Topological Quantum Computation

Zhenghan Wang

Microsoft Research Station Q, CNSI Bldg Rm 2237, University of California, Santa Barbara, CA 93106-6105, U.S.A.
E-mail address: zhenghwa@microsoft.com

2010 *Mathematics Subject Classification.* Primary 57-02, 18-02; Secondary 68-02, 81-02

Key words and phrases. Temperley-Lieb category, Jones polynomial, quantum circuit model, modular tensor category, topological quantum field theory, fractional quantum Hall effect, anyonic system, topological phases of matter

To my parents, who gave me life.
To my teachers, who changed my life.
To my family and Station Q, where I belong.

Contents

x

Preface

The factors of any integer can be found quickly by a quantum computer. Since P. Shor discovered this efficient quantum factoring algorithm in 1994 [**S**], people have started to work on building these new machines. As one of those people, I joined Microsoft Station Q in Santa Barbara to pursue a topological approach in 2005. My dream is to braid non-abelian anyons. So long hours are spent picturing quasiparticles in fractional quantum Hall liquids. From my UCSB office, I often see small sailboats on the Pacific. Many times I am lost in thought imagining that they are anyons and the ocean is an electron liquid. Then to carry out a topological quantum computation is as much fun as jumping into such small sailboats and steering them around each other.

Will we benefit from such man-made quantum systems besides knowing factors of large integers? A compelling reason comes from R. Feynman: a quantum computer is an efficient universal simulator of quantum mechanics [**Fe82**]. Later, an efficient simulation of topological quantum field theories was given by M. Freedman, A. Kitaev, and the author [**FKW**]. These results support the idea that quantum computers can efficiently simulate quantum field theories, though rigorous results depend on mathematical formulations of quantum field theories. So quantum computing literally promises us a new world. More speculatively, while the telescope and microscope have greatly extended the reach of our eyes, quantum computers would enhance the power of our brains to perceive the quantum world. Would it then be too bold to speculate that useful quantum computers, if built, would play an essential role in the ontology of quantum reality?

Topological quantum computation is a paradigm to build a large scale quantum computer based on topological phases of matter. In this approach, information is stored in the lowest energy states of many-anyon systems and processed by braiding non-abelian anyons. The computational answer is accessed by bringing anyons together and observing the result. Topological quantum computation stands uniquely at the interface of quantum topology, quantum physics, and quantum computing, enriching all three subjects with new problems. The inspiration comes from two seemingly independent themes which appeared around 1997. One was Kitaev's idea of fault-tolerant quantum computation by anyons [**Ki1**], and the other was Freedman's program to understand the computational power of topological quantum field theories [**Fr1**]. It turns out that these ideas are two sides of the same coin: the algebraic theory of anyons and the algebraic data of a topological quantum field theory are both modular tensor categories. The synthesis of the two ideas ushered in topological quantum computation. The topological quantum computation model is efficiently equivalent to other models of quantum computation such as the quantum circuit model in the sense that all models solve the same class of problems in polynomial time [**FKLW**].

Besides its theoretical esthetic appeal, the practical merit of the topological approach lies in its error-minimizing hypothetical hardware: topological phases of matter are fault-avoiding or deaf to most local noises. There exist semi-realistic local model Hamiltonians whose ground states are proven to be error-correction codes such as the celebrated toric code. It is an interesting question to understand if fault-avoidance will survive in more realistic situations, such as at finite temperatures or with thermal fluctuations. Perhaps no amount of modeling can be adequate for us to understand completely Mother Nature, who has repeatedly surprised us with her magic.

We do not have any topological qubits yet. Since scalability is not really an issue in topological quantum computation—rather, the issue is controlling more anyons in the system—it follows that demonstrating a single topological qubit is very close to building a topological quantum computer. The most advanced experimental effort to build a topological quantum computer at this writing is fractional quantum Hall quantum computation. There is both experimental and numerical evidence that non-abelian anyons exist in certain 2-dimensional electron systems that exhibit the fractional quantum Hall effect. Other experimental realizations are conceived in systems such as rotating bosons, Josephson junction arrays, and topological insulators.

This book expands the plan of the author's 2008 NSF-CBMS lectures on knots and topological quantum computing, and is intended as a primer for mathematically inclined graduate students. With an emphasis on introduction to basic notions and current research, the book is almost entirely about the mathematics of topological quantum computation. For readers interested in the physics of topological quantum computation with an emphasis on fractional quantum Hall quantum computing, we recommend the survey article [**NSSFD**]. The online notes of J. Preskill [**P**] and A. Kitaev's two seminal papers [**Ki1, Ki2**] are good references for physically inclined readers. The book of F. Wilczek [**Wi2**] is a standard reference for the physical theory of anyons, and contains a collection of reprints of classical papers on the subject.

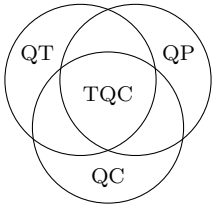
The CBMS conference gave me an opportunity to select a few topics for a coherent account of the field. No efforts have been made to be exhaustive. The selection of topics is personal, based on my competence. I have tried to cite the original reference for each theorem along with references which naturally extend the exposition. However, the wide-ranging and expository nature of this monograph makes this task very difficult if not impossible. I apologize for any omission in the references.

The contents of the book are as follows: Chapters 1,2,4,5,6 are expositions, in some detail, of Temperley-Lieb-Jones theory, the quantum circuit model, ribbon fusion category theory, topological quantum field theory, and anyon theory, while Chapters 3,7,8 are sketches of the main results on selected topics. Chapter 3 is on the additive approximation of the Jones polynomial, Chapter 7 is on the universality of certain anyonic quantum computers, and Chapter 8 is on mathematical models of topological phases of matter. Finally, Chapter 9 lists a few open problems. Chapters 1,2,3 give a self-contained treatment of the additive approximation algorithm. Moreover, universal topological quantum computation models can be built from some even half theories of Jones algebroids such as the Fibonacci theory

[**FLW1**]. Combining the results together, we obtain an equivalence of the topological quantum computation model with the quantum circuit model. Chapters 1,2,3, based on graphical calculus of ribbon fusion categories, are accessible to entry-level graduate students in mathematics, physics, or computer science. A ribbon fusion category, defined with 6j symbols, is up to equivalence just some point on a real algebraic variety of polynomial equations. Therefore the algebraic theory of anyons is elementary, given basic knowledge of surfaces and their mapping class groups of invertible self transformations up to deformation.

Some useful books on related topics are: for mathematics, Bakalov-Kirillov [**BK**], Kassel [**Kas**], Kauffman-Lins [**KL**], and Turaev [**Tu**]; for quantum computation, Kitaev-Shen-Vyalyi [**KSV**] and Nielsen-Chuang [**NC**]; and for physics, Altland-Simons [**AS**], Di Francesco-Mathieu-Senechal [**DMS**], and Wen [**Wen7**].

Topological quantum computation sits at the triple juncture of quantum topology, quantum physics, and quantum computation:



The existence of topological phases of matter with non-abelian anyons would lead us to topological quantum computation via unitary modular tensor categories.

$$\text{TPM} \longrightarrow \text{UMTC} \longrightarrow \text{TQC}$$

Therefore the practical aspect of topological quantum computation hinges on the existence of non-abelian topological states.

Will we succeed in building a large-scale quantum computer? Only time will tell. To build a useful quantum computer requires unprecedented precise control of quantum systems, and complicated dialogues between the classical and quantum worlds. Though Nature seems to favor simplicity, she is also fond of complexity as evidenced by our own existence. Therefore there is no reason to believe that she would not want to claim quantum computers as her own.

Zhenghan Wang
Station Q, Santa Barbara

Acknowledgments

I would like to thank CBMS and NSF for sponsoring the conference; C. Simmons and J. Byrne for the excellent organization; and A. Basmajian, W. Jaco, E. Rowell, and S. Simon for giving invited lectures. It was a pleasure to lecture on an emerging field that is interdisciplinary and still rapidly developing. Over the years I have had the good fortune to work with many collaborators in mathematics and physics, including M. Freedman, A. Kitaev, M. Larsen, A. Ludwig, C. Nayak, N. Read, K. Walker, and X.-G. Wen. Their ideas on the subject and other topics strongly influence my thinking, especially M. Freedman. He and I have been collaborating ever since I went to UCSD to study under him two decades ago. His influence on me and the field of topological quantum computation cannot be overstated. I also want to thank M. Fisher. Though not a collaborator, repeating his graduate course on condensed matter physics and having many questions answered by him, I started to appreciate the beautiful picture of our world painted with quantum field theory, and to gain confidence in physics. He richly deserves of my apple. In the same vein, I would like to thank V. Jones for bringing me to his mathematical world, and his encouragement. Jones's world is home to me. Last but not least, I would like to thank J. Liptrap for typesetting the book and correcting many errors, and D. Sullivan for smoothing the language of the Preface. Of course, errors that remain are mine.

CHAPTER 1

Temperley-Lieb-Jones Theories

This chapter introduces Temperley-Lieb, Temperley-Lieb-Jones, and Jones algebroids through planar diagrams. Temperley-Lieb-Jones (TLJ) algebroids generalize the Jones polynomial of links to colored tangles. Jones algebroids, semisimple quotients of TLJ algebroids at roots of unity, are the prototypical examples of ribbon fusion categories (RFCs) for application to TQC. Some of them are conjectured to algebraically model anyonic systems in certain fractional quantum Hall (FQH) liquids, with Jones-Wenzl projectors (JWPs) representing anyons. Our diagrammatic treatment exemplifies the graphical calculus for RFCs. Special cases of Jones algebroids include the Yang-Lee, Ising, and Fibonacci theories.

Diagrammatic techniques were used by R. Penrose to represent angular momentum tensors and popularized by L. Kauffman's reformulation of the Temperley-Lieb algebras. Recently they have witnessed great success through V. Jones's planar algebras and K. Walker's blob homology.

1.1. Generic Temperley-Lieb-Jones algebroids

The goal of this section is to define the generic Jones representations of the braid groups by showing that the generic Temperley-Lieb (TL) algebras are direct sums of matrix algebras. Essential for understanding the structure of the TL algebras are the Markov trace and the Jones-Wenzl idempotents or JWPs. We use the magical properties of the JWPs to decompose TL algebras into matrix algebras. Consequently we obtain explicit formulas for the Jones representations of the braid groups.

1.1.1. Generic Temperley-Lieb algebroids.

DEFINITION 1.1. *Let $\mathbb{F}$ be a field. An $\mathbb{F}$-algebroid Λ is a small $\mathbb{F}$-linear category. Recall that a category Λ is small if its objects, denoted as Λ^0, form a set, rather than a class. A category is $\mathbb{F}$-linear if for any $x, y \in \Lambda^0$ the morphism set $\mathrm{Hom}(x, y)$ is an $\mathbb{F}$-vector space, and for any $x, y, z \in \Lambda^0$ the composition map*

$$\mathrm{Hom}(y, z) \times \mathrm{Hom}(x, y) \to \mathrm{Hom}(x, z)$$

is bilinear. We will denote $\mathrm{Hom}(x, y)$ sometimes as ${}_x\Lambda_y$.

The term "$\mathbb{F}$-algebroid" [**BHMV**] emphasizes the similarity between an $\mathbb{F}$-linear category and an $\mathbb{F}$-algebra. Indeed, we have:

PROPOSITION 1.2. *Let Λ be an $\mathbb{F}$-algebroid. Then for any $x, y \in \Lambda^0$, ${}_x\Lambda_x$ is an $\mathbb{F}$-algebra and ${}_x\Lambda_y$ is a ${}_y\Lambda_y - {}_x\Lambda_x$ bimodule.*

The proof is left to the reader, as we will do most of the time in the book. It follows that an $\mathbb{F}$-algebroid is a collection of algebras related by bimodules. In the

following, when $\mathbb{F}$ is clear from the context or $\mathbb{F} = \mathbb{C}$, we will refer to an $\mathbb{F}$-algebroid just as an algebroid.

Let A be an indeterminant over $\mathbb{C}$, and $d = -A^2 - A^{-2}$. We will call A the Kauffman variable, and d the loop variable. Let $\mathbb{F}= \mathbb{C}[A, A^{-1}]$ be the quotient field of the ring of polynomials in A. Let $I = [0, 1]$ be the unit interval, and $\mathcal{R} = I \times I$ be the square in the plane. The generic Temperley-Lieb (TL) algebroid $\mathrm{TL}(A)$ is defined as follows. An object of $\mathrm{TL}(A)$ is the unit interval with a finite set of points in the interior of I, allowing the empty set. The object I with no interior points is denoted as $\mathbf{0}$. We use $|x|$ to denote the cardinality of points in x for $x \in \mathrm{TL}(A)^0$. Given $x, y \in \mathrm{TL}(A)^0$, the set of morphisms $\mathrm{Hom}(x, y)$ is the following $\mathbb{F}$-vector space:

If $|x| + |y|$ is odd, then $\mathrm{Hom}(x, y)$ is the 0-vector space. If $|x| + |y|$ is even, first we define an (x, y)-TL diagram. Identify x with the bottom of $\mathcal{R}$ and y with the top of $\mathcal{R}$. A TL-diagram or just a diagram D is the square $\mathcal{R}$ with a collection of $\frac{|x|+|y|}{2}$ smooth arcs in the interior of $\mathcal{R}$ joining the $|x| + |y|$ points on the boundary of $\mathcal{R}$ plus any number of smooth simple closed loops in $\mathcal{R}$. All arcs and simple loops are pairwise non-intersecting, and moreover, all arcs meet the boundary of $\mathcal{R}$ perpendicularly. Note that when $|x| = |y| = 0$, TL diagrams are just disjoint simple closed loops in $\mathcal{R}$, including the empty diagram. The square with the empty diagram is denoted by $\mathbf{1}_0$. For examples, see the diagrams below.

Two diagrams D_1, D_2 are d-isotopic if they induce the same pairing of the $|x| + |y|$ boundary points (Fig. 1.1). Note that D_1, D_2 might have different numbers of simple closed loops. Finally, we define $\mathrm{Hom}(x, y)$ to be the $\mathbb{F}$-vector space with basis the set of (x, y)-TL diagrams modulo the subspace spanned by all elements of the form $D_1 - d^m D_2$, where D_1 is d-isotopic to D_2 and m is the number of simple closed loops in D_1 minus the number in D_2. Note that any diagram D in $\mathrm{Hom}(\mathbf{0}, \mathbf{0})$ is d-isotopic to the empty diagram. Hence a diagram D with m simple closed loops as a vector is equal to $d^m \mathbf{1}_0$.

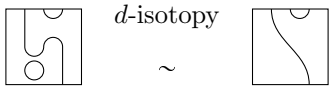


FIGURE 1.1. d-isotopic diagrams.

Composition of morphisms is given first for diagrams. Suppose D_1, D_2 are diagrams in $\mathrm{Hom}(y, z)$ and $\mathrm{Hom}(x, y)$, respectively. The composition of D_1 and D_2 is the diagram $D_1 D_2$ in $\mathrm{Hom}(x, z)$ obtained by stacking D_1 on top of D_2, rescaling the resulting rectangle back to $\mathcal{R}$, and deleting the middle horizontal line (Fig. 1.2).

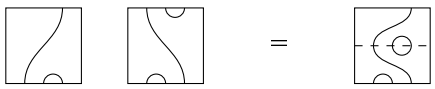


FIGURE 1.2. Composition of diagrams.

Composition preserves d-isotopy, and extends uniquely to a bilinear product

$$\mathrm{Hom}(y, z) \times \mathrm{Hom}(x, y) \to \mathrm{Hom}(x, z).$$

We are using the so-called optimistic convention for diagrams: diagrams are drawn from bottom to top. A general morphism $f \in \mathrm{Hom}(x, y)$ is a linear combination of TL diagrams. We will call such f a formal diagram.

Notice that all objects x of the same cardinality $|x|$ are isomorphic. We will not speak of natural numbers as objects in $\mathrm{TL}(A)$ because they are used later to denote objects in Temperley-Lieb-Jones categories. We will denote the isomorphism class of objects x with $|x| = n$ by 1^n. By abuse of notation, 1^n will be considered as an object.

1.1.2. Generic TL algebras.

DEFINITION 1.3. *Given a natural number $n \in \mathbb{N}$, the generic* TL *algebra* $\mathrm{TL}_n(A)$ *is just the algebra* $\mathrm{Hom}(1^n, 1^n)$ *in the generic* TL *algebroid. Obviously* $\mathrm{TL}_n(A)$ *is independent of our choice of the realization of* 1^n *as an object x such that* $|x| = n$. *By definition* $\mathrm{Hom}(\mathbf{0}, \mathbf{0}) = \mathbb{F}$.

DEFINITION 1.4. *The Markov trace of* $\mathrm{TL}_n(A)$ *is an algebra homomorphism* $\mathrm{Tr} : \mathrm{TL}_n(A) \to \mathbb{F}$ *defined by a tracial closure: choosing n disjoint arcs outside the square $\mathcal{R}$ connecting the bottom n points with their corresponding top points, for a TL diagram D, after connecting the $2n$ boundary points with the chosen n arcs and deleting the boundary of $\mathcal{R}$, we are left with a collection of disjoint simple closed loops in the plane. If there are m of them, we define* $\mathrm{Tr}(D) = d^m$ (*Fig.* 1.3). *For a formal diagram, we extend the trace linearly.*

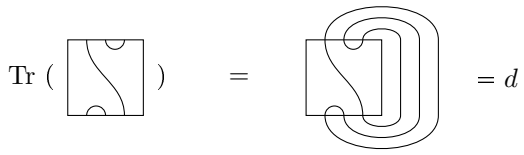


FIGURE 1.3. Markov trace.

There is an obvious involution $X \mapsto \overline{X}$ on $\mathrm{TL}_n(A)$. Given a TL diagram D, let $\overline{D}$ be the image of D under reflection through the middle line $I \times \frac{1}{2}$. Then $X \mapsto \overline{X}$ is extended to all formal diagrams by the automorphism of $\mathbb{F}$ which takes A to A^{-1} and restricts to complex conjugation on $\mathbb{C}$. The Markov trace then induces a sesquilinear inner product, called the Markov pairing, on $\mathrm{TL}_n(A)$ by the formula $\langle X, Y \rangle = \mathrm{Tr}(\overline{X}Y)$ for any $X, Y \in \mathrm{TL}_n(A)$ (Fig. 1.4).

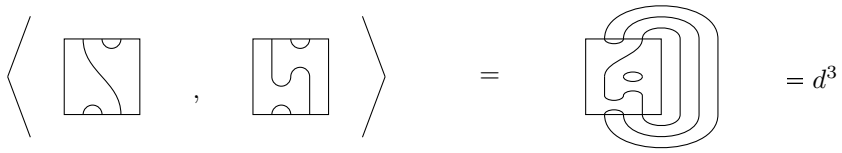


FIGURE 1.4. Markov pairing.

Define the nth Chebyshev polynomial $\Delta_n(d)$ inductively by $\Delta_0 = 1$, $\Delta_1(d) = d$, and $\Delta_{n+1}(d) = d\Delta_n(d) - \Delta_{n-1}(d)$. Let $c_n = \frac{1}{n+1}\binom{2n}{n}$ be the Catalan number.

There are c_n different TL diagrams $\{D_i\}$ in $\mathrm{TL}_n(A)$ consisting only of n disjoint arcs up to isotopy in $\mathcal{R}$ connecting the $2n$ boundary points of $\mathcal{R}$. These c_n diagrams span $\mathrm{TL}_n(A)$ as a vector space. Let $M_{c_n \times c_n} = (m_{ij})$ be the matrix of the Markov pairing of $\{D_i\}$ in a certain order, i.e. $m_{ij} = \mathrm{Tr}(\overline{D}_i D_j)$. Then

$$\mathrm{Det}(M_{c_n \times c_n}) = \pm \prod_{i=1}^{n} \Delta_i(d)^{a_{n,i}} \tag{1.5}$$

where $a_{n,i} = \binom{2n}{n-i-2} + \binom{2n}{n-i} - 2\binom{2n}{n-i-1}$. Formula (1.5) is derived in [**DGG**]. Let $\{U_i\}$, $i = 1, 2, \ldots, n-1$, be the TL diagrams in $\mathrm{TL}_n(A)$ shown in Fig. 1.5.

FIGURE 1.5. Generators of TL.

THEOREM 1.6.

(1) The diagrams $\{D_i\}$, $i = 1, 2, \ldots, \frac{1}{n+1}\binom{2n}{n}$, *form a basis of* $\mathrm{TL}_n(A)$ *as a vector space, and* $\mathrm{TL}_n(A)$ *is generated as an algebra by* $\{U_i\}$, $i = 0, 1, \ldots, n-1$.

(2) $\mathrm{TL}_n(A)$ *has the following presentation as an abstract algebra with generators* $\{U_i\}_{i=0}^{n-1}$ *and relations:*

$$U_i^2 = dU_i \tag{1.7}$$

$$U_i U_{i\pm 1} U_i = U_i \tag{1.8}$$

$$U_i U_j = U_j U_i \quad \text{if} \quad |i-j| \geqslant 2 \tag{1.9}$$

(3) Generic $\mathrm{TL}_n(A)$ *is a direct sum of matrix algebras over* $\mathbb{F}$.

PROOF.

(1) It suffices to show that every basis diagram D_i is a monomial in the generators U_i. Fig. 1.6 should convince the reader to construct his/her own proof. The dimension of the underlying vector space of $\mathrm{TL}_n(A)$ is the number of isotopic diagrams without loops, which is one of the many equivalent definitions of the Catalan number.

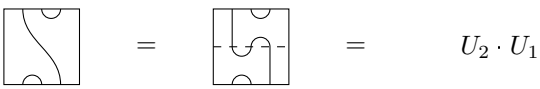


FIGURE 1.6. Decomposition into U_i's.

(2) By drawing diagrams, we can easily check relations (1.7), (1.8), and (1.9) in $\mathrm{TL}_n(A)$. It follows that there is a surjective algebra map ϕ from $\mathrm{TL}_n(A)$ onto the abstract algebra with generators $\{U_i\}$ and relations (1.7), (1.8), and (1.9). Injectivity of ϕ follows from a dimension count: the dimensions of the underlying vector spaces of both algebras are given by the Catalan number.

(3) Formula (1.5) can be used to deduce that generic $\mathrm{TL}_n(A)$ is a semisimple algebra, hence a direct sum of matrix algebras. An explicit proof is given in Sec. 1.1.6.

□

The generic TL algebras $\mathrm{TL}_n(A)$ first appeared in physics, and were rediscovered by V. Jones [**Jo3**]. Our diagrammatic definition is due to L. Kauffman [**Kau**].

1.1.3. Generic representation of the braid groups. The most important and interesting representation of the braid group B_n is the Jones representation discovered in 1981 [**Jo2, Jo4**], which led to the Jones polynomial, and the earlier Burau representation, related to the Alexander polynomial.

The approach pioneered by Jones is to study finite-dimensional quotients of the group algebra $\mathbb{F}[B_n]$, which are infinite-dimensional representations of the braid group: $b \in B_n$, $b(\sum c_i g_i) = \sum c_i (b g_i)$. If a finite-dimensional quotient is given by an algebra homomorphism, then the regular representation on $\mathbb{F}[B_n]$ descends to the quotient, yielding a finite-dimensional representation of B_n.

$\mathrm{TL}_n(A)$ is obtained as a quotient of $\mathbb{F}[B_n]$ by the Kauffman bracket (Fig. 1.7).

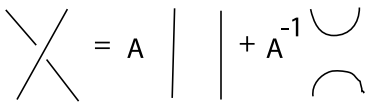


FIGURE 1.7. Kauffman bracket.

Recall the n-strand braid group B_n has a presentation with generators

$$\{\sigma_i \mid i = 1, 2, \ldots, n-1\}$$

and relations

$$\sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{if } |i-j| \geqslant 2, \qquad\qquad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}.$$

The Kauffman bracket induces a map $\langle , \rangle : \mathbb{F}[B_n] \to \mathrm{TL}_n(A)$ by the formula $\langle \sigma_i \rangle = A \cdot \mathrm{id} + A^{-1} U_i$.

PROPOSITION 1.10. *The Kauffman bracket $\langle , \rangle : \mathbb{F}[B_n] \to \mathrm{TL}_n(A)$ is a surjective algebra homomorphism.*

The proof is a straightforward computation.

DEFINITION 1.11. *Since generic $\mathrm{TL}_n(A)$ is isomorphic to a direct sum of matrix algebras over $\mathbb{F}$, the Kauffman bracket $\langle , \rangle$ maps B_n to non-singular matrices over $\mathbb{F}$, yielding a representation ρ_A of B_n called the generic Jones representation.*

It is a difficult open question to determine whether ρ_A sends nontrivial braids to the identity matrix, i.e., whether the Jones representation is faithful. Next we will use Jones-Wenzl projectors to describe the Jones representation explicitly.

1.1.4. Jones-Wenzl projectors. In this section we show the existence and uniqueness of the Jones-Wenzl projectors.

THEOREM 1.12. *Generic $\mathrm{TL}_n(A)$ contains a unique p_n characterized by:*

- $p_n \neq 0$.
- $p_n^2 = p_n$.

- $U_i p_n = p_n U_i = 0$ *for all* $1 \leqslant i \leqslant n-1$.

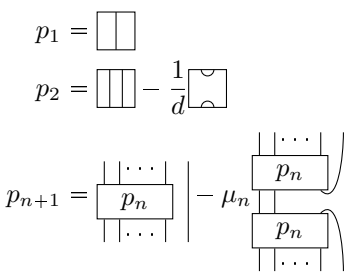
Furthermore p_n *can be written as* $p_n = 1 + U$, *where* $U = \sum c_j m_j$, *where* m_j *are nontrivial monomials of* U_i*'s,* $1 \leqslant i \leqslant n-1$, *and* $c_j \in \mathbb{F}$.

PROOF. For uniqueness, suppose p_n exists and can be expanded as $p_n = c1 + U$. Then $p_n^2 = p_n(c1 + U) = p_n(c1) = cp_n = c^2 1 + cU$, so $c = 1$. Let $p_n = 1 + U$ and $p_n' = 1 + V$, both having the properties above, and expand $p_n p_n'$ from both sides:

$$p_n' = 1 \cdot p_n' = (1 + U)p_n' = p_n p_n' = p_n(1 + V) = p_n \cdot 1 = p_n.$$

Existence is completed by an inductive construction of p_{n+1} from p_n, which also reveals the exact nature of the "generic" restriction on the loop variable d. The induction is as follows, where $\mu_n = \Delta_{n-1}(d)/\Delta_n(d)$.

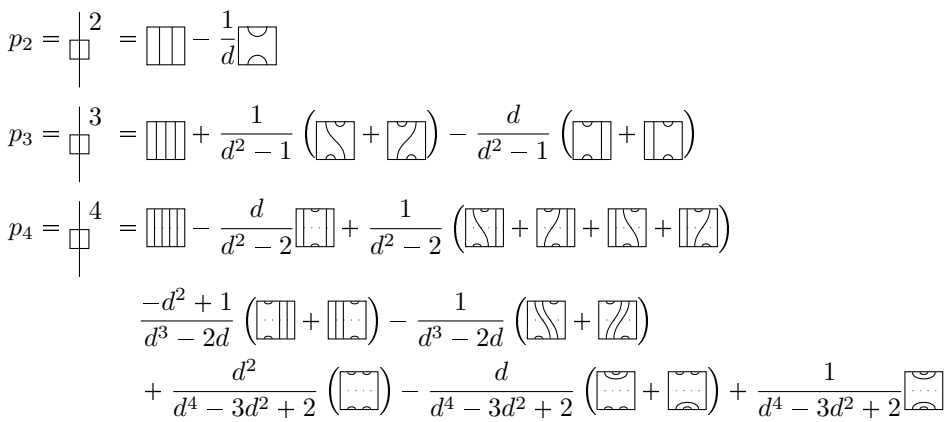
(1.13)

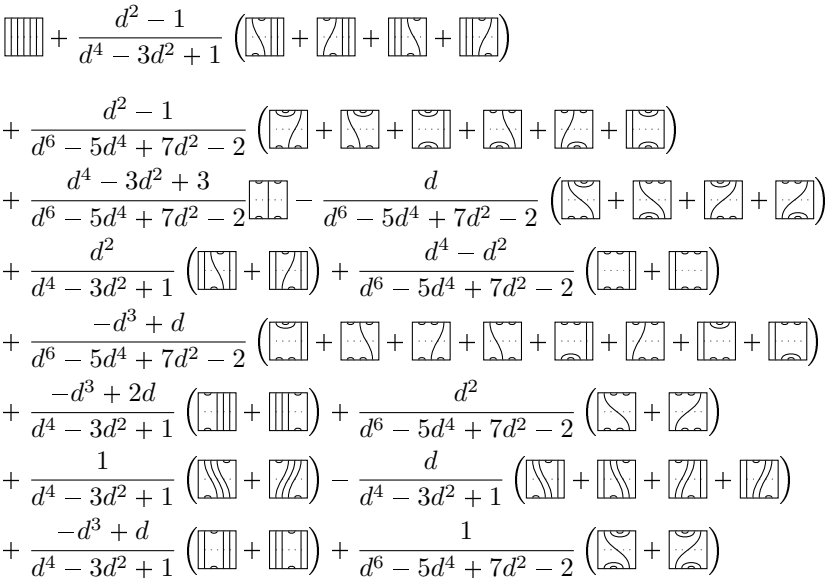


It is not difficult to check that $U_i p_n = p_n U_i = 0$, $i < n$. (The most interesting case is U_{n-1}.) □

Tracing the inductive definition of p_{n+1} yields $\mathrm{Tr}(p_1) = d$ and $\mathrm{Tr}(p_{n+1}) = \mathrm{Tr}(p_n) - \frac{\Delta_{n-1}}{\Delta_n}\mathrm{Tr}(p_n)$, showing that $\mathrm{Tr}(p_{n+1})$ satisfies the Chebyshev recursion (and the initial data). Thus $\mathrm{Tr}(p_n) = \Delta_n$.

Jones-Wenzl idempotents were discovered by V. Jones [**Jo1**], and their inductive construction is due to H. Wenzl [**Wenz**]. We list the explicit formulas for p_2, p_3, p_4, p_5.



$p_5 =$  $=$ 

1.1.5. Trivalent graphs and bases of morphism spaces. To realize each TL diagram as a matrix, we study representations of $\mathrm{TL}_n(A)$=$\mathrm{Hom}(1^n, 1^n)$. If $|y| = n$, then for any object x, $\mathrm{Hom}(x, y)$ is a representation of $\mathrm{TL}_n(A)$ by composition of morphisms: $\mathrm{TL}_n(A) \times \mathrm{Hom}(x, y) \to \mathrm{Hom}(x, y)$. Therefore we begin with the analysis of the morphism spaces of the TL algebroid.

To analyze these morphism spaces, we introduce colored trivalent graphs to represent some special basis elements. Let G be a uni-trivalent graph in the square $\mathcal{R}$, possibly with loops and multi-edges, such that all trivalent vertices are in the interior of $\mathcal{R}$ and all uni-vertices are on the bottom and/or top of $\mathcal{R}$. The univalent vertices together with the bottom or top of $\mathcal{R}$ are objects in $\mathrm{TL}(A)$. A coloring of G is an assignment of natural numbers to all edges of G such that edges with uni-vertices are colored by 1. An edge colored by 0 can be dropped, and an edge without a color is colored by 1. A coloring is admissible for a trivalent vertex v of G if the three colors a, b, c incident to v satisfy

(1) $a + b + c$ is even.
(2) $a + b \geqslant c, \quad b + c \geqslant a, \quad c + a \geqslant b.$

Let G be a uni-trivalent graph with an admissible coloring whose bottom and top objects are x, y. Then G represents a formal diagram in $\mathrm{Hom}(x, y)$ as follows. Split each edge of color l into l parallels held together by a Jones-Wenzl projector p_l. For each trivalent vertex v with colors a, b, c, admissibility furnishes unique natural numbers m, n, p such that $a = m + p$, $b = m + n$, $c = n + p$, allowing us to smooth v into a formal diagram as in Fig. 1.8. To simplify drawing and notation,

FIGURE 1.8. Trivalent vertex.

for any formal diagram in $\mathrm{Hom}(x, y)$, we will not draw the square $\mathcal{R}$ with the understanding that that the univalent vertices are representing some objects. Also a natural number l beside an edge always means the presence of the Jones-Wenzl projector p_l.

We will consider many relations among formal diagrams, so we remark that one relation can lead to many new relations by the following principle.

LEMMA 1.14 (Principle of annular consequence). *Suppose the square $\mathcal{R}$ is inside a bigger square S. In the annulus between $\mathcal{R}$ and S, suppose there are formal diagrams connecting objects on $\mathcal{R}$ and S. Then any relation r of formal diagrams supported in $\mathcal{R}$ induces one supported in S by including the relation r into S, and deleting the boundary of the old $\mathcal{R}$. The resulting new relation r' will be called an annular consequence of r (Fig. 1.9). More generally, S can be any compact surface, in which case we will call r' a generalized annular consequence of r.*

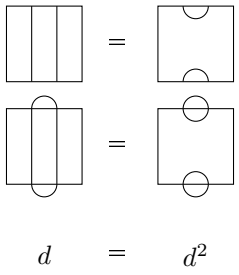


FIGURE 1.9. Annular consequence.

PROPOSITION 1.15. *Let x, y be two objects such that $|x| + |y| = 2m$. Then*

(1) $\dim \mathrm{Hom}(x, y) = \frac{1}{m+1}\binom{2m}{m}$.

(2) Let G be a uni-trivalent tree connecting x and y. Then the collection of all admissible colorings of G forms a basis of $\mathrm{Hom}(x, y)$.

PROOF.

(1) Without loss of generality, we may assume $|x| \geqslant |y|$. By bending arms down (Fig. 1.10), we see that $\mathrm{Hom}(x, y) \cong \mathrm{TL}_m(A)$ as vector spaces.

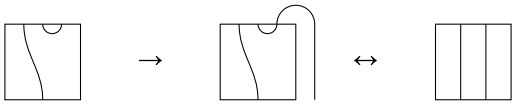


FIGURE 1.10. Bending arms down.

(2) Counting admissible colorings of G gives the right dimension. For linear independence, note that the Markov pairing on $\mathrm{TL}_n(A)$ extends to any $\mathrm{Hom}(x, y)$, and is nondegenerate. (This will be easier to see after Sec. 1.1.6.)

□

1.1.6. Generic Temperley-Lieb-Jones categories. Generic TL(A) has a tensor product given by horizontal "stacking": juxtaposition of diagrams. Using this tensor product, denoted as $\otimes$, we see that any object y with $|y| = n$ is isomorphic to a tensor power of an object x with $|x| = 1$, i.e., $1^n = 1^{\otimes n}$. For our applications to TQC, we would like to have $x^{\otimes m}$ "collapsible" to a direct sum of finitely many "simple" objects for all sufficiently large m. To achieve this, we enlarge generic TL(A) to the generic Temperley-Lieb-Jones (TLJ) algebroid, then take a finite "quotient." In this section, we describe the generic TLJ categories, which have generic TL(A) as subcategories.

Let A be an indeterminant as before. The objects of TLJ(A) are objects of TL(A) with natural number colors: each marked point in I receives a natural number. A point colored by 0 can be deleted. A point without a color is understood to be colored by 1, hence $\mathrm{TL}(A)^0 \subset \mathrm{TLJ}(A)^0$. Morphisms in $\mathrm{Hom}(x, y)$ for $x, y \in \mathrm{TLJ}(A)^0$ are formal $\mathbb{F}$-linear combinations of uni-trivalent graphs connecting x, y with admissible compatible colorings. Again, an edge without a color is colored by 1, and an edge of color 0 can be deleted, along with its endpoints. TLJ(A) has a tensor product as in TL(A): horizontal juxtaposition of formal diagrams. The empty object is a tensor unit. Every object is self-dual. The involution $X \mapsto \overline{X}$, extended to TLJ(A), is the duality for morphisms.

THEOREM 1.16. *TLJ(A) and TL(A) are ribbon tensor categories, but not ribbon fusion categories.*

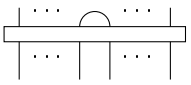
Categories of strings and tangles first appeared in [**Y, Tu**] to organize quantum invariants of links. For a detailed treatment of TLJ(A) and TL(A) as ribbon tensor categories, see [**Tu**]. We will define a ribbon fusion category in Chap. 4. Here we will list the properties of TLJ(A) that make it into a ribbon tensor category, which is essentially an abstraction of the pictures that we will draw. Generic TLJ(A) is not a fusion category because it has infinitely many simple object types, one for each JWP p_n.

DEFINITION 1.17. *An object x in an algebroid is simple if* $\mathrm{Hom}(x, x) \cong \mathbb{F}$.

Let n denote the isomorphism class of a single point colored by n. By abuse of notation, we will treat n as an object of TLJ(A). Note that $n \ncong 1^n$ for $n > 1$. For instance, while 3 is simple, 1^3 is not, because $\dim \mathrm{Hom}(1^3, 1^3) = 5$.

PROPOSITION 1.18. *Let $a, b, c \in \mathbb{N}$ be objects of* TLJ(A).

(1) A JWP kills any turn-back:


$= 0$

(2) $\mathrm{Hom}(a, b) = \begin{cases} \mathbb{C} & \text{if } a = b \\ 0 & \text{otherwise} \end{cases}$

(3) $\mathrm{Hom}(a \otimes b, c) = \begin{cases} \mathbb{C} & \text{if } a, b, c \text{ are admissible} \\ 0 & \text{otherwise} \end{cases}$

(4) Let x be an object consisting of k points with colors $a_1, \ldots, a_k$ and y be an object consisting of l points with colors $b_1, \ldots, b_l$. Let G be a uni-trivalent tree connecting x and y with compatible colorings. Then the admissible colorings of G form a basis of

$$\mathrm{Hom}(x, y) \cong \mathrm{Hom}(a_1 \otimes \cdots \otimes a_k, b_1 \otimes \cdots \otimes b_l).$$

PROOF.

