flux/charge composites are called *dyons* and their quantum numbers come about in a slightly different way. The relevant remark is that for flux carrying particles, the invariance under (2.15) does not completely fix the quantum numbers to coincide with the conjugacy classes (2.17). The reason is that there may be global transformations g, which

commute with a given flux h, and which can therefore be used to fix an additional internal charge degree of freedom [11]. These $g \in H$ form the *normalizer* subgroup $N(h) \subset H$,

$$N(h) = \{g \in H | gh = hg\}. \tag{2.22}$$

Because the $N(h)$ and $N(ghg^{-1})$ are isomorphic, the normalizer group can be associated with the corresponding conjugacy class C of the element h and denoted just by N_C. It follows that the charges carried by the dyons are labeled by the irreducible representations Γ_{N_C} and thus by combining both the gauge invariant flux and charge labels, the distinct dyons should be labeled by the pairs (C, Γ_{N_C}) as their good quantum numbers. As the pure fluxes and charges, also dyons carry an internal vector space, which now is a direct product of the flux and charge vector spaces

$$V_\Gamma^C \equiv V_{\Gamma_{N_C}}^C = V_C \otimes V_{\Gamma_{N_C}}, \tag{2.23}$$

with the basis given by the tensor product of the bases (2.18) and (2.20)

$$\{|h, i\rangle\}_{i=1,\ldots,|\Gamma|}^{h \in C}, \quad \langle h, i | h', j \rangle = \delta_{h,h'} \delta_{i,j}. \tag{2.24}$$

The Full Particle Spectrum

The dyons offer a natural generalization of the particle spectrum of the anyon model. The different physical particles are organized into degenerate multiplets, which are labeled by the the conjugacy classes C and irreducible normalizer representations Γ_{N_C} of the gauge group H. The pairs (C, Γ_{N_C}) are the good quantum numbers, which are usually said to define the *superselection sectors* of the model. All particles carrying same quantum numbers are treated as indistinguishable particles, which each carry an internal flux and/or charge vector space V_Γ^C. The pure flux and charge sectors appear as special cases corresponding to trivial conjugacy class and trivial representations, respectively.

Since each superselection sector is always labeled by two different quantum numbers, both which may or may not be trivial, but which are always different for different sectors, the notation can be simplified by labeling each particle with only a single label

$$a := (C, \Gamma_{N_C}). \tag{2.25}$$

In every model there is one special sector, the superselection sector corresponding to the conjugacy class $C(e)$ of the trivial element and the trivial representation $\Gamma_{N_{C(e)}}$ of its normalizer. This unique sector will labeled by

$$1 := \left(C(e), \Gamma_{N_{C(e)}}\right). \tag{2.26}$$

It is known as the *vacuum sector*, because it corresponds to having no particle at all. The full particle spectrum M is then formally given by the set of labels

$$M = \left\{1, a_1, a_2, \ldots, a_{|M|-1}\right\}, \tag{2.27}$$

where $|M|$ denotes the number the different superselection sectors.

Using the dyons as the most general particle types allows also the generalization of the global symmetry transformations (2.15) as well as of the the topological interactions (2.12) - (2.14). To account for the possible charge degrees of freedom, every $g \in H$ transformation, acting on some flux state $|h\rangle$, should be decomposed such that

$$g = g'\tilde{g}, \qquad g' \notin N_{C(h)}, \quad \tilde{g} \in N_{C(h)}. \tag{2.28}$$

If such decomposition exists for some $\tilde{g} \neq e$, the $\tilde{g}$ part of g commutes with h, and can be implemented as a non-trivial transformation in the charge sector. Then, the action of global symmetry transformations (2.15) on arbitrary states of the model can be summarized by

$$g \in H : |h, q\rangle \mapsto |ghg^{-1}, \Gamma(\tilde{g})q\rangle, \qquad \tilde{g} \in N_{C(h)}. \tag{2.29}$$

Similarly, all the topological interactions (2.13) - (2.14) can now be captured by the compact expressions

$$\begin{aligned} R|h,q\rangle|h',q'\rangle &= |hh'h^{-1}, \Gamma(\tilde{h})q'\rangle|h,q\rangle, & \tilde{h} \in N_{C(h')}, \\ R^{-1}|h,q\rangle|h',q'\rangle &= |h',q'\rangle|h'^{-1}hh', \Gamma^{-1}(\tilde{h'})q\rangle, & \tilde{h'} \in N_{C(h)}. \end{aligned} \tag{2.30}$$

Using these results one can finally check that braiding also bears a gauge invariant meaning, i.e. that (2.16) is satisfied

$$\begin{aligned} Rg|h,q\rangle|h',q'\rangle &= R|ghg^{-1}, \Gamma(\tilde{g})q\rangle \ |gh'g^{-1}, \Gamma'(\tilde{g})q'\rangle, \\ &= |ghh'h^{-1}g^{-1}, \Gamma'(\widetilde{ghg^{-1}})\Gamma'(\tilde{g})q'\rangle \ |ghg^{-1}, \Gamma(\tilde{g})q\rangle, \\ gR|h,q\rangle|h',q'\rangle &= g|hh'h^{-1}, \Gamma'(\tilde{h'})q'\rangle \ |h,q\rangle, \\ &= |ghh'h^{-1}g^{-1}, \Gamma'(\tilde{g})\Gamma'(\tilde{h})q'\rangle \ |ghg^{-1}, \Gamma(\tilde{g})q\rangle. \end{aligned} \tag{2.31}$$

These expressions are equal, because the isomorphy of the normalizers, $N(h) \simeq N(ghg^{-1})$, implies

$$\widetilde{ghg^{-1}} = \tilde{g}\tilde{h}\tilde{g}^{-1}. \tag{2.32}$$

Using then the representation properties $\Gamma(ab) = \Gamma(a)\Gamma(b)$ and $\Gamma(a^{-1}) = \Gamma^{-1}(a)$, it follows that

$$\Gamma'(\widetilde{ghg^{-1}})\Gamma'(\tilde{g}) = \Gamma'(\tilde{g})\Gamma'(\tilde{h})\Gamma'^{-1}(\tilde{g})\Gamma'(g) = \Gamma'(\tilde{g})\Gamma'(\tilde{h}), \tag{2.33}$$

which completes proving that the action of B_N commutes with global $g \in H$ symmetry transformations (2.16).

After all this work, one still has not even got a glimpse of the topologically protected subspaces, which was the main motivation for considering quantum computation with anyons. The closest thing resembling them are the internal flux/charge vector spaces (2.23), which,

however, were not robust storages for quantum information. The genuine invariant features of the model are the particle types M (2.27), which can change only under the process of fusion [11]. Hence, what remains in the discussion are the fusion rules which dictate what happens when two anyons are brought together. It will be shown that related to them, there exist a further internal space which is finally the one protected by topology. All this is most conveniently discussed in terms of Hopf algebras, which offer a natural description of anyons by unifying the given physically motivated arguments in terms of more rigorous mathematical formalism.

2.3 The Algebraic Structure of Non-Abelian Anyons

All the preceding discussion can be unified by extending the residual H symmetry into a quantum group symmetry. By doing so, instead of treating the different excitations appearing in the model as having fundamentally a different origin, the topological excitations being classified by the fundamental group (2.4), but the matter excitations being classified the representations Γ of H, they can be classified by the unitary irreducible representations of this single extended symmetry structure.

There is a physical way of motivating the appearance of this quantum symmetry by considering the allowed physical operations, i.e. the ones commuting with the action of the residual symmetry group. These are the independent measurements of both flux and charge by using quantum interference experiments [11]. They are captured by "interference amplitudes" of the form $\langle h,q|\langle h',q'|R^2|h',q'\rangle|h,q\rangle$, which, because of (2.16), are invariant under global symmetry transformations. However, the measurements of flux or charge are described in different ways. First, the measurements of flux correspond to projecting onto some flux eigenstate in the vector space V_a carried by a particle a. They are described by projectors P_h, which satisfy the flux projector algebra

$$P_h P_{h'} = \delta_{h,h'} P_h, \qquad h, h' \in H. \tag{2.34}$$

On the other hand, the measurement of charge corresponds to determining the representation Γ in which a given particle a transforms. These can be determined, at least in principle, by the transformation properties under all the $g \in H$ transformations. Therefore, the structure of allowed physical operations in an anyon system is, in principle, fully captured by the projectors (2.34) and the $g \in H$ transformations. However, since $g \in H$ transformations act on general flux states by (2.29), P_h and g do not in general commute

$$gP_h = P_{ghg^{-1}}g. \tag{2.35}$$

All the possible combinations of these two elementary physical operations form the set of elements

$$\{P_h\ g\}_{h,g\in H}, \tag{2.36}$$

whose elements, due to the non-commutativity of P_h and g, do not commute either. Instead, they obey the relation

$$P_h g \cdot P_{h'} g' = \delta_{h,gh'g^{-1}} P_h \; g \; g', \tag{2.37}$$

which can taken as a multiplication rule for the elements $P_h g$. The idea is now to treat the set of elements (2.36) as the elements of the extended symmetry algebra $D(H)$. Indeed, these elements are known to generate a so called quantum double $D(H)$ of H, which is a *quasitriangular Hopf algebra* [2, 11, 31]. It arises naturally as an extended symmetry algebra on any systems where the fundamental group coincides with the the residual gauge group (2.4).

The full quasitriangular Hopf algebra structure is given by $\{D(H), \cdot, \Delta, \epsilon, \mathcal{S}, \mathcal{R}\}$, where the mappings are formally given by [24, 33]

$$\cdot : \quad D(H) \otimes D(H) \to D(H), \tag{2.38}$$

$$\Delta : \quad D(H) \to D(H) \otimes D(H), \tag{2.39}$$

$$\epsilon : \quad D(H) \to \mathbb{C}, \tag{2.40}$$

$$\mathcal{S} : \quad D(H) \to D(H), \tag{2.41}$$

$$\mathcal{R} : \quad D(H) \otimes D(H) \to D(H) \otimes D(H). \tag{2.42}$$

There are a number of defining relations these structures have to obey in order to constitute a Hopf algebra. First, from the *multiplication* $\cdot$ one assumes associativity

$$(D(H) \cdot D(H)) \cdot D(H) = D(H) \cdot (D(H) \cdot D(H)) \,. \tag{2.43}$$

Analogously, the *co-multiplication* Δ has to satisfy *coassociativity*

$$(\Delta \otimes \mathrm{id})\Delta\,(D(H)) = (\mathrm{id} \otimes \Delta)\Delta\,(D(H)) \,. \tag{2.44}$$

The coassociativity tells how the action of $D(H)$ can be extended on tensor products of vector spaces. The quasitriangular structure of $D(H)$ is given by the unique element $\mathcal{R} \in D(H) \otimes D(H)$, *the universal R-matrix*, which has to satisfy the quasitriangularity conditions

$$\begin{aligned} \mathcal{R}\Delta\,(D(H)) &= (\sigma \circ \Delta\,(D(H)))\mathcal{R}, \\ (\mathrm{id} \otimes \Delta)(\mathcal{R}) &= \mathcal{R}_{13}\mathcal{R}_{12}, \\ (\Delta \otimes \mathrm{id})(\mathcal{R}) &= \mathcal{R}_{13}\mathcal{R}_{23}, \end{aligned} \tag{2.45}$$

where σ is a transposition map, $\sigma \circ (a \otimes b) = b \otimes a$, and the $\mathcal{R}_{ij}$ act on the ith and jth factor of $D(H) \otimes D(H) \otimes D(H)$ [33]. When combined, the the last two imply that $\mathcal{R}$ satisfies also the abstract *Quantum Yang-Baxter equation*

$$\mathcal{R}_{12}\mathcal{R}_{13}\mathcal{R}_{23} = \mathcal{R}_{23}\mathcal{R}_{13}\mathcal{R}_{12}. \tag{2.46}$$

Finally, the *co-unit* ϵ and the *antipode* $\mathcal{S}$ are defined as mappings obeying the respective relations

$$(\epsilon \otimes \mathrm{id})\Delta(D(H)) = \ (\mathrm{id} \otimes \epsilon)\Delta(D(H)) \ = D(H), \tag{2.47}$$

$$\cdot(\mathcal{S} \otimes \mathrm{id})\Delta(D(H)) = \cdot(\mathrm{id} \otimes \mathcal{S})\Delta(D(H)) = \epsilon(D(H)). \tag{2.48}$$

The counit ϵ plays the role of unit mapping with respect to comultiplication, whereas the antipodal map $\mathcal{S}$ serves to provide the inverse elements of $D(H)$.

Now, for the quantum double $D(H)$ with the set of elements (2.36), these objects are given by [2, 11, 33]

$$\Delta(P_h g) = \sum_{h' \cdot h'' = h} P_{h'} g \otimes P_{h''} g, \tag{2.49}$$

$$\mathcal{R} = \sum_{h,g \in H} P_g \otimes P_h g, \tag{2.50}$$

$$\epsilon(P_h g) = \delta_{h,e}, \tag{2.51}$$

$$\mathcal{S}(P_h g) = P_{g^{-1}h^{-1}g} g^{-1}, \tag{2.52}$$

with the multiplication $\cdot$ already given by (2.37). To show that the structure of $D(H)$ is indeed given by these objects, one should prove that they satisfy the definitions above. First, the coassociativity (2.44) is nearly trivial, since by just using the definition (2.49) and then renaming the indices suitably, one can immediately write both sides as

$$(\mathrm{id} \otimes \Delta)\Delta(P_h g) = (\Delta \otimes \mathrm{id})\Delta(P_h g) = \sum_{h' \cdot h'' \cdot h''' = h} P_{h'} g \otimes P_{h''} g \otimes P_{h'''} g. \tag{2.53}$$

The quasitriangularity conditions (2.45) can be proven as follows

$$\begin{aligned}
\mathcal{R}\Delta(P_a b) &= \left(\sum_{h,g} P_g \otimes P_h g \right) \left(\sum_{a' \cdot a'' = a} P_{a'} b \otimes P_{a''} b \right), \\
&= \sum_{h,g} \sum_{a' \cdot a'' = a} \delta_{g,a'} \delta_{g^{-1}hg,a''} P_g b \otimes P_h g b, \\
&= \sum_{h,g} \delta_{a,hg} P_g b \otimes P_h g b, \\
&= \sum_{x,y} \delta_{a,bxb^{-1}byb^{-1}} P_{byb^{-1}} b \otimes P_{bxb^{-1}} byb^{-1} b, \\
&= \sum_{x,y} \sum_{a' \cdot a'' = a} \delta_{a',bxb^{-1}} \delta_{a'',byb^{-1}} P_{a''} b \otimes P_{a'} by, \\
&= \left(\sum_{a' \cdot a'' = a} P_{a''} b \otimes P_{a'} b \right) \left(\sum_{x,y} P_y \otimes P_x y \right), \\
&= (\sigma \circ \Delta(P_a b))\mathcal{R},
\end{aligned} \tag{2.54}$$

where the summation indices have been relabeled as $h = bxb^{-1}$ and $g = byb^{-1}$. This is allowed, because the sums run over all the elements $h, g \in H$, and thus relabeling only permutes the

terms in the sum. Likewise,

$$\begin{aligned}
\mathcal{R}_{13}\mathcal{R}_{12} &= \left(\sum_{h,g} P_g \otimes \mathbf{1} \otimes P_h g\right)\left(\sum_{a,b} P_a \otimes P_b a \otimes \mathbf{1}\right), \\
&= \sum_{h,g}\sum_{a,b} \delta_{g,a} P_g \otimes P_b a \otimes P_h g, \\
&= \sum_{g,h,b} P_g \otimes P_b g \otimes P_h g, \\
&= \sum_{x,g}\sum_{x=x'\cdot x''} P_g \otimes P_{x'} g \otimes P_{x''} g, \\
&= (\mathrm{id} \otimes \Delta)(\mathcal{R}),
\end{aligned} \tag{2.55}$$

and

$$\begin{aligned}
\mathcal{R}_{13}\mathcal{R}_{23} &= \left(\sum_{h,g} P_g \otimes \mathbf{1} \otimes P_h g\right)\left(\sum_{a,b} \mathbf{1} \otimes P_a \otimes P_b a\right), \\
&= \sum_{h,g}\sum_{a,b} \delta_{h,gbg^{-1}} P_g \otimes P_a \otimes P_h g a, \\
&= \sum_{g,a,b} P_g \otimes P_a \otimes P_{gbg^{-1}} g a, \\
&= \sum_{y,x}\sum_{x=x'\cdot x''} P_{x'} \otimes P_{x''} \otimes P_y x, \\
&= (\Delta \otimes \mathrm{id})(\mathcal{R}),
\end{aligned} \tag{2.56}$$

where the summation indices have again in both been relabeled suitably. Finally, the definitions for the counit ϵ (2.47) and the antipode $\mathcal{S}$ (2.48) can be proven by

$$\begin{aligned}
(\epsilon \otimes \mathrm{id})\Delta(P_h g) &= (\epsilon \otimes \mathrm{id})\left(\sum_{h'h''=h} P_{h'} g \otimes P_{h''} g\right), \\
&= \sum_{h'h''=h} \delta_{h',e} \otimes P_{h''} g = P_h g, \\
&= \sum_{h'h''=h} P_{h'} g \otimes \delta_{h'',e}, \\
&= (\mathrm{id} \otimes \epsilon)\Delta(P_h g),
\end{aligned} \tag{2.57}$$

where one can write $\delta_{h,e}P_h g = P_h g \otimes \delta_{h,e} = \delta_{h,e} \otimes P_h g$, and

$$\begin{aligned}
\cdot(\mathcal{S}\otimes \mathrm{id})\Delta(P_h g) &= \cdot \sum_{h'h''=h} P_{g^{-1}h'^{-1}g} g^{-1} \otimes P_{h''} g, \\
&= \sum_{h',h''} \delta_{h'h'',h} \delta_{h'^{-1},h''} P_{g^{-1}h'^{-1}g}, \\
&= \sum_{h'} \delta_{h,e} P_{g^{-1}h'^{-1}g} = \delta_{h,e} = \epsilon(P_h g), \\
&= \sum_{h'} \delta_{h,e} P_{h'}, \\
&= \sum_{h'h''=h} \delta_{h',h''^{-1}} P_{h'}, \\
&= \cdot \sum_{h'h''=h} P_{h'} g \otimes P_{g^{-1}h''^{-1}g} g^{-1}, \\
&= \cdot(\mathrm{id}\otimes \mathcal{S})\Delta(P_h g),
\end{aligned} \tag{2.58}$$

where the completeness of the projectors, $\sum_h P_h = \sum_h P_{g^{-1}h^{-1}g} = 1$, has been used.

This concludes the summary of the algebraic structure of the quantum double $D(H)$. However, although one could loosely argue for the rise of $D(H)$ in physical terms, by themselves these abstract structures offer only very little insight to how they can be used to deal with the anyons in a holistic manner. To get back to physics, one must consider the representation theory of $D(H)$.

2.3.1 Representation Theory for the Quantum Double $D(H)$

It is known from the general theory of Hopf algebras that the representation space, the left $D(H)$-module, of a quantum double $D(H)$ is given by a H-graded vector space, $V = \bigoplus_{h\in H} V_h$, where H also acts in a compatible way according to [33]

$$|g \cdot v| = g|v|g^{-1}, \qquad \forall v \in V, \quad g \in H. \tag{2.59}$$

Here $g\cdot$ denotes the action of $g \in H$, $v \in V_h \subset V$ is a vector and $|v| = h$ is the degree of v. Recalling that $g \in H$ are the residual symmetry transformations, this abstract compatibility condition expresses that the representation space V decomposes into the irreducible subspaces transforming onto themselves under the action of H. Such spaces were already encountered during the preliminary discussion, which paved the way for the algebraic treatment, and with a slight reinterpretation, these results can now be directly taken into use.

It was argued how the superselection sectors, or the particle spectrum M (2.27), of the anyon model are formed when the gauge group of the system is the non-abelian group H. It was found that they are in general degenerate, which implied that each particle a could be thought as carrying an internal vector space V_a. Now, the quantum double $D(H)$ expresses the extended symmetry algebra of a model with the gauge group H. Therefore, it should act irreducibly in these internal vector spaces, which can now be mathematically interpreted as

the subspaces, which correspond to the gradation of the $D(H)$-module and which are simultaneously compatible with (2.59). Hence, in the language of the present algebraic treatment, the particle spectrum M should be understood as a collection of vector spaces V_a each carrying a particular irreducible representation Π_a of $D(H)$

$$M = \{(V_a, \Pi_a)\}_{a=1,\dots,|M|}. \tag{2.60}$$

Having already considered the spaces V_a in connection with dyons (2.23), the basis in each being given by $|k,i\rangle \in V_a$ (2.24), one should now find how the action of $D(H)$ is represented in them.

Recall that for an element $P_h g \in D(H)$ one assigned the physical interpretation of a global $g \in H$ transformation followed by a projection onto the flux eigenstate $|h\rangle$. To preserve this interpretation, for a state $|k,i\rangle \in V_a$, the action of $D(H)$ should be represented by

$$P_h g: \quad |k,i\rangle \to \Pi_a(P_h g)|k,i\rangle = \delta_{h,gkg^{-1}} |gkg^{-1}, \Gamma_a(\tilde{g})i\rangle, \tag{2.61}$$

where $\tilde{g} \in N(k)$ is the part of g commuting with k (2.28). In order this to be a valid representation in V_a, it should respect the group algebra (2.37) of $D(H)$

$$\Pi_a(P_h g)\Pi_a(P'_{h'} g')|k,i\rangle = \delta_{h,gh'g^{-1}} \Pi_a(P_h gg')|k,i\rangle. \tag{2.62}$$

This can checked by considering the following actions of $D(H)$:

$$\Pi_a(P_h g)\Pi_a(P_{h'} g')|k,i\rangle = \underbrace{\delta_{h,gg'kg'^{-1}g^{-1}}\ \delta_{h',g'kg'^{-1}}}_{=\delta_{h,gh'g^{-1}}} |gg'kg'^{-1}g^{-1}, \Gamma_a(\tilde{g})\Gamma_a(\tilde{g'})i\rangle, \tag{2.63}$$

$$\delta_{h,gh'g^{-1}}\Pi_a(P_h gg')|k,i\rangle = \underbrace{\delta_{h,gh'g^{-1}}\ \delta_{h,gg'kg'^{-1}g^{-1}}}_{=\delta_{h',g'h'g'^{-1}}} |gg'kg'^{-1}g^{-1}, \underbrace{\Gamma_a(\widetilde{gg'})}_{=\Gamma_a(\tilde{g})\Gamma_a(\tilde{g'})} i\rangle. \tag{2.64}$$

These expressions are equal if the values of the delta functions are equal for a fixed k and for all $g, g', h, h' \in H$. This is true, because if either $\delta_{h,gh'g^{-1}} = 0$ or $\delta_{h',g'hkg'^{-1}} = 0$, both sides of (2.62) are immediately zero. It can be seen from the two different expressions for the delta functions above, that it is not possible to have other equal to unity and simultaneously the other equal to zero. To only alternative to having both equal to zero is to have both equal to unity, which again satisfies (2.62). The identity $\Gamma_a(\widetilde{gg'}) = \Gamma_a(\tilde{g})\Gamma_a(\tilde{g'})$ follows again from the isomorphism $N(k) \simeq N(gkg^{-1})$ (2.32). Therefore, (2.61) is indeed a viable representation of $D(H)$ in the space V_a.

The extension of the action of $D(H)$ on multi-particle states is given formally by the comultiplication (2.49). Particularly, in terms of the representation (2.61), the action on two-particle state $|k,i\rangle|k',j\rangle \in V_a \otimes V_b$ is given by

$$\begin{aligned}\Pi_a \otimes \Pi_b\left(\Delta(P_h g)\right)|k,i\rangle|k',j\rangle &= \sum_{h'\cdot h''=h} \delta_{h',gkg^{-1}}\delta_{h'',gk'g^{-1}} |gkg^{-1}, \Gamma_a(\tilde{g})i\rangle|gk'g^{-1}, \Gamma_b(\tilde{g})j\rangle, \\ &= \delta_{h,gkk'g^{-1}} |gkg^{-1}, \Gamma_a(\tilde{g})i\rangle|gk'g^{-1}, \Gamma_b(\tilde{g})j\rangle. \end{aligned} \tag{2.65}$$

Physically this corresponds to implementing a residual g transformation separately on each particle and subsequently projecting out the total flux of the combined system. Therefore, the action (2.49) of $D(H)$ determines the globally conserved properties of the two particle quantum system and the coassociativity (2.44) implies that the action of $D(H)$ can be extended through comultiplication to an arbitrary number of states with similar interpretation.

Using (2.61), the representations for the counit ϵ (2.51) and the antipode $\mathcal{S}$ (2.52) are given by

$$\Pi_a\left(\epsilon(P_h g)\right)|k,i\rangle = \delta_{h,e}|k,i\rangle, \tag{2.66}$$

$$\Pi_a\left(\mathcal{S}(P_h g)\right)|k,i\rangle = \delta_{h^{-1},k}|g^{-1}kg, \Gamma_a(\tilde{g}^{-1})i\rangle. \tag{2.67}$$

One can see that the action of ϵ is represented trivially in an arbitrary space V_a, and therefore the counit implements a trivial symmetry transformation. Physically this signals the existence of vacuum $1 \in M$. The representation of the antipode acts non-trivially, but the physics can be extracted by considering the following

$$\begin{aligned}\Pi_a(P_h g)\Pi_a\left(\mathcal{S}(P_h g)\right)|k,i\rangle &= \Pi_a(P_h g)\left(\delta_{h^{-1},k}|g^{-1}kg, \Gamma_a(\tilde{g}^{-1})i\rangle\right), \\ &= \delta_{h,k}\delta_{h^{-1},k}|k, \Gamma_a(\tilde{g})\Gamma_a(\tilde{g}^{-1})i\rangle, \\ &= \delta_{h,h^{-1}}|k,i\rangle.\end{aligned} \tag{2.68}$$

The combined action of the elements $P_h g$ and $\mathcal{S}(P_h g)$ is proportional to the trivial transformation, and thus as expected from the general theory of Hopf algebras [33], the antipode plays the role of inverse. Physically this corresponds to the implementation of inverse transformations and hence of also to the existence of anti-particles $\bar{a} \in M$. Generally one can define the anti-particles as transforming in the conjugate representation, which can be defined with the aid of the antipode [2]

$$\overline{\Pi}_a(P_h g) \equiv \Pi_a^T(\mathcal{S}(P_h g)), \tag{2.69}$$

where T denotes transposition. The anti-particles are unique in a sense that for each particle a, there is only one other particle $\bar{a}$, which can fuse to give the vacuum. However, because of the topological degeneracy, this does not mean that a fusion with an anti-particle would always give the vacuum, but that there are no particles b, other than the anti-particle $\bar{a}$, which when fused with a may give the vacuum [32]. This curious property will play a key role in the next section.

The final piece of structure is the universal R-matrix (2.50). It is of primary interest since it satisfies the quantum Yang-Baxter equation (2.46), and hence representations of $\mathcal{R}$ can be used to define representations of the braid group. Because $\mathcal{R} \in D(H) \otimes D(H)$, it acts in $V_a \otimes V_b$, and one can therefore define physical braid operator R by

$$R_{ab} = \sigma \circ (\Pi_a \otimes \Pi_b)(\mathcal{R}), \tag{2.70}$$

where the σ is an operator performing the spatial exchange of the particle positions. Using (2.61), the action of R_{ab} on a two particle state is then given by

$$\begin{aligned} R_{ab}|k,i\rangle|k',j\rangle &= \sigma \circ \left((\Pi_a \otimes \Pi_b)(\sum_{h,g} P_g \otimes P_h g)|k,i\rangle|k',j\rangle \right), \\ &= \sigma \circ \left(\sum_{h,g} \delta_{g,k}\delta_{h,gk'g^{-1}}|k,i\rangle|gk'g^{-1},\Gamma_b(\tilde{g})j\rangle \right), \\ &= \sigma \circ \left(\sum_{h} \delta_{h,kk'k^{-1}}|k,i\rangle|kk'k^{-1},\Gamma_b(\tilde{k})j\rangle \right), \\ &= \sigma \circ \left(|k,i\rangle|kk'k^{-1},\Gamma_b(\tilde{k})j\rangle \right), \\ &= |kk'k^{-1},\Gamma_b(\tilde{k})j\rangle|k,i\rangle. \end{aligned} \tag{2.71}$$

Comparing this to (2.30), one can see that the action of the universal R-matrix in the space $V_a \otimes V_b$, as defined by (2.70), coincides with the action of the braid operator on the flux/charge eigenstates by implementing the Aharonov-Bohm effect (2.6) and the flux metamorphosis (2.7) on all conceivable states in the model. Because of the transposition map σ in the definition R, it does not satisfy the abstract quasitriangularity conditions (2.45), but the conditions [11]

$$\begin{aligned} R\Delta\left(D(H)\right) &= \left(\Delta\left(D(H)\right)\right)R, \\ (\mathrm{id} \otimes \Delta)(R) &= (\mathbf{1} \otimes R)(R \otimes \mathbf{1}), \\ (\Delta \otimes \mathrm{id})(R) &= (R \otimes \mathbf{1})(\mathbf{1} \otimes R), \end{aligned} \tag{2.72}$$

The first of these expresses the already familiar property (2.16), i.e. that braiding commutes with residual symmetry transformations and conserves the total flux. When combined, the last two imply that R satisfies the Yang-Baxter equation (2.11)

$$(R \otimes \mathbf{1})(\mathbf{1} \otimes R)(R \otimes \mathbf{1}) = (\mathbf{1} \otimes R)(R \otimes \mathbf{1})(\mathbf{1} \otimes R), \tag{2.73}$$

and thus the representations (2.70) indeed define representations of the braid group.