(1) Exercise.
(2) Recall that an edge of color l harbors a JWP p_l. JWPs kill any turn-backs, therefore every morphism in $\mathrm{Hom}(a,b)$ is proportional to the identity if $a=b$ and 0 otherwise.
(3) If a,b,c are not admissible, then there will be turn-backs.
(4) Same as the $\mathrm{TL}(A)$ case.

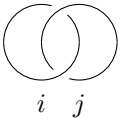
□

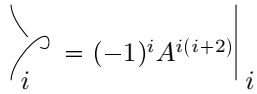
So far everything is in the plane, but we are interested in links. The bridge is provided by the Kauffman bracket. The Kauffman bracket resolves a crossing of a link diagram into a linear combination of TL diagrams, hence a link diagram is just a formal diagram. In particular, any link diagram L is in $\mathrm{Hom}(\mathbf{0},\mathbf{0})$, and hence $=\lambda \mathrm{id}_{\mathbf{0}}$ as a morphism. The scalar λ, which is a Laurent polynomial of A, is called the Kauffman bracket of L, denoted as $\langle L\rangle_A$ or $\langle L\rangle$.

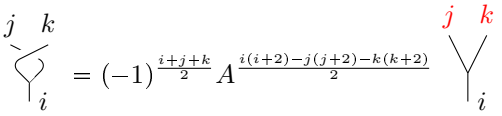
PROPOSITION 1.19. *Let* $[m]_A=\frac{A^{2m}-A^{-2m}}{A^2-A^{-2}}$ *be the quantum integer and* $[m]!$ *be the quantum factorial* $[m]_A[m-1]_A\cdots[1]_A$. *Note the loop variable* $d=-[2]_A$.

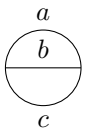
(1)  $=\Delta_i$

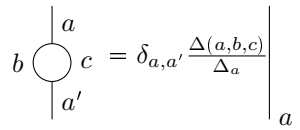
(2) *(no tadpole)*  $=\delta_{a,0}\Delta_b$

(3) $\tilde{s}_{ij}=$  $=(-1)^{i+j}[(i+1)(j+1)]_A$

(4)  $=(-1)^i A^{i(i+2)}$

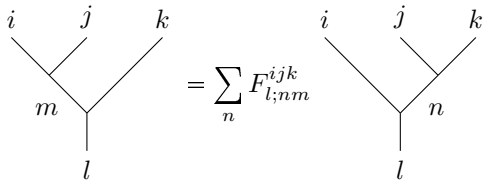
(5) 

(6) $\Delta(a,b,c)=$  $=\frac{(-1)^{m+n+p}[m+n+p+1]![m]![n]![p]!}{[m+n]![n+p]![p+m]!}$

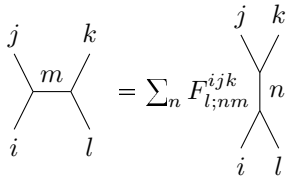
(7)  $=\delta_{a,a'}\frac{\Delta(a,b,c)}{\Delta_a}$

PROOF. We leave them as exercises, or see [**KL**]. □

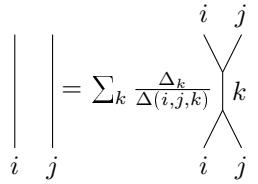
Given any i,j,k,l, we have two different bases of $\mathrm{Hom}(l, i\otimes j\otimes k)$ by labeling two different trees:



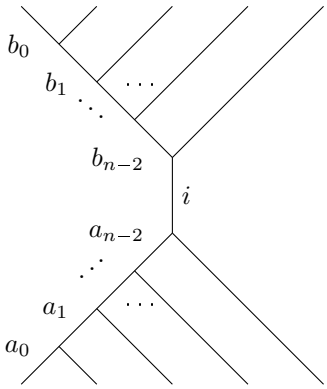
This change of basis matrix $(F^{ijk}_l)_{nm} = F^{ijk}_{l;nm}$ is called an F-matrix, and the $\{F^{ijk}_{l;nm}\}$ are called 6j symbols. In general graphical calculus for RFCs, we only draw graphs whose edges are transversal to the x-direction, i.e., no horizontal edges. But in TLJ theories, this subtlety is unnecessary. Therefore we will draw the F-matrix as



As a special case, we have



Finally, we are ready to see that each TL diagram in $\mathrm{TL}_n(A)$ is an explicit matrix. Consider the following uni-trivalent tree Γ:



LEMMA 1.20. *The admissible labelings of* Γ *form a basis of* $\mathrm{TL}_n(A)$*, denoted as* $e^B_{A;i} = \{e^{b_0,\dots,b_{n-2}}_{a_0,\dots,a_{n-2};i}\}$*, where* $B = (b_0, \dots, b_{n-2})$*,* $A = (a_0, \dots, a_{n-2})$*.*

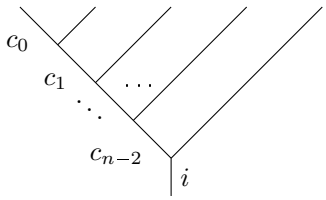
LEMMA 1.21.

$$\mathrm{Tr}(e^B_{A;i}) = \delta_{AB} \frac{\Delta(i,1,a_{n-2})}{\Delta_{a_{n-2}}} \frac{\Delta(a_{n-2},1,a_{n-1})}{\Delta_{a_{n-3}}} \cdots \frac{\Delta(a_2,1,a_1)}{\Delta_{a_1}} \Delta(a_1,1,1).$$

Note $a_0 = b_0 = 1$*.*

PROOF. Use Prop. 1.19(7) repeatedly. □

For $i \in \{0, 1, \dots, n\}$ and $i = n \mod 2$, fix a basis of $\mathrm{Hom}(i, 1^n)$, denoted as $\{e_{C;i} = e_{c_0,c_1,\dots,c_{n-2};i}\}$ where $C = (c_0, c_1, \dots, c_{n-2})$, by labeling the following tree:



LEMMA 1.22. *The basis $\{e_{c_0,\dots,c_{n-2};i}\}$ is orthogonal with respect to the Markov pairing.*

PROOF.

$$\langle e_{C;i}, e_{C';i'} \rangle = \delta_{i,i'}\delta_{C,C'} \frac{\Delta(1,1,c_1)}{\Delta_{c_1}} \frac{\Delta(c_1,1,c_2)}{\Delta_{c_2}} \cdots \frac{\Delta(c_{n-3},1,c_{n-2})}{\Delta_{c_{n-2}}} \Delta(c_{n-2},1,i).$$

□

THEOREM 1.23.

(1) *Each $e^B_{A;i}$ is a matrix unit up to a scalar on $\mathrm{Hom}(i, 1^n)$ with respect to the basis $\{e_{C;i}\}$. Explicitly,*

$$e^B_{A;i}(e_{C;i'}) = \delta_{ii'}\delta_{AC} \frac{\mathrm{Tr}(e^A_{A;i})}{\Delta_i} e_{B;i}$$

so that $e^B_{A;i}$ has exactly one nonzero entry.

(2) *Given a braid $\sigma \in B_n$, the Jones representation $\rho_A(\sigma)$ as a matrix is obtained by stacking σ onto the top of each $e_{C;i}$, resolving the crossings with the Kauffman bracket, and then expanding the resulting formal diagrams in the basis $\{e_{C;i}\}$ for each irreducible sector $i \in \{0, 1, \dots, n\}$ and $i = n \mod 2$.*

This theorem follows from existing works on TL algebras and Jones representations.

1.1.7. Colored Jones polynomials. More convenient for our applications is the Kauffman bracket for framed unoriented links, which is a variation of the Jones polynomial for oriented links. The Jones polynomial for oriented links can be obtained from the Kauffman bracket by multiplying by a power of A depending on the writhe.

A coloring of a link L is a labeling of each component by a natural number. This natural number is different from the framing. We always use the blackboard framing for link diagrams, i.e., the framing from a parallel copy of each component in the plane. Suppose L_D is a link diagram of L. Then L_D is in $\mathrm{Hom}(\mathbf{0}, \mathbf{0})$, hence a scalar multiple of $\mathrm{id}_{\mathbf{0}}$. This scalar $\langle L \rangle_A$ will be called the colored Kauffman bracket of L. If L is oriented with all components colored by a and $w(L)$ is the writhe of the link diagram L_D, then

$$J_a(L;t) = (-A^{a(a+2)})^{-w(L)} \langle L \rangle_A$$

is the colored Jones polynomial at $t = A^{-4}$. When $a = 1$, $J_a(L;t)$ is the usual Jones polynomial.

1.1.8. Colored Jones representations. The Jones representation can be extended to colored Jones representations of braid groups B_n for any coloring. If there is more than one color, then we get a representation of a subgroup of B_n. For example, if all colors are pairwise distinct, then we get a representation of the pure braid group PB_n. How those braid group representations decompose into irreducibles seems to be unknown.

1.1.9. $\mathrm{TLJ}(A)$ at roots of unity. To be directly applicable to quantum computation, we need to work over $\mathbb{C}$, not the field of rational functions in A. Therefore we will specialize A to a nonzero complex number. The structure of $\mathrm{TLJ}(A)$ is very sensitive to the choice of A. Given $A \in \mathbb{C}\backslash\{0\}$, we call $d = -A^2 - A^{-2}$ the loop value

THEOREM 1.24.

(1) *If $A \in \mathbb{C}\backslash\{0\}$ such that the loop value d is not a root of any Chebyshev polynomial Δ_i, $i = 1, 2, \ldots$, then the structure of $\mathrm{TLJ}(A)$ is the same as generic $\mathrm{TLJ}(A)$.*

(2) *If $A \in \mathbb{C}\backslash\{0\}$ such that the loop value d is a root of some Chebyshev polynomial Δ_i, $i = 1, 2, \ldots$, then some JWPs are undefined and for all sufficiently large n, $\mathrm{TL}_n(A)$'s are not matrix algebras, i.e., not semisimple.*

This theorem is well-known to experts.

The structure of $\mathrm{TL}_n(A)$ at roots of unity is analyzed in [**GW**]. When $A \in \mathbb{C}\backslash\{0\}$ such that d is a root of some Δ_i, then A is a root of unity. The structure of $\mathrm{TLJ}(A)$ depends essentially on the order of A. We are interested in semisimple quotients of $\mathrm{TLJ}(A)$ in the next section, called Jones algebroids.

1.2. Jones algebroids

When the Kauffman variable A is specialized to roots of unity, the Markov pairing becomes degenerate and some JWPs are undefined in $\mathrm{TLJ}(A)$. So $\mathrm{TLJ}(A)$ is not a semisimple algebroid anymore. Some semisimple quotients of the TLJ algebroids when A is a root of unity were discovered by V. Jones, so they will be called Jones algebroids. We assume A is either a primitive $4r^{\text{th}}$ root of unity for arbitrary $r \geqslant 3$ or a primitive $2r^{\text{th}}$ root of unity for odd $r \geqslant 3$. We will denote the Jones algebroid with a choice of A by $V_{A,k}$, or just V_A or V_k if no confusion arises, where $k = r - 2$ is called the level of the theory.

Fix an A and a k as above. Then the loop value d becomes a root of some Chebyshev polynomial Δ_i. Since Δ_i appears in the denominator in the definition of the JWPs p_n, some p_n are undefined. The first JWP that is undefined for our choice of A is p_r. Therefore we restrict our discussion to $p_0, \ldots, p_{r-1}$. By convention attaching p_0 to a strand is the same as coloring by 0. From Eqn. (1.13) we have $\operatorname{Tr} p_i = \Delta_i = (-1)^i[i+1] = (-1)^i \frac{A^{2i+2} - A^{-2i-2}}{A^2 - A^{-2}}$. If $A^{4r} = 1$, then $\operatorname{Tr} p_{r-1} = 0$. For our choice of A, $\operatorname{Tr} p_i \neq 0$ for $i = 0, \ldots, r-2$. (By convention $\operatorname{Tr} p_0 = 1$.) Therefore p_{r-1} is a vector of norm 0 under the Markov pairing. Actually, any vector in the radical of the Markov pairing is a generalized annular consequence of p_{r-1} [**Fr2, FNWW**]. We denote the radical by $\langle p_{r-1} \rangle$.

DEFINITION 1.25.

(1) *Given A as above, $L = \{0, \ldots, k\}$ is called the label set, and each $i \in L$ is called a label.*

(2) *The objects of V_A are labeled points in I where the labels are from L. For morphisms, given two objects $a, b \in V_A^0$, $V_A(a,b) = \mathrm{Hom}(a,b)/\langle p_{r-1}\rangle$, where $\mathrm{Hom}(a,b)$ is the morphism space of $\mathrm{TLJ}(A)$ specialized to A and $\langle p_{r-1}\rangle$ is the radical above.*

THEOREM 1.26.

(1) *V_A is a semisimple algebroid. In particular, the quotients $\mathrm{TL}_n(A)/\langle p_{r-1}\rangle$ of the TL algebras $\mathrm{TL}_n(A)$, denoted as $J_n(A)$, are semisimple algebras, and hence are direct sums of matrix algebras. $J_n(A)$ will be called the Jones algebra at A.*
(2) *The Kauffman bracket defines a representative of the braid groups as in the generic case for each A. These are the Jones representations ρ_A of braid groups.*
(3) *The images of all braid generators σ_i have eigenvalues among $\{A, -A^{-3}\}$. Hence all eigenvalues of $\rho(\sigma_i)$ are roots of unity of order $\leqslant 4r$.*

This theorem is a categorical version of Jones representations.

Jones representations are reducible, which is important for applications in interferometric experiments in $\nu = 5/2$ FQH liquds. We will refer to each irreducible summand as a sector. The sectors for ρ_A on B_n are in 1–1 correspondence with $i \in L$, $i = n \mod 2$. These Jones representations of B_n differ from the original Jones representations from von Neumann algebras by an abelian representation of B_n. See Sec. 1.4. As we saw in the generic case, in order to find the Jones representation explicitly, we introduce the trivalent bases of morphism spaces. Since our colors are now truncated to labels, we have to impose more conditions on the admissible labels.

DEFINITION 1.27. *Three labels a, b, c are k-admissible if*

(1) *$a + b + c$ is even.*
(2) *$a + b \geqslant c, \quad b + c \geqslant a, \quad c + a \geqslant b$.*
(3) *$a + b + c \leqslant 2k$.*

A trivalent vertex is k-admissible if its three colors are k-admissible.

LEMMA 1.28. *Let a, b, c be labels. Then the following are equivalent:*

(1) *a, b, c are k-admissible.*
(2) *$\Delta(a, b, c) \neq 0$.*
(3) *$\mathrm{Hom}(a \otimes b, c) \neq 0$.*

The extra condition $a+b+c \leqslant 2k$ is very important. It has an origin in CFT as the positive energy condition. With the truncation of colors from natural numbers to labels $L = \{0, \ldots, k\}$ and the new positive energy condition, all formulas for the generic TLJ algebroids in Prop. 1.19 apply to Jones algebroids. The same is true for the F-matrices.

Jones algebroids are our prototypical examples of RFCs, so let us describe their structures and introduce new terminology. First we have a label set L, which is the isomorphism classes of simple objects. The number of labels is called the rank of the theory. For the Jones algebroid V_A, the label set is $L = \{0, \ldots, k\}$, so it is of rank $= k + 1 = r - 1$. The tensor product is given by horizontal juxtaposition of formal diagrams. The fusion rules are the tensor decomposition rules for a representative set of the simple objects. Jones algebroids have a direct sum on objects, denoted as $\oplus$. Therefore fusion rules for labels are written as $a \otimes b = \bigoplus N_{ab}^c c$, where N_{ab}^c

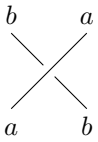
are natural numbers representing the multiplicity of c in $a \otimes b$. By Lem. 1.28 N_{ab}^c is 1 if a, b, c are k-admissible and 0 otherwise. Note that 0 is the trivial label, and $0 \otimes a = a$ for any a.

The next structure for a RFC is rigidity: a dual object for each object. The axioms for rigidity are to ensure that we can straighten out zigzags:

It demands the existence of special morphisms called births and deaths. In V_A, they are represented by

Then zigzags can always be straightened out. It follows that all simple objects of V_A are self-dual.

Another structure in a RFC is braiding. In V_A, for objects a, b, it is simply a formal diagram in $\mathrm{Hom}(a \otimes b, b \otimes a)$:

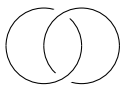


Braidings should be compatible with the other structures. When compatibility holds, we have a RFC. The first nice thing about a RFC is that we can define the quantum trace of any $f \in V_A(x, x)$. In V_A, the Markov trace is the quantum trace. Now more terminologies:

(1) quantum dimension of a label: $d_i =$  $= \Delta_i$

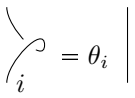
(2) S-matrix: Let $D^2 = \sum_{i \in L} d_i^2$,

$$\tilde{s}_{ij} = \quad = (-1)^{i+j}[(i+1)(j+1)],$$



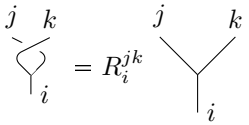
and $s_{ij} = \frac{1}{D}\tilde{s}_{ij}$. Then $S = (s_{ij})$ is called the modular S-matrix. There are two choices of D. We usually choose the positive D, but sometimes we need the negative D (see Sec. 1.3).

(3) Twist:



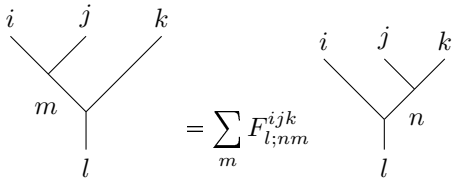
$$\theta_i = (-1)^i A^{i(i+2)}$$

(4) Braiding eigenvalues:



$$R_i^{jk} = (-1)^{\frac{i+j+k}{2}} A^{\frac{i(i+2)-j(j+2)-k(k+2)}{2}}$$

(5) F-matrix:



$\{F_{l;nm}^{ijk}\}$ can be determined by various tracings of the identity.

DEFINITION 1.29. *A RFC is a modular tensor category (MTC) if* $\det S \neq 0$.

THEOREM 1.30.

(1) If A is a primitive $4r^{\text{th}}$ root of unity, then S is nondegenerate, hence V_A is modular.

(2) If r is odd, and A is a primitive $2r^{\text{th}}$ root of unity, then $\tilde{S} = \tilde{S}_{\text{even}} \otimes \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, where $\tilde{S}_{\text{even}}$ is the submatrix of $\tilde{S}$ indexed by even labels. Furthermore, $\det \tilde{S}_{\text{even}} \neq 0$.

Part (1) is well-known, and part (2) can be found in [**FNWW**].

For each odd level k, all the even labels $L^{\text{even}} = \{0, 2, \ldots, k-1\}$ form a closed tensor subcategory, which is modular. We denote this even subcategory by V_A^{even}.

1.3. Yang-Lee theory

When $A = e^{\pi i/5}$ for level $k = 3$, the even subtheory of V_A has label set $L^{\text{even}} = \{0, 2\}$. We will rename them as $0 = 1, 2 = \tau$ to conform to established notation. This will be our first nontrivial MTC. It corresponds to a famous non-unitary CFT in statistical mechanics, called the Yang-Lee singularity, hence its name. The data for this theory is summarized as below. Obvious data such as $1 \otimes \tau = \tau$ and $F_\tau^{1\tau\tau} = 1$ are omitted.

Label set: $L = \{1, \tau\}$

Fusion rules: $\tau^2 = 1 \oplus \tau$

Quantum dimensions: $\{1, 1-\phi\}$, where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio

Twist: $\theta_1 = 1,\ \theta_\tau = e^{-2\pi i/5}$

S-matrix: $S = -\frac{1}{\sqrt{3-\phi}} \begin{pmatrix} 1 & 1-\phi \\ 1-\phi & -1 \end{pmatrix}$

Braidings: $R_1^{\tau\tau} = e^{2\pi i/5},\quad R_\tau^{\tau\tau} = e^{\pi i/5}$

F-matrices: $F_\tau^{\tau\tau\tau} = \begin{pmatrix} -\phi & 2-\phi \\ -1-2\phi & \phi \end{pmatrix}$

We remark on a subtle point about central charge. The Yang-Lee CFT has central charge $c = -22/5$. It is known that the topological central charge c_{top} of the corresponding MTC satisfies the identity $c_{\text{top}} = c \mod 8$ through

$$\frac{p_+}{D} = e^{\pi i/4c}$$

where $p_{\pm 1} = \sum_{i\in L} \theta_i^{\pm 1} d_i^2$ and $D^2 = \sum_{i\in L} d_i^2$ [**FG**]. It is common to choose D as the positive root of $\sum_{i\in L} d_i^2$. But for the Yang-Lee theory, it is the negative root of $\sum_i d_i^2$ that satisfies this identity, which is consistent with the S-matrix

$$s_{00} = -\frac{1}{\sqrt{3-\phi}}$$

Note that the Yang-Lee CFT is the minimal model $M(2,5)$.

1.4. Unitarity

To apply the Jones algebroids to quantum physics, we need unitary theories. The definition of a unitary MTC can be found in Sec. 4.3 or [**Tu**]. In particular, all quantum dimensions must be positive real numbers. For Jones algebroids, when $A = \pm ie^{\pm 2\pi i/4r}$, all quantum dimensions are positive, and the resulting MTCs are unitary. For specificity, we make the following choices:

- When r is even, $A = ie^{-2\pi i/4r}$, which is a primitive $4r^{\text{th}}$ root of unity.
- When r is odd and $r = 1 \mod 4$, $A = ie^{2\pi i/4r}$, which is a primitive $2r^{\text{th}}$ root of unity.
- When r is odd and $r = 3 \mod 4$, $A = ie^{-2\pi i/4r}$, which is also a primitive $2r^{\text{th}}$ root of unity.

When r is odd, the Jones algebroids are not modular.

THEOREM 1.31.

(1) For any root of unity A, the Jones representation preserves the Markov pairing.

(2) For the above choices of A, the Markov pairing is positive definite, hence the Jones representations are unitary.

PROOF.

(1) Let $\sigma \in B_n$. It suffices to consider basis diagrams. We have

$$\begin{aligned}\langle \rho_A(\sigma)D_1, \rho_A(\sigma)D_2\rangle &= \text{Tr}(\overline{D}_1\overline{\rho_A(\sigma)}\rho_A(\sigma)D_2) = \text{Tr}(\overline{D}_1\rho_A(\sigma^{-1})\rho_A(\sigma)D_2)\\ &= \text{Tr}(\overline{D}_1 D_2)\\ &= \langle D_1, D_2\rangle\end{aligned}$$

(2) Using Lem. 1.21, we can check that the Markov pairing on the basis in Lem. 1.22 is diagonal with positive norm.

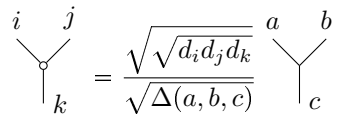
□

Although our theories are unitary, the F-matrices are not in general unitary. Unitary F-matrices are required for physical applications, hence we need to change bases to make the F-matrices unitary. Inspired by the Levin-Wen model [**LW1**], we choose the following normalizations:

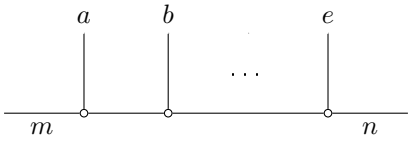
$$\theta^u(i,j,k) = \sqrt{d_i d_j d_k}$$

Since the norm of a trivalent vertex with colors a, b, c is $\Delta(a, b, c)$, our unitary normalization of a trivalent vertex is related to the default one by

(1.32)



Since 6j symbols are given in terms of d_i and $\theta(a, b, c)$, any formula in the old normalization is easily rewritten in the unitary normalization. One nice property of the unitary normalization is that the norm of



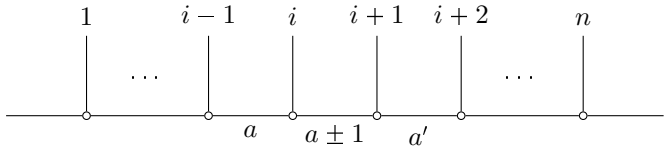
is $\sqrt{d_m d_a d_b \cdots d_e d_n}$, depending only on $m, a, b, \ldots, e, n$, i.e., independent of the interior colors.

Next we will explicitly describe the unitary Jones representations ρ_A of braid groups. To do so, we apply the Kauffman bracket to a braid generator $\sigma_i \in B_n$:

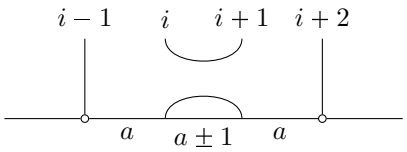
$$\rho_A(\sigma_i) = A \cdot \mathrm{id} + A^{-1}\rho_A(U_i), \quad \text{where } U_i \text{ is the } \mathrm{TL}_n(A) \text{ generator.}$$

Hence to compute the Jones representation $\rho_A(\sigma_i)$ it suffices to compute $\rho_A(U_i)$. $\rho_A(U_i)$ acts on the vector space $\mathrm{Hom}(t, 1^n)$ spanned by $\{e_{C;t}\}$ in Lem. 1.22. For unitary representations, we will use the normalized basis $\{e^U_{C;t}\}$, where $e^U_{C;t}$ is obtained from $e_{C;t}$ by modifying each trivalent vertex as in Fig. 1.32.

$\rho_A(U_i)(e^U_{C;t}) = \rho_A(U_i)$

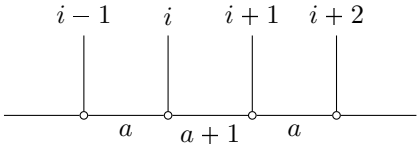


$=$

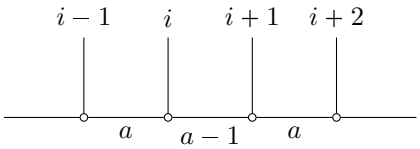


For $a \neq 0$ or k, let

$$e_{a+} = \frac{1}{\sqrt{\langle e^U_{C;t}, e^U_{C;t}\rangle}}$$



$$e_{a-} = \frac{1}{\sqrt{\langle e^U_{C;t}, e^U_{C;t}\rangle}}$$



If $a = 0$ or k, then $\rho_A(U_i)$ is the scalar $\delta_{aa'} \cdot d$ on e_{a+} or e_{a-} respectively. If $a \neq 0$ or k, then $\rho_A(U_i)$ restricted to the 2-dimensional subspace $\{e_{a+}, e_{a-}\}$ is

$$\begin{pmatrix} \frac{\Delta_{a+1}}{\Delta_a} & \frac{\sqrt{\Delta_{a+1}\Delta_{a-1}}}{\Delta_a} \\ \frac{\sqrt{\Delta_{a+1}\Delta_{a-1}}}{\Delta_a} & \frac{\Delta_{a-1}}{\Delta_a} \end{pmatrix}$$

Therefore $\rho_A(U_i)$ consists of 2×2 or 1×1 blocks, as does $\rho_A(\sigma_i)$.

The original Jones representations from von Neumann algebras are given in terms of projectors $\{e_i\}$ for the Jones algebras. The generators $\{e_i\}$ are related to $\{U_i\}$ by $e_i = U_i/d$. In the unitary cases,

$$\begin{aligned} e_i &= e_i^+, \quad e_i^2 = e_i \\ e_i e_j &= e_j e_i, \quad |i-j| \geqslant 2 \\ e_i e_{i\pm 1} e_i &= \frac{1}{d^2} e_i \end{aligned}$$

Then $\rho_A^J(\sigma_i) = -1 + (1+q)e_i$ is the original Jones representation, where $q = A^{-4}$. Since e_i has eigenvalues among $\{0, 1\}$, $\rho_A^J(\sigma_i)$ has eigenvalues among $\{-1, q\}$.

In the Kauffman bracket,

$$\rho_A(\sigma_i) = A\mathrm{id} + A^{-1}U_i = -A(-1 + (1+q)e_i).$$

Hence $\rho_A(\sigma_i) = -A\rho_A^J(\sigma_i)$. The representation of B_n given by $\sigma_i \mapsto -A$ is abelian. Hence Jones representations ρ_A, ρ_A^J in two different normalizations are projectively the same. But as linear representations, the orders of the braid generators are different.

1.5. Ising and Fibonacci theory

Throughout the book, we will focus on two theories: Ising and Fibonacci. Besides their mathematical simplicity and beauty, they are conjectured physically to model non-abelian states in FQH liquids at filling fraction $\nu = 5/2$ and $\nu = 12/5$.

1.5.1. Ising theory. Ising theory is the $A = ie^{-2\pi i/16}$, level $k = 2$ Jones algebroid. We will also call the resulting unitary MTC the Ising MTC, and the unitary TQFT the Ising TQFT. The label set for the Ising theory is $L = \{0, 1, 2\}$. It is related to the Witten-SU(2)-Chern-Simons theory at level $k = 2$, but not the same [**RSW**]. In physics, the three labels $0, 1, 2$ are named $1, \sigma, \psi$, and we will use this notation. The explicit data of the Ising theory:

Label set: $L = \{1, \sigma, \psi\}$

Fusion rules: $\sigma^2 = 1 + \psi,\ \psi^2 = 1,\ \psi\sigma = \sigma\psi = \sigma$

Quantum dimensions: $d_1 = 1,\ d_\sigma = \sqrt{2},\ d_\psi = 1$

Twist: $\theta_1 = 1,\ \theta_\sigma = e^{2\pi i/16},\ \theta_\psi = -1$

S-matrix: $$S = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}$$

Braidings: $R_1^{\sigma\sigma} = e^{-\pi i/8},\ R_1^{\psi\psi} = -1,\ R_\sigma^{\psi\sigma} = R_\sigma^{\sigma\psi} = -i,\ R_\psi^{\sigma\sigma} = e^{3\pi i/8}$

F-matrices: $$F_\sigma^{\sigma\sigma\sigma} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ F_\sigma^{\psi\sigma\psi} = F_\psi^{\sigma\psi\sigma} = -1$$

Currently non-abelian Ising anyons are closest to experimental realization: the non-abelian anyon σ is believed to be realized in $p+ip$ superfluids [**RG**], and its $SU(2)_2$ counterpart by the charge $e/4$ quasiparticle in $\nu = 5/2$ FQH liquids [**MR, GWW**]. The simple object ψ is a Majorana fermion in physics. No Majorana fermions have been detected in physics. Ising theory is related to the Ising model in statistical mechanics, chiral superconductors, and FQH liquids at $\nu = 5/2$. For application to TQC, we need to know the closed images of the resulting braid group representations. In this regard, Ising theory is weak: the image of each braid group is finite, though bigger than the corresponding symmetric group. This may make the Ising theory easier to find in real materials.

The Jones representation ρ_A^J at $r = 4$ of B_n is irreducible of degree $2^{\frac{n-1}{2}}$ if n is odd, and reducible to two irreducible representations of degree $2^{\frac{n}{2}-1}$ if n is even. To describe the image, we define groups E_m^1 which are nearly extra-special 2-groups when m is even.

DEFINITION 1.33. *The group E_m^1 has a presentation with generators $x_1, \ldots, x_m$ and relations*

$$\begin{aligned} x_i^2 &= 1 && 1 \leqslant i \leqslant m \\ x_i x_j &= x_j x_i && |i-j| \geqslant 2 \\ x_{i+1} x_i &= -x_i x_{i+1} && 1 \leqslant i \leqslant m \end{aligned}$$

where -1 means an order two central element.

For m even, E_m^1 has only one irreducible representation of degree > 1: an irreducible representation V_1 of degree $2^{m/2}$. For m odd, E_m^1 has two irreducible representations W_1, W_2 of degree > 1, both of degree $2^{m-1/2}$. Let PB_n be the pure braid subgroup of B_n, defined by the exact sequence

$$1 \longrightarrow PB_n \longrightarrow B_n \longrightarrow S_n \longrightarrow 1.$$

THEOREM 1.34.

(1) *The image $\rho_A^J(PB_n)$ as an abstract group is E_{n-1}^1, and the unitary Jones representation ρ_A^J of PB_n factors through to V_1 and $W_1 \oplus W_2$ respectively for n odd and n even.*
(2) *$\rho_A^J(B_n)$ fits into the exact sequence*

$$1 \longrightarrow E_{n-1}^1 \longrightarrow \rho_A^J(B_n) \longrightarrow S_n \longrightarrow 1.$$

(3) *Projectively, we have*

$$1 \longrightarrow \mathbb{Z}_2^{n-1} \longrightarrow \rho_A^{\text{proj}}(B_n) \longrightarrow S_n \longrightarrow 1$$

which splits only when n is even.

The projective image (3) is from [**Jo3**]. A related result for images of $\rho_A^\gamma(\sigma_i)$ is in [**R1**] for n even. For a proof, see [**FRW**].

Recall the Majorana fermions $\{\gamma_i\}$ form the algebra with relations

$$\gamma_i^\dagger = \gamma_i, \quad \gamma_i\gamma_j + \gamma_j\gamma_i = 2\delta_{ij}.$$

THEOREM 1.35. *The Jones algebra $J_n(A)$ for $A = \pm ie^{\pm \pi i/8}$ is isomorphic to the complex Clifford algebra.*

PROOF. Let $e_i = U_i/\sqrt{2}$ as before. Then $\mathrm{TL}_n(A)$ is generated by $\{e_1, \ldots, e_{n-1}\}$ with relations $e_i^+ = e_i$, $e_i^2 = e_i$, $e_i e_{i\pm1} e_i = \frac{1}{2} e_i$. The unitary Jones representation $\rho_A^J(\sigma_i)$ is $\sigma_i = -1 + (1+q)e_i$, hence $\sigma_i^2 = 1 - 2e_i$, $q = \sqrt{-1}$. Note we write $\rho_A^J(\sigma_i)$ simply as σ_i. Then $\sigma_i^2\sigma_j^2 = \sigma_j^2\sigma_i^2$ for $|i-j| \geqslant 2$ and $\sigma_i^2\sigma_{i+1}^2 + \sigma_{i+1}^2\sigma_i^2 = 0$, which is equivalent to $p_3 = 0$. Let $\gamma_i = (\sqrt{-1})^{i-1}\sigma_i^2 \cdots \sigma_1^2$. Then $\{\gamma_i\}$ forms the Majorana algebra. Conversely, we have $\sigma_i^2 = \sqrt{-1}\gamma_i\gamma_{i+1}$. □

This theorem is from [**Jo3**].

We have already seen two different normalizations of the Jones representation at $r = 4$ or level $k = 2$: the Jones normalization and the Kauffman bracket normalization. There is also a third normalization related to the γ-matrices:

$$\rho_A^\gamma(\sigma_i) = e^{\pi/4\gamma_{i+1}\gamma_i} = \frac{1}{\sqrt{2}}(1 + \gamma_{i+1}\gamma_i).$$

The orders of $\rho_A^J(\sigma_i)$, $\rho_A^\gamma(\sigma_i)$, and $\rho_A(\sigma_i)$ are 4, 8, and 16 respectively. Although all three normalizations have the same projective image, their linear images are in general different. For example, for the γ-matrix representation of PB_n, instead of E_{n-1}^1, the image is E_{n-1}^{-1} [**FRW**]. In $\nu = 5/2$ FQH liquid, since the quasiparticle has charge $e/4$, the Nayak-Wilczek representation is the Jones normalization. In terms of γ-matrices, $\rho_A^J(\sigma_i) = e^{\pi i/4}\rho_A^\gamma(\sigma_i) = e^{\pi i/4}e^{\frac{\pi}{4}\gamma_{i+1}\gamma_i}$ [**NW**].

In physics, the Jones braid group representation is understood as automorphisms of Majorana fermions [**I**]:

$$\rho_A^J(\sigma_i)(\gamma_j) = \rho_A^J(\sigma_i)\gamma_j\rho_A^J(\sigma_i)^{-1}$$

Then

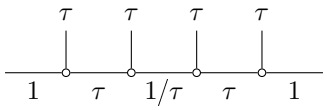
$$\begin{aligned} \gamma_i &\mapsto \gamma_{i+1} \\ \gamma_{i+1} &\mapsto -\gamma_i \\ \gamma_j &\mapsto \gamma_j \text{ if } j \neq i, i+1 \end{aligned}$$

1.5.2. Fibonacci theory. If $A = ie^{2\pi i/20}$, $k = 3$, then the Jones algebroid, which is not modular, has label set $L = \{0, 1, 2, 3\}$. The subcategory consisting of only even labels $\{0, 2\}$ is called the Fibonacci theory. The established notation for the two labels $\{0, 2\}$ is $\{1, \tau\}$. Let $\phi = \frac{1+\sqrt{5}}{2}$ be the golden ratio.

Label set:	$L = \{1, \tau\}$
Fusion rules:	$\tau^2 = 1 \oplus \tau$
Quantum dimensions:	$\{1, \phi\}$
Twist:	$\theta_1 = 1,\ \theta_\tau = e^{4\pi i/5}$
S-matrix:	$S = \frac{1}{\sqrt{2+\phi}} \begin{pmatrix} 1 & \phi \\ \phi & -1 \end{pmatrix}$
Braidings:	$R_1^{\tau\tau} = e^{-4\pi i/5}\ \ R_\tau^{\tau\tau} = e^{3\pi i/5}$
F-matrices:	$F_\tau^{\tau\tau\tau} = \begin{pmatrix} \phi^{-1} & \phi^{-1/2} \\ \phi^{-1/2} & -\phi^{-1} \end{pmatrix}$

The Fibonacci theory is related to the Yang-Lee theory by a Galois conjugate. They have the same fusion rules, hence all degrees of the braid group representations are the same Fibonacci numbers. As a consequence of the density of the braid group

representations of the Fibonacci theory, it is possible to design a universal TQC using τ's. Fibonacci theory can also be realized directly using the quantum groups G_2 and F_4. The representation of B_4 on $\mathrm{Hom}(1, \tau^{\otimes 4})$ has a basis



In this basis,

$$\rho_A(\sigma_1) = \rho(\sigma_3) = \begin{pmatrix} e^{-4\pi i/5} & 0 \\ 0 & e^{3\pi i/5} \end{pmatrix}$$

$$\rho_A(\sigma_2) = \begin{pmatrix} \phi^{-1}e^{4\pi i/5} & \phi^{-1/2}e^{-3\pi i/5} \\ \phi^{-1/2}e^{-3\pi i/5} & -\phi^{-1} \end{pmatrix}$$

It is not known if there exists a braid σ such that

$$\rho_A(\sigma) = \lambda \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

for some scalar λ, i.e., we don't know if the NOT gate in quantum computing (QC) can be realized exactly in the Fibonacci theory up to an overall phase.