To summarize, in an anyon model based on a finite gauge group H, an internal vector space of N particles carries representations of both $D(H)$ and B_N given by $((\Pi_a)^{\otimes N},(V_a)^{\otimes N})$ and R_{ab}, respectively, for each $a, b \in M$. Therefore, the algebraic construction with the quantum double $D(H)$ as an extended symmetry algebra, captures all the features of an anyon model as derived based on purely quantum mechanical considerations. However, it also allows one to go further by providing a way to tackle the theory of fusion which was unaccessible before. This will be the topic of the next section where the long sought topologically protected subspaces will finally be discovered.

2.3.2 The Topological Hilbert Space

When two particles are fused together, the quantum numbers M should be conserved. However, as one is now considering an anyon model with degenerate superselection sectors, i.e. a non-abelian model, it is not at all obvious how the quantum numbers should be added up. One the other hand, since the irreducible representations Π_a of $D(H)$ are used to classify the distinct particles, it is natural to demand that the outcome of the fusion has to transform also in some irreducible representations of $D(H)$. Now, in addition to assigning quantum numbers to distinct particles, the Π_a describe also the transformation properties under $D(H)$ transformations, and thus one could as well consider the tensor products of single particle representations $\Pi_a \otimes \Pi_b$, which could be thought of as describing the transformation properties and quantum numbers of a composite two-particle system. However, the first quasitriangularity condition (2.72) shows that $D(H)$ and B_N commute and can thus be simultaneously diagonalized. This, on the other hand, means that the N-particle representations $((\Pi_a)^{\otimes N}, {}^{(}V_a)^{\otimes N})$ are in general reducible and hence under the action of $D(H) \times B_N$, the multi-particle representations breaks down to a direct sum of irreducible representations [11]. The possible outcomes of a fusion of two particles are then determined by the decomposition of $\Pi_a \otimes \Pi_b$ into irreducible representations, i.e. the Clebsch-Gordan series

$$\Pi_a \otimes \Pi_b = \bigoplus_c N_{ab}^c \Pi_c, \tag{2.74}$$

where N_{ab}^c stands for the multiplicity of the irreducible representation Π_c in the decomposition. These numbers are determined by using the orthogonality of the characters of irreducible representations [11, 24]

$$N_{ab}^c = \frac{1}{|H|} \sum_{h,g} \mathrm{tr}\left(\Pi_a \otimes \Pi_b(\Delta(P_h g))\right) \mathrm{tr}\left(\Pi_c(P_h g)\right)^* . \tag{2.75}$$

In more physical terms, given two particles a and b, the decomposition (2.74) state which particles c can be be formed, i.e. it provides the *fusion rules* of the model. If for some particles $N_{ab}^c \geq 2$, there exist N_{ab}^c ways of obtaining the particle c. The fusion rules are the most interesting feature of the representation theory of $D(H)$, at least as far as topological quantum computation is concerned, because they encode the robust features of multi-particle systems. The whole preceding discussion has been presented to argue for their emergence, and much of it will not play a role anymore. Yet, the discussion has not been in vain, because to actually calculate the fusion multiplicities (2.75) for a given model, one still needs to understand how to derive the representation spaces V_a (2.60) and the representations Π_a (2.61).

The Fusion Algebra and the Fusion Spaces

The new starting point is to consider the decomposition (2.74) as an abstract *fusion algebra*,

$$a \times b = \sum_c N_{ab}^c \; c, \tag{2.76}$$

which is both commutative and associative [32, 42]

$$\begin{aligned} a \times b = b \times a, \quad &\Leftrightarrow \quad N_{ab}^{c} = N_{ba}^{c}, \\ (a \times b) \times d = a \times (b \times d), \quad &\Leftrightarrow \quad \sum_{x} N_{ab}^{x} N_{xd}^{c} = \sum_{x} N_{ax}^{c} N_{bd}^{x}. \end{aligned} \tag{2.77}$$

The physics underlying these two properties is the conservation of the quantum numbers: given that the outcome will be c, it does not matter in which order the particles are fused.

The fusion algebra can be thought as assigning each label set $\{a, b, c\} \in M$ a *fusion space* V_{ab}^{c} of dimension

$$\dim(V_{ab}^{c}) = N_{ab}^{c}. \tag{2.78}$$

The vector space V_{ab}^{c} is spanned by so called *fusion states*, which form the orthonormal basis

$$\{|ab; c, \mu\rangle\}_{\mu=1,\ldots,N_{ab}^{c}}, \quad \langle ab; c, \mu | ab; c, \mu' \rangle = \delta_{\mu,\mu'}, \tag{2.79}$$

and have the physical interpretation of corresponding to the inequivalent and distinguishable ways a and b can fuse to form c. One can as well consider more general fusion spaces V_{ab} carried by particles a and b and where the fusion outcome is not fixed. The structure of such spaces is given by the direct sum over all the subspaces indexed by the possible fusion outcomes c

$$V_{ab} = \bigoplus_{c} V_{ab}^{c}, \qquad \dim(V_{ab}) = \sum_{c} N_{ab}^{c}. \tag{2.80}$$

Since for each c there is a proper subspace, the orthonormal basis in V_{ab} is given by

$$\{|ab; c, \mu\rangle\}_{\mu=1,\ldots,N_{ab}^{c}}^{c}, \quad \langle ab; c, \mu | ab; c', \mu' \rangle = \delta_{c,c'} \delta_{\mu,\mu'}. \tag{2.81}$$

From the definition (2.80), one can see that $\dim(V_{ab}) > 1$ only for non-abelian models. In an abelian model there would be no topological degeneracy and the outcome of every fusion would always be unique. The topological Hilbert space would coincide with the only subspace labeled by a single c, $V_{ab} \simeq V_{ab}^{c}$, and thus $\dim(V_{ab}) = N_{ab}^{c} = 1$ for all a and b. Since one wants to consider the fusion spaces as an arena for quantum computation, this reinforces the notion that quantum computation with anyons is only possible for a non-abelian model [42].

The two-particle fusion spaces (2.78) and (2.80) serve as simple examples of what are sometimes called *topological Hilbert spaces*. However, they are hardly of particular interest, because unless there is fusion degeneracy, i.e. $N_{ab}^{c} \geq 2$, V_{ab}^{c} can not be used to encode quantum information. Consequently, the fusion spaces V_{ab} are directly out of the question, because one cannot form superpositions of states belonging to different superselection sectors [32]. To overcome these restrictions, one must consider the more general fusion spaces $V_{a_1,\ldots,a_N}^{c}$ carried by some N-particles, whose total charge has been restricted to c. To study their structure, one needs to decompose them in terms of the elementary fusion spaces V_{ab}^{c}. Because the fusion algebra is associative (2.77), multi-particle fusion spaces $V_{a_1,\ldots,a_N}^{c}$ can be decomposed

as a direct sum of subspaces corresponding to different fusion orders. For example, one decomposition is realized by fusing always the two left most particles

$$V^c_{a_1\ldots a_N} \simeq \bigoplus_{b_1,b_2,\ldots,b_{N-2}} V^{b_1}_{a_1a_2} \otimes V^{b_2}_{b_1a_3} \otimes \cdots \otimes V^c_{b_{N-2}a_N}, \tag{2.82}$$

where $b_1, b_2, \ldots, b_N$ are particles which may occur during intermediate stages of fusing all the particles together. From this expression, one can immediately read off the dimension of $V^c_{a_1,\ldots,a_N}$,

$$\dim(V^c_{a_1\ldots a_N}) = N^c_{a_1\ldots a_N} = \sum_{b_1,b_2,\ldots,b_{N-2}} N^{b_1}_{a_1a_2} N^{b_2}_{b_1a_3} \cdots N^c_{b_{N-2}a_N}. \tag{2.83}$$

Of course, this particular fusion order is not the only possible choice for the decomposition. Any other choice would give as viable alternative decomposition. Yet, regardless of how one does the decomposition, the N-particle fusion space always decomposes as a direct sum of $N-2$ two-particle fusion spaces, and all the different choices correspond to isomorphic representations of the same space $V^c_{a_1,\ldots,a_N}$. Since one needs to pick one to proceed with the analysis, the decomposition (2.82) is as good as any. It is known as the *standard basis decomposition*, which often serves as the most practical choice due to its simple structure [42]. The *standard basis* corresponding to this decomposition is given by the tensor product of the subspace bases

$$\{|a_1a_2;b_1,\mu_1\rangle|b_1a_3;b_2,\mu_2\rangle\cdots|b_{N-2}a_N;c,\mu_{N-1}\rangle\}. \tag{2.84}$$

The orthonormality of these spaces is given by the orthonormality of the individual basis states (2.81). Working with basis of this form a rather awkward due to the large number of indices, and thus in analogy with (2.79), it is useful to adopt a more compact notation by denoting these basis states by

$$\{|a_1a_2\cdots a_N;c,\mu\rangle\}_{\mu=0,1,\ldots,N^c_{a_1a_2\cdots a_N}}, \quad \langle a_1a_2\cdots a_N;c,\mu|a_1a_2\cdots a_N;c,\mu'\rangle = \delta_{\mu,\mu'}, \tag{2.85}$$

where the index μ counts now both the fusion state degeneracies as well as the distinct intermediate fusion outcomes.

The observation above that the fusion algebra is associative allowed one to decompose the N-particle fusion spaces in terms of smaller subspaces. There are also quite a few other relations between different fusion spaces that the fusion algebra implies [32, 42]. First, the commutativity implies a natural fusion space isomorphism

$$V^c_{ab} \simeq V^c_{ba}. \tag{2.86}$$

This observation can be extended to N particles by saying that all fusion spaces corresponding to permutations of the lower indices are isomorphic. The label c can therefore be said to define the superselection sector of the fusion space $V^c_{a_1,\ldots,a_N}$, which can not change in any physical process in which only the particles $a_1,\ldots,a_N$ participate. Second, the existence of

unique anti-particles induces further natural isomorphisms between the fusion spaces V_{ab}^{c}. The starting point is the fusion space V_{a1}^{a} where no fusion occurs. This space can be thought as corresponding to free propagation and hence it is one-dimensional by definition, $\dim(V_{a1}^{a}) = N_{a1}^{a} = 1$. Since the anti-particle $\bar{a}$ is unique for a given a, the space $V_{a\bar{a}}^{1}$ where total annihilation occurs must also be one-dimensional, $\dim(V_{a\bar{a}}^{1}) = N_{a\bar{a}}^{1} = 1$. More specifically, these spaces are isomorphic [32]

$$V_{a1}^{a} \simeq V_{a\bar{a}}^{1} \simeq V_{1}^{a\bar{a}}. \tag{2.87}$$

The last isomorphism in (2.87) also implies that a pair of particles created out of vacuum always carries conjugate labels. These isomorphisms can be generalized to arbitrary fusion spaces by adopting a convention that the indices can be raised and lowered by replacing them with their conjugates

$$V_{ab}^{c} \simeq \ V_{ab\bar{c}}^{1} \simeq V_{a\bar{c}}^{\bar{b}} \simeq \cdots . \tag{2.88}$$

All fusion spaces isomorphic to each other are also of same dimension. The physics underlying these isomorphisms is still the conservation of total charge - all the fusion spaces corresponding to fusion processes conserving the same total charge are isomorphic.

The fusion algebra can also be used to partition M into various useful subsets. For example, the fusion outcomes of the particles a and b form the set

$$M_{ab} = \{c\}_{\forall c \in M, N_{ab}^{c} \neq 0}, \qquad M_{ab} \subset M. \tag{2.89}$$

Another kinds of partitions, if such exist in a given model, are the subsets $M_i \subset M$, which are closed under the fusion algebra (2.76)

$$M_i \times M_i \to M_i. \tag{2.90}$$

The existence of such sets is of interest, because particles in such M_i would span a subalgebra of the complete fusion algebra, and they could therefore be treated independently of any other particles appearing in the model. Consequently, the fusions spaces carried by particle in M_i form a proper subspace of the full fusion space, which is closed under operations involving only these particles. From the point of view of quantum computation, these subalgebras are a desirable feature, because the possibility to restrict to dealing with only a limited number of particles types can significantly simplify the discussion.

The primary reason to study topological quantum computation is that the fusion spaces are protected from decoherence by topology. The states in $V_{a_1,\ldots,a_N}^{c}$ are robust in the presence of local external perturbations. By external perturbations one means for example interactions with environment such as photons or ordinary matter, which can cause deviataions in the quasiparticle trajectories, but can not change the superselection sector in the topological Hilbert space. Only interactions or fusions with external quasiparticles can cause this and thus the primary error source to be controlled is the spontaneous creation of particle - anti-particle pairs. Otherwise, in principle, there are no other sources of error. The pair creation is

not assumed to be a significant obstacle, because it is exponentially suppressed with decreasing temperature and thus one can deal with it with sufficient cooling [31, 42]. Having now finally identified the arena for topological quantum computation, it is time to consider what one can do there, i.e. how the braid group is represented.

Braiding in the Topological Hilbert Space

The commutativity of the fusion algebra (2.76) implied the fusion space isomorphisms (2.86). This, on the other hand, implies that there exists a unique unitary intertwiner map

$$R: \quad V_{ab}^{c} \to V_{ba}^{c}, \tag{2.91}$$

which relates the isomorphic fusion spaces. Absorbing the convention of the placement of the particles on a line (2.5) on the placement of the indices in V_{ab}^{c}, R then has an additional interpretation of implementing the transposition of adjacent particles. The isomorphism (2.91) relating two representation tensor products of $D(H)$ should be map commuting with the action of $D(H)$, and such a map is already familiar. It is the braid operator (2.70) obtained from the universal R-matrix, which by (2.72) satisfies this property and which hence acts in the fusion spaces as (2.91) [24, 32, 33]. In general, the applications of R will be referred to as *R-moves*, which can be considered as the actions of braid group generators on two-particle fusion spaces. When expressed as a matrix acting on the basis states of the isomorphic fusion spaces, an R-move relates the two bases $|ab;c,\mu\rangle \in V_{ab}^{c}$ and $|ba;c,\mu'\rangle \in V_{ba}^{c}$ by the expansion

$$|ab;c,\mu\rangle = R_{ba}^{c}|ba;c,\mu\rangle = \sum_{\mu'} (R_{ba}^{c})_{\mu}^{\mu'}|ba;c,\mu'\rangle. \tag{2.92}$$

This is a very general expression, but the exact form of the unitary matrix R_{ab}^{c} is constrained by certain consistency conditions to be discussed in a while.