1.6. Yamada and chromatic polynomials

There is a close relationship between graphs and alternating links through the medial graph construction. The Jones polynomial of an alternating link L is the same as the Tutte polynomial $T(G; x, y)$ of the corresponding graph G_L specialized to $xy = 1$. We point out a relation between the Yamada polynomial, which is a colored Jones polynomial for trivalent graphs, and the chromatic polynomial, which is the Tutte polynomial specialized to the real axis.

Given any graph G, the chromatic polynomial $\chi_G(k)$ is a polynomial in k such that when k is a positive integer, then $\chi_G(k)$ is the number of k-colorings of vertices of G such that no two vertices connected by an edge are given the same color. If the graph G is planar and trivalent, then the colored Jones polynomial for G with each edge colored by p_2 is a Laurent polynomial in the loop variable d. This polynomial is called the Yamada polynomial, denoted as $Y_G(d)$.

THEOREM 1.36. *If G is a planar graph and $\hat{G}$ its dual, then*

$$d^{-V}\chi_G(d^2) = Y_{\hat{G}}(d)$$

where $V = (\#$ vertices of $G) = (\#$ faces of $\hat{G})$.

For a proof, see [**FFNWW**].

1.7. Yang-Baxter equation

We will use the unitary Jones representations of braids to do quantum computation. In the quantum circuit model of QC, the computational space is a tensor product of qudits, manifesting the locality of quantum mechanics explicitly. In TQC, the lack of natural tensor decompositions makes the topological model inconvenient for implementing QCM algorithms. It is desirable to have unitary solutions of the Yang-Baxter equation $R\colon V \otimes V \circlearrowleft$ so we can have a quantum computational model based on braiding with obvious locality.

We have a choice for qudits, either V or $V \otimes V$, but both choices run into problems: we don't have good realizations of the Yang-Baxter space V in real materials, and no unitary solutions of the Yang-Baxter equation are known to the author such that the resulting representations of the braid groups have infinite images. There is clearly a tension between unitarity and locality for braid group representations. The first nontrivial unitary solution [**D**] is the Bell matrix

$$R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

which is related to Ising theory. There is also a 9×9 unitary solution, which is related to the Jones polynomial at a 6th root of unity:

$$R = \frac{1}{\sqrt{3}} \begin{pmatrix} w & 0 & 0 & 0 & \overline{q}^2 & 0 & 0 & 0 & w \\ 0 & w & 0 & 0 & 0 & w & q & 0 & 0 \\ 0 & 0 & w & \overline{q}w^2 & 0 & 0 & 0 & \overline{q}w^2 & 0 \\ 0 & 0 & qw^2 & w & 0 & 0 & 0 & w^2 & 0 \\ wq^2 & 0 & 0 & 0 & w & 0 & 0 & 0 & q^2 \\ 0 & 1 & 0 & 0 & 0 & w & qw & 0 & 0 \\ 0 & \overline{q}w & 0 & 0 & 0 & \overline{q} & w & 0 & 0 \\ 0 & 0 & qw^2 & w^2 & 0 & 0 & 0 & w & 0 \\ 1 & 0 & 0 & 0 & \overline{q}^2 w & 0 & 0 & 0 & w \end{pmatrix}$$

where $w = e^{\pm 2\pi i/3}$ and $|q| = 1$ [**RW**].

CHAPTER 2

Quantum Circuit Model

This chapter introduces the quantum circuit model for quantum computing (QC), emphasizing universality, and quantum algorithms for simulating quantum physics.

Informatics is the study of storing, processing and communicating information. The mathematical treatment of information starts with bit strings $\{0,1\}^* = \bigcup_{n\geqslant 0} \mathbb{Z}_2^n$. Pythagoreas once said "everything is a number." Every number has a binary expansion in terms of 0's and 1's, so we can encode everything by infinite bit strings. But in this book we will consider only finite bit strings, i.e., vectors in the $\mathbb{Z}_2$-vector space $\mathbb{Z}_2^n$ for some n, unless stated otherwise.

A key informatical notion is complexity, a measure of resource-dependent difficulty. Complexity classes of computational problems are defined relative to resources such as time, space, and accuracy. As bit strings $x \in \mathbb{Z}_2^n$ encode information, families of Boolean maps from bit strings to bit strings

$$f(x) = \left\{ f_n(x) : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^m \right\}$$

encode computing problems. Computability theory selects a class of problems which are algorithmically computable.

In its most liberal form, information processing can be thought of as a black box:

- The initial input x is encoded onto some physical system.
- The evolution of the physical system processes x.
- The computational result $f(x)$ is read out through some measurement of the system.

The physical system used to process x can be classical or quantum, which determines whether we are doing classical or quantum information theory. It is interesting to ponder whether other physical theories could be employed to process information. As alluded to in the introduction, the computational power of quantum field theory is presumably the same as that of quantum mechanics. Also, the logical issue of computability does not concern us because quantum computers and classical computers solve the same class of computing problems. Rather, our interest is to process classical information more efficiently.

How do we compute quantum mechanically? For simplicity, suppose we are given a map $f\colon \mathbb{Z}_2^n \circlearrowleft$ that we need to compute. Choose a quantum system with state space $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}[\mathbb{Z}_2^n]$. For each input $x \in \mathbb{Z}_2^n$, represent x as a basis state $|x\rangle \in (\mathbb{C}^2)^{\otimes n}$. Then ideally we would like to implement a unitary matrix U_x in $(\mathbb{C}^2)^{\otimes n}$ so that $U_x|x\rangle = |f(x)\rangle$ (Fig. 2.1).

But we don't know which U_x would efficiently send $|x\rangle$ to $|f(x)\rangle$ or even just close to $|f(x)\rangle$ explicitly (this is the quantum algorithm issue), and if U_x exists, how to implement U_x in a laboratory (this is the engineering issue). For very few

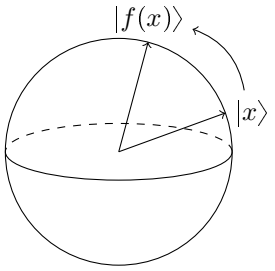


FIGURE 2.1. Quantum computation.

problems such as factoring, we have efficient classical algorithms to give us quantum circuits U_x.

The unit of information is the bit and an information resource is modeled by a random variable X. We will only consider discrete random variables. A random variable X is a function defined on the sample space of an event S: all possible outcomes. Associated to a random variable $X : S \to \{x_1, x_2, \ldots, x_n\}$ is its probability distribution $p(X)$. The function $p(X)$ takes the values of X to the nonnegative reals. The value $p(X = x_i) = p_i$ is the probability that the random variable X assumes the value x_i. Note that $\sum_{i=1}^{n} p_i = 1, p_i \geqslant 0$.

DEFINITION 2.1. *The information content of a random variable X with probability distribution $p(X = x_i) = p_i$ is $I(X) = -\sum_{i=1}^{n} p_i \log_2 p_i$.*

If someone receives a message x encoded by a bit string in $\mathbb{Z}_2^n$, how much information does he gain? The amount of information depends on how many other messages he might receive and their probability distribution. If every message is encoded by some bit string in $\mathbb{Z}_2^n$, and every length n bit string is equally likely, i.e., the probability distribution is the constant function 2^{-n} on $\mathbb{Z}_2^n$, then when he receives a string x, his information gain is $I(p) = -\sum_{i=1}^{n} 2^{-n} \log_2 2^{-n} = n$ bits. On the other hand, if he knew beforehand that he would receive the bit string $111\ldots1 \in \mathbb{Z}_2^n$, then how much information did the message give him? It is 0. Indeed, now the probability distribution is $p(111\ldots1) = 1$ and all other values $= 0$. Substituting this into $I(p) = -\sum_{i=1}^{n} p_i \log_2 p_i$, indeed $I(p) = 0$. Therefore information is relative and measures some kind of uncertainty or ignorance.

2.1. Quantum framework

Quantum theory gives a set of rules to associate random variables to states and observables of a quantum system. Thus quantum systems are natural information resources.

The Hilbert space formulation of quantum mechanics has the following axioms:

(1) *State space:* Just as in classical mechanics, a quantum system possesses a state at any moment. A Hilbert space L describes all possible states. Any nonzero vector $|v\rangle$ represents a state, and two nonzero vectors $|v_1\rangle$ and $|v_2\rangle$ represent the same state iff $|v_1\rangle = \lambda|v_2\rangle$ for some scalar $\lambda \neq 0$. Quantum computation uses ordinary finite-dimensional Hilbert space $\mathbb{C}^m$, whose states correspond to $\mathbb{C}P^{m-1}$. Therefore information is stored in state vectors or more precisely, points on $\mathbb{C}P^{m-1}$.

Hilbert space embodies the superposition principle. This most salient feature of quantum mechanics has everything to do with its computational power.

(2) *Evolution:* If a quantum system is governed by a Hamiltonian H, then its state vector $|\psi\rangle$ is evolved by solving the Schrödinger equation $i\hbar\frac{\partial|\psi\rangle}{\partial t} = H|\psi\rangle$. When the state space is finite-dimensional, the solution is $|\psi_t\rangle = e^{-\frac{i}{\hbar}tH}|\psi_0\rangle$ for some initial state $|\psi_0\rangle$. Since H is Hermitian, $e^{-\frac{i}{\hbar}tH}$ is a unitary matrix. Therefore we will just say states evolve by unitary matrices. In quantum computation, we apply unitary transformations to state vectors $|\psi\rangle$ to process the information encoded in $|\psi\rangle$. Hence information processing in quantum computation is multiplication by unitary matrices.

(3) *Measurement:* Measurement of a quantum system is given by a Hermitian operator M such as the Hamiltonian (= total energy). Since M is Hermitian, its eigenvalues are real. If they are pairwise distinct, we say the measurement is complete. Given a complete measurement M with eigenvalues $\{\lambda_i\}$, let $\{e_i\}$ be an orthonormal basis of eigenvectors of M corresponding to $\{\lambda_i\}$. If we measure M in a normalized state $|\psi\rangle$, which can be written as $|\psi\rangle = \sum_i a_i|e_i\rangle$, then the system will be in state $|e_i\rangle$ with probability $|a_i|^2$ after the measurement. This is called projective measurement and is our read-out for quantum computation.

Measurement interrupts the deterministic unitary evolution and outputs a random variable $X\colon \{e_i\} \to \{\lambda_i\}$ with probability distribution $p(X = \lambda_i) = |a_i|^2$, and hence is the source of the probabilistic nature of quantum computation.

(4) *Composite system:* If two systems with Hilbert spaces L_1 and L_2 are brought together, then the state space of the joint system is $L_1 \otimes L_2$. Composite systems have entangled states, which baffle many people, including Einstein.

The construction of the Hilbert space L and the Hamiltonian H for a given quantum system is in general difficult. If we start with a classical system, then a procedure to arrive at L and H is called quantization. Sometimes we don't even have a classical system to begin with.

2.2. Qubits

While bits model on-off switches, qubits model 2-level quantum systems. The states of a bit are $\mathbb{Z}_2 = \{0, 1\}$, and the states of a qubit are redundantly represented by $\mathbb{C}^2 = \mathbb{C}[\mathbb{Z}_2]$. This relation $\mathbb{C}^2 = \mathbb{C}[\mathbb{Z}_2]$ extends to n-qubits $(\mathbb{C}^2)^{\otimes n}$, yielding the group algebra $\mathbb{C}[\mathbb{Z}_2^n]$ of $\mathbb{Z}_2^n$. Therefore bit strings are basis vectors for n-qubits.

What is a qubit? An abstract notion of a qubit depends on the theoretical model of a 2-level quantum system. In the Hilbert space formulation of quantum theory, a qubit is defined as: a Hilbert space $\cong \mathbb{C}^2$ representing qubit states, evolution of states by matrices in $\mathrm{U}(2)$, measurements given by 2×2 Hermitian operators, and the probabilistic interpretation of measurements. Very often we use the word qubit to mean a state of a qubit.

Mathematically, a qubit state is given by a non-zero vector $|\psi\rangle \in \mathbb{C}^2$. Since any $|\psi'\rangle = \lambda|\psi\rangle$ with $\lambda \neq 0$ represents the same state, a qubit state is an equivalence class of vectors, i.e., a point on the Riemann sphere $\mathbb{C}P^1$. The Riemann sphere

representing all qubit states is called the Bloch sphere. Hence qubit states are in 1–1 correspondence with points of the Bloch sphere.

A measurement M of a qubit is given by a 2×2 Hermitian matrix. Without loss of generality, we may assume that the eigenvalues are among ± 1. If the two eigenvalues are equal, then $M = \pm \mathrm{Id}$, so measurement does nothing. If M is complete, then it is equivalent to one of the form $v \cdot \sigma = x\sigma_x + y\sigma_y + z\sigma_z$, where $v = (x, y, z) \in S^2$ and $\sigma = (\sigma_x, \sigma_y, \sigma_z)$, where $\sigma_x, \sigma_y, \sigma_z$ are the Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

If you send your friend a qubit state (as a Christmas gift), how much information does she gain? If she is a quantum being, then she obtains an infinite amount of information. If a classical being, she gets at most one bit. Giving a qubit state is the same as identifying a point on the Bloch sphere, hence the information content is infinite. But for a classical being, a measurement is required to access the information. The output is a random variable with two possible outcomes. Therefore the information gain is at most one bit. So the infinite amount of information contained in the qubit state is not directly accessible to classical beings. In this sense a qubit state contains both more and less than a bit.

THEOREM 2.2. *Given an unknown qubit state $|\psi\rangle$, on average only $\frac{1}{2\ln 2}$ bits of information can be obtained by a single complete measurement.*

PROOF. Since the qubit state $|\psi\rangle$ is unknown, we choose a random complete measurement and only one measurement can be performed because the qubit state is destroyed after the measurement. Then we will average the information gain over all possible measurements.

Given a complete measurement M on $\mathbb{C}^2$, let $|v_0\rangle$ and $|v_1\rangle$ be the eigenvectors of M with eigenvalues λ_0 and λ_1. If we measure M, then the normalized state $|\psi\rangle$ projects onto either $|v_0\rangle$ or $|v_1\rangle$ with probability $|\alpha|^2$ or $|\beta|^2$ respectively, where $\alpha = \langle v_0|\psi\rangle$ and $\beta = \langle v_1|\psi\rangle$. Therefore the information we acquire by measuring M is $-(|\alpha|^2 \log_2 |\alpha|^2 + |\beta|^2 \log_2 |\beta|^2)$. Any two complete measurements are equivalent via a unitary transformation $U\colon M \mapsto UMU^\dagger$, which changes the eigenvectors v_i of M to Uv_i. The resulting probability distribution of measuring $|\psi\rangle$ using $UMU^\dagger$ is $|\alpha^U|^2$ and $|\beta^U|^2$, where $\alpha^U = \langle v_0|U\psi\rangle$ and $\beta^U = \langle v_1|U\psi\rangle$. So instead of averaging over all measurements M, we can fix a single measurement M and average over all qubit states. Without loss of generality, we can fix the measurement to be σ_z. Qubit states are parametrized by the Bloch sphere, so the average information is

$$I = -\frac{1}{4\pi} \int_{\mathbb{C}P^1} (|\alpha|^2 \log_2 |\alpha|^2 + |\beta|^2 \log_2 |\beta|^2) dS,$$

where dS is the area element and 4π comes from the area of the 2-sphere. To carry out this integral, we need an explicit parametrization of the Bloch sphere. A qubit state $\alpha|0\rangle + \beta|1\rangle$ is represented by an equivalence class $z = \beta/\alpha \in \mathbb{C}P^1$. By stereographic projection, it is the same as (x_1, x_2, x_3) in the standard 2-sphere. In

spherical coordinates, we have

$$I = -\frac{1}{4\pi}\int_0^{2\pi}\int_0^{\pi}\left[\left(\frac{1-cos\theta}{2}\right)log_2\left(\frac{1-cos\theta}{2}\right) + \left(\frac{1+cos\theta}{2}\right)log_2\left(\frac{1+cos\theta}{2}\right)\right]\sin\theta d\theta d\phi$$
$$= \frac{1}{2\ln 2}$$

□

This theorem is from [**CF**].

The situation is different for a known qubit state. If a qubit state is known, then it can be prepared repeatedly and measured differently. So given a qubit state and a number $0 \leqslant \alpha \leqslant 1$, we can obtain α bits of information by choosing the appropriate measurement. In general, given a qudit $|\psi\rangle \in \mathbb{C}^m, m \geqslant 3$, the average information obtained by doing a single measurement is $\frac{1}{\ln 2}\sum_{k=2}^{m}\frac{1}{k}$. If m is sufficiently large, the average information is approximately $\log_2 m - \frac{1-\gamma}{\ln 2}$, where $\gamma = 0.57722\ldots$ is Euler's constant.

2.3. n-qubits and computing problems

An n-qubit state is a nonzero vector in $(\mathbb{C}^2)^{\otimes n}$ up to nonzero scalars. Basis elements of $(\mathbb{C}^2)^{\otimes n}$ are in 1–1 correspondence with n-bit strings in $\mathbb{Z}_2^n$. This bit string basis is called the computational basis, and can be pictured as the vertices of an n-cube. It allows us to include classical computation into quantum computation: classical information processing uses only the basis vectors of n-qubits. We also denote $|i_1\cdots i_k\rangle$ as $|I\rangle$, where $i_1\cdots i_k$ is the binary expansion of $I \in \{0,1,\ldots,2^n-1\}$.

A computing problem is a Boolean map $f : \{0,1\}^* \circlearrowleft$, where $\{0,1\}^* = \bigcup_{n\geqslant 0}\mathbb{Z}_2^n$, which will be presented in the following Garey-Johnson form. A decision problem is simply a computing problem with range $\{0,1\}$.

- Problem: Primality
- Instance: an integer $N > 0$.
- Question: Is N prime?

As a Boolean map, primality is the function

$$f(x) = \begin{cases} 0 & \text{if } x \text{ is the binary expansion of a composite number} \\ 1 & \text{if } x \text{ is the binary expansion of a prime number} \end{cases}$$

An efficient classical algorithm to determine primality was recently developed.

- Problem: Factoring
- Instance: an integer $N > 0$.
- Question: What is the largest prime factor of N?

No efficient classical algorithm is known for factoring. One of the exciting achievements in quantum computation is Shor's factoring algorithm.

2.4. Universal gate set

A gate set $\mathcal{S}$ is the elementary operations that we will carry out repeatedly to complete a computational task. Each application of a gate is considered a single step, hence the number of gate applications in an algorithm represents consumed time, and is a complexity measure. A gate set should be physically realizable

and complicated enough to perform any computation given enough time. It is not mathematically possible to define when a gate set is physical as ultimately the answer comes from physical realization. Considering this physical constraint, we will require that all entries of gate matrices are algebraic numbers when we define complexity classes depending on a gate set. Generally, a gate set $\mathcal{S}$ is any collection of unitary matrices in $\bigcup_{n=1}^{\infty} \mathrm{U}(2^n)$. Our choice is

$$\mathcal{S} = \{H, \sigma_z^{\pm 1/4}, \mathrm{CNOT}\}$$

where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{is the Hadamard matrix}$$

$$\sigma_z^{\pm 1/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pm \pi i/4} \end{pmatrix} \qquad \text{is called the } \pi/8 \text{ gates}$$

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \text{in the basis } \big\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\big\} \text{ of two qubits.}$$

It is called controlled-NOT because the first qubit is the control bit, so that when it is $|0\rangle$, nothing is done to the second qubit, but when it is $|1\rangle$, the NOT gate is applied to the second qubit.

Definition 2.3.

(1) *An n-qubit quantum circuit over a gate set $\mathcal{S}$ is a map $U_L \colon (\mathbb{C}^2)^{\otimes n} \circlearrowleft$ composed of finitely many matrices of the form $\mathrm{id}_p \otimes g \otimes \mathrm{id}_q$, where $g \in \mathcal{S}$ and p, q can be 0.*

(2) *A gate set is universal if the collection of all n-qubit circuits forms a dense subset of $\mathrm{SU}(2^n)$ for any n.*

The gate set $\mathcal{S} = \{H, \sigma_z^{\pm 1/4}, \mathrm{CNOT}\}$ will be called the standard gate set, which we will use unless stated otherwise.

Theorem 2.4.

(1) *The standard gate set is universal.*

(2) *Every matrix in $\mathrm{U}(2^n)$ can be efficiently approximated up to an overall phase by a circuit over $\mathcal{S}$.*

The proof of (1) is quantum circuit design: implementation of unitary matrices with gates combined with knowledge of finite subgroups of $\mathrm{SU}(2)$. Statement (2) follows from (1) by the Kitaev-Solovay algorithm. An important trick, based on $[\mathrm{SU}(2), \mathrm{SU}(2)] = \mathrm{SU}(2)$, is to represent matrices in $\mathrm{SU}(2)$ as nested commutators.

Definition 2.5. *A matrix is 2-level if it is of the form*

$$\begin{pmatrix} a & b & & & \\ c & d & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

up to simultaneous permutation of rows and columns, i.e., with respect to the underlying basis, it is nontrivial on a subspace of dimension at most 2.

LEMMA 2.6. *Any unitary matrix U is a product of 2-level unitary matrices. In the case $U\colon (\mathbb{C}^2)^{\otimes n} \circlearrowleft$, the 2-level matrices are not necessarily of the form* $\mathrm{id}\otimes A\otimes\mathrm{id}$ *for some 2×2 unitary matrix A.*

DEFINITION 2.7. *A unitary matrix $\Lambda^{n-1}U\colon (\mathbb{C}^2)^{\otimes n} \circlearrowleft$ is a generalized controlled-U gate if there exists $U\in \mathrm{U}(2)$ such that*

$$\Lambda^{n-1}U|x_1\cdots x_n\rangle = \begin{cases} |x_1\cdots x_n\rangle & \text{if } x_i = 0 \text{ for some } 1\leqslant i\leqslant n-1 \\ |x_1\cdots x_{n-1}Ux_n\rangle & \text{if } x_i = 1 \text{ for all } 1\leqslant i\leqslant n-1 \end{cases}$$

where $|x_1\cdots x_{n-1}Ux_n\rangle = |x_1\cdots x_{n-1}\rangle\otimes U|x_n\rangle$.

LEMMA 2.8. *Every 2-level unitary matrix on $(\mathbb{C}^2)^{\otimes \mathrm{n}}$ is a composition of generalized controlled gates and 2×2 unitary matrices. Furthermore, this decomposition can be done efficiently.*

PROOF. Given a nontrivial 2-level matrix M, suppose $|x\rangle = |x_1\cdots x_n\rangle$, $|y\rangle = |y_1\cdots y_n\rangle$ are the two basis vectors on which M is nontrivial. Choose bit strings $I_1,\ldots,I_m$ in $\mathbb{Z}_2^n$ such that each I_{i+1} differs from I_i by 1 bit, with $|I_1\rangle = |x\rangle$ and $|I_m\rangle = |y\rangle$. One choice is a shortest path from $|x\rangle$ to $|y\rangle$ on the n-cube $\mathbb{Z}_2^n$. Then bring $|x\rangle$ adjacent to $|y\rangle$ through the $|I_1\rangle,\ldots,|I_m\rangle$, perform a generalized controlled-U gate, and afterwards bring $|x\rangle$ back to its original place. Note the control qubits might not be exactly the first $n-1$ qubits in the controlled-U gate, but some NOT gates can be used to fix this. □

LEMMA 2.9. *Any $\Lambda^{n-1}U$ gate can be realized by a quantum circuit over* $\{\mathrm{U}(2), \mathrm{CNOT}\}$.

PROOF. For all $U\in \mathrm{SU}(2)$,

$$U = V[A_1,\sigma_x]V^\dagger = V[[A_2,\sigma_x],\sigma_x]V^\dagger = \cdots$$

where $A_n = \begin{pmatrix} e^{i\alpha/2^n} & 0 \\ 0 & e^{-i\alpha/2^n} \end{pmatrix}$ and $e^{i\alpha}, e^{-i\alpha}$ are the two eigenvalues of U. Then deleting any σ_x collapses U to Id, which is a CNOT gate operation. An illustration should suffice to see the design. If $U = [[A,\sigma_x],\sigma_x]$, then $\Lambda^2 U$ is realized by Fig. 2.2. □

PROOF OF THM. 2.4. By Lemmas 2.6, 2.8, 2.9 it suffices to show that quantum circuits over $\{H,\sigma_z^{\pm 1/4}\}$ are dense in $\mathrm{SU}(2)$. The only nontrivial subgroups of $\mathrm{SU}(2)$ are S^1 and a few finite subgroups. So it suffices to show that quantum circuits are dense in two different circles of $\mathrm{SU}(2)$. □

2.5. Quantum circuit model

DEFINITION 2.10. *Let $\mathcal{S}$ be the gate set $\{H,\sigma_z^{\pm 1/4},\mathrm{CNOT}\}$. A problem $f : \{0,1\}^* \circlearrowleft$ (represented by $f_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^{m(n)}$) is in BQP (i.e., can be solved efficiently by a QC) if $\exists$ polynomials $a(n), g(n) : \mathbb{N} \circlearrowleft$ satisfying $n+a(n) = m(n)+g(n)$ and $\exists$ a classical efficient algorithm to output a function $\delta(n) : \mathbb{N}\to\{0,1\}^*$ describing a quantum circuit $U_{\delta(n)}$ over $\mathcal{S}$ of size $O(\mathrm{poly}(n))$ such that*

$$U_{\delta(n)}|x,0^{a(n)}\rangle = \sum_I a_I|I\rangle$$

$$\sum_{|I\rangle = |f(x)z\rangle} |a_I|^2 \geqslant 3/4, \quad \text{where } z\in\mathbb{Z}_2^{g(n)}$$

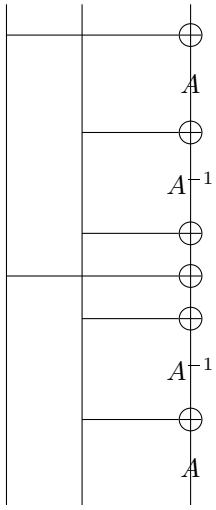


FIGURE 2.2. Quantum circuit realizing $\Lambda^2 U$.

The $a(n)$ qubits are ancillary working space, so we initialize an input $|x\rangle$ by appending $a(n)$ zeros and identify the resulting bit string as a basis vector in $(\mathbb{C}^2)^{\otimes(n+a(n))}$. The $g(n)$ qubits are garbage. The classical algorithm takes as input the length n and returns a description of the quantum circuit $U_{\delta(n)}$. For a given $|x\rangle$, the probability that the first $m(n)$ bits of the output equal $f_n(x)$ is $\geqslant 3/4$.

The class BQP is independent of the choice of gate set as long as the gate set is efficiently computable. The threshold $3/4$ can be replaced by any constant between $1/2$ and 1. In our definition of BQP, the quantum circuit $U_{\delta(n)}$ is uniform for all inputs $|x\rangle$ of length n. In Shor's algorithm, the quantum circuit for a fixed n depends on the input $|x\rangle$, but there is an efficient classical algorithm to convert Shor's algorithm into our formulation of BQP [**KSV**].

2.6. Simulating quantum physics

The QCM is an abstract quantum system with locality built in explicitly. The tensor decomposition allows us to choose only local unitary transformations to evolve the quantum system.

Realistic quantum Hamiltonians also have built-in locality, so it is natural for the QCM to simulate local Hamiltonians. A Hamiltonian H is k-local for some fixed integer k if $H = \sum_{i=1}^{L} H_i$ such that each H_i acts nontrivially only on at most k subsystems, and L is some constant. A more precise definition can be found in Chap. 8.

DEFINITION 2.11. *A Hamiltonian is content if* $[H_i, H_j] = 0$ *for any* i, j. *Otherwise it is frustrated.*

- Problem: Quantum simulation
- Instance: Fix a $k \geqslant 2$, a k-local Hamiltonian $H = \sum_{i \in L} H_i$ on an n-qubit system, an initial state $|\psi_0\rangle$, an evolution time t, and an error threshold $\delta > 0$.

- Question: Find a state $|\tilde{\psi}_f(t)\rangle$ such that

$$|\langle\tilde{\psi}_f(t)|e^{-\frac{i}{\hbar}Ht}|\psi_0\rangle|^2 \geqslant 1-\delta.$$

THEOREM 2.12. *There is a quantum algorithm of running time* $\mathrm{poly}(1/\delta)$ *to solve quantum simulation.*

This theorem was conjectured by Feynman and proven by S. Lloyd [**Ll**].

The algorithm is based on the Trotter formula. Let A, B be Hermitian operators. Then for any t,

$$\lim_{n\to\infty}\left(e^{iAt/n}e^{iBt/n}\right)^n = e^{i(A+B)t}$$

To illustrate, consider a content Hamiltonian $H=\sum_{i=1}^{L}H_i$. Then

$$e^{-\frac{i}{\hbar}Ht} = e^{-\frac{i}{\hbar}H_1t}e^{-\frac{i}{\hbar}H_2t}\cdots e^{-\frac{i}{\hbar}H_Lt}$$

for all t. If we pick a $\Delta t>0$ such that $|\langle\tilde{\psi}_f|e^{-\frac{i}{\hbar}Hn\Delta t}|\psi_0\rangle|^2 \geqslant 1-\delta$ for some $n\sim \mathrm{poly}(1/\delta)$ and $n\Delta t\sim t$, then with $\{e^{-\frac{i}{\hbar}H_i\Delta t}\}$ as a gate set, an efficient simulation is obvious.

For the frustrated case, we select a Δt and an approximation method with the prescribed accuracy. Using

$$e^{i(A+B)\Delta t} = e^{iA\Delta t}e^{iB\Delta t}+O(\Delta t^2) \quad \text{or}$$
$$e^{i(A+B)\Delta t} = e^{iA\frac{\Delta t}{2}}e^{iB\Delta t}e^{iA\frac{\Delta t}{2}}+O(\Delta t^3)$$

we then implement $e^{-iH\Delta t}$ by a qubit circuit over $\{e^{-iH_i\Delta t}\}$ and iterate j steps, until $j\Delta t\sim t_f$.

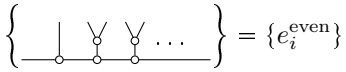
TQFTs have constant Hamiltonians H, which can be normalized to $H\equiv 0$, so Lloyd's simulation algorithm does not apply. But efficient simulation of TQFTs does exist. It might also be strange that a system with $H\equiv 0$ can have any interesting dynamics. While TQFTs have no continuous evolution except for an overall abelian phase, which makes their ground states an ideal place for quantum memory, they do have discrete evolutions.

THEOREM 2.13. *Fix a TQFT* (V,Z). *Given a surface* Σ, *possibly with labeled boundary, and a mapping class group* $\mathcal{M}(\Sigma)$ *element* b *in the standard generators of* $\mathcal{M}(\Sigma)$, *there exists a quantum circuit to simulate the representative matrix* $\rho(b)$ *of* b *afforded by* V *in* $\mathrm{poly}(|b|)$ *steps, where* $|b|$ *is the length of* b *in the standard generators.*

We illustrate this theorem with the braid group case. The n-strand braid group B_n has a presentation

$$\left\{\sigma_1,\ldots,\sigma_{n-1} \mid \sigma_i\sigma_j=\sigma_j\sigma_i \text{ if } |i-j|\geqslant 2,\ \sigma_i\sigma_{i\pm1}\sigma_i=\sigma_{i\pm1}\sigma_i\sigma_{i\pm1}\right\}$$

Therefore the braid generators separate into two classes: odd ones $\{\sigma_1,\sigma_3,\ldots\}$ and even ones $\{\sigma_2,\sigma_4,\ldots\}$. Within each class, the braid generators commute, and so can be simultaneously diagonalized. Suppose $V(\Sigma)$ is the representation space of B_n. Then there are two bases $\{e_i^{\mathrm{odd}}\},\{e_i^{\mathrm{even}}\}$ such that all odd (even) braid generators σ_i are diagonal on $\{e_i^{\mathrm{odd}}\}$ ($\{e_i^{\mathrm{even}}\}$).



The change of basis from $\{e_i^{\text{odd}}\}$ to $\{e_i^{\text{even}}\}$ and back can be implemented efficiently. The simulation is illustrated in Fig. 2.3. Given a braid b written in braid generators, say the first generator is odd, implement it on $\{e_i^{\text{odd}}\}$, continue till encountering an even generator, then switch to $\{e_i^{\text{even}}\}$ by F, and back and forth... For more details see [**FKW**]. To find the factors of a 100 digit integer with Shor's algorithm,

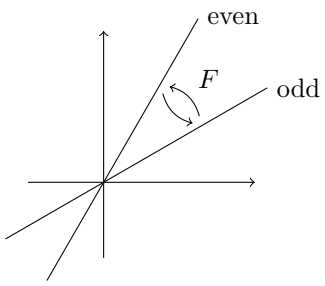


FIGURE 2.3. Basis change for braid simulation.

we would have to apply millions of quantum gates coherently without errors to hundreds of qubits, which is not possible with current technologies. On the other hand, a quantum computer could do interesting simulation with a few hundred operations on dozens of qubits that would take a classical computer Avogadro's number of operations to simulate. While quantum factoring of large integers seems far off, quantum toy machines for simulating quantum physics are very much within reach.

The most famous quantum algorithm is factoring, but the most useful is arguably simulation of quantum physics. By simulating quantum systems, we will better understand quantum materials such as FQH liquids, superconductors, and molecules. Quantum computing could even advance drug discovery.

CHAPTER 3

Approximation of the Jones Polynomial

In this chapter, we outline the quantum algorithm to efficiently approximate Jones evaluations and discuss their distribution in the plane. The algorithm applies equally to colored Jones evaluations and, with adequate notation, to all quantum invariants of links from RFCs.

3.1. Jones evaluation as a computing problem

The Jones polynomial $J(L;t)$ of an oriented link L in S^3 is a Laurent polynomial of $t^{\pm 1/2}$ with integer coefficients. Given L and a root of unity q, we wish to compute the Jones evaluation $J(L;q) \in \mathbb{Z}[q^{\pm 1/2}] \subset \mathbb{C}$. Since $J(L;q)$ is a partition function of a unitary topological quantum field theory (TQFT) only when $q = e^{\pm 2\pi i/r}$, $r \in \mathbb{Z}_+$, we will focus on these special roots of unity.

Computation of $J(L;q)$ is a map

$$J(L;q)\colon \{\text{oriented links } L\} \to \mathbb{Z}[q^{\pm 1/2}].$$

But computing problems are maps $f\colon \{0,1\}^* \circlearrowleft$, so we must encode the input L and the output $J(L;q)$ as bit strings. L can be given in many ways, e.g., by a link diagram or the plat or trace closure of a braid. Any such presentation can be encoded as a bit string. Over the basis of $\mathbb{Q}(q^{\pm 1/2})$ given by powers of $q^{1/2}$, we may write $J(L;q)$ as a string of integers, which is easily encoded as bit string. Hence with encodings the computation of $J(L;q)$ is a map

$$J(L;q)\colon \{0,1\}^* \circlearrowleft$$

Can we compute $J(L;q)$ efficiently? The computation can be either quantum mechanical or classical. Moreover rather than the exact answer we can ask for an approximation according to various approximation schemes. Therefore there are many ways to formulate the computation of the Jones polynomial as a computing problem. We will study two of them:

(1) Classical exact computation of $J(L;q)$
   - Problem: CEJ
   - Instance: An oriented link L, and $q = e^{\pm 2\pi i/r}$.
   - Question: What is $J(L;q)$ as a bit string?

(2) Quantum approximation of $J(L;q)$
   - Problem: QAJ_r
   - Instance: An unoriented link $\hat{\sigma}^{\mathrm{plat}}$ as the plat closure of a braid $\sigma \in B_{2n}$, and $q = e^{\pm 2\pi i/r}$.
   - Question: What is $\left|J(\hat{\sigma}^{\mathrm{plat}};q)/[2]^m\right|^2$ approximately?

For CEJ_r, the relevant complexity class is $\mathrm{FP}^{\#\mathrm{P}}$—the class of functions polynomial time Turing reducible to a function in #P. Since #P is not as well-known as P, we

recall its definition here. #P consists of counting problems, functions $f\colon \{0,1\}^* \to \mathbb{N}$, with the answer in $\mathbb{N}$ encoded as a bit string.

DEFINITION 3.1. *A counting relation is a subset $R \subset \{0,1\}^* \times \{0,1\}^*$ such that*

(1) There exists a polynomial $p(t)$ such that if $(x,y) \in R$, then $|y| \leqslant p(|x|)$.
(2) The characteristic function for the subset $L = \{x2y \mid (x,y) \in R\} \subset \{0,1,2\}^*$ is in FP*. The set $R(x) = \{y \mid (x,y) \in R\}$ will be called the solution for x. The counting function associated to R is the function $f_R : \{0,1\}^* \to \mathbb{N}$ such that $f_R(x) = |R(x)|$.*

Nondeterministic Turing machines give rise to counting relations. Given a nondeterministic Turing machine M and a polynomial $p(t)$, let

$$R_M(x) = \{y \mid y \text{ is a certificate for } x \text{ with } |y| \leqslant p(x)\}$$

Then R_M is the solution of a counting relation. A counting problem $f\colon \{0,1\}^* \to \mathbb{N}$ is in #P if $f = f_R$ for some counting relation R.

3.2. $\mathrm{FP}^{\#\mathrm{P}}$-completeness of Jones evaluation

Computing the Jones polynomial classically is hard: either by the skein relation or state sums. This difficulty is likely to be intrinsic as evidenced by the following theorem:

THEOREM 3.2.

(1) $\mathrm{CEJ}_r \in \mathrm{FP}$ if $r = 1,2,3,4,6$.
(2) CEJ_r is $\mathrm{FP}^{\#\mathrm{P}}$-complete if $r \neq 1,2,3,4,6$.

We will call the root $q = e^{\pm 2\pi i/r}$ easy if $r = 1,2,3,4,6$ and hard otherwise. Note that $1,2,3,4,6$ are the only rotational symmetries of a translation invariant lattice in the plane. Therefore the Jones evaluations $J(L;q)$ lie in a lattice for the easy roots.

The first proof of this theorem [**V**] deduces the complexity from Tutte polynomials. A recent direct proof [**WY**] depends on density results for Jones representations [**FLW2**]. $J(L;q)$ has a classical knot-theoretic interpretation at each easy root:

- $J(L;1) = (-2)^{c(L)}$, where $c(L)$ is the number of components of L.
- $J(L;-1) = \Delta_L(-1)$, where Δ_L is the Alexander polynomial of L, which is polynomial time computable as a polynomial.
- $J(L;e^{2\pi i/3}) = 1$.
- $J(L;i) = \begin{cases} 0 & \text{if } \mathrm{Arf}(L) \text{ does not exist} \\ (-2\sqrt{2})^{c(L)} \cdot (-1)^{\mathrm{Arf}(L)} & \text{otherwise} \end{cases}$
- $J(L;e^{\pi i/3}) = \delta(L) i^{c(L)} (i\sqrt{3})^m$, where $\delta(L) = \pm 1$ and m is the first $\mathbb{Z}_3$–Betti number of the double cyclic branched cover of L.

For the hard roots, it is commonly stated that CEJ_r is #P-hard. From this result it can be deduced that CEJ_r is $\mathrm{FP}^{\#\mathrm{P}}$-complete. $J(L;t)$ of an alternating link L is the specialization to $xy = 1$ of the Tutte polynomial $T(G_L;x,y)$ of the medial planar graph G_L [**Ja**]. On the Tutte plane there are #P-complete counting problems, such as k-colorings of graphs for $k \geqslant 3$. Using Lagrangian interpolation we can reduce Jones evaluation to a counting problem in polynomial time. This hardness result of Jones evaluations is independent of the presentation of L as a link diagram or

braid closure. There are polynomial time algorithms to convert a link diagram to a braid closure.

The Tutte polynomial is a graph invariant in two variables x, y. Many graph invariants in physics and computer science are specializations of the Tutte polynomial. It can be defined using the deletion-contraction relation:

DEFINITION 3.3. *If G has no edges, then $T(G; x, y) = 1$. Otherwise, for any edge e,*

$$T(G;x,y) = \begin{cases} xT(G/e;x,y) & \text{if } e \text{ is an isthmus } (=\text{bridge}), \\ yT(G\backslash e;x,y) & \text{if } e \text{ is a loop}, \\ T(G/e;x,y) + T(G\backslash e;x,y) & \text{otherwise}, \end{cases}$$

where G/e (resp. $G\backslash e$) is the graph G with e contracted (resp. deleted). Obviously $T(G; x, y)$ is a polynomial in the variables x, y, called the Tutte polynomial.

The faces of a link diagram D can be 2-colored, say black–white, such that faces sharing an edge have different colors. For simplicity, assume D is alternating (otherwise use signed graphs). To convert D into a graph G_D, pick a 2-coloring and let vertices of G_D be black faces, connecting two vertices iff they share a crossing. To go from a graph G to a link diagram D_G, we first construct the so-called medial graph $m(G)$ of G: vertices of $m(G)$ are midpoints of edges of G, and two vertices are connected by an edge in $m(G)$ if the corresponding edges in G are consecutive edges of a face including the infinite face. An oriented link diagram is positive if every crossing is positive.

PROPOSITION 3.4. *If D is a positive alternating link diagram, then $\langle D\rangle = A^{2V-E-2}T(G; -A^{-4}, -A^4)$, where V (resp. E) is the number of vertices (resp. edges) in the associated graph G of D.*

THEOREM 3.5. *The complexity of computing the Tutte polynomial of a planar graph at an algebraic point (x, y) in the Tutte plane is* P *if $(x-1)(y-1) \in \{1, 2\}$ or $(x, y) \in \{(1, 1), (-1, -1), (e^{2\pi i/3}, e^{4\pi i/3}), (e^{4\pi i/3}, e^{2\pi i/3}\}$, and* $\mathrm{FP}^{\#\mathrm{P}}$ *otherwise.*

This theorem is in [**V**]. Let H_q be the curve $(x-1)(y-1) = q$ in the Tutte plane. For G planar and $q \in \mathbb{Z}_+\backslash\{1\}$, $T(G, x, y)$ specialized to H_q is the partition function of the q-state Potts model. Along H_1, $T(G; x, y) = x^E(1-x)^{V-E-k}$, where E, V, k denote respectively the number of edges, vertices, and connected components of G. Along H_2, $T(G; x, y)$ is the partition function of the Ising model, which is exactly solvable for planar graphs. Specializing to $xy = 1$ yields Thm. 3.2.

3.3. Quantum approximation

This section describes a quantum approximation algorithm for Jones evaluation at $q = e^{\pm 2\pi i/r}$. When q is easy, we need not approximate $J(L; q)$ since it can be computed exactly in polynomial time. Hence we will consider only hard roots for $r = 5$ or $r \geqslant 7$. The goal is

THEOREM 3.6. QAJ_r *is* BQP*-complete for $r \neq 1, 2, 3, 4, 6$.*

In this section, we will only prove one direction: $\mathrm{QAJ}_r \in \mathrm{BQP}$, i.e., there exists an efficient quantum algorithm to approximate $J(L; q)$. There are various approximation schemes; ours is an additive approximation of $|J(L; q)|^2$. One drawback is the dependence on how L is presented: if L is given as the plat closure $\hat{\sigma}^{\mathrm{plat}}$ of a

braid $\sigma \in B_{2n}$, then we are approximating $|J(\hat{\sigma}^{\text{plat}}; q)/d^n|^2$ up to additive errors. Obviously the errors are sensitive to the approximation scheme, though a friendlier approximation such as FPRAS is unlikely [**Wel**].

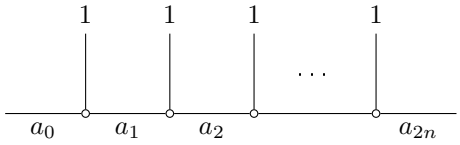
THEOREM 3.7. *For $q = e^{\pm 2\pi i/r}$, there is an efficient classical algorithm which, given a length m braid word $\sigma \in B_{2n}$ and an error threshold $\delta > 0$, outputs a size* $\text{poly}(n, m, 1/\delta)$ *quantum circuit returning a random variable $0 \leqslant Z(\sigma) \leqslant 1$ with*

$$\Pr\left\{\left|\left|\frac{J(\hat{\sigma}^{\text{plat}}; q)}{d^n}\right|^2 - Z(\sigma)\right| \leqslant \delta\right\} \geqslant \frac{3}{4} \tag{3.8}$$

The proof follows from a detailed analysis of the Jones representation ρ of braids.

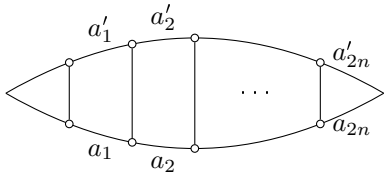
Recall ρ is unitary for Kauffman variable $A = \pm ie^{\pm 2\pi i/4r}$ when $q = A^{-4}$. One unnormalized basis for the representation is

$e^U_{B;a_{2n}} =$



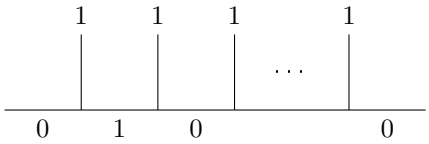
where $a_i \in \{0, 1, \ldots, r-2\}$ and $B = (a_0, \ldots, a_{2n})$. By parity of fusion rules, each a_{2n} is even and corresponds to an irreducible summand of ρ. For our plat closure case, $a_{2n} = 0$; we will denote $e^U_{B;0}$ as e^U_B. The inner product of two basis vectors $e^U_{B_1}, e^U_{B_2}$ is the evaluation of the trivalent network

$\langle e^U_{B_1}, e^U_{B_2}\rangle =$



Let $\{e^U_B\}$ be the orthogonal basis with respect to this inner product.

Let $|\text{cup}\rangle =$



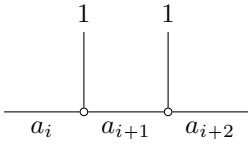
$= \bigcup\bigcup\cdots\bigcup$

and $|\text{cap}\rangle = |\text{cup}\rangle^\dagger$ $= \bigcap\bigcap\cdots\bigcap$

Then $|J(\hat{\sigma}^{\text{plat}}; q)| = \langle \text{cap}|\rho(\sigma)|\text{cup}\rangle$. Note $\langle \text{cap}|\text{cup}\rangle = d^n$.

LEMMA 3.9. *$\rho(\sigma)$ can be efficiently implemented by a quantum circuit.*

PROOF. Around any two adjacent vertices, we have part of the basis picture



From the fusion rules, $a_{i+1} = a_i \pm 1$. Now we can turn a basis vector into a bit string by starting from $0 = a_0$: each next bit is 1 if a_{i+1} increases from a_i or 0 if a_{i+1} decreases from a_i. This is an efficient embedding of the representation space $\mathrm{Hom}(0, 1^{2n})$ into $(\mathbb{C}^2)^{\otimes 2n}$, which turns each basis vector e_B^U into a bit string $I_B = (b_0, b_1, \ldots, b_{2n})$, where $b_0 = b_{2n} = 0$. Elementary braids act on each e_B^U by vertical stacking. The calculation in Thm. 1.31 shows $\rho_A(\sigma_i)$ is block diagonal with at most 2×2 blocks, which depend only on $a_{i+1} \in \{0, 1, \ldots, k\}$. The label a_{i+1} can be computed efficiently from the bit string I_B as $a_{i+1} = a_i + (-1)^{b_i+1}$. We store the values of a_{i+1} in a few ancillary qubits. Then $\rho_A(\sigma_i)$ is a unitary matrix on the $(i+1)$-qubit and the ancillary qubits. Such matrices can be efficiently simulated by quantum gates. □

Each run of the algorithm returns a random variable $\tilde{Z}(\sigma) \in [0, 1]$ such that

$$\Pr\big(\tilde{Z}(\sigma) = 1\big) = \big|\langle \mathrm{cap}|\rho(\sigma)|\mathrm{cup}\rangle\big|^2 = \left|\frac{J(\hat{\sigma}^{\mathrm{plat}}; q)}{d^n}\right|^2$$

Let $Z(\sigma)$ be the average of $\tilde{Z}(\sigma)$ over $\mathrm{poly}(1/\delta)$ iterations. Then Eqn. (3.8) follows from the Chernoff bound [**NC**]. The approximation algorithm follows from the simulation theorem in [**FKW**] with the exact nature of the approximation clarified in [**BFLW**]. It was observed in [**AJL**] that the algorithm can be strengthened to approximate $J(L; q)$ as a complex number. An algorithm approximating non-unitary Jones evaluations is given in [**AAEL**]. Quantum approximation to non-unitary points appears surprising, but computing problems are not bound by unitarity. In [**SJ**], the difference between the plat and trace closures is examined: approximating the trace closure of Jones evaluations is complete for the one clean qubit model, which is expected to be strictly weaker than QCM.

The approximation applies to the colored Jones polynomial without much modification other than using qudits, and similarly to other quantum link invariants.

3.4. Distribution of Jones evaluations

Given $t \in \mathbb{C}\backslash\{0\}$, the Jones evaluations $J(L; t)$ of all links L form a subset of the complex plane $\mathbb{C}$. We can ask how they are distributed. There are two obvious cases: discrete and dense. At an easy root q, Jones evaluations lie in a lattice, while at a hard root, they are is dense. Non-density seems to be related to computationally easy specializations. It is tempting to guess that computational tractability of this problem is related to certain lattice structures in the evaluation, but that is not quite true. In the case of the Alexander-Conway polynomial in the variable $z = t^{1/2} + t^{-1/2}$, the whole polynomial is polynomial time computable and all specializations lie on the real axis. On the other hand, as discussed in Sec. 7.6, computing the Reshetikhin-Turaev invariant at a fourth root of unity for arbitrary 3-manifolds is #P-hard, though all 3-manifold invariants lie in $\mathbb{Z}[\omega]$, where ω is some primitive sixteenth root of unity

The limiting distribution depends on the filtration of all links. For B_n we use the standard generators $\{\sigma_1^{\pm}, \ldots, \sigma_{n-1}^{\pm}\}$, and non-reduced braid words. Given a special root $q = e^{\pm 2\pi i/r}$, a braid index n, and a subset $S \subset \mathbb{C}$, let $N_{r,n,l,S}$ be the number of length l non-reduced braid words with Jones evaluation in S.

Theorem 3.10.

(1) *At an easy root* q, $\{J(L;q)\}$ *lies in the lattice* $\mathbb{Z}[q^{\pm 1/2}]$. *At a hard root* q, $\{J(L;q)\}$ *is dense in* $\mathbb{C}$.
(2) $N_{r,n,l,S}/(2n)^l$ *limits to a measure* $\mu_{r,n}$ *on* $\mathbb{C}$ *in the weak-*$*$ *limit as* $l \to \infty$.
(3) *In the weak-*$*$ *limit* $\mu_{r,n}$ *has a limit* μ_r, *the Gaussian* $e^{-\frac{z\bar{z}}{\sigma_r}} dz d\bar{z}/2\pi\sigma_r$, *where* $\sigma_r = r/\sin^2(2\pi/r)$.

For a proof, see [**FLW2**].

The same result holds for braids whose closures are knots. It follows that Jones evaluation under this filtration centers around the origin. It is an interesting question to find links such that $J(L;q) = 0$, because zeros of Jones polynomials, in general of partition functions, contain interesting information about the physical system. For the easy roots q, it is very likely that every lattice point in $\mathbb{Z}[q^{\pm 1/2}]$ is realized by a knot. Computer plotting of such Jones evaluations of prime knots up to 13 crossings seems to show a different distribution [**DLL**], which hints at the dependence on filtration of knots.

CHAPTER 4

Ribbon Fusion Categories

This chapter introduces the most important concept of the book: ribbon fusion categories (RFCs). In the literature, they are also called premodular categories. With an extra nondegeneracy condition for the braiding, they are called modular tensor categories (MTCs). Unitary modular tensor categories (UMTCs) are the algebraic models of anyons and the algebraic data for unitary TQFTs. In the end we list all UMTCs of rank $\leqslant 4$.

4.1. Fusion rules and fusion categories

Group theory is an abstraction of symmetry, which is fundamental to mathematics and physics. Finite groups are closely related to the classification of crystals. Fusion categories can be regarded as quantum generalizations of finite groups. The simplest finite groups are abelian. Pursuing this analogy, we can consider RFCs as quantum generalizations of finite abelian groups.

DEFINITION 4.1.

(1) *A label set L is a finite set with a distinguished element 1 and an involution $\hat{\ }: L \circlearrowleft$ such that $\hat{1} = 1$. Elements of L are called labels, 1 is called the trivial label, sometimes written 0, and $\hat{\ }$ is called duality.*

(2) *A fusion rule on a label set L is a binary operation $\otimes\colon L \times L \to \mathbb{N}^L$, where $\mathbb{N}^L$ is the set of all maps from L to $\mathbb{N} = \{0, 1, 2, \ldots\}$ satisfying the following conditions. First we introduce some notation. Given $a, b \in L$, we will write formally $a \otimes b = \bigoplus N_{ab}^c c$ where $N_{ab}^c = (a \otimes b)(c)$. When no confusion arises, we write $a \otimes b$ simply as ab, so $a^2 = a \otimes a$. Then the conditions on $\otimes$ are: for all $a, b, c, d \in L$,*

(i) $(a \otimes b) \otimes c = a \otimes (b \otimes c)$, *i.e.,* $\sum_{x \in L} N_{ab}^x N_{xc}^d = \sum_{x \in L} N_{bc}^x N_{ax}^d$

(ii) $N_{a1}^c = N_{1a}^c = \delta_{ca}$

(iii) $N_{ab}^1 = N_{b\hat{a}}^1 = \delta_{b\hat{a}}$

We say a triple of labels (a, b, c) is admissible if $N_{ab}^c \neq 0$. We often refer to an instances of the equation $a \otimes b = \bigoplus N_{ab}^c c$ as a fusion rule, though technically $\otimes$ itself is the fusion rule. Since $1 \otimes a = a = a \otimes 1$, in the future we would not list such trivial fusion rules.

EXAMPLE 4.2. *A finite group G is a label set with elements of G as labels, trivial label 1, and $\hat{g} = g^{-1}$. A fusion rule on G is $g \otimes h = gh$, i.e., $(g \otimes h)(k) = \delta_{gh,k}$.*

EXAMPLE 4.3 (Tambara-Yamagami [**TY**]). *Given a finite group G, the label set $L = G \sqcup \{m\}$, where $m \notin G$, with fusion rule*

$$g \otimes h = gh, \qquad m \otimes g = g \otimes m = m, \qquad m^2 = \bigoplus_{g \in G} g$$

for $g, h \in G$. When $G = \mathbb{Z}_2$, this is the Ising fusion rule.

EXAMPLE 4.4. *Fermionic Moore-Read fusion rule: the label set is*

$$L = \{1, \alpha, \psi, \alpha', \sigma, \sigma'\}$$

If the subset $\{1, \alpha, \psi, \alpha'\}$ *is identified with* $\{0, 1, 2, 3\} = \mathbb{Z}_4$*, then the fusion rule for* $\{1, \alpha, \psi, \alpha'\}$ *agrees with* $\mathbb{Z}_4$*. The others are*

$$\sigma\sigma' = \sigma'\sigma = 1 \oplus \psi \qquad \sigma^2 = (\sigma')^2 = \alpha \oplus \alpha'$$
$$\sigma\psi = \psi\sigma = \sigma \qquad \sigma'\psi = \psi\sigma' = \sigma'$$
$$\sigma\alpha = \sigma\alpha' = \alpha\sigma = \alpha'\sigma = \sigma' \qquad \sigma'\alpha = \sigma'\alpha' = \alpha\sigma' = \alpha'\sigma' = \sigma$$

A fusion rule on a label set L is part of the notion of a fusion category. There are several equivalent definitions of a fusion category, e.g., in categorical language or with 6j symbols. An analogous situation is the definition of a connection in differential geometry: either coordinate-free or with Christoffel symbols. The categorical definition is more common in the mathematical literature; 6j symbols are more convenient for physics and quantum computing. This section presents the 6j symbol definition.

DEFINITION 4.5. *A fusion rule is multiplicity-free if* $N_{ab}^c \in \{0, 1\}$ *for any* a, b, c*.*

Examples 4.2, 4.3, 4.4 are all multiplicity-free. For a non–multiplicity-free fusion rule realized by fusion categories, consider

EXAMPLE 4.6 ($\frac{1}{2}E_6$ fusion rule). *Label set* $L = \{1, x, y\}$*,*

$$x^2 = 1 \oplus 2x \oplus y, \qquad xy = yx = x, \qquad y^2 = 1.$$

For simplicity we will only consider multiplicity-free fusion rules.

DEFINITION 4.7 (6j symbols). *Given a fusion rule on a label set* L*, a 6j symbol system is a map* $F\colon L^6 \to \mathbb{C}$ *satisfying the conditions enumerated below. We say a sextuple of labels* (a, b, c, d, n, m) *is admissible if* (a, b, m)*,* (m, c, d)*,* (b, c, n)*, and* (a, n, d) *are admissible (see Fig. 4.1). We write* $F_{d;nm}^{abc}$ *for* $F(a, b, c, d, n, m)$*, and* F_d^{abc} *for the matrix with* (n, m)*-entry* $F_{d;nm}^{abc}$*, where the indices* n, m *range over all labels making* (a, b, c, d, n, m) *admissible.*

(1) Admissibility:
  (i) If (a, b, c, d, n, m) *is not admissible, then* $F_{d;nm}^{abc} = 0$*.*
  (ii) Each matrix F_d^{abc} *is invertible.*

(2) Pentagon axiom: for all $a, b, c, d, e, f, p, q, m \in L$*,*

$$\sum_n F_{q;pn}^{bcd} F_{f;qe}^{and} F_{e;nm}^{abc} = F_{f;qm}^{abp} F_{f;pe}^{mcd}$$

$F_{d;nm}^{abc}$ *is called a 6j symbol;* F_d^{abc} *is called an* F*-matrix. Note that in our convention an* F*-matrix may be empty, i.e., the* 0×0 *identity matrix. Fig. 4.1 gives the pictorial intuition for* F*, to be made rigorous in the next section.*

A 6j symbol system leads to a binary operation $\otimes$ on L-graded vector spaces with consistent associativity, but not necessarily to a monoidal or fusion category. A monoidal category needs a unit, furnished by the triangle axiom below. A fusion category furthermore needs consistent duals—rigidity.

DEFINITION 4.8. *A 6j fusion system is a 6j symbol system satisfying*

(1) Triangle axiom: $F_d^{abc} = \mathrm{Id}$ *whenever* $1 \in \{a, b, c\}$*.*

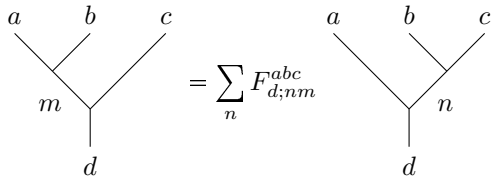


FIGURE 4.1. Diagrammatic 6j symbol definition.

(2) Rigidity: For any $a \in L$, let $G^{\hat{a}a\hat{a}}_{\hat{a}}$ be the inverse matrix of $F^{\hat{a}a\hat{a}}_{\hat{a}}$, with (m,n)-entry $G^{\hat{a}a\hat{a}}_{\hat{a};mn}$. Then $F^{a\hat{a}a}_{a;11} = G^{\hat{a}a\hat{a}}_{\hat{a};11}$.

DEFINITION 4.9. *Two 6j fusion systems F and $\tilde{F}$ with label set L are gauge equivalent if there is a function $f\colon L^3 \to \mathbb{C}\colon (a,b,c) \mapsto f^{ab}_c$, called a gauge transformation, such that:*

(1) $f^{ab}_c \neq 0$ iff (a,b,c) is admissible.
(2) $f^{1a}_a = f^{a1}_a = 1$ for all $a \in L$.
(3) Rectangle axiom: for all $a,b,c,d,n,m \in L$,

$$f^{bc}_n f^{an}_d F^{abc}_{d;nm} = \tilde{F}^{abc}_{d;nm} f^{ab}_m f^{mc}_d$$

DEFINITION 4.10.

(1) An automorphism of a fusion rule is a label permutation α satisfying $N^{\alpha(z)}_{\alpha(x)\alpha(y)} = N^z_{xy}$ for all x,y,z.
(2) Two 6j fusion systems sharing labels are equivalent if they are gauge equivalent up to a label permutation. Note that this permutation is necessarily an automorphism.

THEOREM 4.11.

(1) 6j fusion systems up to equivalence are in 1–1 correspondence with fusion categories up to $\mathbb{C}$-linear monoidal equivalence.
(2) (Ocneanu rigidity) There are only finitely many equivalence classes of fusion categories with a given fusion rule.

The first statement is in [**Y1**]. For a proof of the second, see [**ENO, Ki2, Hag**].

EXAMPLE 4.12. *Let G be an finite abelian group, viewed as a fusion rule as in Exmp. 4.2. Then 6j fusion systems up to gauge equivalence are in 1–1 correspondence with $H^3(G;\mathbb{C}^\times)$. By Thm. 4.11, the number of fusion categories is the number of orbits of $H^3(G;\mathbb{C}^\times)$ under automorphisms of G. If $G = \mathbb{Z}_m$, then $H^3(G;\mathbb{C}^\times) \cong \mathbb{Z}_m$. A generator is given by the 3-cocycle $f\colon G^3 \to \mathbb{C}^\times$*

$$f(a,b,c) = e^{2\pi i \overline{a}\left(\overline{b}+\overline{c}-\overline{b+c}\right)/m^2}$$

where $\overline{x} \in \{0,1,\dots,m-1\}$ is the residue of x modulo m. The cocycle f corresponds to the 6j fusion system F given by $F^{a,b,c}_{abc;bc,ab} = f(a,b,c)$. For $m = 3$, the cocycles f and f^2 are equivalent by a permutation of G, hence there are only two fusion categories with fusion rule $\mathbb{Z}_3$.

Fusion categories with fusion rules in Exmps. 4.3 and 4.6 are classified in [**TY**] and [**HH**] respectively. The case of nilpotent fusion rules with maximal subgroups of index two, generalizing Exmps. 4.3 and 4.4, is analyzed in [**Li**].

The cardinality of the label set is called the rank of the fusion category. Classification of fusion categories can be pursued like classification of finite groups, but this is too difficult for now. For our applications, our fusion categories have more structure, in particular braidings (Fig. 4.2). While the dual of an object is analogous to the inverse in group theory, braiding is the analogue of abelianity.

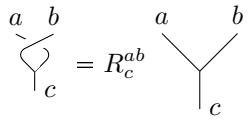


FIGURE 4.2. Braiding

DEFINITION 4.13. *A braiding on a 6j symbol system with label set L is function $L^3 \to \mathbb{C}\colon (a,b,c) \mapsto R_c^{ab}$ such that*

(1) $R_c^{ab} \neq 0$ if (a,b,c) is admissible.

(2) Hexagon axiom: For all $a,b,c,d,e,m \in L$,

$$(R_e^{ac})^{\pm 1} F_{d;em}^{bac} (R_m^{ab})^{\pm 1} = \sum_n F_{d;en}^{bca} (R_d^{an})^{\pm 1} F_{d;nm}^{abc}$$

As we can see, a braided 6j fusion system has an enormous amount of data. It is almost impossible to remember the equations if we don't have good book-keeping. Fortunately, there is a graphical calculus to organize everything, which not only makes all equations easy to derive, but also makes physical sense. The next section introduces this graphical calculus as a calculus for morphism spaces which also serves as a book-keeping device.

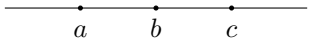
A braided fusion category is not always ribbon, which requires a pivotal structure compatible with the braiding, and does not necessarily have a well-behaved trace which defines quantum invariants. We will define these structures in the next section using graphical calculus.

4.2. Graphical calculus of RFCs

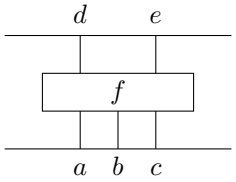
In categorical language, a fusion category $\mathcal{C}$ is a rigid semisimple $\mathbb{C}$-linear monoidal category with finitely many isomorphism classes of simple objects such that the monoidal unit is simple. Recall that an object x is simple iff $\mathrm{Hom}(x,x) \cong \mathbb{C}$. It follows that the morphism space $\mathrm{Hom}(x,y)$ between any two objects x,y is a finite-dimensional vector space. To finite approximation, a fusion category is a collection of compatible vector spaces labeled by pairs of objects. The graphical calculus of a RFC is a calculus of bases of these morphism spaces. Colored links for unitary theories have a direct interpretation as anyon trajectories in (2+1)-spacetime, and quantum invariants of links become amplitudes of these physical processes. We will return to this physical interpretation in Chap. 6. For graphical calculus, we assume our category is strict.

The label set of a 6j fusion system is the set of isomorphism classes of simple objects in the categorical definition of a fusion category. The tensor product of labels induced by any representative set of simple objects is given by the fusion rule. The F-matrix F_d^{abc} is a basis-change matrix of $\mathrm{Hom}(d, a \otimes b \otimes c)$ since our fusion category is strict (or an identification of $\mathrm{Hom}(d,(a\otimes b)\otimes c)$ with $\mathrm{Hom}(d, a\otimes(b\otimes c))$ if

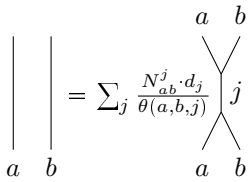
$\mathcal{C}$ is not strict). We are going to use graphs to represent special morphisms between tensor products and direct sums of simple objects. Labeled points on the real axis such as



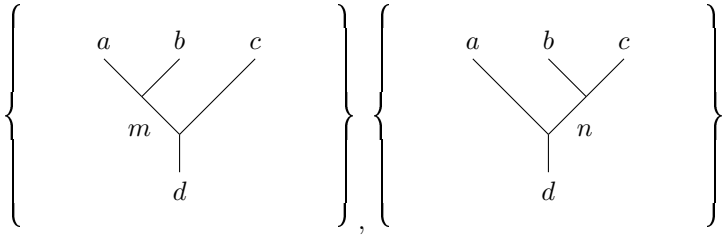
represent the object $a\otimes b\otimes c\otimes\cdots$, which is well-defined since our category is strict. A morphism such as $f\colon a\otimes b\otimes c\to d\otimes e$ is represented as



in the coupon notation. Recall that in our convention, morphisms or time flow upwards. We don't draw arrows in our graphs. Semisimplicity implies that it suffices to consider only trivalent morphisms. For example,



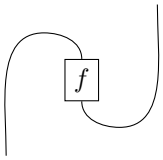
where $\theta(a,b,c)=\sqrt{d_a d_b d_c}$ is called the θ-symbol. The graphs



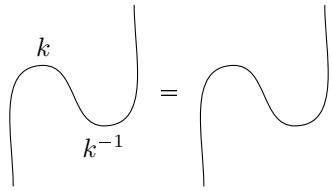
both are bases of the vector space $\mathrm{Hom}(d, a\otimes b\otimes c)$. Therefore there is a matrix relating the two bases, which is the F-matrix F_d^{abc} in a 6j fusion system. The unit is depicted as emptiness or a point labeled 1. Therefore a strand labeled 1 can be dropped or introduced anywhere. To represent right rigidity, we choose special morphisms $b_x\in\mathrm{Hom}(1, x\otimes x^*)$ and $d_x\in\mathrm{Hom}(x^*\otimes x, 1)$ and draw them as

We can then define the dual of $f\colon x \to y$ as follows

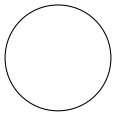
$$f^*\colon y^* \to x^*$$

$f^* =$ 

making * into a contravariant functor $^*\colon \mathcal{C} \circlearrowleft$. Note that



for any $k \in \mathbb{C}\backslash\{0\}$. Since we have no graphical representation for left rigidity, diagrams like



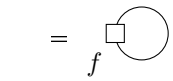
which would be the quantum trace of id_x, do not yet have an interpretation. To define the quantum trace, we need our fusion category to have a pivotal structure.

Definition 4.14.

(1) If there are isomorphisms $\phi_x\colon x \to x^{**}$ such that
(i) $\phi_{x\otimes y} = \phi_x \otimes \phi_y$
(ii) $f^{**} = f$
then we say the fusion category is pivotal.

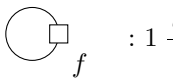
(2) In a pivotal category, we can define a right trace and a left trace, but they are not necessarily equal. Given $f\colon x \circlearrowleft$,

$$\mathrm{Tr}^r(f) = d_{x^*} \circ (\phi_x \otimes \mathrm{id}_{x^*}) \circ (f \otimes \mathrm{id}_{x^*}) \circ b_x$$

$=$ 

$: 1 \xrightarrow{b_x} x \otimes x^* \xrightarrow{f\otimes \mathrm{id}_{x^*}} x \otimes x^* \xrightarrow{\phi_x \otimes \mathrm{id}_{x^*}} x^{**} \otimes x^* \xrightarrow{d_{x^*}} 1$

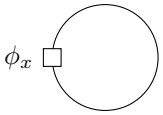
$$\mathrm{Tr}^l(f) = d_x \circ (d_{x^*} \otimes f) \circ (\mathrm{id} \otimes \phi_x^{-1}) \circ b_{x^*}$$

$=$ 

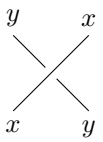
$: 1 \xrightarrow{b_{x^*}} x^* \otimes x^{**} \xrightarrow{\mathrm{id}\otimes\phi_x^{-1}} x^* \otimes x \xrightarrow{\mathrm{id}_{x^*}\otimes f} x^* \otimes x \xrightarrow{d_x} 1$

(3) If $\mathrm{Tr}^r(f) = \mathrm{Tr}^l(f)$ for all f, then the pivotal category is spherical.

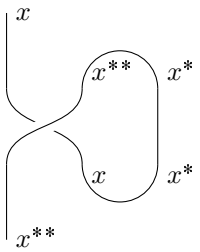
With the insertion of ϕ_x into our diagrams, each diagram has an interpretation. In particular, the quantum trace



of any object x is defined. It is conjectured that every fusion category is pivotal [**ENO**]. If the fusion category is also braided, then we will represent the braiding $c_{x,y}\colon x \otimes y \to y \otimes x$ by



A braiding also gives an isomorphism $\psi_x\colon x^{**} \mapsto x$ by



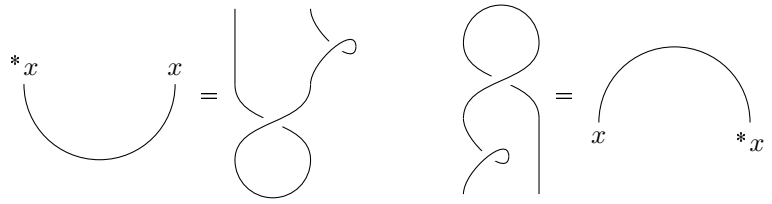
which usually does not satisfy $\psi_{x\otimes y} = \psi_x \otimes \psi_y$.

Definition 4.15.

(1) A braiding is compatible with a pivotal structure ϕ_a if the isomorphism $\theta_a = \psi_a\phi_a$ satisfies $\theta_{a^*} = \theta_a^*$. (Note that * is not complex conjugation).
(2) A RFC is a pivotal fusion category with a compatible braiding.

In the graphical calculus θ_a is given as

with the understanding that ϕ_a is applied. Therefore morphisms in a RFC can be conveniently represented by graphs in the plane with trivalent vertices and crossings, which are invariant under topological changes. Expressed differently, the axioms of a RFC are formulated so that it has a graphical calculus for morphisms which is fully topologically invariant in the plane. Left birth and death are given by



RFCs can also be defined with 6j symbols.

Proposition 4.16.

(1) *A fusion category given by a 6j fusion system is pivotal if there is a choice of a root of unity t_a for each label a satisfying the pivotal axioms:*

$$t_1 = 1$$
$$t_{a*} = t_a^{-1}$$
$$t_a^{-1} t_b^{-1} t_c = F^{a,b,c^*}_{1;a^*,c} F^{b,c^*,a}_{1;a^*,a} F^{c^*,a,b}_{1;b^*,b}$$

for each admissible triple (a, b, c). The $\{t_a\}$ will be called pivotal coefficients.

(2) *The pivotal structure is spherical if all $t_a = \pm 1$.*

(3) *A braided spherical category is ribbon.*

When a braided fusion category has multiplicity, it seems unknown if there is always a choice of bases of triangular spaces $V_c^{ab} = \mathrm{Hom}(c, a \otimes b)$ so that the braidings on V_c^{ab} are all diagonal.

All equations among RFC morphisms have graphical calculus descriptions. We leave them to the reader for practice. For example, the pentagon and hexagon axioms take the form of Figs. 4.3, 4.4. Summarizing, we defined a RFC in terms

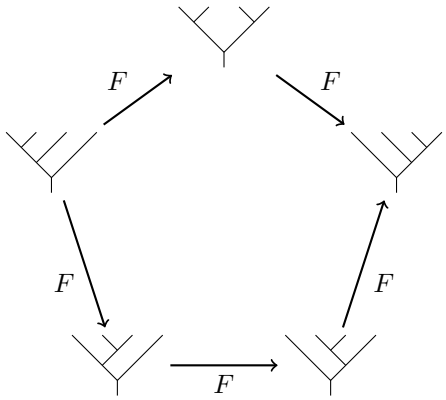


FIGURE 4.3. Schematic of the pentagon axiom.

of 6j symbols $\{F^{abc}_{d;nm}\}$, braidings $\{R^{ab}_c\}$, and pivotal coefficients $\{t_i\}$.

THEOREM 4.17. *A RFC with multiplicity-free fusion rule is a collection of numbers $\{F^{abc}_{d;mn}\}, \{R^{ab}_c\}, \{t_i = \pm 1\}$ satisfying the pentagon, triangle, rigidity, hexagon, and pivotal axioms.*

A similar theorem holds for RFCs with multiplicities. In the general case, braidings also have gauge freedom.

4.3. Unitary fusion categories

A fusion category is rigid, so it has both left and right duals for each object. We denote the right birth/death by b_x, d_x and the left birth/death by b'_x, d'_x. The definition of a unitary fusion category is from [**Mu1**], and the definition of a unitary RFC is from [**Tu**].

DEFINITION 4.18. *Let $\mathcal{C}$ be a fusion category.*

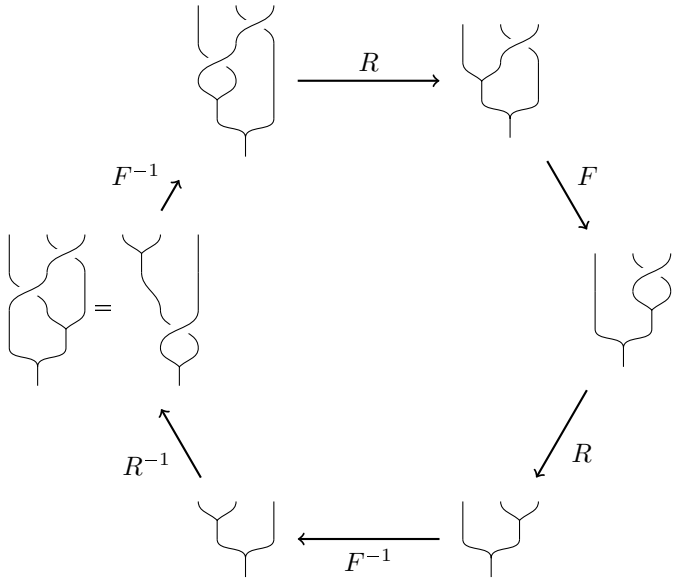


FIGURE 4.4. Schematic of the hexagon axiom.