There exists also a second intertwiner map relating the isomorphic N-particle fusion spaces. The associativity of the fusion algebra allowed one to decompose multi-particle fusion spaces by different fusion orders with no fusion order being singled out by any physical principle. Since all the possible decompositions are still representations of the same fusion space [32], the alternative representations should be related by some unique unitary map

$$F_{abc}^{d}: \quad V_{abc}^{d} \simeq \bigoplus_{x\in M_{ab}} V_{ab}^{x}\otimes V_{xc}^{d} \to V_{abc}^{d} \simeq \bigoplus_{x\in M_{bc}} V_{ax}^{d}\otimes V_{bc}^{x}, \tag{2.93}$$

In analogy to the R-moves (2.91), these maps are known as the *F-moves*, which act on the basis states as

$$|ab;e,\mu\rangle|ec;d,\nu\rangle = \sum_{\substack{x\in M_{bc},\\ \mu',\nu'}} \left(F_{abc}^{d}\right)_{e\mu\nu}^{x\mu'\nu'} |ax;d,\mu'\rangle|bc;x,\nu'\rangle. \tag{2.94}$$

Since the canonical basis in the fusion spaces was chosen to coincide with the distinct fusion channels, an F-move can be interpreted as implementing a basis change in the fusion spaces

by switching between the possible fusion orders. As the R-moves, also the F-moves are constrained by certain consistency conditions.

These consistency conditions arise, because R- and F-moves define isomorphisms between different spaces and therefore certain combinations of them have to be compatible with each other. These conditions go under the names of *pentagon* and *hexagon equations*. Consider first the fusion space $V^e_{abcd} = \bigoplus_{x\in M_{ab}, y\in M_{xc}} V^x_{ab}\otimes V^y_{xc}\otimes V^e_{yd}$ in the standard basis decomposition. Both of the F-move sequences,

$$\bigoplus_{\substack{x\in M_{ab},\\ y\in M_{xc}}} V^x_{ab}\otimes V^y_{xc}\otimes V^e_{yd} \xrightarrow{F^e_{xcd}} \bigoplus_{\substack{x\in M_{ab},\\ y'\in M_{cd}}} V^x_{ab}\otimes V^e_{xy'}\otimes V^{y'}_{cd} \xrightarrow{F^e_{aby'}} \bigoplus_{\substack{x'\in M_{by'},\\ y'\in M_{cd}}} V^e_{ax'}\otimes V^{x'}_{by'}\otimes V^{y'}_{cd}, \quad (2.95)$$

and

$$\begin{aligned}\bigoplus_{x\in M_{ab}, y\in M_{xc}} V^x_{ab}\otimes V^y_{xc}\otimes V^e_{yd} &\xrightarrow{F^y_{abc}} \bigoplus_{x'\in M_{bc}, y\in M_{ax'}} V^y_{ax'}\otimes V^{x'}_{bc}\otimes V^e_{yd}\\ &\xrightarrow{F^e_{ax'd}} \bigoplus_{x'\in M_{bc}, y'\in M_{x'd}} V^e_{ay'}\otimes V^{x'}_{bc}\otimes V^{y'}_{x'd}\\ &\xrightarrow{F^{y'}_{bcd}} \bigoplus_{x''\in M_{cd}, y'\in M_{bx''}} V^e_{ay'}\otimes V^{y'}_{bx''}\otimes V^{x''}_{cd},\end{aligned} \quad (2.96)$$

yield the same decomposition and thus in terms of the matrix elements (2.94), the F have to satisfy

$$\sum_{\substack{y'\in M_{cd}\\ x'\in M_{by'}}} \left(F^e_{aby}\right)^{x'}_{x}\left(F^e_{xcd}\right)^{y'}_{y} = \sum_{\substack{x'\in M_{bc}\\ y'\in M_{x'd}, x''\in M_{cd}}} \left(F^y_{bcd}\right)^{x''}_{x'}\left(F^e_{ax'd}\right)^{y'}_{y}\left(F^y_{abc}\right)^{x'}_{x}. \quad (2.97)$$

This is the *pentagon equation* with the summation over the fusion state indices $\mu,\nu,\ldots$ suppressed.

Similarly one can consider the fusion space $V^d_{abc}\simeq\bigoplus_{x\in M_{ab}} V^x_{ab}\otimes V^d_{xc}\simeq\bigoplus_{x\in M_{bc}} V^d_{ax}\otimes V^x_{bc}$. Starting from the first one, the latter decomposition can then be reached either by

$$\bigoplus_{x\in M_{ab}} V^x_{ab}\otimes V^d_{xc} \xrightarrow{R^x_{ab}\otimes\mathrm{id}} \bigoplus_{x\in M_{ab}} V^x_{ba}\otimes V^d_{xc} \xrightarrow{F^d_{bac}} \bigoplus_{x'\in M_{ac}} V^d_{bx'}\otimes V^{x'}_{ac} \xrightarrow{\mathrm{id}\otimes R^{x'}_{ac}} \bigoplus_{x'\in M_{ac}} V^d_{bx'}\otimes V^{x'}_{ca}, \quad (2.98)$$

or by

$$\bigoplus_{x\in M_{ab}} V^x_{ab}\otimes V^d_{xc} \xrightarrow{F^d_{abc}} \bigoplus_{x'\in M_{bc}} V^d_{ax'}\otimes V^{x'}_{bc} \xrightarrow{(\mathrm{id}\otimes R^d_{ax'})\cdot\sigma} \bigoplus_{x'\in M_{bc}} V^{x'}_{bc}\otimes V^d_{x'a} \xrightarrow{F^d_{bca}} \bigoplus_{x''\in M_{ca}} V^d_{bx''}\otimes V^{x''}_{ca}. \quad (2.99)$$

This means that in terms of the matrix elements (2.94) and (2.92), the *hexagon equation* reads

$$\sum_{x'\in M_{ac}} R^{x'}_{ac}\left(F^d_{bac}\right)^{x'}_{x} R^x_{ab} = \sum_{\substack{x'\in M_{bc},\\ x''\in M_{ca}}} \left(F^d_{bca}\right)^{x''}_{x'} R^d_{ax'}\left(F^d_{abc}\right)^{x'}_{x}. \quad (2.100)$$

By the so called *MacLane's coherence theorem*, there are no further consistency conditions [32, 42], and thus (2.97) and (2.100) define viable and consistent anyon models, which are completely characterized by their solutions.

From the point of view of quantum computation, it is assuring that viable anyon models are defined by solutions to only two polynomial equations. On the other hand, since these solutions give the representations of the R- and F-moves as the only fundamental structure, the tools to construct various transformations in the fusion spaces are very limited. Particularly, one wishes to construct the representation of the braid group in an N-particle fusion space $V^c_{a_1,\ldots,a_N}$, i.e. find how the braid group acts on the standard basis (2.85). However, since the this space is associated with only one particular arrangement of the indices $a_1,\ldots,a_N$, it can not by itself carry a representation of braid group. In contrast, the viable space should include all the spaces associated with different permutations of the lower indices, which can in general be written as

$$V^c = \bigoplus_{a_1,\ldots,a_N} V^c_{a_1,\ldots,a_N}. \tag{2.101}$$

Anticipating the things to come, this is also the general structure one assumes from the potential computational spaces. Because braiding is in practice the only way to apply transformations, one must include all the permutations of the labels in order to prevent transformations taking states out of the computational space.

Considering the V^d_{abc} in the standard basis as the simplest non-trivial multi-particle fusion space, an R-move, as defined by (2.91), implements then the transformation

$$R : V^d_{abc} \to V^d_{bac}, \tag{2.102}$$

which acts only on the two left most particles. As argued earlier, R can be interpreted as a generator of the braid group $\sigma_1 \to R$, but to construct an arbitrary braid on three particles as the tensor product (2.10), one needs also a second generator $\sigma_2 \to B$ which together with (2.102) satisfies the Yang-Baxter equation (2.11). This meas that one wishes to find an unitary operator implementing the transformation

$$B : V^d_{abc} \to V^d_{acb}. \tag{2.103}$$

Considering the limited number of tools at disposal, it is evident that the F-move has to be utilized. The solution is to first apply an F-move to switch into a basis where the R-moves are well defined, applying an R-move there and return to the standard basis by applying the inverse F^{-1}-move [42]. Using this procedure the *B-move*, the action of an arbitrary generator

of the braid group in the standard basis, can be constructed as successive R- and F-moves

$$\begin{aligned}
|abc;d\rangle &= |ab;x,\mu\rangle|xc;d,\nu\rangle, \\
&= \sum_{x'\in M_{bc},\mu',\nu'} |ax';d,\mu'\rangle|bc;x',\nu'\rangle \left(F^d_{abc}\right)^{x'\mu'\nu'}_{x\mu\nu}, \\
&= \sum_{x'\in M_{bc},\mu',\nu',\nu''} |ax';d,\mu'\rangle|cb;x',\nu''\rangle \left(R^{x'}_{cb}\right)^{\nu''}_{\nu'} \left(F^d_{abc}\right)^{x'\mu'\nu'}_{x\mu\nu}, \qquad (2.104) \\
&= \sum_{\substack{x'\in M_{bc},\mu',\nu',\nu'' \\ x''\in M_{ac},\mu'',\nu'''}} |ac;x'',\mu''\rangle|x''b;d,\nu'''\rangle \left([F^{-1}]^d_{acb}\right)^{x'',\mu'',\nu'''}_{x',\mu',\nu''} \left(R^{x'}_{cb}\right)^{\nu''}_{\nu'} \left(F^d_{abc}\right)^{x'\mu'\nu'}_{x\mu\nu}, \\
&= \sum_{x''\in M_{ac},\mu'',\nu'''} |ac;x'',\mu''\rangle|x''b;d,\nu'''\rangle \left(B^d_{acb}\right)^{x'',\mu'',\nu'''}_{x,\mu,\nu}, \\
&= B^d_{acb}|acb;d\rangle.
\end{aligned}$$

Suppressing the fusion state indices over which one always sums, the elements of the matrix representation B^d_{acb} in the space V^d_{acb} can be defined by

$$\left(B^d_{acb}\right)^{x''}_{x} = \sum_{x'\in M_{bc}} \left([F^{-1}]^d_{acb}\right)^{x''}_{x'} \left(R^{x'}_{cb}\right) \left(F^d_{abc}\right)^{x'}_{x}, \qquad (2.105)$$

which means that the action of B_N in the standard basis is completely characterized by R- and F-moves.

This concludes the overview of the non-abelian anyon model based on a finite residual gauge group H. The model is fully described by the quasitriangular Hopf algebra $D(H)$, the quantum double of H. The defining structures are the particle spectrum M (2.60), which label the superselection sectors arising as the irreducible representations of $D(H)$, the fusion rules (2.76) specified by the fusion multiplicities $\{N^c_{ab}\}_{a,b,c\in M}$ (2.75), and the R- (2.50) and F-moves (2.93) describing braiding properties. The discussion has in no way been a rigorous treatment of the algebraic structure of anyons and the presented topics have been chosen due to their relevance in the light of topological quantum computation. For a more rigorous and detailed treatment, one is referred to [18, 20] and [32]. The reason to go through all this trouble is the discovery of the topological Hilbert space, which has the exceptional property for being insensitive to local perturbations. Quantum information encoded there would be intrinsically protected from decoherence. With the topological Hilbert space as the playground and the R and F as the tools at the repertoire, it now remains to be studied how quantum computation can be executed in this long-sought arena. To put things into a bit more concrete setting, a specific anyon model will be presented next.

S_3	e	x	xy	xy^2	y	y^2
e	e	x	xy	xy^2	y	y^2
x	x	e	y	y^2	xy	xy^2
xy	xy	y^2	e	y	xy^2	x
xy^2	xy^2	y	y^2	e	x	xy
y	y	xy^2	x	xy	y^2	e
y^2	y^2	xy	xy^2	x	e	y

Table 2.1: Multiplication table of S_3

2.4 The S_3 Anyon Model

As an example of the abstract construction of the previous section, an anyon model based on the non-abelian group S_3 will be considered. This particular example was chosen, because S_3 is the simplest non-abelian group and its application to topological quantum computation, although in quite a different setting, has been considered in [34]. Unlike the Chern-Simons type models, which seem to rise naturally in fractional Quantum Hall states [22, 42, 45], no natural systems exhibiting S_3 symmetry are currently known. However, there has been proposals for preparing such experimentally [15], and the simple structure of S_3 may well be one which can be artificially constructed in the future.

S_3 is the symmetry group of an equilateral triangle, which is generated by the reflections with respect to any one of the three diagonals and by the 120 deg rotations around their intersection point. The respective symmetry groups are the cyclic groups Z_2 and Z_3, which are generated by x and y satisfying $x^2 = e$ and $y^3 = e$, respectively. Mathematically, S_3 can then be expressed as the direct product

$$S_3 = Z_2 \times Z_3, \tag{2.106}$$

with the elements given by

$$S_3 = \{x^n y^m\}_{n=0,1}^{m=0,1,2} = \{e, x, xy, xy^2, y, y^2\}. \tag{2.107}$$

The generators x and y satisfy the relations

$$xy = y^2 x, \qquad x^2 = e, \qquad y^3 = e \tag{2.108}$$

which enable one to construct the multiplication table of S_3 (Table 2.1).