(1) *A conjugation on* $\mathcal{C}$ *is an assignment of a morphism* $\overline{f} \in \mathrm{Hom}(y,x)$ *to each morphism* $f \in \mathrm{Hom}(x,y)$ *which is conjugate linear and satisfies:*

$$\overline{\overline{f}} = f, \qquad \overline{f \otimes g} = \overline{f} \otimes \overline{g}, \qquad \overline{f \circ g} = \overline{g} \circ \overline{f}.$$

(2) *A fusion category is unitary if there exists a conjugation such that* $f = 0$ *whenever* $\overline{f} \circ f = 0$.

(3) *A RFC* $\mathcal{C}$ *is Hermitian if there exists a conjugation such that*
   (i) $\overline{b_x} = d'_x$ *and* $\overline{d_x} = b'_x$
   (ii) $\overline{c_{x,y}} = c^{-1}_{x,y}$
   (iii) $\overline{\theta_x} = \theta_x^{-1}$

(4) *A RFC* $\mathcal{C}$ *is unitary if* $\mathcal{C}$ *is Hermitian and* $\mathrm{Tr}(f\overline{f}) \geqslant 0$ *for every* f.

PROPOSITION 4.19.

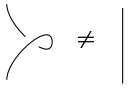
(1) *Unitary fusion categories are spherical* [**Y2, Ki2**].
(2) *Self-dual pivotal fusion categories are spherical* [**Hag**].

CONJECTURE 4.20. *A RFC with all quantum dimensions* $d_i > 0$ *is unitary.*

4.4. Link and 3-manifold invariants

The importance of RFCs is that they define invariants of colored framed links and of 3-manifolds. Given a RFC $\mathcal{C}$, the colors are objects of $\mathcal{C}$; a coloring of a link L is an assignment of objects to components of L. Usually, we choose only simple objects as colors. Given any colored link L with a framing, represent L as a link diagram L_D in the plane. Then L_D defines a morphism $\in \mathrm{Hom}(1,1)$, hence it is $\langle L_D \rangle \mathrm{id}_1$ for some scalar $\langle L_D \rangle$, which is an invariant of L_D up to Reidemeister moves of type RII and RIII. Such invariants are called framed link invariants. In

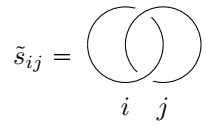
general $\langle L_D \rangle$ is not invariant under RI



because of the twist. Given a RFC, choose a set of representatives $\{x_i\}_{i\in L}$ of isomorphism classes of simple objects, where L is the label set. The link invariant depends only on isomorphism classes of objects, so we will color links by labels.

DEFINITION 4.21. *Given a RFC $\mathcal{C}$ with label set L,*

(1) *For all i, $d_i = \bigcirc_i$ is called the quantum dimension of the label i. Let $D^2 = \sum d_i^2$. Then D is called the global quantum dimension of $\mathcal{C}$. There are two choices of D. When D is real, we will always choose it to be positive unless stated otherwise. Choosing $-D$, we change the topological central charge by 4, and the 3-manifold invariant $Z(X)$ by a multiplicative factor $(-1)^{b_1(X)-1}$.*
(2) *For all i, j, let*



$\tilde{S} = (\tilde{s}_{ij})$ is called the modular $\tilde{S}$-matrix, and $S = \frac{1}{D}\tilde{S}$ is called the modular S-matrix.
(3) *A RFC is modular if $\det S \neq 0$.*
(4) *Let $p_\pm = \sum_i \theta_i d_i^2$. If $\mathcal{C}$ is modular, then $p_+ p_- = D^2$, and $p_+/D = e^{c\pi i/4}$ for some rational number c. The rational number $c \mod 8$ will be called the topological central charge of $\mathcal{C}$.*

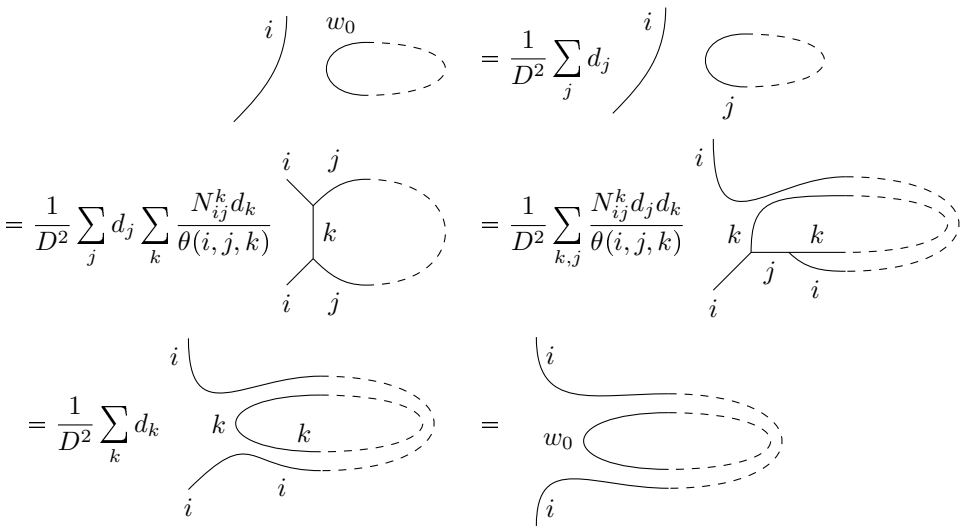
Later we will see that every MTC $\mathcal{C}$ leads to a (2+1)-TQFT. In particular, there will be an invariant $Z_\mathcal{C}$ of closed oriented 3-manifolds. Actually, 3-manifold invariants can be defined without the modularity condition. Let $w_0 = \frac{1}{D^2}\sum_{i\in L} d_i \cdot i$ be a formal sum of all labels. Given a link L, we write $\langle w_0 * L \rangle$ for the framed link invariant given by attaching w_0 to each component of L, formally expanding into a linear combination of colored links, and then evaluating the colored link invariant.

THEOREM 4.22. *Given a RFC with $p_+ \neq 0$ and a 3-manifold M^3 obtained from surgery on a framed link L with m components,*

$$\tau_\mathcal{C}(M^3) = D^{m-1}\left(\frac{D}{p_+}\right)^{\sigma(L)} \langle w_0 * L \rangle$$

is a topological invariant of 3-manifolds, where $\sigma(L)$ is the signature of the framing link (L_{ij}) with a chosen orientation of L. Here L_{ii} is the framing of the component L_i, and L_{ij} is the linking number of the components L_i and L_j.

PROOF. We will show $\langle w_0 * L\rangle$ is invariant under handle slides. Then with the prefactor, $\tau_{\mathcal{C}}(M^3)$ is invariant under blowing up or down a circle.



□

This magical formula is from [**RT, Tu**]. As a remark, we mention a point hidden by this formula. It is well-known that the 3-manifold invariant resulting from a TQFT has a framing anomaly measured by the topological central charge c_{top}. If $c_{\text{top}} \neq 0 \mod 8$, then the 3-manifold invariant is well-defined only for 3-manifolds with some extra structures such as a 2-framing. But in Thm. 4.22, no 2-framing was mentioned or chosen. The formula for $Z_{\mathcal{C}}(M^3)$ implicitly uses the canonical 2-framing.

A RFC actually determines much more: an operator invariant for any colored tangle, in particular a braid group representation for any simple object.

THEOREM 4.23. *In a RFC,*

(1) $d_i d_j = \sum_k N_{ij}^k d_k$
(2) $\tilde{s}_{ij} = \theta_i^{-1}\theta_j^{-1}\sum_k N_{ij}^k d_k \theta_k$
(3) The S-matrix is symmetric and unitary.
(4) If $\det S = 0$, then the first column of S is proportional to another column, so that the degeneracy of S is a degeneracy of double braidings.

For a proof of (1)–(2) see [**Tu, BK**], (3) [**ENO**], (4) [**Bru**].

4.5. Frobenius-Schur indicators

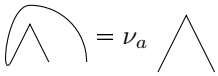
As an application of the graphical calculus, we will discuss the subtle point of Frobenius-Schur indicators in pivotal fusion categories. In finite group representation theory, Frobenius-Schur indicators arise for self-dual irreps. Suppose V is a self-dual irrep of a finite group G. Then there is an isomorphism $\phi_V : V^* \to V$, which can be regarded as an element of $V^{**} \otimes V \cong V \otimes V$. Moreover $V \otimes V$ has a $\mathbb{Z}_2$ action of which ϕ_V is always an eigenvector. Its eigenvalue $\in \{\pm 1\}$ is the classical Frobenius-Schur indicator, denoted by $\nu(V)$. If $\nu(V) = 1$, we say V

is symmetrically self-dual, or real in physics jargon. If $\nu(V) = -1$, we say V is antisymmetrically self-dual or pseudoreal.

If a is a self-dual simple object in a pivotal category, choose a nonzero vector $x_a \in \mathrm{Hom}(a \otimes a, 1)$ and denote it as

Acting on x_a by duality yields another nonzero vector

Since $\dim \mathrm{Hom}(a \otimes a, 1) = \dim \mathrm{Hom}(a^*, a) = 1$, these two vectors differ by a scalar:



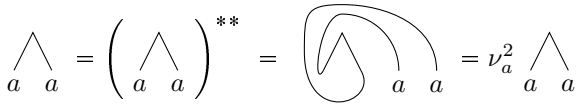
DEFINITION 4.24. *Let a be a simple object in a pivotal fusion category.*

(1) If a is self-dual, then ν_a is called the Frobenius-Schur indicator. Otherwise, we define $\nu_a = 0$.
(2) A pivotal category is unimodal if it has trivial Frobenius-Schur indicator, i.e., $\nu_a = 1$ for every self-dual simple object a.

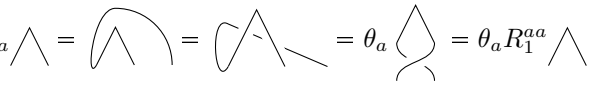
THEOREM 4.25.

(1) $\nu_a = \pm 1$.
(2) $\nu_a = t_a$ if a is self-dual, where t_a is the pivotal coefficient.
(3) $\nu_a = \theta_a R_1^{aa}$ in a RFC.
(4) $\nu_a = \frac{1}{D^2} \sum_{ij} N_{ia}^j d_i d_j \theta_i^2 / \theta_j^2$ in an MTC.

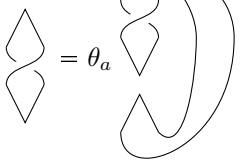
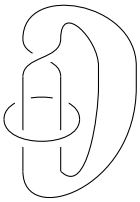
PROOF.

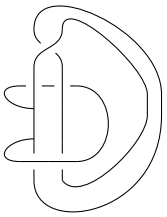
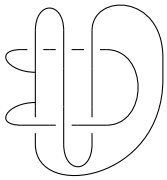
(1) 

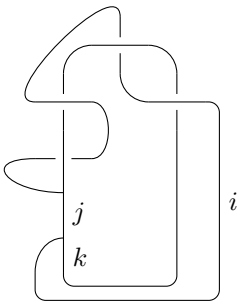
(2) See [**Hag**].

(3) 

(4) In a MTC,

$\nu_a = \theta_a R_1^{aa} = \theta_a$  $= \theta_a$ $= \quad \theta_a$ w_0 

$= \frac{\theta_a}{D^2} \sum_{i,j} \frac{d_i d_j N_{ia}^j}{\theta(i,j,a)}$  $= \frac{\theta_a}{D^2} \sum_{i,j} d_i N_{ia}^j \frac{d_j}{\theta(i,j,a)}$ 

$= \frac{\theta_a}{D^2} \sum_{i,j} \frac{d_i d_j N_{ia}^j}{\theta(i,j,a)}$ 

$= \frac{\theta_a}{D^2} \sum_{i,j} d_i d_j N_{ia}^j (R_j^{ia} R_j^{ai})^{-2} = \frac{\theta_a}{D^2} \sum_{i,j} d_i d_j N_{ia}^j \theta_j^2 \theta_i^{-2} \theta_a^{-2} \theta_a = \frac{1}{D^2} \sum_{ij} d_i d_j N_{ia}^j \frac{\theta_j^2}{\theta_i^2}$

□

The definition of a general Frobenius-Schur indicator is from [**Tu**], as is the notion of unimodality. Theorem 4.25(4) above first appeared in [**Ba**] for CFTs, and holds even for non-self dual simple objects.

CONJECTURE 4.26. *If a simple object a appears as a subobject in $x \otimes x^*$ for some simple object x, then $\nu_a = 1$.*

4.6. Modular tensor categories

When S is singular, the representations of braid groups cannot be extended to representations of the mapping class groups of higher genus surfaces, and hence the RFC does not lead to a TQFT. It turns out that degeneracy of the S-matrix is the only obstruction. Any MTC leads to a TQFT, hence affords projective representations of all mapping class groups.

THEOREM 4.27. *Consider a rank=n MTC with label set L and ith fusion matrix N_i given by $(N_i)_{jk} = N_{ij}^k$. Let S be the modular matrix and $T = (\theta_i \delta_{ij})$ the diagonal twist matrix. Then*

(1) Verlinde formula:

$$N_i \tilde{S} = \tilde{S} \Lambda_i \tag{4.28}$$

for all $i \in \mathcal{L}$, where $\Lambda_i = (\delta_{ab}\lambda_{ia})_{ab}$ is diagonal and $\lambda_{ia} = \tilde{s}_{ia}/\tilde{s}_{1a}$. Picking out the (j,k)-entry we have

$$N_{ij}^k = \sum_{r \in L} \frac{s_{ir} s_{jr} \overline{s}_{kr}}{s_{1r}^2}$$

implying many symmetries among N_{ij}^k: $N_{ij}^k = N_{ji}^k = N_{\hat{i}\hat{j}}^{\hat{k}} = N_{i\hat{k}}^{\hat{j}}$. From Eqn. (4.28), the diagonal entries of Λ_i are the eigenvalues of N_i, and the columns of $\tilde{S}$ are the corresponding eigenvectors.

(2) Modular representation: S and T satisfy
   (i) *$(ST)^3 = e^{c\pi i/4} S^2$*
   (ii) *$S^2 = C$, where $C = (\delta_{i\hat{j}})_{ij}$ is the charge conjugation matrix.*

(3) The modular representation of $\mathrm{SL}(2,\mathbb{Z})$ is a matrix representation. Its projective kernel is a congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$. In particular, the modular representation has finite image.

(4) Vafa's theorem: Let $A_{ij} = 2n N_{i\hat{i}}^j N_{ij}^i + N_{ii}^j N_{j\hat{i}}^i$. Then $\prod_j \theta_j^{A_{ij}} = \theta_i^{\frac{4}{3}\sum A_{ij}}$. It follows that θ_i is a root of unity.

(5) Let $K = \mathbb{Q}(\tilde{s}_{ij})$ be the Galois extension of $\mathbb{Q}$ by entries of $\tilde{S}$. Then the Galois group G is abelian. Moreover $\mathbb{Q}(\tilde{s}_{ij}, D) \subset \mathbb{Q}(\theta_j)$, which is also an abelian Galois extension of $\mathbb{Q}$.

(6) G can be identified with a subgroup of S_n. For each $\sigma \in G$, there exists $\epsilon_{i,\sigma} \in \{\pm 1\}$ for each $i \in L$ such that

$$\begin{aligned} \tilde{s}_{j,k} &= \epsilon_{\sigma(j),\sigma} \epsilon_{k,\sigma} \tilde{s}_{\sigma(j),\sigma^{-1}(k)} \\ \epsilon_{\sigma^{-1}(k),\sigma^{-1}} &= \epsilon_{\sigma(1),\sigma} \epsilon_{1,\sigma} \epsilon_{k,\sigma} \end{aligned}$$

(7) In a self-dual MTC, the pivotal coefficients $\{t_a\}$ are determined by S, T.

The Verlinde formula, Vafa's theorem, and the arithmetical properties of MTCs all originate from CFT. Our concept of an MTC and many of its properties are due to V. Turaev [**Tu**]. The congruence subgroup property is from [**NS, Ba2**].

Recall that a spherical structure also assigns ± 1 to each label. Are the spherical coefficients $\{t_i\}$ and Galois conjugate signs $\epsilon_{i,\sigma}$ of a MTC related?

4.6.1. Quantum group categories. From any simple Lie algebra $\mathfrak{g}$ and $q \in \mathbb{C}$ with q^2 a primitive ℓth root of unity one can construct a ribbon fusion category $\mathcal{C}(\mathfrak{g}, q, \ell)$. One can also use semisimple $\mathfrak{g}$, but the resulting category is easily seen to be a direct product of those constructed from simple $\mathfrak{g}$. We shall say these categories (or their direct products) are of *quantum group type*. There is an oft-overlooked subtlety concerning the degree ℓ of q^2 and the unitarizability of $\mathcal{C}(\mathfrak{g}, q, \ell)$. Let m be the maximal number of edges between any two nodes of the Dynkin diagram for $\mathfrak{g}$ with $\mathfrak{g}$ simple, so that $m = 1$ for Lie types A,D,E, $m = 2$ for Lie types B,C,F_4, and $m = 3$ for Lie type G_2.

THEOREM 4.29. *If $m \mid \ell$, then $\mathcal{C}(\mathfrak{g}, q, \ell)$ is a UMTC for $q = e^{\pm \pi i/\ell}$.*

This theorem culminates a long string of works in the theory of quantum groups. See [**Ro**] for references.

If $m \nmid \ell$, there is usually no choice of q making $\mathcal{C}(\mathfrak{g}, q, \ell)$ unitary. In [**Fi**] it is shown that the fusion category associated with level k representations of the affine Kac-Moody algebra $\hat{\mathfrak{g}}$ is tensor equivalent to $\mathcal{C}(\mathfrak{g}, q, \ell)$ for $\ell = m(k + \check{h}_{\mathfrak{g}})$ where $\check{h}_{\mathfrak{g}}$ is the dual Coxeter number. In these cases the categories are often denoted (X_r, k), where $\mathfrak{g}$ is of Lie type X with rank r and $k = \ell/m - \check{h}_{\mathfrak{g}}$ is the level. The central charge of the corresponding Wess-Zumino-Witten CFT is $\frac{k \dim \mathfrak{g}}{k+\check{h}_{\mathfrak{g}}}$. We will use this abbreviated notation except when $m \nmid \ell$. Each quantum group category $\mathcal{C}(\mathfrak{g}, q, \ell)$ is unimodalizable by choosing different ribbon elements, but unitarity and modularity cannot in general be preserved. Note for (A, q, l), the root of unity $q = e^{\pm \pi i/l}$ here differs from the Jones-Kauffman case, where $q = A^{-4} = e^{\pm 2\pi i/4r}$. The $\mathcal{C}(\mathfrak{g}, q, l)$ TQFTs are the Reshetikhin-Turaev theories at level $k = l - 2$ mathematically, and the Witten-Chern-Simons TQFTs physically.

4.6.2. Quantum doubles.

DEFINITION 4.30. *Let $\mathcal{C}$ be a strict monoidal category and $x \in \mathcal{C}$. A half-braiding e_x for x is a family of isomorphisms $\{e_x(y) \in \mathrm{Hom}_{\mathcal{C}}(xy, yx)\}_{y \in \mathcal{C}}$ satisfying*

(i) Naturality: $\forall f \in \mathrm{Hom}(y, z)$: $\quad (f \otimes \mathrm{id}_x) \circ e_x(y) = e_x(z) \circ (id_x \otimes f)$
(ii) Half-braiding: $\forall y, z \in \mathcal{C}$: $\quad e_x(y \otimes z) = (id_y \otimes e_x(z)) \circ (e_x(y) \otimes \mathrm{id}_z)$
(iii) Unit property: $e_x(1) = \mathrm{id}_x$.

DEFINITION 4.31. *The quantum double or Drinfeld center $\mathcal{Z}(\mathcal{C})$ of a strict monoidal category $\mathcal{C}$ has as objects pairs (x, e_x), where $x \in \mathcal{C}$ and e_x is a half braiding. The morphisms are given by*

$$\mathrm{Hom}\big((x, e_x), (y, e_y)\big) = \big\{f \in \mathrm{Hom}_{\mathcal{C}}(x, y) \mid (\mathrm{id}_z \otimes f) \circ e_x(z) = e_y(z) \circ (f \otimes \mathrm{id}_z) \forall z \in \mathcal{C}\big\}.$$

The tensor product of objects is given by $(x, e_x) \otimes (y, e_y) = (xy, e_{xy})$, where

$$e_{xy}(z) = (e_x(z) \otimes \mathrm{id}_y) \circ (\mathrm{id}_x \otimes e_y(z)).$$

The tensor unit is $(1, e_1)$ where $e_1(x) = \mathrm{id}_x$. The composition and tensor product of morphisms are inherited from $\mathcal{C}$. The braiding is given by $c_{(x,e_x),(y,e_y)} = e_x(y)$.

THEOREM 4.32. *If $\mathcal{C}$ is a spherical fusion category, then $\mathcal{Z}(\mathcal{C})$ is modular.*

This theorem is due to M. Müger [**Mu2**]. If a spherical fusion category $\mathcal{C}$ is defined via a graphical calculus over rectangles, such as the Jones-Kauffman theories, then its quantum double is the annular version of the graphical calculus. This annularization can be generalized to higher categories. See [**Wal2, FNWW**].

4.7. Classification of MTCs

Quantum group categories and quantum doubles of spherical fusion categories provide a large collection of examples of MTCs. Methods from von Neumann algebras, vertex operator algebras, and CFTs also produce MTCs, plus the constructions of simple current extension, coset, and orbifold methods in CFT from known examples. At the moment a classification seems hard. But we mention two directions: the Witt group and low rank classification. Both deepen the analogy between MTCs and abelian groups, so a classification seems plausible.

4.7.1. Witt group. The classical Witt group of quadratic forms on finite abelian groups is important for many applications such as surgery theory in topology. Recently a similar theory has been under development for nondegenerate braided fusion categories. We will give a flavor of the theory for MTCs.

DEFINITION 4.33. *Two MTCs $\mathcal{C}_1, \mathcal{C}_2$ are Witt equivalent if there exist spherical tensor categories A_1 and A_2 such that*

$$\mathcal{C}_1 \boxtimes Z(A_1) \simeq \mathcal{C}_2 \boxtimes Z(A_2)$$

where $Z(A_i)$ are the Drinfeld centers, and $\simeq$ is ribbon equivalence.

It has been shown that Witt equivalence is an equivalence relation, and $\boxtimes$ descends to Witt classes.

THEOREM 4.34. *Witt classes form an abelian group, and $\mathcal{C}$ is in the trivial class iff $C \simeq Z(A)$ for some spherical category A.*

This theorem will be in [**DMNO**].

Very little is known at present about the Witt group $\mathcal{W}_{\mathrm{MTC}}$ of MTCs. For example, we don't know if there exists an element of infinite order. There is an obvious homomorphism $\tilde{c}_{\mathrm{top}} \colon \mathcal{W}_{\mathrm{MTC}} \to \mathbb{Q}/8\mathbb{Z}$. Are there nontrivial homomorphisms other than the one given by the topological central charge?

4.7.2. Low rank UMTCs. There are 35 UMTCs of rank $\leqslant 4$, listed in Table 4.1. By certain transformations, all can be obtained from 10 theories, whose explicit data can be found in [**RSW**]. (In data set 5.3.5 of p. 376 of that paper, $R_1^{\sigma\sigma}$ should be $e^{5\pi i/8}$.)

			A 5 Toric code
A 1 Trivial	A 2 Semion	A 2 $(\mathrm{U}(1), 3)$	A 4 $(\mathrm{U}(1), 4)$
		NA 8 Ising	NA 4 Fib × Semion BU
	NA 2 Fib BU	NA 2 $(A_1, 5)_{\frac{1}{2}}$ BU	NA 2 $(A_1, 7)_{\frac{1}{2}}$ BU
			NA 3 DFib BU

TABLE 4.1. The ith column classifies rank i UMTCs. In each box, the middle indicates the fusion rule; the upper left, whether the theory is abelian (A) or non-abelian (NA); the upper right, the number of distinct theories; and the lower left, the presence of a universal braiding anyon (BU).

CHAPTER 5

(2+1)-TQFTs

In this chapter we formalize the notion of a TQFT and summarize various examples. Our axioms are minor modifications of K. Walker's [**Wal1**], which are consistent only for (2+1)-TQFTs with trivial Frobenius-Schur indicators. The subtle point of Frobenius-Schur indicators significantly complicates the axiomatization. Axiomatic formulation of TQFTs as tensor functors goes back to M. Atiyah, G. Segal, G. Moore and N. Seiberg, V. Turaev, and others.

A TQFT is a quantum field theory (QFT) whose partition functions are topologically invariant. Consequently, a TQFT has a constant Hamiltonian H, which can be normalized to $H \equiv 0$. Systems with constant Hamiltonians can be obtained by restricting any Hamiltonian to its ground states, though most such theories are either trivial or not TQFTs in our sense. In physics jargon, we integrate out higher energy degrees of freedom. Given an initial state of a topological system $|\psi_0\rangle$, by Schrödinger's equation for $H \equiv 0$, the wave function $|\psi_t\rangle$ will be constant on each connected component of the evolution. But there are still choices of constants on different connected components. For an n-particle system on the plane $\mathbb{R}^2$, connected components of n-particle worldlines returning setwise to their initial positions are braids. If the constants are matrices rather than numbers, then time evolution of such TQFTs is given by braid group representations.

The principles of locality and unitarity are of paramount importance in formulating a physical quantum theory. Locality in its most naive form follows from special relativity: information cannot be transmitted faster than the speed of light c, hence a point event at point x cannot affect events at other points y within time t if the distance from x to y exceeds ct. This principle is encoded in TQFTs by axioms arranging that the partition function $Z(X)$ for a spacetime manifold X can be computed from pieces of X, i.e., that we can evaluate $Z(X)$ from a decomposition of X into building blocks X_i such as simplices or handles if the partition functions $Z(X_i)$ are known and the boundaries of X_i are properly decorated. It also proves fruitful to consider the theory beyond the space and spacetime dimensions. In (2+1)-TQFTs, we may define mathematical structures for 4- and 1-dimenional manifolds. Such consideration allows us to trace the framing anomaly in 3-manifold invariants to the anomaly of Virasoro algebras in dimension 1 and signatures of bounded 4-manifolds in dimension 4. Nothing prevents a mathematician from going even further, defining theories for all dimensions. But substantial complications arise even for Chern-Simons theories.

Roughly, a (2+1)-dimensional TQFT consists of two compatible functors (V, Z): a modular functor V and a partition functor Z. The modular functor V associates a vector space $V(Y)$ to any compact oriented surface Y with some extra structures, takes disjoint unions to tensor products and orientation reversals to duals, and is natural with respect to diffeomorphisms which preserve the structures on Y up to

isotopy. The empty set $\varnothing$ is considered a closed manifold of each dimension in $\{0, 1, \ldots\}$. As a closed surface, its associated vector space is $\mathbb{C}$, i.e., $V(\varnothing) = \mathbb{C}$. The partition functor Z assigns a vector $Z(X) \in V(Y)$ for each $Y = \partial X$, X an oriented 3-manifold with some extra structures. The two functors V, Z are compatible for closed surfaces, whose transformations, diffeomorphisms $f\colon Y \circlearrowleft$, each yield two isomorphisms of $V(Y)$ by V and Z. An oriented closed 3-manifold X determines a vector $Z(X) \in V(\varnothing) = \mathbb{C}$, i.e., a number. For X the 3-sphere with link L, Witten's "SU(2)-family" of TQFTs yields Jones polynomial evaluations $Z(S^3, L) = J_L(e^{2\pi i/r})$, $r = 1, 2, 3, \ldots$, which mathematically are the Reshetikhin-Turaev invariants based on quantum groups.

5.1. Quantum field theory

The origins of QFT lie in constructing a relativistic quantum mechanics and unifying particles and fields. Quantum field theory treats systems of various degrees of freedom through the creation and annihilation process. The central notion in QFT is that of a quantum field. To arrive at a quantum field, we usually start with a classical system. Then a quantization procedure is employed to find a description of the corresponding quantum system. But in general, quantization is neither direct nor unique. We recall the rudiments of QFT to familiarize the reader with the language.

5.1.1. Classical formalisms and quantizations. In classical mechanics, there are the Lagrangian and Hamiltonian formalisms, so quantization can be done with either formalism. Consider a particular system in a space X. Trajectories of n particles in X are described by curves in the configuration space $C_n(X) \subset X^n$. The positions of these particles at each moment form a point in $C_n(X)$. In the Lagrangian formalism, we have a Lagrangian density defined on the tangent bundle of the configuration space $L : TC_n(X) \to \mathbb{R}$. For simplicity, consider only one particle moving on a line, i.e., $C_n(X) = \mathbb{R}$ for a pointed particle with mass m, attached to a spring with spring constant k. In this case, the kinetic energy is $T = \frac{1}{2}m\dot{x}^2$, and the potential energy is $V(x) = \frac{1}{2}kx^2$. Then the Lagrangian density is $L = T - V$, where $(x, \dot{x})$ are coordinates for the tangent bundle. The dynamics is determined by an action S which takes real values for all possible trajectories $\gamma : I \to \mathbb{R}$:

$$S[\gamma] = \int_I L(\dot{\gamma})dt.$$

The least action principle selects classical trajectories through extremals of the action S. The equation for extremals is the Euler-Lagrange equation

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{q}}\right) - \frac{\partial L}{\partial q} = 0.$$

For our example $q = x$, $\dot{q} = \dot{x}$, so it reduces to Newton's second law $\ddot{x} + kx = 0$ for a point mass. In the Hamiltonian formalism, the dynamics is determined by the total energy Hamiltonian $H = T + U$ of the system. The equations of motion are

$$\dot{q} = \frac{\partial H}{\partial p} \qquad\qquad \dot{p} = -\frac{\partial H}{\partial q}$$

which again reduce to Newton's second law. Hence the Lagrangian and Hamiltonian formalisms are equivalent. In general, their relationship is given by the Legendre

transformation. The Hamiltonian is defined on the cotangent bundle of the configuration space, whose coordinates are position and momentum (q, p), while the coordinates for the Lagrangian density are position and velocity $(q, \dot{q})$. The proportion constant of momentum and velocity is the particle's rest mass. In classical theory we consider particles with well-defined rest mass, so often the Lagrangian and Hamiltonian formalisms are equivalent via the Lengendre transformation. But in QFT, particles such as photons have no rest mass, so the two formalisms are not obviously equivalent. In some situations it is hard, if not impossible, even to describe the theory using the Hamiltonian formalism, e.g., the case of TQFTs.

In the Lagrangian formalism we quantize through path integrals, which directly implement the superposition principle of quantum mechanics. In the situation above, the amplitude $U(x_a, x_b; t) = \langle x_b | e^{-\frac{i}{\hbar}Ht} | x_a \rangle$ for a particle to travel from one point x_a to another x_b in a given time t is the sum $\sum_{\text{all paths}} e^{iA(\gamma)}$. Since there are infinitely many possible paths, we will write the sum as an integral $\int_{\text{all paths}} e^{iA(\gamma)} \mathcal{D}\gamma$ for some $\mathcal{D}_\gamma$. Classically, the particle should follow only one path; the path integral will be dominated by a classical path in a classical limit. The saddle-point approximation tells us that the path integral is dominated by the stationary paths: $\frac{\delta}{\delta\gamma(t)}(A(\gamma(t)) = 0$. Since the classical path is an extremal of the action, the phase factor $A(\gamma)$ in the path integral might be chosen to be the action $S[\gamma]$ up to a constant factor, which turns out to be $i/\hbar$. We set $\hbar = 1$ from now on.

Path integral quantization is evaluation of the path integral $\int e^{iS[\gamma]} \mathcal{D}\gamma$. It preserves many classical symmetries and reveals a close relationship between QFT and statistical mechanics, where path integrals are called partition functions. The Lagrangian and Hamiltonian formalisms are equivalent when both are applicable:

$$U(x_a, x_b; T) = \langle x_b | e^{-iHT} | x_a \rangle = \int e^{iS[x(t)]} \mathcal{D}x.$$

Field theory considers the following situation: a $(d+1)$-dimensional spacetime manifold X, and a space $\Phi(X)$ of locally defined data on X. In general, X does not split into a product $Y \times \mathbb{R}$. Elements of $\Phi(X)$ are called field configurations. Our main example is gauge theory, which will be discussed in the next section. Some other examples are

(1) $\Phi(X)$ is all smooth maps $\phi : X \to \mathbb{R}^m$, e.g. in QED.
(2) $\Phi(X)$ is all smooth functions $\phi : X \to M$ where M is a fixed Riemannian n-manifold, e.g., $M = S^2$ in σ models.
(3) $\Phi(X)$ is all smooth metrics on X, e.g. in gravity.

In physics, we want to make "local observations" of fields $\phi \in \Phi(X)$. So for each $x \in X$ we consider maps $F_x : \Phi(X) \to \mathbb{C}$ such that $F_x(\phi)$ depends only on the behavior of ϕ on a neighborhood of x. In the above examples, we might have

(1) $F_x(\phi) = \phi(x)$.
(2) $F_x(\phi) = f(\phi(x))$ for some fixed function $f \colon M \to \mathbb{C}$.
(3) $F_x(\phi)$ is the scalar curvature of ϕ at x.

To quantize a theory, we need a probability measure on $\Phi(X)$ so that we can evaluate "expectation value" $\langle F_x \rangle$, or "correlation functions" $\langle F_{x_1} \cdots F_{x_k} \rangle$ of local observables $F_{x_1}, \ldots, F_{x_k}$ at points $x_1, \ldots, x_k$. Correlation functions contain all the physics of a theory. It is extremely hard to construct probability measures. But formal interpretation and manipulation of these integrals have led to meaningful results, and the path integral formalism is a very powerful tool in QFT.

Formally, locality is expressed as follows. Given a field ϕ on a surface $Y = \partial X$, consider the path integral

$$Z_k(X) = \int e^{ikS(\phi)} D\phi$$

now over the class of fields on X which extend ϕ, where R is some coupling constant. This defines a function on the space of fields of Y. Let $V(Y)$ be the vector space of functions on fields of Y. Then a bounding manifold X defines a vector in this space through the path integral. If X is a union of two pieces X_1, X_2 with common boundary Y, then each piece X_i gives rise to a vector in $V(Y)$. The locality property means that $Z(X) = \langle Z(X_1), Z(X_2)\rangle$, which requires that the action is additive.

Now suppose Y has two connected components Y_1 and Y_2. Then a pair of fields ϕ_i on Y_i leads to a number $M(\phi_1, \phi_2)$. Therefore $Z(X)$ gives rise to a linear map from $V(Y_1)$ to $V(Y_2)$.

As a quantum theory $V(Y_1 \amalg Y_2) = V(Y_1) \otimes V(Y_2)$, so we impose $V(\varnothing) = \mathbb{C}$ in order to have a nontrivial theory.

5.2. Witten-Chern-Simons theories

The prototypical example of physical TQFTs is Witten's Chern-Simons theory. In Witten-Chern-Simons (WCS) gauge theory, we fix a semisimple Lie group G and a level k. For simplicity, we assume G is simply-connected. Given a spacetime 3-manifold X and a G-principle bundle P on X, let $\mathcal{B}(X)$ be the space of connections on P, and $\mathcal{A}(X)$ be its quotient modulo gauge transformations. Connections are called gauge fields or gauge potentials. The Lagrangian density of a gauge field $A \in \mathcal{B}$ in the WCS theory is the Chern-Simons 3-form $\operatorname{tr}(A \wedge dA + \frac{2}{3}A^3)$, and the action is the Chern-Simons functional

$$\mathrm{CS}(A) = \frac{1}{8\pi^2} \int_X \operatorname{tr}\big(A \wedge dA + \frac{2}{3}A^3\big).$$

To get a (2+1)-TQFT, we need to define a complex number for each closed oriented 3-manifold X which is a topological invariant, and a vector space $V(Y)$ for each closed oriented 2-dimensional surface Y. For $k \geqslant 1$, the 3-manifold invariant of X is the path integral

$$Z_k(X) = \int_{\mathcal{A}} e^{2\pi i k \mathrm{CS}(A)} \mathcal{D}A,$$

where the integral is over all gauge classes of connections on P, and the measure $\mathcal{A}$ has yet to be defined rigorously. It is healthy, probably also wise, for mathematicians to take the path integral seriously and keep in mind that mathematical conclusions derived with path integrals are mathematical conjectures. The level k is called the coupling constant of the theory; $1/k$ plays the role of the Planck constant. A closely related 3-manifold invariant was discovered rigorously by N. Reshetikhin and V. Turaev based on the quantum groups of G at roots of unity $q = e^{\pm \pi i/l}$, where $l = m(k + h^\vee)$, where $m = 1$ if G is of type A, D, E; $m = 2$ for types B, F; $m = 3$ for G_2; and $h^\vee$ is the dual Coxeter number of G. For $\mathrm{SU}(N)$, $h^\vee = N$. To define a vector space for a closed oriented surface Y, let X be an oriented 3-manifold with boundary Y. Fix a connection a on the restriction of P to Y, and let

$$Z_k(a) = \int_{(\mathcal{A}, a)} e^{2\pi i k \mathrm{CS}(A)} \mathcal{D}A,$$

integrating over all gauge classes $\mathcal{A}$ of connections of A on P over X whose restrictions to Y are gauge equivalent to a. This defines a functional on all connections $\{a\}$ on the principle G-bundle P over Y. By forming formal finite sums, we obtain an infinite-dimensional vector space $S(Y)$. In particular, a 3-manifold X with $\partial X = Y$ defines a vector in $S(Y)$. The path integral on the disk introduces relations among the functionals. Modding them out, we get a finite-dimensional quotient of $S(Y)$, which is the desired vector space $V(Y)$. Again, such finite-dimensional vector spaces were constructed mathematically by N. Reshetikhin and V. Turaev from semisimple Lie algebras. The invariant of closed oriented 3-manifolds and the vector spaces associated to closed oriented surfaces form part of the Reshetikhin-Turaev TQFT based on G at level=k. A subtlety arises in WCS theory regarding the measure $\mathcal{D}A$. The action, i.e., the exponential Chern-Simons functional, is topologically invariant, but the formal measure $\mathcal{D}A$ depends on the geometry of a lift of $\mathcal{A}$ in all gauge fields. This leads to the framing anomaly. Consequently, we have 3-manifold invariants only for 3-manifolds with extra structures such as 2-framings [**A**].