The conjugacy classes (2.17) and normalizers (2.22) are summarized in Table 2.2. One can see that there are only two distinct non-trivial conjugacy classes

$$C_x \equiv \{x, xy, xy^2\}, \qquad C_y \equiv \{y, y^2\}. \tag{2.109}$$

The first one contains all the three elements which are generated by both x and y whereas the second contains the two elements which are generated by y alone. Hence, there are also

C_a	=	$\{gag^{-1} \mid g \in S_3\}$	N_a	=	$\{ag = ga \mid g \in S_3\}$	
C_e	=	$\{e\}$	N_e	=	$\{e, x, xy, xy^2, y, y^2\}$	$\simeq S_3$
C_x	=	$\{x, xy, xy^2\}$	N_x	=	$\{e, x\}$	$\simeq Z_2$
C_{xy}	=	$\{x, xy, xy^2\}$	N_{xy}	=	$\{e, xy\}$	$\simeq Z_2$
C_{xy^2}	=	$\{x, xy, xy^2\}$	N_{xy^2}	=	$\{e, xy^2\}$	$\simeq Z_2$
C_y	=	$\{y, y^2\}$	N_y	=	$\{e, y, y^2\}$	$\simeq Z_3$
C_{y^2}	=	$\{y, y^2\}$	N_{y^2}	=	$\{e, y, y^2\}$	$\simeq Z_3$

Table 2.2: Conjugacy classes and normalizers of S_3

S_3	e	x	xy	xy^2	y	y^2
Γ_1	1	1	1	1	1	1
Γ_{-1}	1	-1	-1	-1	1	1
Γ_2	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \omega \\ \bar{\omega} & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \bar{\omega} \\ \omega & 0 \end{pmatrix}$	$\begin{pmatrix} \bar{\omega} & 0 \\ 0 & \omega \end{pmatrix}$	$\begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}$

Table 2.3: Unitary irreducible representation of S_3

two distinct non-trivial internal flux vector spaces: the three-dimensional V_x with basis given by the states $\{|x\rangle, |xy\rangle, |xy^2\rangle\}$ and the two-dimensional V_y with the basis given by the states $\{|y\rangle, |y^2\rangle\}$. Likewise, there are only two non-trivial normalizers, which will be denoted by

$$N_x \equiv N_x \simeq N_{xy} \simeq N_{xy^2} \simeq Z_2, \qquad N_y \equiv N_y \simeq N_{y^2} \simeq Z_3. \tag{2.110}$$

Strictly speaking, the normalizers N_x, N_{xy} and N_{xy^2} are different groups, but they are isomorphic and for the purposes here, they can be treated in practice as being equal. To establish the particle spectrum (2.60), one must consider the unitary irreducible representations of each of the normalizers. Their multiplicity is given by the number of conjugacy classes of the respective normalizer. It was already noted that S_3 has 3 conjugacy classes. Furthermore, Z_2 and Z_3 have 2 and 3 conjugacy classes, respectively, because they are abelian groups, which means that each element forms its own conjugacy class. One particular choice for the unitary irreducible representations of these three groups is given in Tables 2.3 and 2.4, where $\omega = \exp(\frac{i\pi}{3})$ is the primitive cube root of unity. One can see that there is only one higher dimensional irreducible representation, the Γ_2 of S_3, to which one associates a two-dimensional charge vector space V_2 with the basis given by some orthonormal states $\{|1\rangle, |2\rangle\}$ (2.20). All the other irreducible representations, and hence also the associated charge vector spaces are one-dimensional.

Forming the tensor products of the flux and charge spaces (2.23), one can establish the superselection sectors, which define the particle spectrum of the model (Table 2.5). Altogether there are eight superselection sectors, which means that in addition to the vacuum 1, there are seven distinct particles. The internal flux and/or charge spaces associated with each sector transform irreducibly under the action of $D(S_3)$, and to study the structure of the fusion spaces of the model, one should find these irreducible representations Π_a of $D(S_3)$ (2.61).

Z_2	e	x	Z_3	e	y	y^2
Γ_1	1	1	Γ_1	1	1	1
Γ_{-1}	1	-1	Γ_ω	1	ω	$\bar{\omega}$
			$\Gamma_{\bar{\omega}}$	1	$\bar{\omega}$	ω

Table 2.4: Unitary irreducible representations of Z_2 and Z_3

There are a few things which help in constructing the representations. First, instead of the representations $\Pi(P_h g)$, it is enough to find the separately the representations $\Pi(P_h)$ and $\Pi(g)$. The elements $P_h g \in D(H)$ were interpreted as implementing a global $g \in H$ transformation and subsequently projecting onto the flux eigenstate $|h\rangle$, and the representations should also respect this structure by obeying

$$\Pi_a(P_h g)|k,i\rangle = \Pi_a(P_h)\Pi_a(g)|k,i\rangle, \qquad g \in S_3, h \in C_a, \tag{2.111}$$

where $\Pi_a(P_h)$ forms a representation of the projector algebra in V_a and the matrix $\Pi_a(g)$ fully specifies how the state transforms. The values of h have been restricted to the conjugacy class C_a of H, because other cases would be identically zero. The reason for this is that since arbitrary $g \in S_3$ transformations can not change the superselection sector, one can only project onto those flux eigenstates which span the flux space. In terms of the representations of $D(H)$ this means

$$\Pi_a(P_h g) = \Pi_a(P_h)\Pi_a(g) = 0, \qquad \forall h \notin C_a. \tag{2.112}$$

The second helpful piece of information is that the representations $\Pi(P_h g)$, $h, g \in S_3$ respect the group composition. Since S_3 is generated by the elements x and y, also all the representations should be generated by the representations of the group generators

$$\Pi_a(x^m y^m) = \Pi_a(x^m)\Pi_a(y^m) = (\Pi_a(x))^m (\Pi_a(y))^n . \tag{2.113}$$

Therefore, since the internal spaces V_Γ^C are either one-, two- or three-dimensional, it is enough to find the one-, two- and three-dimensional representations $\Pi(x)$ and $\Pi(y)$. Representations for all other elements can be constructed by multiplying them according to Table 2.1. Third, when forming representations for each superselection sector, there should exist a conjugate representation $\overline{\Pi}_a(g) = \Pi_a^T(g^{-1})$ (2.69) for each representation $\Pi_a(g)$, such that

$$\Pi_a(g)\overline{\Pi}_a(g) = \mathbf{1}, \qquad \forall h, g \in S_3. \tag{2.114}$$

The conjugate representations could be constructed by using the definition of the antipodal map, but there is no specific need for this. Finding the irreducible representations carried by each sector exhausts the model completely. Having found all the representations, one can then check which representations are conjugate and whether there are self-conjugate representations.

M	$V_\Gamma^C = V_C \otimes V_\Gamma$	$\dim(V_C)\cdot\dim(V_\Gamma) = \dim(V_\Gamma^C)$
1	$V_1 \equiv V_1^e$	$1\cdot 1 = 1$
Λ_1	$V_{\Lambda_1} \equiv V_{-1}^e$	$1\cdot 1 = 1$
Λ_2	$V_{\Lambda_2} \equiv V_{-1}^e$	$1\cdot 2 = 2$
Φ_0	$V_{\Phi_0} \equiv V_1^x$	$3\cdot 1 = 3$
Φ_1	$V_{\Phi_1} \equiv V_{-1}^x$	$3\cdot 1 = 3$
Ω_0	$V_{\Omega_0} \equiv V_1^y$	$2\cdot 1 = 2$
Ω_+	$V_{\Omega_+} \equiv V_\omega^y$	$2\cdot 1 = 2$
Ω_-	$V_{\Omega_-} \equiv V_{\bar\omega}^y$	$2\cdot 1 = 2$

Table 2.5: The particle spectrum M of the S_3 anyon model

The different superselection sectors are best discussed separately, but before proceeding, one should choose representations for the bases. The simplest and most convenient choice is to represent the basis states in the two-dimensional spaces V_1^y, V_ω^y and $V_{\bar\omega}^y$ by the column vectors

$$|y\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |y^2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{2.115}$$

and in the three dimensional spaces V_1^x and V_{-1}^x by the column vectors

$$|x\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |xy\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad |xy^2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \tag{2.116}$$

On these bases the projector representations $\Pi_a(P_h)$ are given by the diagonal matrices

$$\Pi^y(P_y) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \Pi^y(P_{y^2}) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.117}$$

$$\Pi^x(P_x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \Pi^x(P_{xy}) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \Pi^x(P_{xy^2}) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{2.118}$$

respectively. Strictly speaking, also the basis in the pure charge space V_2^e is represented similarly as in (2.115), $|1\rangle = (1,0)^T$ and $|2\rangle = (0,1)^T$. However, since the flux part is trivial, one does not apply the projectors P_h in this space.

Consider first the vacuum V_1^e and the spaces V_{-1}^e and V_2^e. Because the flux space is trivial, there is no flux degree of freedom, and every $g \in S_3$ transformation orbit is identical

$$g: \quad |e,i\rangle \to |e,\Gamma(g)i\rangle, \qquad \forall g \in S_3. \tag{2.119}$$

Hence, the representations of $D(S_3)$ coincide exactly with the irreducible representations of S_3

$$\Pi_a^e(g) = \Gamma_a(g), \qquad a = 1, -1, 2, \tag{2.120}$$

which are already given in Table 2.3.

Consider then the three-dimensional spaces V_1^x and V_{-1}^x, with the bases $|k,i\rangle \in V_a^x$, $k \in C_x, a \in \{1,-1\}$. Here the crucial observation is that by using (2.108), the elements $g \in C_x$ can be written in the form (2.28)

$$\begin{aligned} x &= y\ xy &&= y^2\ xy^2, \\ xy &= y\ xy^2 &&= y^2\ x, \\ xy^2 &= y\ x &&= y^2\ xy, \end{aligned} \tag{2.121}$$

whereas for the elements in C_y there is no such decomposition. This means that every $g \in C_x$ can be written as $g = g'\tilde{g}$, where the $\tilde{g} \in N(k)$ part can be implement in the charge space. The representations can then be inferred by considering the following transformation orbits

$$\begin{aligned} x : |xy,i\rangle &\to |xy^2,\Gamma_a(xy)i\rangle \to |xy,\Gamma_a(xy^2)\Gamma_a(xy)i\rangle, \quad |x,i\rangle \to |x,\Gamma_a(x)i\rangle, \\ xy : |x,i\rangle &\to |xy^2,\Gamma_a(x)i\rangle \to |x,\Gamma_a(xy^2)\Gamma_a(x)i\rangle, \quad |xy,i\rangle \to |xy,\Gamma_a(xy)i\rangle, \\ xy^2 : |x,i\rangle &\to |xy,\Gamma_a(x)i\rangle \to |x,\Gamma_a(xy)\Gamma_a(x)i\rangle, \quad |xy^2,i\rangle \to |xy^2,\Gamma_a(xy^2)i\rangle, \end{aligned} \tag{2.122}$$

$$\begin{aligned} y : |x,i\rangle &\to |xy,i\rangle \to |xy^2,i\rangle \to |x,i\rangle, \\ y^2 : |x,i\rangle &\to |xy^2,i\rangle \to |xy,i\rangle \to |x,i\rangle. \end{aligned} \tag{2.123}$$

One can aee that each of the $g \in C_x$ transformations commutes trivially with itself, and thus implements a transformation only in the charge sector, but maps the other two states into each other. Likewise, (2.123) shows how the $g \in C_y$ transformations only cyclically permute the basis states.

Analogously with the treatment above, the representations in the remaining three two-dimensional spaces V_1^y, V_ω^y and $V_{\bar{\omega}}^y$, with the bases $|k,i\rangle \in V_a^y, k \in C_y, a \in \{1,\omega,\bar{\omega}\}$, can be inferred by considering the following $g \in S_3$ transformation orbits

$$\begin{aligned} x : |y,i\rangle &\to |y^2,i\rangle \to |y,i\rangle, \\ xy : |y,i\rangle &\to |y^2,\Gamma_a(y),i\rangle \to |y,\Gamma_a(y^2)i\rangle, \\ xy^2 : |y,i\rangle &\to |y^2,\Gamma_a(y^2),i\rangle \to |y,\Gamma_a(y)i\rangle, \end{aligned} \tag{2.124}$$

$$\begin{aligned} y : |y,i\rangle &\to |y,\Gamma_a(y)i\rangle, \quad |y^2,i\rangle \to |y^2,\Gamma_a(y)i\rangle, \\ y^2 : |y,i\rangle &\to |y,\Gamma_a(y^2)i\rangle, \quad |y^2,i\rangle \to |y^2,\Gamma_a(y^2)i\rangle. \end{aligned} \tag{2.125}$$

This time there is no need to decompose the transformations as in (2.121), because the $g \in C_x$ are already of the desired form with $x \notin N(k)$, but $y, y^2 \in N(k)$. Also, the last two just state the obvious result that y commutes with itself and thus implements a transformation only in the charge space.

The matrix representations $\Pi_a(g), g \in S_3$, implementing the actions (2.119) and (2.122) - (2.125) on the basis states representations (2.115) and (2.116) are shown in Table 2.6. One can see that except for the representations Π_ω^y and $\Pi_{\bar{\omega}}^y$, which are conjugate to each other, all the other are self-conjugate. Recalling that particles transforming in conjugate representations are regarded as anti-particles, one can conclude that in an S_3 anyon model (Table 2.5), the

$\Pi_a(g)$	e	x	xy	xy^2	y	y^2
Π^e_1	1	1	1	1	1	1
Π^e_{-1}	1	-1	-1	-1	1	1
Π^e_2	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \omega \\ \bar{\omega} & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \bar{\omega} \\ \omega & 0 \end{pmatrix}$	$\begin{pmatrix} \bar{\omega} & 0 \\ 0 & \omega \end{pmatrix}$	$\begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}$
Π^x_1	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$
Π^x_{-1}	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$
Π^y_1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Π^y_ω	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \omega \\ \omega & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \bar{\omega} \\ \bar{\omega} & 0 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}$	$\begin{pmatrix} \bar{\omega} & 0 \\ 0 & \bar{\omega} \end{pmatrix}$
$\Pi^y_{\bar{\omega}}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \bar{\omega} \\ \bar{\omega} & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \omega \\ \omega & 0 \end{pmatrix}$	$\begin{pmatrix} \bar{\omega} & 0 \\ 0 & \bar{\omega} \end{pmatrix}$	$\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}$

Table 2.6: The irreducible representations $\Pi(g)$ of $D(S_3)$

$\mathrm{tr}(\Pi_a(P_h g))$		e	x	xy	xy^2	y	y^2
Π^e_1	P_e	1	1	1	1	1	1
Π^e_{-1}	P_e	1	-1	-1	-1	1	1
Π^e_2	P_e	2	0	0	0	-1	-1
$\Pi^x_{1,}$	P_x	1	1	0	0	0	0
	P_{xy}	1	0	1	0	0	0
	P_{xy^2}	1	0	0	1	0	0
Π^x_{-1}	P_x	1	-1	0	0	0	0
	P_{xy}	1	0	-1	0	0	0
	P_{xy^2}	1	0	0	-1	0	0
Π^y_1	P_y	1	0	0	0	1	1
	P_{y^2}	1	0	0	0	1	1
Π^y_ω	P_y	1	0	0	0	ω	$\bar{\omega}$
	P_{y^2}	1	0	0	0	ω	$\bar{\omega}$
$\Pi^y_{\bar{\omega}}$	P_y	1	0	0	0	$\bar{\omega}$	ω
	P_{y^2}	1	0	0	0	$\bar{\omega}$	ω

Table 2.7: The non-zero characters $\mathrm{tr}(\Pi_a(P_h g))$ of $D(S_3)$

particles Ω_+ and Ω_- are anti-particles of each other, $\overline{\Omega}_+ = \Omega_-$, but all other particles are their own anti-particles.