5.3. Framing anomaly

Framing anomaly manifests the Virasoro central charge in 2–3 dimensions. As alluded to in the last section, the WCS path integral requires an extra structure on spacetime manifolds X in order to be well-defined, even formally. A framing of X is sufficient, but weaker structures are possible. It is related to the integration domain being on gauge equivalence classes rather than the affine space of gauge fields. Given two oriented compact 3-manifolds X_1, X_2 such that both ∂X_1 and ∂X_2 have Y as a component, X_1 and X_2 can be glued by a diffeomorphism $f\colon -Y \to Y$. If X_1 and X_2 are framed, then f does not necessarily preserve the framing, hence the framing anomaly arises.

In 2 dimensions, it means that representations of mapping class groups afforded by TQFTs are in general only projective.

Framing can be weakened in various ways: 2-framings, p_1-structures. Another choice is the signature of a bounding 4-manifold, so an integer attached to a 3-manifold. This weakening is equivalent to the 2-framing, but not to p_1-structures. On a 3-manifold M, the quantum invariant is well-defined after M is equipped with extra structures. It has been confusing that in the Reshetikhin-Turaev definition of a 3-manifold invariant, $\tau(M)$, choices of 2-framings or p_1-structures are not explicitly made. What happens here is that the 3-manifold invariant is defined through a surgery link L of M. The surgery link presentation of M implies that we have chosen a 4-manifold W such that $\partial W = M$. The signature of W is a weakening of the framing that is sufficient for $\tau(M)$ to be well-defined. Therefore the invariant $Z(M)$ is the computation of $\tau(M)$ with the canonical 2-framing.

5.4. Axioms for TQFTs

The framing anomaly and Frobenius-Schur indicators greatly complicate TQFT axioms. We will resolve the former using extended manifolds, and the latter with more rigid boundary conditions. It is very important for us to distinguish between isomorphisms and canonical isomorphisms for objects in categories, so we will write $\simeq$ for the former and $\cong$ for the latter.

To handle Frobenius-Schur indicators, we use simple objects in a strict fusion category to label boundary components of surfaces. Physically, this means that boundaries of surfaces are marked by anyons rather than their types.

For framing anomaly, our solution is also inspired by physical applications. We use extended manifolds to get well-defined vector spaces $V(Y)$ for surfaces Y with structures, and isomorphisms $V(f)$ for structure-preserving diffeomorphisms f. The resulting representation of mapping class groups is not linear, but projective in an explicit manner determined by the central charge.

5.4.1. Boundary conditions for TQFTs. When a quantum state lives on Y, and Y is cut along a submanifold S, immediate states arise on S, and the original state on Y is a sum over the immediate states on S. Therefore if a surface Y has boundary, certain conditions for ∂Y have to be specified for the vector space $V(Y)$ to be part of a TQFT. We use a strict fusion category $\mathcal{C}$ to specify boundary conditions for surfaces in a (2+1)-TQFT. A strict label set L^{str} for $\mathcal{C}$ is a finite set $\{l_i\}_{i\in I}$ of representatives of isomorphism classes of simple objects, where I is a finite index set with a distinguished element 0 such that $l_0 = 1$. The index set I is the usual label set. Note L^{str} is more rigid than a label set. An involution $\hat{}\colon I \circlearrowleft$ of labels is given by $\hat{\imath} = j$ if $l_j \simeq \hat{l}_i$. Note that $\hat{l}_i$ might not be in L^{str}. If $\mathcal{C}$ is unimodal and pivotal, an ordinary label set suffices.

5.4.2. Extended manifolds. For general TQFTs, the vector spaces $V(Y)$ for oriented surfaces Y are not defined canonically even when their boundaries are labeled, due to the framing anomaly in 2 dimensions.

Definition 5.1. *A Lagrangian subspace of a surface Y is a maximal isotropic subspace of $H_1(Y;\mathbb{R})$ with respect to the intersection pairing of $H_1(Y;\mathbb{R})$.*

If a surface Y is planar, i.e., $Y \subset \mathbb{R}^2$, then the intersection pairing on $H_1(Y;\mathbb{R})$ is zero, so there is a unique Lagrangian subspace, namely $H_1(Y;\mathbb{R})$. It follows that the TQFT representations of the braid groups are actually linear. If Y is the torus T^2, then $H_1(Y;\mathbb{R}) \cong \mathbb{R}^2$, and the pairing is $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ in a meridian longitude basis. Hence every line in $\mathbb{R}^2$ is a Lagrangian subspace.

Definition 5.2. *An extended surface Y is a pair (Y,λ), where λ is a Lagrangian subspace of $H_1(Y;\mathbb{R})$. An extended 3-manifold X is a 3-manifold with an extended boundary $(\partial X,\lambda)$.*

More generally, a 3-manifold X can be also extended with a 2-framing, p_1-structure, or the signature of a bounding 4-manifold. Every 3-manifold X has a canonical 2-framing [**A**]. We consider only extended 3-manifolds with canonical extensions. So a closed 3-manifold is really the extended 3-manifold with the canonical extension. For example, consider extending a 3-manifold X by a 2-framing, i.e., a homotopy class of trivializations of two copies $TX \oplus TX$ of the tangent bundle of X. For $S^1 \times S^2$, there is actually a canonical framing, the one invariant under rotations of S^1, so the canonical 2-framing is twice the canonical framing. For S^3, there are no canonical framings, but there is a canonical 2-framing $T_L \oplus T_R$, where T_L, T_R are the left- and right-invariant framings.

Note that if $\partial X = Y$, then Y has a canonical Lagrangian subspace $\lambda_X = \ker\big(H_1(Y;\mathbb{R}) \to H_1(X;\mathbb{R})\big)$. In the following, the boundary Y of a 3-manifold X is always extended by the canonical Lagrangian subspace λ_X unless stated otherwise. Extended planar surfaces are just regular surfaces.

To resolve the anomaly for surfaces, we extend the category of surfaces to labeled extended surfaces. Given a strict fusion category $\mathcal{C}$ and an oriented surface Y, a labeled extended surface is a triple $(Y;\lambda,l)$, where λ is a Lagrangian subspace of $H_1(Y;\mathbb{R})$, and l is an assignment of an object $U\in\mathcal{C}^0$ to each boundary circle. Moreover each boundary circle is oriented by the induced orientation from Y and endowed with a parametrization by an orientation preserving map from the standard circle S^1.

Given two labeled extended surfaces $(Y_i;\lambda_i,l_i)$, $i=1,2$, their disjoint union is the labeled extended surface $(Y_1\sqcup Y_2;\lambda_1\oplus\lambda_2,l_1\cup l_2)$. Gluing of surfaces must be carefully defined to be compatible with boundary structures and Lagrangian subspaces. Given two components γ_1,γ_2 of ∂Y parameterized by ϕ_1,ϕ_2 and labeled by objects U and U' respectively, let gl be the diffeomorphism $\phi_2 r\phi_1^{-1}$, where r is the standard involution of the circle S^1. Then the glued surface Y_{gl} is the quotient space of Y by the identification $\mathrm{gl}\colon\gamma_1\to\gamma_2$. If Y is extended by λ, then Y_{gl} is extended by $q_*(\lambda)$, where $q\colon Y\to Y_{\mathrm{gl}}$ is the quotient projection. The boundary surface ∂M_f of the mapping cylinder M_f of a diffeomorphism $f: Y\circlearrowleft$ of an extended surface $(Y;\lambda)$ has an extension by the inclusions of λ, which is not the canonical extension.

Labeled diffeomorphisms of labeled extended surfaces are diffeomorphisms of the underlying surfaces preserving orientation, boundary parameterization, and labeling. Note we do not require preservation of Lagrangian subspaces. The category of oriented labeled extended surfaces and labeled diffeomorphisms will be denoted as $\mathcal{X}^{2,e,l}$.

5.4.3. Axioms for TQFTs. The anomaly of a TQFT is a root of unity, written $\kappa=e^{\pi ic/4}$ to match physical convention, where $c\in\mathbb{Q}$ is well-defined mod 8 and referred to as the central charge. Thus a TQFT is anomaly-free iff its central charge c is 0 mod 8.

Definition 5.3. *A (2+1)-TQFT with strict fusion category $\mathcal{C}$, strict label set L^{str}, and anomaly κ consists of a pair (V,Z), where V is a functor from the category $\mathcal{X}^{2,e,l}$ of oriented labeled extended surfaces to the category $\mathcal{V}$ of finite-dimensional vector spaces and linear isomorphisms up to powers of κ, and Z assigns a vector $Z(X,\lambda)\in V(\partial X;\lambda)$ to each oriented 3-manifold X with extended boundary $(\partial X;\lambda)$, where ∂X is extended by the Lagrangian subspace λ. We will use the notation $Z(X)$,$V(\partial X)$ if ∂X is extended by the canonical Lagrangian subspace λ_X. V is called a modular functor. In physical language Z is the partition function if X is closed; we will call Z the partition functor. $V(Y)$ is completely reducible if boundary components of Y are labeled by non-simple objects.*

Furthermore, V and Z satisfy the following axioms.

Axioms for V:

(1) Empty surface axiom: $V(\varnothing)=\mathbb{C}$.

(2) Disk axiom:

$$V(B^2;l)\cong\begin{cases}\mathbb{C} & \text{if } l \text{ is the trivial label,}\\ 0 & \text{otherwise,}\end{cases}\qquad \text{where } B^2 \text{ is a 2-disk.}$$

(3) Annular axiom:

$$V(\mathcal{A};a,b)\simeq\begin{cases}\mathbb{C} & \text{if } a\simeq\hat{b},\\ 0 & \text{otherwise,}\end{cases}$$

where $\mathcal{A}$ is an annulus and $a,b\in L^{\mathrm{str}}$ are strict labels. Furthermore, $V(\mathcal{A};a,b)\cong\mathbb{C}$ if $a\cong\hat{b}$.

(4) Disjoint union axiom:
$V(Y_1\sqcup Y_2;\lambda_1\oplus\lambda_2,l_1\sqcup l_2)\cong V(Y_1;\lambda_1,l_1)\otimes V(Y_2;\lambda_2,l_2)$.
The isomorphisms are associative, and compatible with the mapping class group actions.

(5) Duality axiom: $V(-Y;l)\cong V(Y;\hat{l})^*$. *The isomorphisms are compatible with mapping class group actions, orientation reversal, and the disjoint union axiom as follows:*

(a) The isomorphisms $V(Y)\to V(-Y)^*$ and $V(-Y)\to V(Y)^*$ are mutually adjoint.

(b) Given $f:(Y_1;l_1)\to(Y_2;l_2)$ and letting $\bar{f}:(-Y_1;\hat{l_1})\to(-Y_2;\hat{l_2})$, we have $\langle x,y\rangle=\langle V(f)x,V(\bar{f})y\rangle$, where $x\in V(Y_1;l_1)$, $y\in V(-Y_1;\hat{l_1})$.

(c) $\langle\alpha_1\otimes\alpha_2,\beta_1\otimes\beta_2\rangle=\langle\alpha_1,\beta_1\rangle\langle\alpha_2,\beta_2\rangle$ whenever

$$\alpha_1\otimes\alpha_2\in V(Y_1\sqcup Y_2)=V(Y_1)\otimes V(Y_2)$$
$$\beta_1\otimes\beta_2\in V(-Y_1\sqcup -Y_2)=V(-Y_1)\otimes V(-Y_2).$$

(6) Gluing Axiom: *Let Y_{gl} be the extended surface obtained from gluing two boundary components of an extended surface Y. Then*

$$V(Y_{\mathrm{gl}})\cong\bigoplus_{l\in L}V(Y;(l,\hat{l}))$$

where $l,\hat{l}$ are strict labels for the glued boundary components. The isomorphism is associative and compatible with mapping class group actions.

Moreover, the isomorphism is compatible with duality as follows: Let

$$\bigoplus_{j\in L}\alpha_j\in V(Y_{\mathrm{gl}};l)=\bigoplus_{j\in L}V(Y;l,(j,\hat{\jmath}))$$
$$\bigoplus_{j\in L}\beta_j\in V(-Y_{\mathrm{gl}};\hat{l})=\bigoplus_{j\in L}V(-Y;\hat{l},(j,\hat{\jmath})).$$

Then there is a non-zero real number s_j for each label j such that

$$\left\langle\bigoplus_{j\in L}\alpha_j,\bigoplus_{j\in L}\beta_j\right\rangle=\sum_{j\in L}s_{j\in L}\langle\alpha_j,\beta_j\rangle.$$

Axioms for Z:

(1) Disjoint axiom: $Z(X_1\sqcup X_2)=Z(X_1)\otimes Z(X_2)$.

(2) Naturality axiom: *If $f:(X_1,(\partial X_1,\lambda_1))\to(X_2,(\partial X_2,\lambda_2))$ is a diffeomorphism, then $V(f):V(\partial X_1)\to V(\partial X_2)$ sends $Z(X_1,\lambda_1)$ to $Z(X_2,\lambda_2)$.*

(3) Gluing axiom: *If $\partial X_i=-Y_i\sqcup Y_i$ for $i=1,2$, then*

$$Z(X_1\sqcup_{Y_2}X_2)=\kappa^nZ(X_1)Z(X_2)$$

where $n=\mu\big((\lambda_-X_1),\lambda_2,(\lambda_+X_2)\big)$ is the Maslov index. More generally, suppose X is an oriented 3-manifold, $Y_1,Y_2\subset\partial X$ are disjoint surfaces

extended resp. by $\lambda_1, \lambda_2 \subset \lambda_X$*, and* $f : Y_1 \to Y_2$ *is an orientation-reversing diffeomorphism sending* λ_1 *to* λ_2*. Then*

$$V(\partial X) \simeq \sum_{l_1,l_2} V(Y_1; l_1) \otimes V(Y_2; l_2) \otimes V\big(\partial X \backslash (Y_1 \cup Y_2); (\hat{l_1}, \hat{l_2})\big)$$

by multiplying by κ^m*, where* l_i *runs through all labelings of* Y_i *and* $m = \mu(K, \lambda_1 \oplus \lambda_2, \Delta)$*. Hence* $Z(X) = \bigoplus_{l_1,l_2} \kappa^m \sum_j \alpha^j_{l_1} \otimes \beta^j_{l_2} \otimes \gamma^j_{\hat{l_1},\hat{l_2}}$*. If gluing* Y_1 *to* Y_2 *by* f *results in the manifold* X_f*, then*

$$Z(X_f) = \kappa^m \sum_{j,l} \langle V(f)\alpha^j_l, \beta^j_l \rangle \gamma^j_{\hat{l},l}$$

(4) Mapping cylinder axiom: *If* Y *is closed and extended by* λ*, and* $Y \times I$ *is extended by* $\lambda \oplus (-\lambda)$*, then* $Z(Y \times I, \lambda \oplus (-\lambda)) = \mathrm{id}_{V(Y)}$*. More generally,*

$$Z(\mathrm{I}_{\mathrm{id}}, \lambda \oplus (-\lambda)) = \bigoplus_{l \in L(Y)} \mathrm{id}_l$$

where I_{id} *is the mapping cylinder of* $\mathrm{id} : Y \circlearrowleft$*, and* id_l *is the identity in* $V(Y; l) \otimes V(Y; l)^*$*.*

For the definitions of $\lambda_\pm X_i, K, \Delta$ in the gluing axiom for Z, see [**Wal1, FNWW**]. First we derive some easy consequences of the axioms.

Proposition 5.4.

(1) $V(S^2) \cong \mathbb{C}$*.*
(2) $\dim V(T^2)$ *is the number of labels.*
(3) $Z(X_1 \# X_2) = \frac{Z(X_1) \otimes Z(X_2)}{Z(S^3)}$*.*
(4) Trace formula: Let X *be a bordism of a closed surface* Y *extended by* λ*, and let* X_f *be the closed* 3*-manifold obtained by gluing* Y *to itself with a diffeomorphism* f*. Then* $Z(X_f) = \kappa^m \operatorname{Tr}_{V(Y)}(V(f))$*, where* $m = \mu(\lambda(f), \lambda_Y \oplus f_*(\lambda), \Delta_Y)$*, where* $\lambda(f)$ *is the graph of* f_* *and* Δ_Y *is the diagonal of* $H_1(-Y; \mathbb{R}) \oplus H_1(Y; \mathbb{R})$*.*
(5) $Z(Y \times S^1) = \dim(V(Y))$*.*
(6) $Z(S^1 \times S^2) = 1$*,* $Z(S^3) = 1/D$*.*

For a TQFT with anomaly, the representations of the mapping class groups are projective in a very special way. From the axioms, we deduce

Proposition 5.5. *The representations of the mapping class groups are given by the mapping cylinder construction: given a diffeomorphism* $f : Y \circlearrowleft$*, with* Y *extended by* λ*, the mapping cylinder* Y_f *induces a map* $V(f) = Z(Y_f) : V(Y) \circlearrowleft$*. We have* $V(fg) = \kappa^{\mu(g_*(\lambda), \lambda, f_*^{-1}(\lambda))} V(f)V(g)$*.*

It follows that the anomaly can be incorporated by an extension of the bordisms X. In particular, modular functors yield linear representations of certain central extensions of the mapping class groups.

For strict labels a, b, c, we have vector spaces $V_a = V(B^2; a)$, $V_{ab} = V(\mathcal{A}_{ab})$, $V_{abc} = V(P_{abc})$, where P is a pair of pants or three-punctured sphere. Denote the standard orientation-reversing maps on $B^2, \mathcal{A}_{ab}, P_{abc}$ by ψ. Then $\psi^2 = \mathrm{id}$, therefore ψ induces identifications $V_{abc} = V^*_{\hat{a}\hat{b}\hat{c}}$, $V_{a\hat{a}} = V^*_{a\hat{a}}$, and $V_1 = V_1^*$. Choose bases $\beta_1 \in V_1, \beta_{a\hat{a}} \in V_{a\hat{a}}$ such that $\langle \beta_a, \beta_a \rangle = 1/d_a$.

PROPOSITION 5.6.

$$Z(B^2 \times I) = \beta_1 \otimes \beta_1, \quad Z(S^1 \times B^2) = \beta_{11}, \quad Z(X \backslash B^3) = \frac{1}{D} Z(X) \otimes \beta_1 \otimes \beta_1.$$

PROOF. Regard the 3-ball B^3 as the mapping cylinder of $\mathrm{id} : B^2 \circlearrowleft$. By the mapping cylinder axiom, $Z(B^3) = \beta_1 \otimes \beta_1$. Gluing two copies of B^3 together yields S^3. By the gluing axiom $Z(S^3) = s_{00} = 1/D$, whence the third equation. □

PROPOSITION 5.7. *The left-handed Dehn twist of $B^2, \mathcal{A}_{ab}, P_{abc}$ along a boundary component labeled by a acts on $V_1, V_{a\hat{b}}, V_{abc}$, resp., by multiplication by a root of unity θ_a. Furthermore $\theta_1 = 1$, $\theta_a = \theta_{\hat{a}}$.*

5.4.4. Framed link invariants and modular representation. Let L be a framed link in a closed oriented 3-manifold X. The framing of L determines a decomposition of the boundary tori of the link compliment $X \backslash \mathrm{nbd}(L)$ into annuli. With respect to this decomposition,

$$Z(X \backslash \mathrm{nbd}(L)) = \bigoplus_l J(L; l) \beta_{a_1 \hat{a_1}} \otimes \cdots \otimes \beta_{a_n \hat{a_n}}$$

where $J(k; l) \in \mathbb{C}$ and $l = (a_1, \ldots, a_n)$ ranges over all labelings of the components of L. $J(L; l)$ is an invariant of the framed, labeled link $(L; l)$. When (V, Z) is a Jones-Kauffman or RT TQFT, and $X = S^3$, the resulting link invariant is a version of the celebrated colored Jones polynomial evaluated at a root of unity. This invariant can be extended to an invariant of labeled, framed graphs.

A framed link L in S^3 represents a closed 3-manifold $\mathcal{S}^3(L)$ via surgery. Using the gluing formula for Z, we can express $Z(\mathcal{S}^3(L))$ as a linear combination of $J(L; l)$:

$$Z(\mathcal{S}^3(L)) = \sum_l c_l J(L; l).$$

Consider the Hopf link H_{ij} labeled by $i, j \in I$. Let $\tilde{s}_{ij}$ be the link invariant of H_{ij}. Note that components with the trivial label may dropped from the link when computing the invariant. Thus the first row of $\tilde{S} = (\tilde{s}_{ij})$ consists of invariants of the unknot labeled by $i \in I$. Denote $\tilde{s}_{i0}$ as d_i, called the quantum dimension of the label i. Prop. 5.7 assigns to each i a root of unity θ_i, called the twist of i. Define

$$D^2 = \sum_{i \in L} d_i^2, \qquad S = \frac{1}{D} \tilde{S}, \qquad T = (\delta_{ij} \theta_i).$$

Then S, T give rise to a projective representation of $\mathrm{SL}(2, \mathbb{Z})$, the mapping class group of T^2.

5.4.5. Verlinde algebras and formulas. Let $T^2 = S^1 \times S^1 = \partial D^2 \times S^1$ be the standard torus. Define the meridian to be the curve $\mu = S^1 \times 1$ and the longitude to be the curve $\lambda = 1 \times S^1$, $1 \in S^1$.

Let (V, Z) be a TQFT. Then the Verlinde algebra of (V, Z) is the vector space $V(T^2)$ with a multiplication defined as follows. The two annular decompositions of T^2 by splitting along μ and λ respectively determine two bases of $V(T^2)$, denoted $m_a = \beta_{a\hat{a}}$, $l_a = \beta_{\hat{a}a}$ and related by the modular S-matrix as follows:

$$l_a = \sum_b s_{ab} m_b, \qquad m_a = \sum_b s_{\hat{a}b} l_b.$$

Define $N_{abc} = \dim V(P_{abc})$. Then

$$m_b m_c = \sum_a N_{a\hat{b}\hat{c}} m_a.$$

This multiplication makes $V(T^2)$ into an algebra, called the Verlinde algebra of (V, Z).

In the longitude basis $\{l_a\}$, the multiplication becomes

$$l_a l_b = \delta_{ab} s_{0a}^{-1} l_a.$$

This multiplication also has an intrinsic topological definition: $Z(P \times S^1)$ gives rise to a linear map $V(T^2) \times V(T^2) \to V(T^2)$ by regarding $P \times S^1$ as a bordism from $T^2 \sqcup T^2$ to T^2.

The fusion coefficients N_{abc} can be expressed in terms of entries of S:

$$N_{abc} = \sum_{x \in L} \frac{s_{ax} s_{bx} s_{cx}}{s_{0x}}$$

More generally, for a genus=g surface Y with m boundary components labeled by $l = (a_1 \cdots a_m)$,

$$\dim V(Y) = \sum_{x \in L} s_{0x}^{2-2g-n} \left(\prod s_{a_i x}\right). \tag{5.8}$$

5.4.6. Unitary TQFTs. A modular functor is unitary if each $V(Y)$ is endowed with a positive-definite Hermitian pairing

$$\langle , \rangle : \overline{V(Y)} \times V(Y) \to \mathbb{C},$$

and each morphism is unitary. The Hermitian structures are required to satisfy compatibility conditions as in the naturality axiom of a modular functor. In particular,

$$\left\langle \bigoplus_i v_i, \bigoplus_j w_j \right\rangle = \sum_i s_{i0} \langle v_i, w_i \rangle.$$

Note this implies that all quantum dimensions of particles are positive reals. Moreover, the following diagram commutes for all Y:

$$\begin{array}{ccc} V(Y) & \xrightarrow{\cong} & V(-Y)^* \\ \cong \downarrow & & \downarrow \cong \\ \overline{V(Y)^*} & \xrightarrow{\cong} & \overline{V(-Y)} \end{array}$$

A TQFT is unitary if its modular functor is unitary and its partition function satisfies $Z(-X) = \overline{Z(X)}$.

5.5. Jones-Kauffman TQFTs

The best understood examples of TQFTs are Jones-Kauffman $(V_{\mathrm{JK}},\ Z_{\mathrm{JK}})$. They have trivial Frobenius-Schur indicators but framing anomaly. Fix a primitive $4r$th root of unity A for $r \geqslant 3$. Given an oriented closed surface Y, we need to associate a vector space $V(Y)$ to Y. Choose an oriented 3-manifold M^3 such that $\partial M^3 = Y$. Let $V_A(Y, M^3)$ be the space of Jones-Kauffman skein classes of M^3 as below. The dimension of $V_A(Y, M^3)$ is independent of the choice of M^3, therefore

for all choices of M^3, $V_A(Y, M^3)$'s are isomorphic as vector spaces. But the isomorphism for two different choices of M^3 is not canonical, hence not all axioms of a TQFT are satisfied.

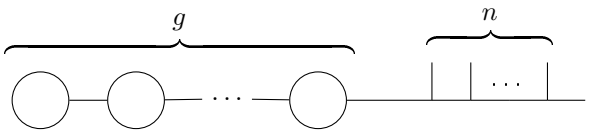
5.5.1. Skein spaces. Fix $A \neq 0$ and consider an oriented 3-manifold X with or without boundary. Let $\tilde{K}_A(X)$ be the vector space spanned by all links in X. Let $K_A(X)$ be the quotient vector space obtained from $\tilde{K}_A(X)$ by imposing two relations: the Kauffman bracket and $p_{r-1} = 0$. The Kauffman bracket and JWP are applied locally inside any topological 3-ball. Skein spaces are the most important objects for the study of diagram and Jones-Kauffman TQFTs.

THEOREM 5.9. *Let A be a primitive $4r$th root of unity, $r \geqslant 3$. Then*

(1) $K_A(S^3) = \mathbb{C}$.
(2) The empty link $\varnothing$ is nonzero in $K_A(\#(S^1 \times S^2))$ and $K_A(Y \times S^1)$ for any oriented closed surface Y.
(3) $K_A(X_1 \# X_2) \cong K_A(X_1 \sqcup X_2)$ canonically.
(4) If $\partial X_1 = \partial X_2$, then $K_A(X_1) \simeq K_A(X_2)$, not canonically. An isomorphism can be constructed from a 4-manifold W such that $\partial W = -\partial X_1 \sqcup \partial X_2$; this isomorphism depends only on the signature of W.
(5) If the empty link $\varnothing$ is nonzero in $K_A(X)$ for a closed 3-manifold X, then $K_A(X) \cong \mathbb{C}$ canonically.
(6) $K_A(-X) \times K_A(X) \to K_A(D_X)$ is nondegenerate. Therefore $K_A(-X) \simeq K_A^*(X)$, though not canonically.
(7) $K_A(Y \times I) \to \mathrm{End}(K_A(X))$ is an algebra isomorphism if $\partial X = Y$.

This theorem is a collection of results scattered throughout the literature, and is known to experts. A formal treatment can be found in [**BHMV**], and a proof in [**FNWW**].

5.5.2. Jones-Kauffman modular functor. The strict fusion categories for Jones-Kauffman TQFTs are the Jones algebroids. Fix $A = ie^{\pm 2\pi i/4r}$ for $r \geqslant 4$ even or $A = \pm e^{\pm 2\pi i/4r}$ for arbitrary $r \geqslant 3$. Let $L = \{0, \ldots, r-2\}$ be the label set. Let (Y, λ) be an oriented extended surface. If Y is closed, choose an oriented 3-manifold X such that $\ker\big(H_1(Y, R) \to H_1(X, R)\big) = \lambda$. Then all such $K_A(X)$ are canonically isomorphic by choosing a 4-manifold W with boundary $X_1 \sqcup -X_2 \sqcup (Y \times I)$ and signature $\sigma(W) = 0$. Let $V_{\mathrm{JK}}(Y) = K_A(X)$ for any such X. When Y has multiple boundary components, labeled by $l, \ldots$, first we cap them off with disks and choose an extended 3-manifold X bounding the capped off surface $\hat{Y}$, then insert a JWP p_l to the boundary component labeled by l perpendicular to the filled-in disk. Let $V_{\mathrm{JK}}(Y)$ be the relative skein class space $K_A(X)$ such that all skein classes are terming as p_l at boundary components labeled by l. A basis of $V_{\mathrm{JK}}(Y)$ is given by admissible labelings of the following graph:



where g is the genus of Y and n is the number of boundary components. The mapping class group action can be defined in various ways. Conceptually, given a diffeomorphism $f\colon Y \circlearrowleft$, let M_f be its mapping cylinder. Then M_f can be obtained

by surgery on a link L_f in $Y \times I$; labeling each component of L_f by w_0 defines an element in $K_A(Y \times I)$. $K_A(Y \times I)$ acts on $K_A(Y \times I) \cong \mathrm{End}(K_A(X))$ as an algebra isomorphism by $(Y \times I) \sqcup_Y (Y \times I) \cong Y \times I$. Since $K_A(Y \times I)$ is the full matrix algebra, and any matrix algebra isomorphism is of the form $A \otimes A^{-1}$, the action of M_f on $K_A(Y \times I)$ is of the form $A_f \otimes A_f^{-1}$ for some nondegenerate operator $A_f \colon K_A(X) \circlearrowleft$. We define $\rho_A(f)$ to be A_f, revealing clearly that $\rho_A(f)$ is a projective representation. Concretely, f can be written as a composition of Dehn twists. For a Dehn twist on a simple closed curve c, push c into $Y \times I$ and label it by w_0. Then by absorbing the collar, $(Y \times I) \cup X \cong X$ induces an action of c on $K_A(X) = V(Y)$.

For the Hermitian product, for any (Y, λ), choose H_g to be a handlebody such that the canonical extension of H_g is λ. Then $-H_g \sqcup_h H_g$ becomes S^3 for the standard homeomorphism $h \colon -Y \circlearrowleft$. Then skein classes $x \in K_A(-H_g)$, $y \in K_A(H_g)$ form formal links in S^3, whose link invariant is $\langle x, y \rangle$. This is the same as

$$K_A(-H_g) \times K_A(-H_g) \to K_A(DH_g) = K_A(\#(S^1 \times S^2)) = \mathbb{C}.$$

5.5.3. Jones-Kauffman partition functor. Let X be an oriented 3-manifold such that $\partial X = Y$. If Y is extended by the canonical Lagrangian subspace λ_X, then the empty link $\varnothing$ in X defines an element in $V_A(Y) = K_A(X)$. This skein class is $Z(X) \in V_A(Y)$. Concretely, suppose $Y = \partial H_g$, where H_g is a handlebody such that

$$\ker\big(H_1(Y; \mathbb{R}) \to H_1(H_g; \mathbb{R})\big) = \lambda.$$

Then X can be obtained by surgery on a link L_X in H_g. Color each component of L_X by w_0. Then $Z(X)$ is the vector $D^{m-1} \big(\frac{D}{p_+}\big)^{\sigma(L_X)} \langle w_0 * L_X \rangle$ in $K_A(H_g) = V_A(Y)$. If Y is not extended by λ, which is not the canonical Lagrangian subspace λ_X, then we choose a 4-manifold W of signature 0 such that $\partial W = -X \sqcup (Y \times I) \sqcup H_g$, where H_g is a handlebody satisfying

$$\ker\big(H_1(Y; \mathbb{R}) \to H_1(H_g; \mathbb{R})\big) = \lambda_X$$

The 4-manifold W induces an isomorphism

$$\Phi_W \colon K_A(X) \to K_A(H_g) = V_A(Y, \lambda).$$

The image of the empty link $\varnothing \in K_A(X)$ under Φ_W is $Z(X) \in V_A(Y, \lambda)$. $Z(X)$ is independent of the choice of W. For treatment using p_1-structures, see [**BHMV**].

5.6. Diagram TQFTs

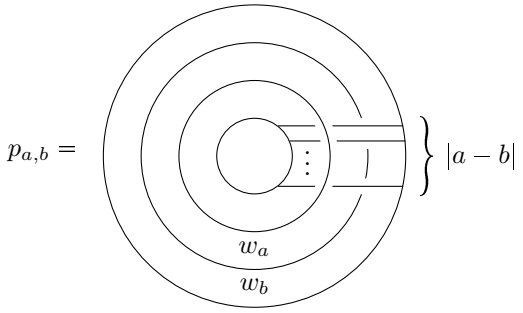
Diagram TQFTs (V_{TV}, Z_{TV}) are the easiest in the sense that the two complications for TQFTs, Frobenius-Schur indicators and framing anomaly, don't arise. They are quantum doubles of Jones-Kauffman theories, first defined in [**TV**] based on triangulation. Our definition is intrinsic. In this section, surfaces and 3-manifolds are neither extended nor oriented, though V_{TV} is defined for nonorientable surfaces as well.

5.6.1. Diagram fusion categories. Diagram TQFTs can be defined for many choices of the Kauffman variable A. We will focus on $A = \pm i e^{2\pi i/4r}$ for $r \geqslant 4$ even, and $A = \pm e^{\pm 2\pi i/4r}$ for arbitrary $r \geqslant 3$. In both cases, A is a primitive $4r$th root of unity. In general any primitive $4r$th or $2r$th root of unity suffices. Again we will refer to the theory with a fixed A as a level $k = r-2$ theory. The strict fusion category for level k is as follows (it is ribbon). The label set is $L = \{(a, b) \mid a, b = 0, 1, \ldots, k\}$,

of rank $(k+1)^2$. The fusion rule is a product of the fusion rule for Jones algebroids: $(a,b)\otimes(c,d) = (a\otimes b, c\otimes d)$ expanded by distributing in both coordinates. For example, in the diagram TQFT from the Ising theory,

$$(\sigma,\sigma)\otimes(\sigma,\sigma) = (1\oplus\psi, 1\oplus\psi) = (1,1)\oplus(1,\psi)\oplus(\psi,1)\oplus(\psi,\psi).$$

Precisely, the diagram fusion category is the annular version of the Jones algebroid. The (a,b) label is the annular version of JWP given graphically by



where the crossing in the diagram is understood to be resolved by the Kauffman bracket, and $w_c = D^{-2}\sum_i \tilde{s}_{c,i} i$. All labels are self-dual, i.e., $\widehat{(a,b)} = (a,b)$.

5.6.2. Diagram modular functor. We first consider a closed surface Y, not necessarily orientable. Let $\mathcal{S}(Y)$ be the linear span of all multi-curves (collections of disjoint simple closed curves) in Y. $\mathcal{S}(Y)$ is an uncountably infinite-dimensional vector space. Now we introduce a local relation among multi-arcs: the Jones-Wenzl projector for the fixed value A. Let $V_{\mathrm{TV}}(Y) = \mathcal{S}(Y)/(p_{r-1})$, the quotient by generalized annular consequences of the JWP $p_{r-1} = 0$. It is not hard to see $V_{\mathrm{TV}}(Y)$ is also $K_A(Y\times I)$.

For a surface Y with boundary ∂Y labeled by $(a,b),\dots$, if the boundary component of ∂Y is labeled by (a,b), then insert $p_{a,b}$ in a small cuff of the boundary circle, and define $V(Y)$ to be spanned by any extension of $\{p_{a,b}\}$'s into multi-curves in Y modulo JWP $p_{r-1} = 0$. The mapping class group action is straghtforward: vectors in $V_{\mathrm{TV}}(Y)$ are spanned by multi-curves, and a diffeomorphism acts on a multi-curve by carrying it to another multi-curve.

5.6.3. Diagram partition functor. Let X be a 3-manifold such that $\partial X = Y$. Then $\partial(-X\sqcup X) = -Y\sqcup Y$. By Thm. 5.9(3), $K_A(-X\sqcup X)\cong K_A(-X\#X)$, and $-X\#X$ can be obtained from surgering a framed link L in $Y\times I$. The link L represents an element $Z_{\mathrm{TV}}(X) = D^m\langle w_0 * L\rangle \in K_A(Y\times I)\cong V_{\mathrm{TV}}(Y)$. To define a Hermitian product on $V_{\mathrm{TV}}(Y)$, we use $V_{\mathrm{TV}}(Y) = K_A(Y\times I)$. Then

$$K_A(-(Y\times I))\times K_A(Y\times I)\to K_A(D(Y\times I)) = K_A(Y\times S^1) = \mathbb{C}.$$

Note that vectors from bounding 3-manifolds X such that $\partial X = Y$ do not span $V_{\mathrm{TV}}(Y)$ because under the isomorphism $V_{\mathrm{TV}}(Y) = V^*_{\mathrm{JK}}(Y)\otimes V_{\mathrm{JK}}(Y)$, elements $Z_{\mathrm{TV}}(X)$ are of the form $v^*\otimes v$ for $v = Z_{\mathrm{JK}}(X)$. When $A = \pm ie^{2\pi i/4r}$, r even, all the Hermitian inner products on $V_{\mathrm{TV}}(Y)$ are positive definite. Hence the diagram TQFTs are unitary for those A's. When $A = \pm e^{\pm 2\pi i/4r}$ and Y is closed, the Hermitian product on $V_{\mathrm{TV}}(Y)$ is also positive definite, though not so for surfaces with boundary. Using diagram TQFTs, we can prove

THEOREM 5.10. *The representations of the mapping class groups of oriented closed surfaces from Jones-Kauffman TQFTs, $k = 1, 2, \ldots$, are asymptotically faithful modulo center, i.e., any noncentral mapping class can be detected in a high enough level represention.*

This theorem was first proven in [**FWW**].

THEOREM 5.11. *The diagram TQFT is equivalent to the quantum double of the Jones-Kauffman TQFT for the same A.*

This theorem is due to K. Walker and V. Turaev [**Wal1, Tu**].