These results can also be inferred from the fusion rules (2.74), which are the real item of interest. To calculate them, one needs the fusion multiplicities N_{ab}^c. They can be obtained by using (2.75), which in the case of S_3 can be written as

$$N_{ab}^c = \frac{1}{6} \sum_{g \in S_3} \sum_{\substack{h \in C_c \\ h' \in C_a}} \mathrm{tr}\left(\Pi_a(P_{h'}g)\right) \mathrm{tr}\left(\Pi_b(P_{h'^{-1}h}g)\right) \mathrm{tr}\left(\Pi_c(P_h g)\right)^* . \tag{2.126}$$

Here one has simplified the expression by using the definition of the comultiplication (2.49) and the trace property $\mathrm{tr}(\Pi_a \otimes \Pi_b(g \otimes h)) = \mathrm{tr}(\Pi_a(g))\mathrm{tr}(\Pi_b(h))$. Also, because of (2.112), the sums over h and h' have been explicitly restricted to values in the conjugacy classes C_a and C_c. Any other values would give identically zero. Having found the representations $\Pi_a(g)$ displayed in Table 2.6, all the representations $\Pi_a(P_h g)$ can be formed by using the property (2.111) and the appropriate projector representations (2.117) or (2.118). To calculate to fusion multiplicities using (2.126), one needs their characters $\mathrm{tr}(\Pi_a(P_h g))$. The ones which are not trivially zero are summarized in Table 2.7. Plugging the characters in (2.126), one obtains the fusion rules (2.74) of the S_3 anyon model:

$$\Pi_1^e \otimes \Pi_1^e = \Pi_1^e, \qquad \Pi_1^e \otimes \Pi_a^b = \Pi_a^b, \quad \forall a, b, \tag{2.127}$$

$$\begin{gathered} \Pi_{-1}^e \otimes \Pi_{-1}^e = \Pi_1^e, \qquad \Pi_{-1}^e \otimes \Pi_2^e = \Pi_2^e, \\ \Pi_2^e \otimes \Pi_2^e = \Pi_1^e \oplus \Pi_{-1}^e \oplus \Pi_2^e, \end{gathered} \tag{2.128}$$

$$\begin{aligned} \Pi_1^x \otimes \Pi_1^x &= \Pi_1^e \oplus \Pi_2^e \oplus \Pi_1^y \oplus \Pi_\omega^y \oplus \Pi_{\bar{\omega}}^y, \\ \Pi_{-1}^x \otimes \Pi_{-1}^x &= \Pi_1^e \oplus \Pi_2^e \oplus \Pi_1^y \oplus \Pi_\omega^y \oplus \Pi_{\bar{\omega}}^y, \\ \Pi_1^x \otimes \Pi_{-1}^x &= \Pi_{-1}^e \oplus \Pi_2^e \oplus \Pi_1^y \oplus \Pi_\omega^y \oplus \Pi_{\bar{\omega}}^y, \end{aligned} \tag{2.129}$$

$$\begin{gathered} \Pi_1^y \otimes \Pi_1^y = \Pi_1^e \oplus \Pi_{-1}^e, \\ \Pi_\omega^y \otimes \Pi_1^y = \Pi_2^e \oplus \Pi_\omega^y, \qquad \Pi_{\bar{\omega}}^y \otimes \Pi_1^y = \Pi_2^e \oplus \Pi_{\bar{\omega}}^y, \\ \Pi_\omega^y \otimes \Pi_\omega^y = \Pi_2^e \oplus \Pi_{\bar{\omega}}^y, \qquad \Pi_{\bar{\omega}}^y \otimes \Pi_{\bar{\omega}}^y = \Pi_2^e \oplus \Pi_\omega^y, \\ \Pi_\omega^y \otimes \Pi_{\bar{\omega}}^y = \Pi_1^e \oplus \Pi_{-1}^e \oplus \Pi_1^y, \end{gathered} \tag{2.130}$$

$$\begin{gathered} \Pi_{-1}^e \otimes \Pi_1^x = \Pi_{-1}^x, \qquad \Pi_{-1}^e \otimes \Pi_{-1}^x = \Pi_1^x, \\ \Pi_{-1}^e \otimes \Pi_1^y = \Pi_1^y, \qquad \Pi_{-1}^e \otimes \Pi_\omega^y = \Pi_\omega^y, \qquad \Pi_{-1}^e \otimes \Pi_{\bar{\omega}}^y = \Pi_{\bar{\omega}}^y, \end{gathered} \tag{2.131}$$

$$\begin{gathered} \Pi_2^e \otimes \Pi_1^x = \Pi_1^x \oplus \Pi_{-1}^x, \qquad \Pi_2^e \otimes \Pi_{-1}^x = \Pi_1^x \oplus \Pi_{-1}^x, \\ \Pi_2^e \otimes \Pi_1^y = \Pi_\omega^y \oplus \Pi_{\bar{\omega}}^y, \qquad \Pi_2^e \otimes \Pi_\omega^y = \Pi_1^y \oplus \Pi_{\bar{\omega}}^y, \qquad \Pi_2^e \otimes \Pi_{\bar{\omega}}^y = \Pi_1^y \oplus \Pi_\omega^y, \end{gathered} \tag{2.132}$$

$$\Pi_{\pm 1}^x \otimes \Pi_1^y = \Pi_1^x \oplus \Pi_{-1}^x, \qquad \Pi_{\pm 1}^e \otimes \Pi_\omega^y = \Pi_1^x \oplus \Pi_{-1}^x, \qquad \Pi_{\pm 1}^e \otimes \Pi_{\bar{\omega}}^y = \Pi_1^x \oplus \Pi_{-1}^x. \tag{2.133}$$

There are a number of general remarks one can make. First, as expected, the trivial sector Π_1^e (2.128) plays the role of the vacuum and all other particles are their own anti-particles except for the particles carrying the conjugate representations Π_ω^y and $\Pi_{\bar{\omega}}^y$ (2.130). Second, all the fusion multiplicities are either zero or one, $N_{ab}^c = 0$ or $1, \forall a, b, c \in M$, meaning there is

no degeneracy associated with the fusion states and thus all the two-particle fusion spaces V_{ab}^{c} (2.78) with a fixed fusion outcome c are one-dimensional. Third, one can notice that some sets of the fusions rules close on themselves meaning that the S_3 fusion algebra has three non-trivial subalgebras (2.90) spanned by the following sets of elements

$$M_1 = \{\Pi_1^e, \Pi_{-1}^e, \Pi_2^e\}, \tag{2.134}$$

$$M_2 = \{\Pi_1^e, \Pi_{-1}^e, \Pi_1^y\}, \tag{2.135}$$

$$M_3 = \{\Pi_1^e, \Pi_{-1}^e, \Pi_2^e, \Pi_1^y, \Pi_\omega^y, \Pi_{\bar{\omega}}^y\}. \tag{2.136}$$

To fully specify the S_3 anyon model, one should find the maps R (2.91) and F (2.93) in all the fusion spaces appearing in the model. However, since for the purposes of the topological quantum computation one can settle with one of the subalgebras, much of this cumbersome work would be in vain. Instead, one should specify the spaces utilized as the computational space and find the matrices representing R and F there. Since this would nearly complete demonstrating the computational power of the anyon model, it is better to move on and consider them in connection with the theory of quantum computation in the topological Hilbert space.

Chapter 3

Quantum Computation in the Topological Hilbert Space

In the previous chapter it was discussed how the representation theory of the quantum double $D(H)$ can be used describe the non-abelian anyons, and how the fusion rules give rise to decoherence-free topological Hilbert spaces. The aim of this chapter is to demonstrate how these topological Hilbert spaces can be utilized as the computational space of a quantum computer. As outlined in the first chapter, the illustration breaks down to *(1)* specifying the computational space $\mathcal{C}$ and showing how qudits are encoded, *(2)* showing how braiding of anyons can simulate quantum gates and *(3)* showing how to perform projective measurements.

To address these problems in more concrete terms, it is useful to anticipate how a quantum computation could be executed in practice. The computational space is initialized by specifying the number, type and relative locations of the particles in the plane. One could consider drawing particle - anti-particle pairs $(a, \bar{a})$, some N particles altogether, out of the vacuum so that the total charge of the system is trivial. The initial state of the system would then reside in $V^1_{a_1 a_2 \ldots a_N}$. The computation is carried out by braiding the anyons in some way, which corresponds to the desired unitary transformations. After the braiding, some or all the anyons are fused together, and observing whether they fuse to vacuum or leave residual particles behind corresponds to the output of the computation.

Anyons arising from the S_3 gauge theory introduced in the last chapter will be used as an example of the theoretical framework for a topological quantum computer. The common features which all topological quantum computer candidate systems should exhibit will be emphasized when encountered, but the discussion is at most illustrative in connection with a particular model. Now, the fusion rules (2.127) - (2.133) of the whole S_3 anyon model are too complicated to serve as an illustrative model. Hence, the simplest fusion subalgebra M_2 (2.135)

$$M_2 = \{1, \Lambda, \Phi\}, \tag{3.1}$$

will be chosen as the model underlying the topological quantum computer. For notational

clarity one has redefined $\Lambda \equiv \Lambda_1$ and $\Phi \equiv \Phi_0$. The respective fusion rules, in the particle notation of fusion algebra 2.76, can be inferred from (2.127) - (2.133)

$$1 \times 1 = 1, \qquad 1 \times \Lambda = \Lambda, \qquad 1 \times \Phi = \Phi, \tag{3.2}$$

$$\Lambda \times \Lambda = 1, \qquad \Lambda \times \Phi = \Phi, \tag{3.3}$$

$$\Phi \times \Phi = 1 + \Lambda, \tag{3.4}$$

The fusion rule for two Φ particles states that this subalgebra is indeed a non-abelian one, because there exist two possible fusion outcomes. Since all the other fusion rules determine the outcomes uniquely, higher dimensional fusion spaces are always carried by Φ particles. Using (3.4) successively gives the fusion rules for a N Φ particles

$$\begin{aligned}
\Phi \times \Phi \times \Phi &= 2\Phi, \\
\Phi \times \Phi \times \Phi \times \Phi &= 2 \cdot 1 + 2\Lambda, \\
\Phi \times \Phi \times \Phi \times \Phi \times \Phi &= 4\Phi, \\
&\cdots \\
(\Phi)^{\times N} &= \begin{cases} 2^{\frac{N-2}{2}} \cdot 1 + 2^{\frac{N-2}{2}}\Lambda, & N \text{ even} \\ 2^{\frac{N-1}{2}}\Phi, & N \text{ odd} \end{cases}
\end{aligned} \tag{3.5}$$

From these one can read off the smallest non-trivial fusion spaces

$$V^{\Phi}_{\Phi^3} \equiv V^{\Phi}_{\Phi\Phi\Phi}, \qquad \dim(V^{\Phi}_{\Phi\Phi\Phi}) = N^{\Phi}_{\Phi^3} = 2, \tag{3.6}$$

$$V^{1}_{\Phi^4} \equiv V^{1}_{\Phi\Phi\Phi\Phi}, \qquad \dim(V^{1}_{\Phi\Phi\Phi\Phi}) = N^{1}_{\Phi^4} = 2, \tag{3.7}$$

$$V^{\Lambda}_{\Phi^3} \equiv V^{\Lambda}_{\Phi\Phi\Phi\Phi}, \qquad \dim(V^{\Lambda}_{\Phi\Phi\Phi\Phi}) = N^{\Lambda}_{\Phi^4} = 2. \tag{3.8}$$

Since one anticipates that the computational space should belong to the vacuum sector, the interest lies particularly in the spaces (3.7), because they could be used to encode a single unit of quantum information. Since the dimension of this space is two, the qubit (1.5) arises naturally as the elementary unit of quantum information.

3.1 The Computational Space

There are a number of general criteria which constrain the identification of the computational space with the fusion spaces. First, the identification should be made such that $\mathcal{C}$ has a decomposition in terms of subspaces $\mathcal{C}^d$ of some dimension $d \geq 2$ (1.7), with d determining the dimension of the qudits to be used. Second, the physics behind the topological Hilbert space constrains the identification further by stating that all the quantum states in the model should belong to the same superselection sector, because otherwise they can not form superpositions [32]. Third, the computational space should include all the states which can be obtained when unitary transformations are performed on the system, i.e. when the particles are braided.

Because the fusion spaces (3.7) are carried by only one types of particles, all the states corresponding to different permutations of the particles are automatically contained therein.

Therefore, as anticipated, one may identify this space with the computational space of a single qubit

$$\mathcal{C}^2 \equiv V^1_{\Phi^4} \simeq V^{\Phi}_{\Phi^3} \simeq \bigoplus_{x\in\{1,\Lambda\}} V^x_{\Phi^2} \otimes V^{\Phi}_{x\Phi} \simeq \bigoplus_{x\in\{1,\Lambda\}} V^x_{\Phi^2} \otimes V^{\Phi}_{x\Phi} \otimes V^1_{\Phi^2}. \tag{3.9}$$

It follows that the computational basis has to be identified with

$$|i\rangle \equiv |\Phi^4; 1, i\rangle \simeq |\Phi^2; x_i\rangle |x_i\Phi; \Phi\rangle, \qquad i = 0, \ldots, N^1_{\Phi^4} - 1 = 0, 1, \tag{3.10}$$

where $x_i \in \{1, \Lambda\}$. Consequently, the m-qubit computational space should then be defined by

$$\mathcal{C} \equiv \left(V^1_{\Phi^4}\right)^{\otimes m}, \tag{3.11}$$

given that such space actually exists in the model, i.e. it corresponds to some fusion space carried by N Φ-particles for some N. Using the standard basis decomposition (2.82) backwards, one can see that $\mathcal{C}$ corresponds in the standard basis to the fusion space

$$\begin{aligned} \mathcal{C} &\equiv \left(V^1_{\Phi^4}\right)^{\otimes m}, \\ &= \left(V^{\Phi}_{\Phi^3}\right)^{\otimes m}, \\ &= \bigoplus_{x_1,\ldots,x_{m-1}=\Phi} V^{x_1}_{\Phi^3} \otimes V^{x_2}_{x_1\Phi^2} \otimes \cdots \otimes V^1_{x_{m-1}\Phi^3}, \\ &\simeq V^1_{\Phi^{2m+2}}, \end{aligned} \tag{3.12}$$

where one has used the observation that the fusion of three Φ-particles, although in two distinct ways, always gives another Φ-particle (3.5). Hence, to encode m qubits, one needs a fusion space carried by $N = 2m+2$ Φ-particles. In general, the dimension of the fusion space carried by N particles can be read off by using the fusion algebra (3.4) successively

$$\begin{array}{r|l} N = & 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ \ldots \\ \hline N^1_{\Phi^N} = & 0\ 1\ 0\ 2\ 0\ 4\ 0\ 8\ 0\ 16\ \ 0\ \ 32\ \ldots \end{array} \tag{3.13}$$

$$\Rightarrow \qquad \dim(V^1_{\Phi^N}) = 2^{\frac{N-2}{2}}, \qquad N \text{ even}, \tag{3.14}$$

which means that the topological Hilbert space grows exponentially with N. Since the fusion multiplicities are zero for all odd N, one can restrict to consider only spaces carried by an even number of particles. This is in line with the anticipated initialization of the quantum computer, where one draws some number of particle - anti-particle pairs out of the vacuum, which implies that one always ends up with an even number of particles.

The basis in $\mathcal{C}$ is given by the tensor product of the computational basis states. Using the decomposition (3.10), an arbitrary m-qubit basis state $|i_1\rangle|i_2\rangle\cdots|i_m\rangle \in \mathcal{C}$ can be expressed in the standard basis of the underlying fusion space $V^1_{\Phi^{2m+2}}$ as

$$\begin{aligned} |i_1\rangle|i_2\rangle\cdots|i_m\rangle &= |\Phi^4; 1, i_1\rangle|\Phi^4; 1, i_2\rangle\cdots|\Phi^4; 1, i_m\rangle, \\ &\simeq |\Phi^2; x_{i_1}\rangle|x_{i_1}\Phi; \Phi\rangle|\Phi^2; x_{i_2}\rangle|x_{i_2}\Phi; \Phi\rangle\cdots|\Phi^2; x_{i_m}\rangle|x_{i_m}\Phi; \Phi\rangle. \end{aligned} \tag{3.15}$$

Since the braiding was defined in the standard basis through the R- and B-moves, (2.102) and (2.103) respectively, they are the decompositions (3.9) and (3.15) which will have to be used to determine to how is braiding in the standard basis related to the unitary transformations in $\mathcal{C}$.

3.2 Braiding and Quantum Gates

To find out how braiding acts in the standard basis of the present model, one should find the R- and F-moves as unitary solutions to the pentagon (2.97) and hexagon (2.100) equations. On the single qubit space $V^1_{\Phi^4} \simeq V^\Phi_{\Phi^3}$, the F-move (2.93) is the map

$$F: \quad \bigoplus_{x\in\{1,\Lambda\}} V^x_{\Phi^2} \otimes V^\Phi_{x\Phi} \to \bigoplus_{x\in\{1,\Lambda\}} V^\Phi_{\Phi x} \otimes V^x_{\Phi^2}, \tag{3.16}$$

which relates two possible bases. Using the second decomposition of (3.9) and considering the two distinct ways (2.95) and (2.96) to implement the transformation

$$\bigoplus_{x\in\{1,\Lambda\}} V^x_{\Phi^2} \otimes V^\Phi_{x\Phi} \otimes V^1_{\Phi^2} \to \bigoplus_{x\in\{1,\Lambda\}} V^1_{\Phi^2} \otimes V^\Phi_{\Phi x} \otimes V^x_{\Phi^2}, \tag{3.17}$$

one can derive the pentagon equation for the model

$$\sum_{y\in\{1,\Lambda\}} \left(F^1_{\Phi^2 y}\right)^\Phi_x \left(F^1_{x\Phi^2}\right)^y_\Phi = \sum_{y,y'\in\{1,\Lambda\}} \left(F^\Phi_{\Phi^3}\right)^{y'}_y \left(F^1_{\Phi y\Phi}\right)^\Phi_\Phi \left(F^\Phi_{\Phi^3}\right)^y_x, \tag{3.18}$$

where $x \in \{1, \Lambda\}$ is now a free index. This polynomial equation states that there are altogether seven different F-moves appearing in the model

$$\{F^1_{\Phi^2 y}, F^1_{y\Phi^2}, F^1_{\Phi y\Phi}, F^\Phi_{\Phi^3}\}_{y=1,\Lambda}. \tag{3.19}$$

However, only one of them, $F^\Phi_{\Phi^3}$, is a genuine matrix, because it is the only one acting in a non-trivial fusion space. As can be seen from the decompositions

$$V^1_{\Phi y\Phi} \simeq V^\Phi_{\Phi y} \otimes V^1_{\Phi\Phi} \simeq V^1_{\Phi\Phi} \otimes V^\Phi_{y\Phi}, \tag{3.20}$$

$$V^1_{\Phi\Phi y} \simeq V^y_{\Phi\Phi} \otimes V^1_{yy} \simeq V^1_{\Phi\Phi} \otimes V^\Phi_{\Phi y}, \tag{3.21}$$

$$V^1_{y\Phi\Phi} \simeq V^\Phi_{y\Phi} \otimes V^1_{\Phi\Phi} \simeq V^1_{yy} \otimes V^y_{\Phi\Phi}, \tag{3.22}$$

all the intermediate fusion spaces are one-dimensional for $\forall y \in \{1, \Lambda\}$. Hence, because of unitarity, the F-moves acting in these spaces have to be proportional to some complex constant of unit norm

$$\left(F^1_{\Phi^2 y}\right)^\Phi_x = a_y \delta_{x,y}, \quad \left(F^1_{x\Phi^2}\right)^y_\Phi = b_y \delta_{x,y}, \quad F^1_{\Phi y\Phi} = c_y, \quad |a_y|^2 = |b_y|^2 = |c_y|^2 = 1 \tag{3.23}$$

for some $a_y, b_y, c_y \in \mathbb{C}$, meaning that these F-moves introduce only overall phases, which are non-physical and can be set to unity, $a_i = b_i = c_i = 1$. The real item of interest is then

the F-move $F^{\Phi}_{\Phi^3}$, which implements an F-move in the computational space of a single qubit. Writing all the indices down, it is represented by a 2×2 unitary matrix,

$$F \equiv F^{\Phi}_{\Phi^3} = \begin{pmatrix} F_{11} & F_{1\Lambda} \\ F_{\Lambda 1} & F_{\Lambda\Lambda} \end{pmatrix}, \tag{3.24}$$

where the components have to satisfy the constraints following from unitarity

$$\begin{cases} |F_{11}|^2 + |F_{1\Lambda}|^2 = 1, \\ |F_{\Lambda\Lambda}|^2 + |F_{\Lambda 1}|^2 = 1, \\ F_{11}(F_{\Lambda 1})^* + F_{1\Lambda}(F_{\Lambda\Lambda})^* = 0. \end{cases} \tag{3.25}$$

Then, simplifying the pentagon equation (3.18) using (3.23), the components are determined as solutions to the polynomial equations

$$\begin{cases} 1 = F_{11}(F_{11} + F_{1\Lambda}) + F_{1\Lambda}(F_{\Lambda 1} + F_{\Lambda\Lambda}) \\ 1 = F_{\Lambda 1}(F_{11} + F_{1\Lambda}) + F_{\Lambda\Lambda}(F_{\Lambda 1} + F_{\Lambda\Lambda}), \end{cases} . \tag{3.26}$$

The set of equations has four types of general solutions

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & e^{i\phi} \\ e^{-i\phi} & 0 \end{pmatrix} \quad \text{and} \quad \pm \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\phi} \\ e^{-i\phi} & -1 \end{pmatrix}, \tag{3.27}$$

where $\phi = [0, 2\pi]$ is an undetermined arbitrary parameter. Of these the three first are trivial in the sense that they only redefine the basis up to some overall phase. Fixing the arbitrary phase by setting $\phi = 0$ and choosing the solution with an overall '+'-sign, the matrix implementing the non-trvial F-move in the standard basis of the model is

$$F = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.28}$$

This solution is of particular interest, because it is the Hadamard gate, which was already encountered as one of the gates in one particular universal gate set (1.20). In the general theory of quantum computation, it is known to implement a canonical basis change [40], and therefore the F-moves in the underlying fusion spaces have in the computational space $\mathcal{C}$ clear interpretations as basis changing unitary gates. Still, it should be kept on mind that F-moves are not physical operations as such, but mathematical tools to tell how do the fusion states look like when studied in a basis other than the standard basis. The genuine physical operation is the braiding, through which one might, or might not be able to implement a transformation of the form (3.28). To show whether this is the case, one should find the matrix representations for the braid group generators.

To find how the braid group acts in the fusion space of the model, one should find the unitary matrices representing the R-moves as solutions to the hexagon equation (2.100), which for the present model reads

$$\sum_{y \in \{1,\Lambda\}} R^{y}_{\Phi\Phi} \left(F^{\Phi}_{\Phi^3}\right)^{y}_{x} R^{x}_{\Phi\Phi} = \sum_{y,y' \in \{1,\Lambda\}} \left(F^{\Phi}_{\Phi^3}\right)^{y'}_{y} R^{\Phi}_{\Phi y} \left(F^{\Phi}_{\Phi^3}\right)^{y}_{x}. \tag{3.29}$$

This time all the $R^{\Phi}_{\Phi y}, y \in \{1, \Lambda\}$, are complex constants with unit norm. This is because the spaces $V^{\Phi}_{\Phi y}$ are one-dimensional, which implies that braiding can only contribute non-physical overall phases, which can again be set to unity. As can be seen from the definition of R-moves (2.91), also $R^{y}_{\Phi\Phi}, y \in \{1, \Lambda\}$ are phases, because there are no fusion degeneracies. However, the fusion space of a single qubit (3.9) is two-dimensional, and the action of braiding depends whether one braids particles which fuse to yield either 1 or Λ [42]. Therefore, these phases are physical and correspond to the eigenvalues of a matrix implementing an R-move in $\mathcal{C}^2$

$$R \equiv \begin{pmatrix} R^{1}_{\Phi\Phi} & 0 \\ 0 & R^{\Lambda}_{\Phi\Phi} \end{pmatrix}. \tag{3.30}$$

Simplifying (3.29) by substituting the elements of F from (3.28), and assuming that R is unitary, the eigenvalues are then determined from the set of equations

$$\begin{cases} \frac{1}{\sqrt{2}}(R^{1}_{\Phi\Phi})^2 + \frac{1}{\sqrt{2}} R^{1}_{\Phi\Phi} R^{\Lambda}_{\Phi\Phi} = 1, \\ -\frac{1}{\sqrt{2}}(R^{\Lambda}_{\Phi\Phi})^2 + \frac{1}{\sqrt{2}} R^{1}_{\Phi\Phi} R^{\Lambda}_{\Phi\Phi} = 1, \\ |R^{\Lambda}_{\Phi\Phi}|^2 = |R^{1}_{\Phi\Phi}|^2 = 1. \end{cases} \tag{3.31}$$

The solutions to these polynomial equations is given by all complex numbers with unit norm obeying the relation

$$(R^{1}_{\Phi\Phi})^2 = e^{i\pi}(R^{\Lambda}_{\Phi\Phi})^2. \tag{3.32}$$

Since all the solutions give a different representation of the same model, the simplest one will be chosen to represent the R-moves in $\mathcal{C}_d$

$$R = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{3.33}$$

This particular matrix appears also in the theory of quantum computation, where it is known as the phase gate S [40].

The R forms a representation of the braid group B_2, the braid group on two strands. To construct the representation of B_N, one needs also a representation of a second generator, which is given in the fusion spaces by a B-move (2.103), which can be constructed according to (2.105). Now, since there is only a single F and a single R acting in $\mathcal{C}^2$, B is given simply by the matrix product

$$B \equiv F^{-1}RF = \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}. \tag{3.34}$$

It can be checked that the R- and B-moves, as represented by (3.33) and (3.34), indeed form the representation of the braid group in $\mathcal{C}^2$, i.e. that they satisfy the Yang-Baxter equation (2.11)

$$RBR = BRB. \tag{3.35}$$

Considering both sides separately, one finds

$$RBR = \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = e^{i\frac{\pi}{4}} F = BRB, \tag{3.36}$$

verifying that (3.35) is indeed satisfied. In addition, as it happens that both sides are proportional to F (3.28), this also demonstrates that F-moves are physically meaningful transformations, which can indeed be implemented by braiding particles.

Another thing to be noticed is

$$R^4 = B^4 = \mathbf{1}, \tag{3.37}$$

which means that one is not dealing with the pure braid group B_N of infinite number of elements, but with a truncated version $B_{N,4}$, i.e. with a group defined by (2.8), (2.9) and an additional relation $\sigma^4 = 1$ [11]. The truncated braid group has a finite number of elements and this sets a limit on the number of different braidings, which could be implemented. For example, the braid group in the fusion space $V_{\Phi^3}^{\Phi}$, which underlies the single qubit space $\mathcal{C}^2$, is $B_{3,4}$, which is freely generated by R and B modulo the relations (3.35) and (3.37). Since braiding is the only tool to perform unitary transformations in $\mathcal{C}$, dealing with truncated braid groups implies that there is also only a limited number of unitary transformations available. However, models with truncated braid groups are not automatically invalid for universal quantum computation since some may generate subgroups which are dense in the unitary group. For instance, even though single qubit unitary transformations are limited to the elements in $B_{3,4}$, even this relatively simple group is of order 96 [11] and it is far from obvious whether it admits universal quantum computation.

Summarizing, all the single qubit operations are given by the elements $b \in B_{3,4}$, which are generated by R and B. Using the universal gate set (1.20) as a reference, the two elementary single qubit quantum gates (1.18) appearing in the model, up to an overall phase, can be chosen to correspond to the braids $\{R, RBR\}$

$$R : |i\rangle \mapsto T^2|i\rangle, \tag{3.38}$$

$$RBR : |i\rangle \mapsto H|i\rangle \tag{3.39}$$

Unfortunately, such a model is not universal for quantum computation. Even though the Hadamard gate H can be realized, instead of the $\frac{\pi}{8}$-phase gate T, one can only produce the phase gate $R = T^2$. Because R and B are the physical braid group generators arising as the solutions to the pentagon and hexagon equations, they are the most elementary unitary transformations implementable implemented on the system. There can not exist a $T \in B_{3,4}$, because then R could be decomposed as two successive even more elementary operations T, which should satisfy the pentagon and hexagon equations. However, no such solutions were obtained and thus even without considering the entangling gates arising through braiding anyons, it can be concluded that the fusion subalgebra (3.1) of the full S_3 anyon model does not admit universal quantum computation.

3.3 Fusion as Projective Measurement

To complete the demonstration of quantum computation in the topological Hilbert spaces, one should show how to perform projective measurements. By braiding the particles one could produce unitary transformations on the system, but no information about the state of the system could be obtained in this way. The topological robustness ensures that the quantum information is not only protected from decoherence, but also well hidden from any outside observer. To get any information out of the fusion space, one must break the topological protection by fusing some or all the particles together. The information residing in the topological Hilbert space can then be inferred by observing the outcome, which is either a Λ particle or the vacuum 1. In the first case one should not observe anything whereas in the second case the annihilation produces photons, which carry the combined energy of the fused particles, and which could be easily detected by conventional means. Because there are only these two possibilities, the outcome of the fusion can be unambiguously deduced.