5.7. Reshetikhin-Turaev TQFTs

Reshetikhin-Turaev TQFTs $(V_{\mathrm{RT}}, Z_{\mathrm{RT}})$ are the most famous TQFTs and are considered to be the mathematical realization of Witten's SU(2)-Chern-Simons TQFTs. Compared to their siblings Jones-Kauffman TQFTs, they are more complicated due to Frobenius-Schur indicators: the spin 1/2 representation in Reshetikhin-Turaev TQFTs has Frobenius-Schur indicator -1, while the corresponding label 1 in Jones-Kauffman has trivial Frobenius-Schur indicator.

The boundary condition category for level $k = l - 2$ theory is the strictification of the quantum group category (A_1, q, l) for $q = e^{\pm \pi i/l}$. We will call the resulting TQFTs the Reshetikhin-Turaev SU(2) level k TQFTs, denoted as $\mathrm{SU}(2)_k$. The label set for Reshetikhin-Turaev $\mathrm{SU}(2)_k$ theory is $L = \{0, 1, \ldots, k\}$, and all labels are self-dual. The fusion rules are the same as the corresponding Jones-Kauffman theory. The label i corresponds to the spin $i/2$ representation of SU(2). For explicit data, let $[n]_q = \frac{q^n - q^{-n}}{q - q^{-1}}$. Recall that $q = e^{\pm \pi i/l}$ is different from the q in the Jones representation $\rho_A^J(\sigma_i)$.

$$d_i = [i+1]_q \qquad \tilde{s}_{ij} = [(i+1)(j+1)]_q \qquad \theta_i = q^{i(i+2)/2}$$

The framed link invariant from Reshetikhin-Turaev differs from the Kauffman bracket $\langle , \rangle$ [**KM1**]. In particular, for the same A, $\tilde{s}_{ij}$ differs by a prefactor $(-1)^{i+j}$, which makes the S-matrix nonsingular for odd levels too. Hence the resulting RFCs are MTCs for all levels and also unitary.

5.8. Turaev-Viro TQFTs

Given a spherical fusion category $\mathcal{C}$, there is a procedure to write down state sums using triangulations of a 3-manifold M^3. The 3-manifold invariant from diagram TQFTs was such an example, which was first obtained by V. Turaev and O. Viro based on the Jones algebroid. It has been stated in various places that the resulting state sum is indeed a 3-manifold invariant. The only complete proof known to the author is the case in [**Tu**]: $\mathcal{C}$ is a unimodal RFC. What is overlooked is the independence of the ordering of the vertices, which requires certain symmetries of the 6j symbols. It has been observed in [**H**] that some symmetries are not always achievable in a spherical fusion category. So it is open, based on published literature, whether every spherical fusion category leads to a state-sum Turaev-Viro TQFT. On the other hand, the Drinfeld center of $\mathcal{C}$ is modular. Therefore there is a Reshetikhin-Turaev type TQFT for each spherical fusion category $\mathcal{C}$. It is believed that the quantum invariants of the two constructions are related by

$$\tau_{\mathcal{C}}^{\mathrm{TV}}(M^3) = \tau_{Z(\mathcal{C})}^{\mathrm{RT}}(M^3).$$

Of course this identity would fail if the left-hand side were not defined.

5.9. From MTCs to TQFTs

In [**Tu**], it has been shown that every MTC leads to a TQFT. There are two of them depending on the choice of D in $D^2 = \sum_{i \in L} d_i^2$. But given a TQFT as in [**Tu**], it is not known if a MTC can be constructed from it. If this were not true, then probably the definition of a TQFT would need modification, as the definition of a MTC is rigid and compatible with physical applications.

CONJECTURE 5.12. *The strict fusion category in the definition of a TQFT in Sec. 5.4 can be extended uniquely to a MTC compatible with the TQFT.*

CHAPTER 6

TQFTs in Nature

This chapter introduces the algebraic theory of anyons using unitary ribbon fusion categories. It follows that quantum invariants of links are amplitudes of physical processes.

6.1. Emergence and anyons

TQFTs are very special quantum field theories. A physical Hamiltonian of interacting electrons in real materials exhibits no topological symmetries. Then it begs the question, is TQFT relevant to our real world? The answer is a resounding yes; it is saved by the so-called emergence phenomenon. The idea is expressed well by a line in an old Chinese poem:

草色遥看近却无

Word for word it is: grass color far see close but not. It means that in early spring, one sees the color of grass in a field from far away, yet no particular green spot can be pointed to. Topological physical systems do exist, though they are rare and difficult to discover.

It is extremely challenging for experimental physicists to confirm the existence of TQFTs in Nature. Physical systems whose low-energy effective theories are TQFTs are called topological states or phases of matter. Elementary excitations in topological phases of matter are particle-like, called quasiparticles to distinguish them from fundamental particles such as the electron. But the distinction has become less and less clear-cut, so very often we call them particles. In our discussion, we will have a physical system of electrons or maybe some other particles in a plane. We will also have quasiparticles in this system. To avoid confusion, we will call the particles in the underlying system constituent particles or slave particles or sometimes just electrons, though they might be bosons or atoms, or even quasiparticles. If we talk about a Hamiltonian, it is often the Hamiltonian for the constituent particles.

While in classical mechanics the exchange of two identical particles does not change the underlying state, quantum mechanics allows for more complex behavior [**LM**]. In three-dimensional quantum systems the exchange of two identical particles may result in a sign-change of the wave function which distinguishes fermions from bosons. Two-dimensional quantum systems—such as electrons in FQH liquids—can give rise to exotic particle statistics, where the exchange of two identical (quasi)particles can in general be described by either abelian or non-abelian statistics. In the former, the exchange of two particles gives rise to a complex phase $e^{i\theta}$, where $\theta = 0, \pi$ correspond to the statistics of bosons and fermions respectively, and $\theta \neq 0, \pi$ is referred to as the statistics of non-abelian *anyons*

[**Wi1**]. The statistics of non-abelian anyons are described by $k \times k$ unitary matrices acting on a degenerate ground-state manifold with $k > 1$ [**FM, FG**]. These unitary matrices form a non-abelian group when $k > 1$, hence the term non-abelian anyons.

Anyons appear as emergent quasiparticles in fractional quantum Hall states [**Hal, MR, Wen3**] and as excitations in microscopic models of frustrated quantum magnets that harbor topological quantum liquids [**Ki1, Ki2, Fr2, FNSWW, LW1**]. While for most quantum Hall states the exchange statistics is abelian, there are quantum Hall states at certain filling fractions, e.g., $\nu = 5/2$ and $\nu = 12/5$, for which non-abelian quasiparticle statistics have been proposed, namely those of so-called Ising and Fibonacci theories, respectively [**RR**].

If many particles live in the same space X, then the configuration space of n such particles depends on the distinguishability of the n particles. For example, if the n particles are pairwise distinct and not allowed to coincide (called hard-core particles), then their configuration space is the n-fold Cartesian product X^n with the big diagonal $\Delta = \{(x_1, \ldots, x_n) \mid x_i = x_j \text{ for some } i \neq j\}$ removed. But if the n particle are instead identical, then the symmetric group S_n acts on $X^n \backslash \Delta$ freely, and the configuration space becomes the quotient space $(X^n \backslash \Delta)/S_n$, denoted as $C_n(X)$.

Now suppose $X = \mathbb{R}^m$, $m \geqslant 1$. The configuration space $C_n(\mathbb{R}^m)$ describes the possible states of n identical hard-core particles in $\mathbb{R}^m$. If the n particles are subject to a quantum description, then their states will correspond to nonzero vectors in some Hilbert space $\mathbb{L}$. Let H be the Hamiltonian, with eigenvalues λ_i ordered as $0 = \lambda_0 < \lambda_1 < \cdots$, where we normalize λ_0 to 0. So the state space $\mathbb{L}$ can be decomposed into energy eigenspaces $\mathbb{L} = \bigoplus_i \mathbb{L}_i$, where $\mathbb{L}_i$ is the eigenspace of the eigenvalue λ_i of H. States in $\mathbb{L}_0$ have the lowest energy, and are called the ground states. States in $\mathbb{L}_i$ for $i > 0$ are excited states. Normally we are only interested in excited states in $\mathbb{L}_1$. The minimal possible states in $\mathbb{L}_1$ which violate local constraints are called elementary excitations. Suppose the non-local properties of the ground states can be isolated into a subspace V_n of $\mathbb{L}_0$. Then for n particles at $p_1, \ldots, p_n$, their non-local properties will be encoded in a non-zero vector $|\psi(p_1, \ldots, p_n)\rangle \in V_n$. Furthermore, let us assume that the non-local properties encoded in V_n are protected by some physical mechanism such as an energy gap. Now start with n particles at positions $p_1, \ldots, p_n$ with the non-local properties in a state $|\psi_0(p_i)\rangle \in V_n$. Suppose the n particles are transformed back to the original positions as a set after some time t, and the non-local properties are in a state $|\psi_1(p_i)\rangle \in V_n$. If V_n has an orthonormal basis $\{e_i\}_1^k$, and we start with $|\psi_0(p_i)\rangle = e_i$, then $|\psi_1(p_i)\rangle$ will be a linear combination of $\{e_i\}$: $e_i \mapsto \sum_{j=1}^k a_{ji} e_j$. The motion of the n particles traverses a loop b in the configuration space $C_n(\mathbb{R}^m)$. If the non-local properties are topological, then the associated unitary matrix $U(b) = (a_{ij})$ depends only on the homotopy class of b. Hence we get a unitary projective representation $\pi_1(C_n(\mathbb{R}^m)) \to \mathrm{U}(V_n)$, which will be called the statistics of the particles.

Definition 6.1. *Given n identical hard-core particles in $\mathbb{R}^m$, their statistics are representations $\rho\colon \pi_1(C_n(\mathbb{R}^m)) \to \mathrm{U}(V_n)$ for some Hilbert space V_n. Particles with $\dim(V_n) = 1$ for all n are called abelian anyons; otherwise they are non-abelian anyons.*

It is well-known:

$$\pi_1(C_n(\mathbb{R}^m)) = \begin{cases} 1, & m = 1, \\ B_n, & m = 2, \\ S_n, & m \geqslant 3. \end{cases}$$

Therefore braid group representations and anyon statistics are the same in dimension two [**Wu**].

6.2. FQHE and Chern-Simons theory

The only real materials that we are certain are in topological states are electron liquids, which exhibit the fractional quantum Hall effect (FQHE).

Eighteen years before the discovery of the electron, E. Hall was studying Maxwell's book *Electricity and Magnetism*. He was puzzled by a statement in the book and performed an experiment to disprove it, discovering the so-called Hall effect. In 1980, K. von Klitzing discovered the integer quantum Hall effect (IQHE), which won him the 1985 Nobel Prize. Two years later, H. Stormer, D. Tsui and A. Gossard discovered the FQHE, which led to the 1998 Nobel Prize for Stormer, Tsui, and R. Laughlin. They were all studying electrons in a plane immersed in a perpendicular magnetic field. Laughlin's prediction of the fractional charge $e/3$ of quasiparticles in $\nu = 1/3$ FQH liquids was experimentally confirmed. Such quasiparticles are anyons, a term introduced by F. Wilczek [**Wi1**]. Braid statistics of anyons were deduced for $\nu = 1/3$, and experiments to confirm braid statistics are making progress.

FQH liquids are new phases of matter that cannot be described with Landau's theory. A new concept—topological order—was proposed, and modular transformations S, T were used to characterize this new exotic quantum order [**Wen1, Wen2**].

6.2.1. Electrons in flatland. The classical Hall effect (Fig. 6.1) is characterized by a Hall current with resistance $R_{xy} = \alpha B$ for some non-universal constant α. One explanation is as follows. Electrons in the square $\{(x, y) \mid 0 \leqslant x, y \leqslant 1\}$ im-

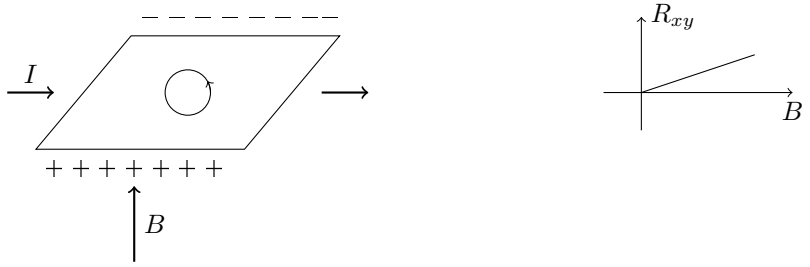


FIGURE 6.1. Classical Hall effect.

mersed in a magnetic field in the z-direction feel the Lorentz force $F = q(v \times B + E)$. When a current flows in the x direction, they consequently move in circles. Electrons on the front edge $y = 0$ will drift to the back edge $y = 1$ due to collisions. Eventually electrons accumulate at the back edge and a current, called Hall current, starts in the y-direction. The Hall resistance depends linearly on B. But when temperature lowers and B strengthens, a surprise is discovered. The Hall resistance is no longer linear with respect to B. Instead it develops so-called plateaux and quantization (Fig. 6.2). What is more astonishing is the quantized value: it is always $R_{xy} = \nu^{-1}h/e^2$, where $\nu =$ integer up to an additive error of 10^{-10}. When B

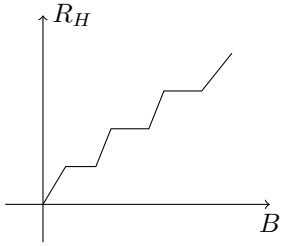


FIGURE 6.2. FQH plateaux.

becomes even bigger, around 30 Tesla, another surprise occurs: ν can be a fraction with odd denominator, such as $\nu = 1/3, 2/5, \ldots$. In 1987 an even denominator FQH liquid was discovered at $\nu = 5/2$.

The problem of an electron in a perpendicular magnetic field was solved by L. Landau in the 1930s. But the fact that there are about 10^{11} electrons per cm^2 in FQH liquids makes the solution of the realistic Hamiltonian for such electron systems impossible, even numerically. The approach in condensed matter physics is to write down an effective theory at low energy and long wavelength which describes the universal properties of the electron systems. The electrons are strongly interacting with each other to form an incompressible electron liquid when the FQHE could be observed. Landau's solution for a single electron in a magnetic field shows that quantum mechanically an electron behaves like a harmonic oscillator. Therefore its energy is quantized to so-called Landau levels. For a finite size sample of a 2-dimensional electron system in a magnetic field, the number of electrons in the sample divided by the number of flux quanta in the perpendicular magnetic field is called the Landau filling fraction ν. The state of an electron system depends strongly on the Landau filling fraction. For $\nu < 1/5$, the electron system is a Wigner crystal: the electrons are pinned at the vertices of a triangular lattice. When ν is an integer, the electron system is an IQH liquid, where the interaction among electrons can be neglected. When ν are certain fractions such as $1/3, 1/5, \ldots$, the electrons are in a FQH state. Both IQHE and FQHE are characterized by the quantization of the Hall resistance $R_{xy} = \nu^{-1} h/e^2$, where e is the electron charge and h the Planck constant, and the exponential vanishing of the longitudinal resistance R_{xx}. There are about 50 such fractions and the quantization of R_{xy} is reproducible up to 10^{-10}. How could an electron system with so many uncontrolled factors such as the disorders, sample shapes, and variations of the magnetic field strength quantize so precisely? The IQHE has a satisfactory explanation both physically and mathematically. The mathematical explanation is based on noncommutative Chern classes. For the FQHE at filling fractions with odd denominators, the composite fermion theory based on U(1) Chern-Simons theory is a great success: electrons combine with vortices to form composite fermions and then with composite fermions, as new particles, to form their own integer quantum Hall liquids. The exceptional case is the observed FQHE $\nu = 5/2$ and its partial hole conjugate $\nu = 7/2$. The leading candidate for $\nu = 5/2$ is the Pfaffian state, and its effective theory for low-energy physics is the Ising TQFT or closely related $\text{SU}(2)_2$. If it were true, the Jones polynomial at 4th roots of unity would have a direct bearing on experimental data for $\nu = 5/2$.

6.2.2. Chern-Simons theory as effective theory. The discovery of the FQHE has cast some doubts on the completeness of Landau theory for states of matter. It is believed that the electron liquid in a FQHE state is in a topological state with a Chern-Simons TQFT as an effective theory. Since topological states are described by TQFTs, we can ask what TQFT represents the $\nu = 1/3$ Laughlin state. It turns out this is not a simple question to answer because TQFTs such as Chern-Simons theories describe bosons rather than fermions. To work with fermions, the answer is a spin TQFT. To work with bosons, we use the so-called flux attachment to convert the electrons into charge flux composites, which are bosonic objects.

How do physicists come to the conclusion that topological properties of FQH liquids can be modeled by Chern-Simons TQFTs? If a transformation is performed from the Chern-Simons Lagrangian to Hamiltonian, the corresponding Hamiltonian is found to be identically 0 because the Chern-Simons 3-form has only first derivative. From an emergent perspective, if a system is examined from longer and longer wavelengths, the behavior of the system is dominated by the lowest derivative terms: m derivatives under the Fourier transform become k^m, where k is the momentum, and the long wavelength limit is $k \to 0$. Therefore Chern-Simons terms become the dominant terms in the long wavelength limit. To make a contact with FQH liquid, we can derive the equation of motion. Then the off-diagonal feature of Hall resistance would be predicted. More definite evidence comes from the edge of a FQH liquid and path integral manipulation. A Luttinger liquid theory is proposed based on this Chern-Simons connection, and predictions from Luttinger liquid edge theory have experimental confirmation. Physically one can also "derive" abelian Chern-Simons theory starting from electrons using path integrals. Of course, many steps are not rigorous, and based on certain physical assumptions.

Witten [**Witt**] discovered that the boundary theory of a Chern-Simons TQFT is a Wess-Zumino-Witten (WZW) CFT. Such a CFT has two applications in FQH liquids: as a description of the boundary (1+1)-system [**Wen4**], and as a description for a (2+0) fixed time slice [**MR**]. The wave function of the electrons in the ground states can be described by a wave function $\psi(z_1, \ldots, z_N)$, where z_i is the position of the ith electron. The Laughlin theory which predicted the charge $e/3$ for quasiparticles in $\nu = 1/3$ FQH liquids is based on the famous Laughlin wave function

$$\prod_{i<j}(z_i - z_j)^3 e^{-\frac{1}{4}\sum |z_i|^2}$$

This wave function can be obtained as the conformal block of a U(1) CFT. As generalized later, electron wave functions are conformal blocks of the corresponding CFTs. Considering all the evidence together, we are confident that Chern-Simons theory describes FQH liquids.

While the case for abelian Chern-Simons theory is convincing, the description of $\nu = 5/2$ with non-abelian Chern-Simons theory has less evidence. In particular, the physical "derivation" of abelian Chern-Simons theory does not apply to $\nu = 5/2$. How is it possible to have non-abelian anyons from electrons? We still don't know. But one possibility is that electrons first organize themselves into states with abelian anyons. Then a phase transition drives them into a non-abelian phase.

6.2.3. Ground states and statistics. To describe new states of matter such as FQH electron liquids, we need new concepts and methods. Consider the following Gedanken experiment. Suppose an electron liquid is confined to a closed

oriented surface Σ, e.g., a torus. The lowest energy states of the system form a Hilbert space $L(\Sigma)$, called the ground state manifold. Furthermore, suppose $L(\Sigma)$ decomposes as $V(\Sigma) \otimes V^{\text{local}}(\Sigma)$, where $V^{\text{local}}(\Sigma)$ encodes the local degrees of freedom. In an ordinary quantum system, the ground state will be unique, so $V(\Sigma)$ is 1-dimensional. But for topological states of matter, $V(\Sigma)$ is often degenerate (more than 1-dimensional), i.e., there are several orthonormal ground states with exponentially small energy differences. This ground state degeneracy in $V(\Sigma)$ is a new quantum number. Hence a topological quantum system assigns each closed oriented surface Σ a Hilbert space $V(\Sigma)$, which is exactly the rule for a TQFT. A FQH electron liquid always has an energy gap in the thermodynamic limit which is equivalent to the incompressibility of the electron liquid. Therefore the ground states manifold is stable if controlled below the gap. Since the ground state manifold has exponentially close energy, the Hamiltonian of the system restricted to the ground state manifold is 0, hence there will be no continuous evolution except an overall abelian phase due to ground state energy. In summary, ground state degeneracy, energy gap, and the vanishing of the Hamiltonian are all salient features of topological quantum systems.

Although the Hamiltonian for a topological system is a constant, there are still discrete dynamics induced by topological changes besides an overall abelian phase. As we mentioned before, given a realistic system, even the ground states have local degrees of freedom. Topological changes induce evolution of the whole system, so within the ground state, states in $V(\Sigma)$ evolve through $V(\Sigma) \otimes V^{\text{local}}(\Sigma)$.

Elementary excitations of FQH liquids are quasiparticles, which are labels for a TQFT; particle types serve as strict labels. Suppose a topological quantum system confined to a surface Σ has elementary excitations localized at well-separated points $p_1, p_2, \dots$ on Σ. Then the ground states of the system outside some small neighborhoods of p_i form a Hilbert space. Suppose this Hilbert space splits into $V(\Sigma; p_i) \otimes V^{\text{local}}(\Sigma; p_i)$ as before. Then associated to the surface with small neighborhoods of p_i removed and each resulting boundary circle labeled by the corresponding quasiparticle is a Hilbert space $V(\Sigma; p_1, \dots, p_n)$. There are discrete evolutions of the ground states induced by topological changes such as the mapping classes of Σ which preserve the boundaries and their labels. An interesting case is the mapping class group of the disk with n punctures—the famous braid group on n-strands, B_n. Suppose the particles can be braided adiabatically so that the quantum system remains in the ground states. Then we have a unitary transformation from the ground states at time t_0 to the ground states at time t_1. Then $V(\Sigma; p_1, \dots, p_n)$ is a projective representation of the mapping class group of Σ. Therefore an anyonic system provides an assignment from a closed oriented surface Σ with anyons at $p_1, \dots, p_n$ to a Hilbert space $V(\Sigma; p_1, \dots, p_n)$ of topological ground states and from braiding of anyons to mapping classes on $V(\Sigma; p_1, \dots, p_n)$.

6.3. Algebraic theory of anyons

A unitary MTC $\mathcal{C}$ gives rise to a modular functor $V_{\mathcal{C}}$, which assigns a Hilbert space $V(Y)$ to each surface Y with extra structure and a projective representation of the mapping class group of Y. Therefore it is natural to use a UMTC to model the topological properties of anyonic systems. We will always assume our categories are strict in this section.

How does an anyon look? Nobody knows. But it is a particle-like topological quantum field. It is important that an anyon can be transported from one location to another by local operators. Although a single anyon cannot be created or removed, its physical size can changed by local operators. Therefore anyons are mobile, indestructible, yet shrinkable by local operators. The mathematical model under UMTCs is a framed point in the plane: a point with a small arrow. Therefore its worldline in $\mathbb{R}^3$ is not really an arc; it is a ribbon. Hence we are interested in framed link invariants instead of just link invariants. In $\mathbb{R}^3$, the information of the ribbon can be encoded by the winding number of the two boundary curves or the linking number of two boundary circles for a closed trajectory (oriented in the same direction). In FQH liquids, an anyon is considered to be a pointlike defect in the uniform electron liquid, so it is called a quasihole. They are attracted to impurities in the sample. In the wave function model of FQH liquids, a quasihole is a coherent superposition of edge excitations.

A dictionary of terminologies is given in Table 6.1. There exists a unique topo-

UMTC	*anyonic system*
simple object	anyon
label	anyon type or topological charge
tensor product	fusion
fusion rules	fusion rules
triangular space V_{ab}^c or V_c^{ab}	fusion/splitting space
dual	antiparticle
birth/death	creation/annihilation
mapping class group representations	anyon statistics
nonzero vector in $V(Y)$	ground state vector
unitary F-matrices	recoupling rules
twist $\theta_x = e^{2\pi i s_x}$	topological spin
morphism	physical process or operator
tangles	anyon trajectories
quantum invariants	topological amplitudes

TABLE 6.1

logical Hermitian product on the modular functor $V(Y)$ so that the representation of the mapping class group is unitary [**Tu**]. Therefore we can always choose a unitary realization of the F-symbols. It is shown in [**HH**] for the $\frac{1}{2}E_6$ theory that the F-matrices cannot be all real, hence the two hexagon axioms are independent. Strictly speaking, for physical application, we only need the recoupling rules to preserve probability, so anti-unitary transformations should also be allowed. We also need caution when interpreting tangles as anyon trajectories and quantum invariants as amplitudes. For example, suppose we create from the vacuum 1 a particle-antiparticle pair x, x^*, separate them, and then annihilate. Surely they will return to the vacuum. But on the other hand, its quantum dimension d_x is supposed to tell us the probability of going back to the vacuum. The point is that when we create a particle-antiparticle pair, we cannot be certain of their types. Therefore creating a particle-antiparticle pair is a probabilistic process. The probability of creating a particle-antiparticle pair of type a is given by d_a^2/D^2, where

d_a is the quantum dimension of a and D is the global quantum dimension of $\mathcal{C}$. Therefore the bigger the quantum dimension, the better the chance to be created given enough energy. In general, a tangle is an operator, therefore it does not have a well-defined amplitude without specifying initial and final states.

One of the most exciting predictions is that in $\nu = 5/2$ FQH liquids, a certain electric current quantity σ_{xx} in interferometric measurement is governed by the Jones polynomial at a 4th root of unity: $\sigma_{xx} \propto |t_1|^2 + |t_2|^2 + 2\mathrm{Re}\big(t_1^* t_2 e^{i\alpha} \langle\psi| M_n |\psi\rangle\big)$, where M_n is the Jones representation of a certain braid [**FNTW**]. More generally, if a FQH state exists at $\nu = 2 + \frac{k}{k+2}$, its non-abelian statistics are conjectured to be closely related to $\mathrm{SU}(2)_k$ [**RR**]. If so, then experimental data directly manifest Jones evaluations. For further applications to FQH liquids, see [**Bo**].

6.3.1. Particle types and fusion rules. To describe a system of anyons, we list the species of the anyons in the system, called the particle types, topological charges, superselection sectors, labels, and other names; we also specify the antiparticle type of each particle type. We will list the particle types as $\{i\}_{i=0}^{n-1}$, and use $\{x_i\}_{i=0}^{n-1}$ to denote a representative set of anyons, where the type of x_i is i.

In any anyonic system, we always have a trivial particle type denoted by 0, which represents the ground states of the system or the vacuum. In the list of particle types above, we assume $x_0 = 0$. The trivial particle is its own antiparticle. The antiparticle of x_i, denoted as x_i^*, is always of the type of another x_j. If x_i and x_i^* are of the same type, we say x_i is self-dual.

To have a nontrivial anyonic system, we need at least one more particle type besides 0. The Fibonacci anyonic system is such an anyonic system with only two particle types: the trivial type 0, and the nontrivial type τ. Anyons of type τ are called the Fibonacci anyons. They are self-dual: the antiparticle type of τ is also τ. We need to distinguish between anyons and their types. For Fibonacci anyons, this distinction is unnecessary, as for any TQFT with trivial Frobenius-Schur indicators.

Anyons can be combined in a process called fusion, which is tensoring two simple objects. Repeated fusions of the same two anyons do not necessarily result in anyons of the same type: the resulting anyons may be of several different types, each with a certain probability. In this sense we can also think of fusion as a measurement. It follows that given two anyons x, y of types i, j, the particle type of the fusion, denoted as $x \otimes y$, is in general not well-defined.

If fusion of an anyon x with any other anyon y (maybe x itself) is always well-defined, then x is called abelian. If neither x nor y is abelian, then there will be anyons of more than one type as the possible fusion results. We say such fusion has *multi-fusion channels* of x and y.

Given two anyons x, y, we write the fusion result as $x \otimes y \cong \bigoplus_i n_i x_i$, where $\{x_i\}$ is a representative set of isomorphism classes of simple objects, and each n_i is a nonnegative integer, called the multiplicity of the occurrence of anyon x_i. Multi-fusion channels correspond to $\sum_i n_i > 1$. Given an anyonic system with anyon representative set $\{x_i\}_{i=0}^{n-1}$, we have $i \otimes j = \bigoplus_{k=0}^{n-1} N_{ij}^k k$. The nonnegative integers N_{ij}^k are called the fusion rules of the anyonic system; the matrix N_i with (j,k)-entry N_{ij}^k is called the ith fusion matrix. If $N_{ij}^k \neq 0$, we say fusion of x_i and x_j to x_k is admissible.

Definition 6.2.

(1) *An anyon x_i is abelian, also called a simple current, if $\sum_k N_{ij}^k = 1$ for every j. Otherwise it is non-abelian.*
(2) *An anyon x_i such that $x_i^2 = 1$ is called a boson if $\theta_i = 1$, a fermion if $\theta_i = -1$, and a semion if $\theta_i = \pm i$.*

PROPOSITION 6.3.

(1) *The quantum dimension of an anyon x_i is the Perron-Frobenius eigenvalue of N_i.*
(2) *An anyon x_i is abelian iff $d_i = 1$.*

PROOF. An anyon is a simple object in a UMTC, so $d_i \geqslant 1$ [**Tu**]. But d_i is the Perron-Frobenius eigenvalue of the fusion matrix N_i. □

6.3.2. Many-anyon states and fusion tree bases. A defining feature of non-abelian anyons is the existence of multi-fusion channels. Suppose we have three anyons a, b, c localized in the plane and well-separated. We would like to know, when all three anyons are brought together to fuse, what kinds of anyons will this fusion result in? When anyons a and b are combined, we may see several anyons. Taking each resulting anyon and combining with c, we would have many possible outcomes. Hence the fusion result is not necessarily unique. Moreover, even if we fix the resulting outcome, there is an alternative arrangement of fusions given by fusing b and c first. For three or more anyons to be fused, there are many such arrangements, each represented graphically by a *fusion tree*.

FIGURE 6.3. Fusion trees.

A *fusion path* is a labeling of a fusion tree whereby each edge is labeled by a particle type, and the three labels around any trivalent vertex represent a fusion admissible by the fusion rules. The top edges are labeled by the anyons to be fused, drawn along a horizontal line; the bottom edge represents the fusion result, also called the total charge of the fused anyons.

In general, given n anyons in the plane localized at certain well-separated places, we will fix a total charge at the ∞ boundary. In theory any superposition of anyons is possible for the total charge, but it is physically reasonable to assume that such a superposition will decohere into a particular anyon if left alone. Let us arrange the n anyons along the real axis of the plane. When we fuse them consecutively, we have a fusion tree as in Fig. 6.4. In our convention, fusion trees go downward. If we want to interpret a fusion tree as a physical process in time, we should also introduce the Hermitian conjugate operator of fusion: splitting of anyons from one to two. Then as time goes upward, a fusion tree can be interpreted as a splitting of one anyon into many.

The ground state manifold of a multi-anyon system in the plane even when the positions of the anyons are fixed might be degenerate: there may be more

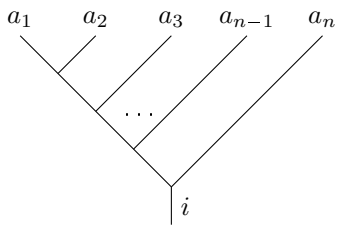


FIGURE 6.4. "Consecutive" fusion tree for anyons $a_1, \ldots, a_n$ with total charge i.

than one ground state. (In reality the energy differences between the different ground states go to 0 exponentially as the anyon separations go to infinity; we will ignore such considerations here, and always assume that anyons are well-separated until they are brought together for fusion.) Such degeneracy is necessary for non-abelian statistics. We claim that fusion paths over a fixed fusion tree represent an orthonormal basis of the degenerate ground state manifold when appropriately normalized.

The fusion tree basis of a multi-anyon system then leads to a combinatorial way to compute the degeneracy: count the number of labelings of the fusion tree, i.e., the number of fusion paths. For example, consider n τ-anyons in the plane with total charge τ, and denote the ground state degeneracy as F_n. Simple counting shows that $F_0 = 0$ and $F_1 = 1$; easy induction then gives $F_{n+1} = F_n + F_{n-1}$. This is exactly the Fibonacci sequence, hence the name of Fibonacci anyons.

6.3.3. F-matrices and pentagons. In the discussion of the fusion tree basis above, we fuse anyons one by one from left to right, e.g., the left fusion tree in Fig. 6.3. We may as well choose any other arrangement of fusions, e.g., the right fusion tree in Fig. 6.3. Given n anyons with a certain total charge, each arrangement of fusions is represented by a fusion tree, whose admissible labelings form a basis of the multi-anyon system.

The change from the left fusion tree to the right in Fig. 6.3 is called the F-move. Since both fusion tree bases describe the same degenerate ground state manifold of 3 anyons with a certain total charge, they should be related by a unitary transformation. The associated unitary matrix is called the F-matrix, denoted as F_d^{abc}, where a, b, c are the anyons to be fused, and d is the resulting anyon or total charge. (Complications from fusion coefficients $N_{ij}^k > 1$ are ignored.)

For more than 3 anyons, there are many more fusion trees. To have a consistent theory, a priori we must specify the change of basis matrices for any number of anyons in a consistent way. For instance, the leftmost and rightmost fusion trees of 4 anyons in Fig. 4.3 are related by two different sequences of applications of F-moves, whose consistency will be referred to as the pentagon. Mac Lane's coherence theorem [**Ma**] guarantees that pentagons suffice, i.e., imply all other consistencies. Note that pentagons are just polynomial equations in F-matrix entries.

To set up the pentagons, we need to explain the consistency of fusion tree bases for any number of anyons. Consider a decomposition of a fusion tree T into two fusion subtrees T_1, T_2 by cutting an edge e into two new edges, each still referred to as e. The fusion tree basis for T has a corresponding decomposition: if i's are the particle types of the theory, for each i we have a fusion tree basis for T_1, T_2 with

the edge e labeled by i. Then the fusion tree basis for T is the direct sum over all i of the tensor product: (the fusion tree basis of T_1) $\otimes$ (the fusion tree basis of T_2).

In the pentagons, an F-move is applied to part of the fusion tree in each step. The fusion tree decomposes into two pieces: the part where the F-move applies, and the remaining part. It follows that the fusion tree basis decomposes as a direct sum of several terms corresponding to admissible new labels.

Given a set of fusion rules N_{ij}^k, solving the pentagons turns out to be a difficult task (even with the help of computers). However, certain normalizations can be made to simplify the solutions. If one of the indices a, b, c of the F-matrix is the trivial type 0, we may assume $F_d^{abc} = 1$. We cannot do so in general if d is trivial.

EXAMPLE 6.4 (Fibonacci F-matrix). *Recall $\tau^2 = 1 \oplus \tau$. A priori there are only two potentially nontrivial F-matrices, which we will denote as*

$$F_1^{\tau\tau\tau} = t, \qquad F_\tau^{\tau\tau\tau} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

where $p, q, r, s, t \in \mathbb{C}$. There are many pentagons even for the Fibonacci fusion rules depending on the four anyons to be fused and their total charges: a priori $2^5 = 32$. But a pentagon is automatically trivial if one of the anyons to be fused is trivial, leaving only two pentagons to solve. Drawing fusion tree diagrams and keeping track of the various F-moves among ordered fusion tree bases, the pentagons become:

$$\begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix}^2 = F_\tau^{\tau\tau\tau} \begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix} F_\tau^{\tau\tau\tau}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & F_\tau^{\tau\tau\tau} \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & F_\tau^{\tau\tau\tau} \end{pmatrix} = \begin{pmatrix} p & 0 & q \\ 0 & t & 0 \\ r & 0 & s \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & F_\tau^{\tau\tau\tau} \end{pmatrix} \begin{pmatrix} p & 0 & q \\ 0 & t & 0 \\ r & 0 & s \end{pmatrix}$$

These matrix equations expand into thirteen polynomial equations over p, q, r, s, t, instances of the pentagon equation for 6j symbol systems (Defn. 4.7). Solving them and constraining the F-matrices to be unitary, we obtain

$$F_1^{\tau\tau\tau} = 1, \qquad F_\tau^{\tau\tau\tau} = \begin{pmatrix} \phi^{-1} & \overline{\xi}\phi^{-1/2} \\ \xi\phi^{-1/2} & -\phi^{-1} \end{pmatrix} \tag{6.5}$$

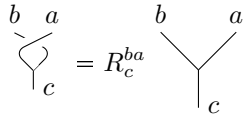
where $\phi = (\sqrt{5}+1)/2$ is the golden ratio and ξ is an arbitrary phase, w.l.o.g. $\xi = 1$.

6.3.4. R-matrix and hexagons. Given n anyons y_i in a surface S, well-separated at fixed locations p_i, the ground states $V(S; p_i, y_i)$ of this quantum system form a projective representation of the mapping class group of S punctured n times. If S is the disk, the mapping class group is the braid group. In a nice basis of $V(S; p_i, y_i)$, the braiding matrix R_{ij} becomes diagonal.

To describe braidings carefully, we introduce some conventions. When we exchange two anyons a, b in the plane, there are two different exchanges which are topologically inequivalent: their world lines are given by braids.

In our convention time goes upwards. We will refer to the left picture as the left-handed braiding R_{ab}^{-1} and the right picture as the right-handed braiding R_{ab}.

Let V_c^{ab} be the ground state manifold of two anyons of types a, b with total charge c. Let us assume each space V_c^{ab} is one-dimensional when (a, b, c) is admissible, and let e_c^{ab} be its fusion tree basis. When anyons a and b are braided by R_{ab}, the state e_c^{ab} in V_c^{ab} is changed into a state $R_{ab}e_c^{ab}$ in V_c^{ba}. Since both $R_{ab}e_c^{ab}$ and e_c^{ba} are non-zero vectors in a one-dimensional Hilbert space V_c^{ba}, they are equal up to a phase, denoted as R_c^{ba}, i.e, $R_{ab}e_c^{ab} = R_c^{ba}e_c^{ba}$.



Here R_c^{ba} is a phase, but in general it is a unitary matrix called an R-matrix. A matrix representing an arbitrary braiding of many anyons can be obtained from R- and F-matrices (and their inverses) via composition and tensoring with identity matrices. We should mention that in general $R_c^{ab} \neq (R_c^{ba})^{-1}$; their product involves twists of particles.