Since one has identified the computational basis with the different fusion outcomes (3.10), determining outcome is equivalent to projecting onto the computational basis. More precisely, the fusion of the two left-most of the four Φ particles realizing the qubit, and the observation of the outcome $x_i \in \{1, \Lambda\}$, i.e. either photons or nothing, is equivalent to applying a projector $P_i = |i\rangle\langle i|$ in $\mathcal{C}^2$

$$x_i : \quad |\psi\rangle \to P_i|\psi\rangle, \qquad |\psi\rangle \in \mathcal{C}^2. \tag{3.40}$$

Comparing this to (1.25), it can be seen that this exactly of the type of correspondence between the physical system and the computational space one set out to look for. Projections onto m-qubit computational space $\mathcal{C}$ can be realized in a similar manner by fusing sequentially from left to right all the $2m+2$ particles. Observing the outcome of each fusion is equivalent to recording the string $x_{i_1}x_{i_2}\cdots x_{i_m}$, which in the in the computational space translates into the projector

$$x_{i_1}x_{i_2}\cdots x_{i_m} : \quad |\psi\rangle \to P_{i_1} \otimes P_{i_2} \otimes \cdots \otimes P_{i_m}|\psi\rangle, \qquad |\psi\rangle \in \mathcal{C}. \tag{3.41}$$

The discussed model offers also a natural measurements on a certain superposition state. The only non-trivial F-move, which relates the two possible bases in the fusion space underlying the qubit (3.9), was solved and found to have the form (3.28). This form was recognized as the Hadamard gate H acting on basis states as (1.20). Because the computational basis was identified exactly with the standard basis, the basis $|\tilde{i}\rangle$ corresponding to fusing the particles from right to left can be expressed in terms of the standard basis by using the F-move

$$|\tilde{i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |\tilde{i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{3.42}$$

Therefore, depending whether photons are observed or not, fusing the two right most particles corresponds to applying the projector $P_{\tilde{i}} = |\tilde{i}\rangle\langle\tilde{i}|$, i.e. projecting in $\mathcal{C}$ onto either of the states $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

For performing projective measurements at the end of the computation, one needs only to consider the fusion of neighboring particles: Fusion of non-neighboring particles would first require braiding which implies a transformation on the system. Therefore, projections onto the computational basis (3.9) take in the presented model always either of the two forms (3.40) or (3.42). The scheme of using fusion to perform projective measurements works well, because there are only possible outcomes, which can be unambiguously distinguished. In more complicated models, i.e. in ones with multiple non-vacuum fusion outcomes, one might want more flexibility and control over the measurement procedure. Such can be provided by the use of quantum interference experiments, which can be used to distinguish between various different quasiparticles. For the case of non-abelian anyons, such experiments have been discussed in detail in [41], but for the present model they offer no additional control and need not be considered here.

Conclusions

It is perhaps a bit of an anti-climax that after investing much effort in obtaining an adequate understanding for considering quantum computation with anyons, the chosen model turns out not to be universal for quantum computation. Actually, without even calculating the braid group representations R and B, the non-universality of the model could have been immediately inferred from the structure of the fusion subalgebra (3.1). These rules are known describe a so called Ising anyons, arising from $SU(2)_2$ Chern-Simons theories [42], whose application to quantum computation has been considered in detail in [7] and [22], because they describe as an effective field theory the topological excitations which are expected to be found in $\nu = 5/2$ fractional Quantum Hall systems. As demonstrated, these particular anyons do not admit universal quantum computation through purely topological means, i.e. by relying only on braiding to produce unitary transformations. However, even with this severe imperfection, they are at the present knowledge the best candidate for a topological quantum computer, and various supplementary non-topological [6], or even topology altering operations [21] have been suggested for promoting these anyon systems to the status of a universal quantum computer. If an anyon system based on the gauge group S_3 can ever be realized, in principle, these same supplementary operations could be used to overcome the non-universality provided by pure braiding.

It is a small consolation that the presented model is not totally useless for topological quantum computation. However, it is not the search for new implementational platforms which has been the objective in this thesis, but the presentation of the anyonic systems, their properties and use as topological quantum computers in as physically motivated and illustrative manner as possible. Apart from John Preskill's exemplary lecture notes [42], there are hardly any accessible introductions to the theory of topological quantum computation. Most of the contemporary research papers tackle the theory of topological quantum computation in terms of mathematics of the most abstract kind and often without any obvious connection to actual physical systems. Even though the mathematical rigor is formidable, such an abstract approach can be very discouraging for newcomers in the field. Therefore, rooting the anyon model in gauge theories and taking the time to argue for the emergence of the fusion spaces were personal choices for addressing the problem in terms more familiar to physicists, and hopefully thereby providing an accessible introduction to the basic concepts of topological quantum computation. Once one got to the fusion spaces, the general theory covered here

has much in common with [42], but topics which were found confusing or lacking in physical explanation have now been attempted to be presented in more detail. It is because of this illustrative approach that one also chose as an example a model, which was known not to be universal for quantum computation, but which allowed explicit calculations to be carried out with the most transparency.

However, it should be pointed out that the potential contribution to quantum computation of the anyon model based on the quantum double $D(S_3)$ was not exhausted by the demonstration that the subalgebra spanned by the particles M_2 (2.135) does not admit universal quantum computation. There were also two other fusion subalgebras M_1 (2.134) and M_3 (2.136), and ultimately the full fusion algebra (2.127) - (2.133), whose properties were not investigated. The last two are likely to contain too many particles for any realizable efficient practical implementation, but the braiding properties the particles spanning M_1, however, could well be worth a closer investigation. The reason is that their fusion subalgebra (2.128) closely resembles the fusion rules of the so called Fibonacci anyons, whose braiding properties are known to be universal for quantum computation [42]. It could be an interesting topic of further research to study whether the braiding properties of the particles in M_1 allow universal quantum computation.

Another open question, although more on the technical side, is the construction of the representations of arbitrary braid group generators out of the R- and F-moves. In the present work only two braid group generators R and B were considered, because it was already found based on single qubit transformations that the model is not universal for quantum computation. If entangling gates would have been considered, one should have constructed the representations of all the four braid group generators in the space $V_{\Phi^5}^{\Phi}$ underlying the two-qubit space. In principle, all the representations should be constructable out of the R- and F-moves, but nowhere in the literature was it discussed how this is done in practice. On the other hand, there have been attempts to find all the four-dimensional unitary representations of the braid group [48], i.e. potential two-qubit gates, but even though these studies constrain the form of the representations, they say nothing about their availability in a given anyon system. Therefore, it could be another topic of further research to develop methods for constructing a representation of an arbitrary braid group generator on a given fusion space.

Bibliography

[1] Y. Aharonov and D. Bohm. Significance of electromagnetic potentials in the quantum theory. *Phys. Rev.*, 115, 1959.

[2] F. A. Bais and C. J. M. Mathy. The breaking of quantum double symmetries by defect condensation, 2006. arXiv: cond-mat/0602115.

[3] F.A. Bais, P. van Driel, and M. de Wild Propitius. Quantum symmetries in discrete gauge theories. *Phys. Lett. B*, 280:63, 1992. arXiv: hep-th/9203046.

[4] F.A. Bais, P. van Driel, and M. de Wild Propitius. Anyons in discrete gauge theories with Chern-Simons terms. *Nucl. Phys. B*, 393:547, 1993. arXiv: hep-th/9203047.

[5] R.J. Baxter. *Exactly Solved Models in Statistical Mechanics*. Academic Press, London, 1982.

[6] Sergei Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Physical Review A*, 71:022316, 2005. arXiv: quant-ph/0403025.

[7] Sergey Bravyi. Universal quantum computation with the $\nu = 5/2$ fractional quantum hall states, 2005. arXiv: quant-ph/0511178.

[8] G. Brennen, D. Leary, and S. Bullock. Criteria for exact qudit universality. *Phys. Rev. A*, 71:052318, 2005. arXiv: quant-ph/0407223.

[9] J.L. Brylinski and R. Brylinski. Universal quantum gates. In R. Brylinski and G. Chen, editors, *Mathematics of Quantum Computation*. Chapman and Hall / CRC Press, Florida, 2002. arXiv: quant-ph/0108062.

[10] Graham P. Collins. Computing with quantum knots. *Scientific American*, 294(4):56–63, April 2006.

[11] M. de Wild Propitius and F.A. Bais. Discrete gauge theories, 1995. arXiv: hep-th/9511201.

[12] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *J. Math. Phys.*, 43:4452, 2002. arXiv: quant-ph/0110143.

[13] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400:97–117, 1985. http://www.qubit.org/oldsite/resource/deutsch85.pdf.

[14] David P DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 51:1015, 1995. arXiv: cond-mat/9407022.

[15] B. Doucot, L.B. Ioffe, and J. Vidal. Discrete non-abelian gauge theories in josephson-junction arrays and quantum computation. *Phys. Rev. B*, 69:214501, 2004. arXiv: cond-mat/0302104.

[16] L.M. Duan, E. Demler, and M.D. Lukin. Controlling spin exchange interactions of ultracold atoms in optical lattices. *Phys. Rev. Lett.*, 91:090402, 2003. arXiv: cond-mat/0210564.

[17] Richard P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467, 1982.

[18] M.H. Freedman, A. Kitaev, M.J. Larsen, and Z. Wang. Topological quantum computation. *Bull. Amer. Math. Soc.*, 40:31, 2004. arXiv: quant-ph/0101025.

[19] M.H. Freedman, A. Kitaev, and Z. Wang. Simulation of topological field theories by quantum computers. *Comm. Math. Phys.*, 227(3):587 – 603, 2002. arXiv: quant-ph/0001071.

[20] Michael Freedman, Michael Larsen, and Zhenghan Wang. A modular functor which is universal for quantum computation, 2000. arXiv: quant-ph/0001108.

[21] Michael Freedman, Chetan Nayak, and Kevin Walker. Tilted interferometry realizes universal quantum computation in the ising tqft without overpasses, 2005. arXiv: cond-mat/0512072.

[22] Michael Freedman, Chetan Nayak, and Kevin Walker. Towards universal topological quantum computation in the $\nu = 5/2$ fractional quantum hall state, 2005. arXiv: cond-mat/0512066.

[23] Michael H. Freedman and Alexei Kitaev. Topological quantum computation. a talk given at the KITP seminar *Exotic Order and Criticality in Quantum Matter* (mar 29 - jul 2, 2004). http://online.kitp.ucsb.edu/online/exotic04/.

[24] J. Fuchs and C. Schweigert. *Symmetries, Lie Algebras and Representations*. Cambridge University Press, Cambridge, 1997.

[25] Daniel Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *Chaos Solitons Fractals*, 10:1749, 1999. arXiv: quant-ph/9802007.

[26] S.J. Lomonaco Jr. An entangled tale of quantum entanglement. In S.J. Lomonaco Jr., editor, *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, volume 58 of *Proceedings of Symposia in Applied Mathematics*. American Mathematical Society, 2002. http://www.csee.umbc.edu/∼lomonaco/ams/Lecture_Notes.html.

[27] L.H. Kauffman. Quantum topology and quantum computation. In S.J. Lomonaco Jr., editor, *Qauntum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, volume 58 of *Proceedings of Symposia in Applied Mathematics*. American Mathematical Society, 2002. http://www.csee.umbc.edu/∼lomonaco/ams/Lecture_Notes.html.

[28] L.H. Kauffman and S.J. Lomonaco Jr. Quantum entanglement and topological entanglement. *New Journal of Physics*, 4:73, October 2002.

[29] L.H. Kauffman and S.J. Lomonaco Jr. Entanglement criteria - quantum and topological. In Pinch and Brandt, editors, *Quantum Information and Computation - Spie Proceedings, 21-22 April, 2003, Orlando, FL*, volume 5105, pages 51–58, 2003. arXiv: quant-ph/0304091.

[30] L.H. Kauffman and S.J. Lomonoco Jr. Braiding operators are universal quantum gates. *New Journal of Physics*, 6(134), October 2004. arXiv: quant-ph/0401090.

[31] A.Y. Kitaev. Fault-tolerant quantum computation by anyons. *Annals. Phys.*, 303:3–20, 2002. arXiv: quant-ph/9707021.

[32] A.Y. Kitaev. Anyons in an exactly solved model and beyond, 2005. arXiv: cond-mat/0506438.

[33] Shahn Majid. *Foundations of Quantum Group Theory*. Cambridge University Press, Cambridge, 1995.

[34] C. Mochon. Anyon computers with smaller groups. *Phys. Rev. A*, 69:032306, 2004. arXiv: quant-ph/0306063.

[35] C. Montonen. The many-anyon problem, 1994. Lectures at the VI Mexican Summer School of Particles and Fields, arXiv:quant-ph/9502071.

[36] G. Moore and N. Read. Nonabelions in the fractional quantum hall effect. *Nucl. Phys.*, B360:362, 1991.

[37] Chetan Nayak and Frank Wilczek. $2n$ quasihole states realize 2^{n-1}-dimensional spinor braiding statistics in paired quantum hall states. *Nucl. Phys.*, B479:529, 1996. arXiv: cond-mat/9605145.

[38] M.A. Nielsen. *Quantum Information Science.* PhD thesis, University of New Mexico, 1998.

[39] M.A. Nielsen. Quantum information science and complex quantum systems, 2002. arXiv: quant-ph/0210005.

[40] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[41] B. J. Overbosch and F. A. Bais. Inequivalent classes of interference experiments with non-abelian anyons. *Phys. Rev. A*, 68:062107, 2001.

[42] J. Preskill. Lecture notes for a course of quantum computation. http://www.theory.caltech.edu/ preskill/ph219/.

[43] J. Preskill. Fault-tolerant quantum computation, 1997. arXiv: quant-ph/9712048.

[44] R. Rodriguez and J.K. Pachos. Conditional Aharonov-Bohm phases with double quantum dots, 2004. arXiv: quant-ph/0405071.

[45] S. Das Sarma, M. Freedman, and C. Nayak. Topologically-protected qubits from a possible non-abelian fractional quantum Hall state. *Physical Review Letters*, 94:166802, 2005. arXiv: cond-mat/0412343.

[46] Alexander Yu Vlasov. Noncommutative tori and universal sets of non-binary quantum gates, 2002. arXiv: quant-ph/0012009.

[47] F. Wilczek, editor. *Fractional Statistics and Anyon Superconductivity.* World Scientific, Singapore, 1990.

[48] Y. Zhang, L.H. Kauffman, and M-L. Ge. Yang-Baxterizations, universal quantum gates and hamiltonians. *Quantum Information Processing*, 4:159, 2005. arXiv: quant-ph/0502015.