THEOREM 6.6.

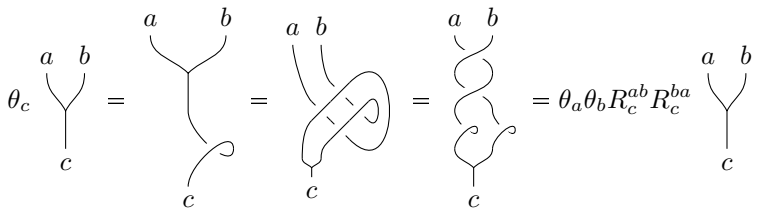
(1) For any particle types a, b, c,

$$R^{ab}R^{ba} = \theta_a^{-1}\theta_b^{-1}\theta_c \mathrm{id}\colon V_c^{ab} \circlearrowleft \qquad \text{if } N_c^{ab} \geqslant 1, \text{ whence}$$

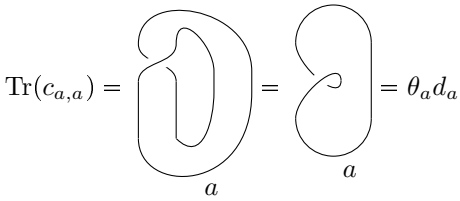
$$R_c^{ab}R_c^{ba} = \theta_a^{-1}\theta_b^{-1}\theta_c \qquad \text{if } N_c^{ab} = 1.$$

(2) Spin-statistics connection: $\mathrm{Tr}(c_{aa}) = \theta_a d_a$.

PROOF. For statement (1),



For statement (2),



□

Statement (1) above is called the suspender formula. The spin-statistics connection was pointed out to me by N. Read.

As we have seen before, anyons can be fused or split, so braidings should be compatible with fusion and splitting. For example, given two anyons c, d, we may first split d to a, b, then braid c with a and then with b, or we may braid c with d first, then split d into a, b. These two processes are physically equivalent, so their resulting matrices should be the same. Applying the two operators to the fusion

tree basis e_m^{cd}, we have an identity in pictures (Fig. 6.5). Both sides are threefold

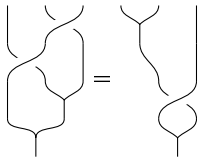


FIGURE 6.5. Right-handed hexagon.

compositions of F-moves and braidings. It follows that a certain product of six matrices equals the identity (Fig. 4.4). This equation is called a hexagon. There is another family of hexagons obtained by replacing all right-handed braidings with left-handed ones. In general, these two families of hexagons are independent of each other. The hexagons imply all other consistency equations for braidings.

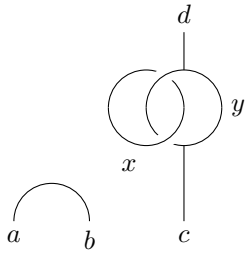
EXAMPLE 6.7 (Fibonacci braiding). *A priori there are eight right-handed Fibonacci hexagons. But braiding with the vacuum is trivial, i.e.,* $R_\tau^{\tau 1} = R_\tau^{1\tau} = R_1^{11} = 1$. *It follows that a hexagon is trivial if one of the three upper labels is trivial, leaving only two right-handed hexagons to solve:*

$$(R_\tau^{\tau\tau\tau})^2 = R_1^{\tau\tau}$$

$$\begin{pmatrix} R_1^{\tau\tau} & 0 \\ 0 & R_\tau^{\tau\tau} \end{pmatrix} F_\tau^{\tau\tau\tau} \begin{pmatrix} R_1^{\tau\tau} & 0 \\ 0 & R_\tau^{\tau\tau} \end{pmatrix} = F_\tau^{\tau\tau\tau} \begin{pmatrix} 1 & 0 \\ 0 & R_\tau^{\tau\tau} \end{pmatrix} F_\tau^{\tau\tau\tau}$$

These expand into five polynomial equations manifesting Defn. 4.13. Left-handed braidings are the same, but with inverted R-symbols. Using Eqn. (6.5)*, our ten-polynomial system boils down to* $R_1^{\tau\tau} = e^{4\pi i/5}$ *and* $R_\tau^{\tau\tau} = e^{-3\pi i/5}$.

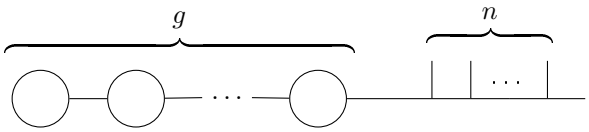
6.3.5. Morphisms as operators. Suppose anyons a, b, c on the x-axis undergo a process adiabatically as follows, from $t = 0$ to $t = 1$:



It is common to interpret the morphism in $\mathrm{Hom}(a \otimes b \otimes c, d)$ as particle trajectories. Then we may ask, what is the amplitude of this process? This question is not quite well-defined for non-abelian anyons because at time $t = 0$, the ground state is not unique. Hence we should instead ask for matrix elements because a morphism in $\mathrm{Hom}(a \otimes b \otimes c, d)$ is an operator.

Given two states at $t = 0$ and $t = 1$, how do we compute matrix elements? Supposing the anyonic system is given by a UMTC $\mathcal{C}$, such matrix elements are part of the operator invariant from $\mathcal{C}$. Then they can be computed by recoupling rules when statistics are given in fusion tree bases. More generally, if n anyons $x_1, \ldots, x_n$ are fixed at $p_1, \ldots, p_n$ on a genus g closed orientable surface Σ_g, the

ground state manifold has a generalized fusion graph basis obtained from labeling the following graph:



6.3.6. Measurement. Measurement is performed by fusing anyons. A particular outcome is given by a fusion graph. Hence the amplitude of measuring a certain outcome is just the matrix element for the initial state and outcome state.

6.4. Intrinsic entanglement

An interesting feature of the tensor product of vector spaces is that neither tensor factor is a canonical subspace of a tensor product. In quantum theory, the Hilbert space of a composite system is the tensor product of the Hilbert spaces of the constituent subsystems.

DEFINITION 6.8. *Consider a Hilbert space* $\mathbb{L} = \bigotimes_{i=1}^{n} \mathbb{L}_i$ *with a fixed tensor decomposition and* $n \geqslant 2$. *A vector* $v \in \mathbb{L}$ *is a product (or separable or decomposable) state if* v *can be written as* $v = \bigotimes_{i=1}^{n} v_i$, *where* $v_i \in \mathbb{L}_i$. *Otherwise* v *is entangled. Classical states are products.*

EXAMPLE 6.9. *The spin-singlet state* $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$ *is an entangled* 2*-qubit state.*

Any two vectors v, w in $\mathbb{C}^N$ span a parallelogram, degenerate iff $v \propto w$, whose area will be denoted as $A(v, w)$. Recall any $v \in (\mathbb{C}^2)^{\otimes n}$ is a linear combination $v = \sum v_I |I\rangle$. For each $1 \leqslant i \leqslant n$ and $x \in \{0, 1\}$, let $\partial_x^i \colon (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes(n-1)}$ be the linear map given by $|b_1 \cdots b_n\rangle \mapsto \delta_{x,b_i} |b_1 \cdots \hat{b}_i \cdots b_n\rangle$, where $\hat{}$ denotes deletion. What ∂_x^i does is identify $(\mathbb{C}^2)^{\otimes(n-1)}$ with the subspace of $(\mathbb{C}^2)^{\otimes n}$ spanned by all n-bit strings with ith bit x.

DEFINITION 6.10. *Given* $v \in (\mathbb{C}^2)^{\otimes n}$, *let* $E(v) = \sum_{i=0}^{n} A^2(\partial_0^i(v), \partial_1^i(v))$.

THEOREM 6.11.

(1) $0 \leqslant E(v) \leqslant n/4$.
(2) $E(v)$ *is invariant under local unitary transformations* $\mathrm{U}(2)^{\otimes n}$.
(3) $E(v) = 0$ *iff* v *is a product state.*

This theorem is from [**MW**].

Note that it takes exponentially many steps to compute $E(V)$ with respect to n. For $n = 9$, it attains a maximum value on $(|000\rangle + |111\rangle)^{\otimes 3}$, which shows some weakness of $E(V)$ as an entanglement measure.

Topological order is an exotic quantum order with nonlocal entanglement. Since topological ground state manifolds have no natural tensor decomposition, it is hard to quantify entanglement. In [**LW2, KP**], it was discovered that intrinsic entanglement of a topological order can be quantified by $\ln D$, where D is the positive global quantum dimension. Consider the ground state $|\psi\rangle$ on S^2, and a disk whose size is large relative to the correlation length. If the constituent degree of freedom is split along the disk, and the outside degree of freedom is traced out, we obtain a density matrix $\rho_L^{\mathrm{ins}}(|\psi\rangle)$. The von Neumann entropy $\rho \ln \rho$ of $\rho_L^{\mathrm{ins}}(|\psi\rangle)$ grows as

$\alpha L - \gamma + O(1/L)$ as $L \to \infty$. The linear coefficient α is not universal and dictated by local physics around the perimeter, but γ is universal.

THEOREM 6.12. *$\gamma = \ln D$ for a UMTC $\mathcal{C}$.*

It would be interesting to find a connection between $E(|\psi\rangle)$ with respect to a lattice realization and $\ln D$. It is possible that a topological ground state has maximal entanglement in any lattice realization.

CHAPTER 7

Topological Quantum Computers

In this chapter non-abelian anyons are used for quantum computing. Universality is explained for Fibonacci anyons. The approximation of Jones evaluations is seen to be just a special case of the approximation of general quantum invariants of links.

Computation by braiding non-abelian anyons is very robust against local errors. Each non-abelian anyon type leads to an anyonic quantum computer. Information is encoded in the collective states of many anyons of the same type at well-separated positions. The lack of continuous evolution due to $H \equiv 0$ naturally protects the encoded information, which is processed by braiding the anyons along prescribed paths. The computational outcome is encoded in the amplitude of this process, which is accessed by bringing anyons together and fusing them. The amplitude of the measurement after braiding is given by the quantum invariant of certain links. Hence anyonic quantum computers approximate quantum invariants of links. More elaborate schemes are based on topological change, e.g., measurement mid-computation or hybridization with nontopological gates. Such adaptive schemes are more powerful than braiding anyons alone.

7.1. Anyonic quantum computers

Every non-abelian anyon type gives rise to an anyonic model of quantum computing [**FKLW**]. Quantum gates are realized by the afforded representations of the braid groups. Topological quantum compiling is to realize, by braiding, unitary transformations desired for QCM algorithms such as Shor's factoring algorithm. Of particular interest are gates.

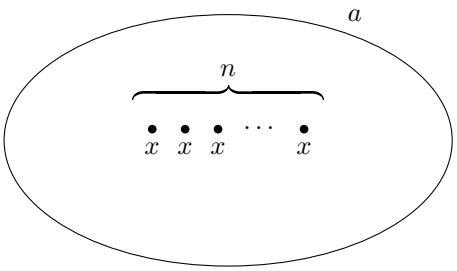
Abstractly, a quantum computer consists of

(1) A sequence of Hilbert spaces V_n whose dimensions are exponential in n. For each n, a state $|\psi_0\rangle$ to initialize the computation.
(2) A collection of unitary matrices in $\mathrm{U}(V_n)$ which can be effectively compiled classically.
(3) A readout scheme based on measurement of quantum states to give the answer.

It is not intrinsic for V_n to have a tensor decomposition, though desirable for certain architectures such as QCM. In TQC, tensor decomposition is unnecessary and inconvenient. Leakage error in TQC arises when a tensor decomposition is forced in order to to simulate QCM, because $\dim V_n$ is rarely a power of a fixed integer for all n. It would be interesting to find algorithms native to TQC beyond approximation of quantum invariants.

Consider a unitary RFC with a non-abelian anyon of type x. Following [**FLW1, FKLW**], we choose the computational subspace as

$V^a_{n,x} =$



Suppose $\Sigma_{g,a_1,\dots,a_l}$ is a genus g oriented surface with l boundary components labeled $a_1,\dots,a_l$. Then by the Verlinde formula,

$$\dim V(\Sigma_{g;a_1,\dots,a_l}) = \sum_{i\in L} s_{0i}^{\chi(\Sigma)} \prod_{j=1}^{l} s_{ia_j}$$

where the s_{ij} are S-matrix entries. It follows that

$$\dim V^a_{n,x} = D^{n-1} \sum_{i\in L} \frac{s_{ia}(s_{ix})^n}{d_i^{n-1}}$$

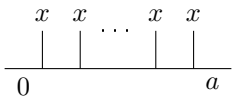
which is exponential in n since x is non-abelian. (We assume $s_{00} = 1/D > 0$.)

To simulate a traditional quantum circuit $U_L : (\mathbb{C}^2)^{\otimes n} \circlearrowleft$ we need to find a braid b making the square

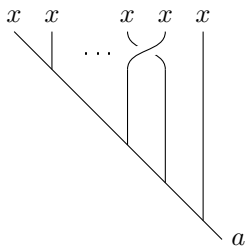
$$\begin{array}{ccc} (\mathbb{C}^2)^{\otimes n} & \xrightarrow{\iota} & V^a_{n,x} \\ {\scriptstyle U_L}\downarrow & & \downarrow{\scriptstyle \rho(b)} \\ (\mathbb{C}^2)^{\otimes n} & \xrightarrow[\iota]{} & V^a_{n,x} \end{array}$$

commute, where $\rho(b)$ is the braid matrix and ι is an embedding of the n-qubit space $(\mathbb{C}^2)^{\otimes n}$ into the ground states $V^a_{n,x}$. This is rarely achievable. Therefore we seek b making the square commute up to arbitrary precision. To achieve universality for quantum computation, we need to implement a universal gate set of unitary matrices. Then universality for anyonic quantum computing becomes the question: can we find braids b whose $\rho(b)$'s approximate a universal gate set efficiently to arbitrary precision? For non-abelian anyons, since the Hilbert spaces always grow exponentially, universality is guaranteed if the braid group representations afforded by the unitary RFC have a dense image in the special unitary groups $\mathrm{SU}(V^a_{n,x})$.

To have computational gates explicitly, we use the fusion tree basis for the Hilbert space $V^a_{n,x}$. The fusion tree basis is in one–one correspondence with admissible labelings of the internal edges of the graph



subject to the fusion rules at each trivalent vertex. The trivalent vertices also need to be indexed if the fusion rules are not multiplicity-free.

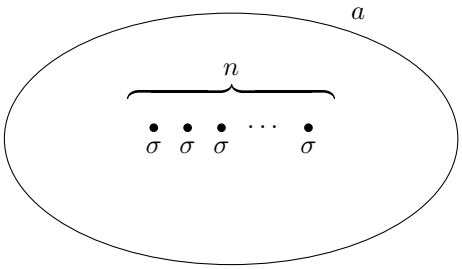


The braiding of two x anyons at positions $i, i+1$ in a fusion tree basis state is represented by stacking the braiding on top of the graph as above. The readout is by bringing anyons together and observing the resulting topological charges.

7.2. Ising quantum computer

There are three kinds of anyons in the Ising TQFT: $1, \sigma, \psi$. The only non-abelian anyon is the σ-particle: $\sigma^2 = 1 \oplus \psi$. The Ising theory is one of the rare happy coincidences where dimensions of multi-σ ground states are powers of 2. Specifically, let

$V_n^a =$

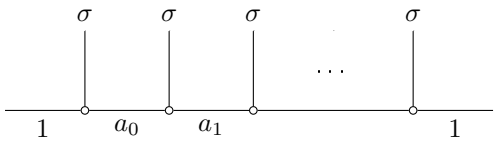


where $a = \sigma$ if n is odd, and $a = 1$ or $a = \psi$ if n is even. Then

$$\dim V_n^a = \begin{cases} 2^{\frac{n}{2}-1} & \text{for } n \text{ even,} \\ 2^{\frac{n-1}{2}} & \text{for } n \text{ odd.} \end{cases}$$

To design our quantum computer, we choose our computational space to be V_n^1, $n =$ even. An unnormalized basis is

$e_B^U =$



where $a_i = \sigma$ if i is even and $a_i = 1$ or $a_i = \psi$ if i is odd. Hence it is naturally identified with $(n/2 - 1)$ qubits. In this definition, we need 4 σ's for 1 qubit and 6 σ's for 2 qubits.

Quantum gates will be unitary matrices in the chosen basis $\{e_B^U\}$. As an abstract group, the image is known to be $\mathbb{Z}_2^{\frac{n}{2}-1} \rtimes S_n$ projectively [**FRW**]. Hence it is impossible to carry out universal quantum computation by braiding alone.

For one qubit, we let $|0\rangle = e_{1\sigma 1\sigma 1}$ and $|1\rangle = e_{1\sigma\psi\sigma 1}$. Then $\rho_4 \colon B_4 \to U(2)$ is given by

$$\rho(\sigma_1) = \rho(\sigma_3) = e^{-\pi i/8} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$
$$\rho(\sigma_2) = e^{-\pi i/8} \begin{pmatrix} \frac{1-i}{2} & \frac{1+i}{2} \\ \frac{1+i}{2} & \frac{1-i}{2} \end{pmatrix}$$

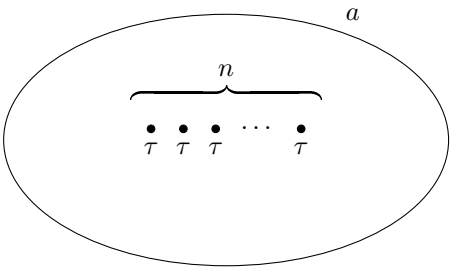
Interestingly $\rho(\sigma_2^2) = e^{-\pi i/4} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is the NOT gate up to an overall phase. For two qubits, if we let

$$|00\rangle = e_{1\sigma 1\sigma 1\sigma 1} \qquad |01\rangle = e_{1\sigma\psi\sigma 1\sigma 1}$$
$$|10\rangle = e_{1\sigma 1\sigma\psi\sigma 1} \qquad |11\rangle = e_{1\sigma\psi\sigma\psi\sigma 1}$$

then $\rho(\sigma_3^{-1}\sigma_4\sigma_3\sigma_1\sigma_5\sigma_4\sigma_3^{-1}) = \text{CNOT}$ up to an overall phase. The Ising computer realizes many Clifford gates exactly, and approximates the Jones polynomial of links at fourth roots of unity.

7.3. Fibonacci quantum computer

There are only two types of anyons in the Fibonacci theory, 1 and τ, and τ is non-abelian: $\tau^2 = 1 \oplus \tau$. Fibonacci theory is the simplest TQFT supporting a braiding-universal TQC, which is very desirable, but we are less confident that τ exists than the Ising σ anyon. Let

$V_n^a =$ 

Then

$$\dim V_n^a = \begin{cases} F_{n-2} & \text{if } a = 1 \\ F_{n-1} & \text{if } a = \tau \end{cases}$$

where F_n is the nth Fibonacci number and $F_{-1} = 0$, whence the name Fibonacci.

The leakage issue arises because the Fibonacci numbers are not all powers of a particular integer, hence there is no natural tensor decomposition of the computational spaces. Simulating QCM requires choosing a computational subspace, leading to leakage. But for TQC, V_n^1 is our computational space, so there is no need to choose a subspace, and hence no leakage.

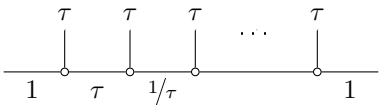
For one qubit, we choose V_4^1 and $|0\rangle = e_{1\tau 1\tau 1}$, $|1\rangle = e_{1\tau\tau\tau 1}$. Then

$$\rho(\sigma_1) = \begin{pmatrix} e^{-4\pi i/5} & 0 \\ 0 & e^{3\pi i/5} \end{pmatrix} \qquad \rho(\sigma_2) = \begin{pmatrix} \phi^{-1}e^{4\pi i/5} & \phi^{-1/2}e^{-3\pi i/5} \\ \phi^{-1/2}e^{-3\pi i/5} & -\phi^{-1} \end{pmatrix}$$

where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio. For n qubits, we choose V_{2n+2}^1 and encode a bit string $i_1 \cdots i_n$ as $e_{1\tau a_{i_1} \tau a_{i_2} \cdots \tau 1}$, where $a_0 = 1$ and $a_1 = \tau$.

THEOREM 7.1. *For any quantum circuit* $U_L\colon (\mathbb{C}^2)^{\otimes n} \circlearrowleft$ *in* $\mathrm{SU}(2^n)$ *and* $\delta > 0$, *there exists a braid* $\sigma \in B_{2n+2}$ *such that* $|\rho(\sigma) - U_L| < \delta$, *and* σ *can be constructed by a Turing machine in time* $\mathrm{poly}(n, 1/\delta)$.

This is a combination of a density result [**FLW1, FLW2**] and the Kitaev-Solovay algorithm. Our design here uses six τ anyons to implement a 2-qubit gate on a 4-dimensional subspace of $V_6^1 \cong \mathbb{C}^5$. Leakage arises when we implement 2-qubit gates on different 2-qubit subspaces. Suppose we want to implement two CNOT gates on V_8^1. Our computational space is spanned by



which is a subspace of $V_8^1 \cong \mathbb{C}^8$. If the first CNOT is on the last six τ anyons, there is a possibility of encoded information in V_6^1 leaking into $V_6^\tau \cong \mathbb{C}^8$. The leakage can be fixed using a stronger density result: the Jones representation is not only dense for each irreducible sector, but also independently dense for all irreducible sectors. Thus we can approximate any pair $(A, B) \subset SU(5) \times SU(8)$ in the representation $V_6^1 \oplus V_6^\tau$. To avoid leakage, we choose a braid implementing $\mathrm{CNOT} \oplus \mathrm{id}$. If we fuse all anyons, the outcome is some colored Jones evaluation. As a variation, if we fuse only the first pair, the outcome is given by the Jones polynomial at some root of unity of a certain link [**FKLW, BFLW**].

7.4. Universality of anyonic quantum computers

A quantum computer is universal if it can simulate any program on another quantum computer, i.e., any given initial state $|\psi_i\rangle$ can be rotated arbitrarily close to any other prescribed state $|\psi_f\rangle$ by applying unitary matrices in polynomial time. Therefore universality of TQC is whether or not the representations of the braid groups B_n are projectively dense.

7.4.1. Universality conjecture. Given a unitary RFC, are there anyons whose braidings are universal for QC?

CONJECTURE 7.2. *If* $D^2 \notin \mathbb{N}$, *then there exists a non-abelian anyon type whose anyonic quantum computer is universal by braiding alone.*

This conjecture is from [**NR**].

7.4.2. N-eigenvalue problem. Given a particular anyon type x, we analyze the braid group representation as follows:

(1) Is the braid representation $V_{n,x}^a$ irreducible for all n? This turns out to be a very difficult question in general. If reducible, we must decompose it into irreps.
(2) The number of distinct eigenvalues of the braiding $c_{x,x}$ is bounded by $\sum_{i \in L} (N_{x,x}^i)^2$. Since all braid generators are mutually conjugate, the closed image $\rho_{n,x,a}(B_n)$ in $\mathrm{U}(V_{n,x}^a)$ is generated by a single conjugacy class.

DEFINITION 7.3. *Let* $N \in \mathbb{Z}_+$. *We say a pair* (G, V), G *a compact Lie group,* V *a faithful irrep of* G, *has the* N*-eigenvalue property if there exists an element* $g \in G$ *such that the conjugacy class of* g *generates* G *topologically and the spectrum* X *of*

$\rho(g)$ has N elements and satisfies the no-cycle property: $u\{1,\xi,\xi^2,\dots,\xi^{n-1}\}\not\subset X$ for any nth root of unity ξ, $n\geqslant 2$, and all $u\in\mathbb{C}^\times$.

The N-eigenvalue problem is to classify all pairs with the N-eigenvalue property. For $N=2,3$, this is completed in [**FLW2**] and [**LRW**]. As a direct corollary, we have

THEOREM 7.4. *Suppose $r\neq 1,2,3,4,6$.*

(1) Given $n\geqslant 4$ if $r=10$, the Jones representation's closed image $\supset \mathrm{SU}(V^a_{n,1})$.
(2) Given $n\geqslant 4$ if $r\geqslant 10$, the anyonic quantum computers based on the Jones representation are universal.

7.5. Topological quantum compiling

Quantum compiling is, at the moment, a black art with unitary matrices. Several aspects of topological quantum compiling are:

(1) Implement interesting gates in QCM within TQC.
(2) Solve interesting-number theoretic questions within TQC.
(3) What is the computational power of certain braid gates such as representations of $(\sigma_1\cdots\sigma_{n-1})$? Since $(\sigma_1\cdots\sigma_{n-1})^n$ is in the center of B_n, it is a scalar matrix on each sector. Hence $(\sigma_1\cdots\sigma_{n-1})$ is like a Hadamard gate.

Specific braiding patterns (compilations) have been produced for Fibonacci anyons [**BHZS, BXMW**] and for general $\mathrm{SU}(2)_k$ anyons [**HBS**].

7.6. Approximation of quantum invariants

There are no difficulties in extending the approximation of the Jones evaluation to any other quantum invariant. Physically, the Jones evaluation is just the amplitude of some trajectory of anyons in an anyonic system. The same approximation works for any anyon in any theory.

In [**FKW**], it is shown that an efficient simulation also exists for mapping class groups. It follows that there are efficient algorithms for approximating 3-manifold invariants. As a comparison, we mention exact computation of 3-manifold invariants and approximation of colored link invariants in arbitrary 3-manifolds.

THEOREM 7.5.

(1) If a 3-manifold M is presented as a framed link L, then computing the Reshetikhin-Turaev invariant $\tau_4(M)$ at a fourth root of unity is #P-hard.
(2) Approximating the Turaev-Viro invariant at a fourth root of unity for a pair (M,L), where L is a colored link in M, is BQP-complete.

Statement (1) is from [**KM2**], and (2) is from [**BrK**].

It is interesting that the images of the Reshetikhin-Turaev representations of mapping class groups at fourth roots of unity are all finite.

THEOREM 7.6. *There is a short exact sequence*

$$1\longrightarrow \rho_4^{\mathrm{RT}}(D_g)\longrightarrow \rho_4^{\mathrm{RT}}(\mathcal{M}_g)\longrightarrow \mathrm{Sp}(2g,\mathbb{Z}_2)\longrightarrow 1$$

where $\rho_4(D_g)$ is a subgroup of $\mathbb{Z}_8^N$ for some N, and D_g is the subgroup of $\mathcal{M}_g$ generated by all squares of Dehn twists on simple closed curves. Note D_g is also the subgroup of $\mathcal{M}_g$ which acts trivially on $H_1(\Sigma_g;\mathbb{Z}_2)$.

7.7. Adaptive and measurement-only TQC

The most promising non-abelian anyon is the Ising σ anyon in $\nu = 5/2$ FQH liquids. Can we achieve universal TQC with σ? The idea is to supplement the error-free unitary gates by braiding σ with nontopological gates. The protocol is worked out in [**Brav, FNW**]. Braiding anyons is a difficult task experimentally, and for the moment, interferometric measurement is more realistic. Happily, braidings can be simulated by interferometric measurements. Therefore measurement-only (MO) universal TQC is also possible [**BFN**].

CHAPTER 8

Topological phases of matter

This chapter covers mathematical models of topological phases of matter: Levin-Wen models for quantum doubles, and wave functions for FQH liquids. In the end, we briefly discuss the inherent fault-tolerance of topological quantum computers.

Since the discovery of the fractional quantum Hall effect(s), a new mathematical framework to describe topological phases has become necessary. FQH liquids have been modeled with wave functions, quantum Chern-Simons theory, CFT/TQFT/MTC, and others. Each approach yields insights into these new phases. While it is not the right moment to coin a definition of topological phases of matter, several working definitions have been proposed: through code-subspace properties, gapped Hamiltonians. We will use the lattice version of gapped Hamiltonian here.

A topological phase of matter is a state of matter whose low-energy effective theory is a TQFT. There are two kinds of (2+1)-TQFTs which are well-studied: quantum doubles, or Drinfeld centers, and Chern-Simons theories. Quantum doubles are well-understood theoretically, as exemplified by Kitaev's toric code model, but their physical relevance is unclear at the moment. Chern-Simons theories are the opposite: their physical relevance to FQH liquids is established, while their Hamiltonian formulation on lattices is a challenge. Quite likely a Hamiltonian formulation does not exist, in the sense of a Hamiltonian for an underlying physical system, such as electrons in FQH liquids rather than TQFTs. Our physical system lives on a compact oriented surface Y, possibly with boundary. We will consider only closed Y, i.e., no anyons present. If there are anyons, i.e., Y has punctures and boundary, then boundary conditions are necessary.

8.1. Doubled quantum liquids

8.1.1. Toric code. A lattice is an embedded graph $\Gamma \subset Y$ whose complementary regions are all topological disks. In physics, vertices of Γ are called sites; edges, bonds or links; and faces, plaquettes.

DEFINITION 8.1. *Given an integer $l > 1$, to each lattice $\Gamma \subset Y$ we associate the Hilbert space $L_{\Gamma,l} = \bigotimes_{\text{edges}} \mathbb{C}^l$ with the standard inner product.*

(1) A Hamiltonian schema (HS) is a set of rules to write down a Hermitian operator H_Γ on $L_{\Gamma,l}$ for each $\Gamma \subset Y$.

(2) A HS is k-local if there exists a constant k such that H_Γ is a sum of Hermitian operators O_k of the form $\mathrm{id} \otimes A \otimes \mathrm{id}$, where A acts on at most k factors of $L_{\Gamma,l}$. We will call a local HS a quantum theory.

EXAMPLE 8.2 (The toric code schema). *In the celebrated toric code, $l = 2$. Let $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ be the Pauli matrices. For each vertex v, define an operator A_v on $L_\Gamma = \bigotimes_{\text{edges}} \mathbb{C}^2$, as a tensor product of σ_z's and identities: A_v acts*

on a qubit $\mathbb{C}^2$ *as* σ_z *if the edge corresponding to* $\mathbb{C}^2$ *touches* v*, and as* $\mathrm{id}_{\mathbb{C}^2}$ *otherwise. Similarly, define a plaquette term* B_p *for each face* p*, as a tensor product of* σ_x*'s and identities:* B_p *acts on a qubit* $\mathbb{C}^2$ *by* σ_x *if the edge corresponding to* $\mathbb{C}^2$ *touches* p*, and as* $\mathrm{id}_{\mathbb{C}^2}$ *otherwise. We normalize the smallest eigenvalue (= lowest energy) to zero. Hence the toric code Hamiltonian is*

$$H = \sum_{\substack{\text{vertices}\\ v}} \frac{I - A_v}{2} + \sum_{\substack{\text{faces}\\ p}} \frac{I - B_p}{2}$$

If our lattices are arbitrary, the toric code Hamiltonian is not k-local for any k because vertex valences in a graph can be arbitrarily large. In condensed matter physics, lattices describe particles such as atoms, and hence are not arbitrary. Therefore it is reasonable, maybe even necessary, to restrict our discussion of HS's to certain types of lattices. In the toric code case, on the torus, we restrict to square lattices. In general, we can restrict to any family of lattices with bounded valence of both the original lattice Γ and its dual $\hat{\Gamma}$. Then the toric code is a local HS, e.g., 4-local for square lattices on T^2. Given a Hamiltonian H_Γ, we denote by $V_0(\Gamma, Y)$ the ground state manifold.

Definition 8.3.

(1) *A HS for a class of lattices is topological if there exists a modular functor* V *such that for any lattice* $\Gamma \subset Y$ *in the class,* $V_0(\Gamma, Y) \cong V(Y)$ *naturally.*
(2) *A modular functor* V *is realized by a HS if there exists a local HS for a class of lattices* $\{\Gamma_i\}$ *such that* $V_0(\Gamma_i, Y) \cong V(Y)$ *naturally, and as* $i \to \infty$*, the number of vertices in* Γ_i *is unbounded.*
(3) *If the eigenvalues of a Hamiltonian* H *are ordered as* $\lambda_0 < \lambda_1 < \cdots$*, then* $\lambda_1 - \lambda_0$ *is the energy difference of the first excited states and the ground states. A Hamiltonian schema is gapped if* $\lambda_1 - \lambda_0 \geqslant c$ *for some constant* $c > 0$ *as the system size measured by the number of vertices goes to* ∞*.*

The existence of a local Hamiltonian realization of a modular functor V tells us theoretically how V will emerge from local degrees of freedom in the low-energy limit. Given a HS, our goal is to understand the ground states. The best-understood cases are the so-called content Hamiltonians: all local terms commute with each other: $H = \sum_i H_i$, $[H_i, H_j] = 0$. The toric code Hamiltonians are content. Frustrated Hamiltonians are extremely hard to solve mathematically, i.e., to find their ground states.

Theorem 8.4. *Let* H *be the toric code Hamiltonian on a lattice* Γ *in a closed surface* Y*, not necessarily orientable. Then*

(1) *Any two terms of* H *(i.e., elements of* $\{A_v\} \cup \{B_p\}$*) commute.*
(2) $V_0(\Gamma, Y) \cong \mathbb{C}[H_1(Y; \mathbb{Z}_2)]$ *naturally.*
(3) $\lambda_1 - \lambda_0 = 2$.
(4) $V_0(\Gamma, Y) \subset L_\Gamma$ *is an error-correcting code.*
(5) *The toric code HS realizes the quantum double of* $\mathbb{Z}_2$.

Proof ideas.

(1) $A_v, A_{v'}$ and $B_p, B_{p'}$ commute since they consist of the same matrices. If v does not touch p, then A_v, B_p commute since σ_x, σ_z act on different qubits. If v touches p, then A_v acts on two qubits corresponding to edges in ∂p. Then A_v, B_p commute since σ_x, σ_z anticommute.

(2) A basis of L_Γ can be identified as $\mathbb{Z}_2$-chains on Γ. On this basis, A_v enforces the cycle condition while B_p enforces a homologous operation.
(3) The eigenvalues of σ_x, σ_z are both ± 1, and all local terms are simultaneously diagonalizable.
(4) The minimal violation of local constraint is 2.
(5) See [**Ki1**].

□

These properties of the toric code Hamiltonians are signatures of our Hamiltonian formulation of topological phases of matter. Though probably too restrictive, we will see in the next section that a large class of examples exists. Elementary excitations in toric codes can also be analyzed explicitly. They are found to be mutual anyons, though abelian. So all data of the quantum double TQFT can be derived.

8.1.2. Levin-Wen model. The Levin-Wen model generalizes the toric code. It is an explicit Hamiltonian formulation of Turaev-Viro TQFTs. As input, it takes a spherical tensor category $\mathcal{C}$. For example, there are two natural spherical tensor categories associated to a finite group G:

(1) The group category, with simple objects elements of G, and trivial F-matrices.
(2) The representation category of G, with simple objects irreducible representations of G.

These two categories are monoidally inequivalent. For example, if $G = S_3$, the symmetric group of order 6, then the group category has rank 6, while its representation category has rank 3. Either can be input to the Levin-Wen model, and the resulting TQFT is the same: either quantum double is a rank 8 MTC.

For the Levin-Wen model, we consider only trivalent graphs Γ in a surface Y. For k-locality, we need to fix the maximum number of edges on a face. In physics, we consider mostly the honeycomb lattice, possibly with some variations. Trivalent graphs are dual to triangulations. Let Δ be a triangulation of a closed surface Y and Γ_Δ be its dual triangulation: vertices are centers of the triangles in Δ, and two vertices are connected by an edge iff the corresponding triangles of Δ share an edge. The dual triangulation Γ_Δ of Δ is a cellulation of Y whose 1-skeleton is a trivalent graph. It is well-known that any two triangulations of Y are related by a finite sequence of two moves and their inverses: the subdivision of a triangle into three new triangles, and the diagonal flip of two triangles sharing an edge. Dualizing the triangulations into cellulations, the two moves become the inflation of a vertex to a triangle and the F move.

The action of the mapping class group can be implemented as follows: consider the moduli space of all triangulations of Y, where two triangulations are equivalent if their dual graphs Γ_Δ are isomorphic as abstract graphs. By a sequence of diagonal flips, we can realize a Dehn twist. Each diagonal flip is a dual F move; their composition is the unitary transformation associated to the Dehn twist.

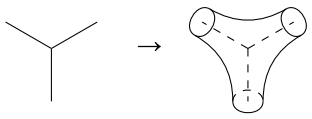
Conjecture 8.5.

(1) Every doubled UMTC $\mathcal{C}$ can be realized as a topological quantum liquid.
(2) If a UMTC is realized by a content HS, then $c_{\text{top}} = 0 \mod 8$.

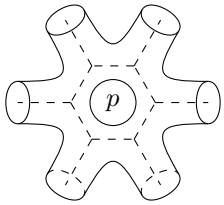
Like the toric code, the Levin-Wen Hamiltonian has two kinds of local terms: of vertex type and plaquette type. To each edge we assign a Hilbert space $\mathbb{C}^l$, where l is the rank of the input spherical category $\mathcal{C}$; for a graph Γ, we have $L_\Gamma = \bigotimes_{\text{edges}} \mathbb{C}^l$. A natural basis is all edge-labelings of Γ by labels. For simplicity, assume $\mathcal{C}$ is multiplicity-free. The Hamiltonian will then be written as

$$H = J_1 \sum_v (I - A_v) + J_2 \sum_p (I - B_p).$$

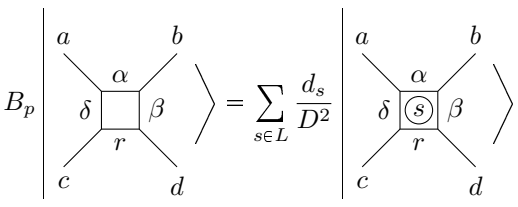
It suffices to define A_v on each basis vector. Given an edge-labeling e_l of Γ, around v there are three labels a, b, c. If (a, b, c) is admissible by the fusion rules, then $A_v|e_l\rangle = |e_l\rangle$, else $A_v|e_l\rangle = 0$. The term B_p is complicated in 6j symbols, but simple to derive and explain when $\mathcal{C}$ is modular, yielding the same general formula. For $\mathcal{C}$ modular, thicken Γ to a solid handlebody N_Γ:



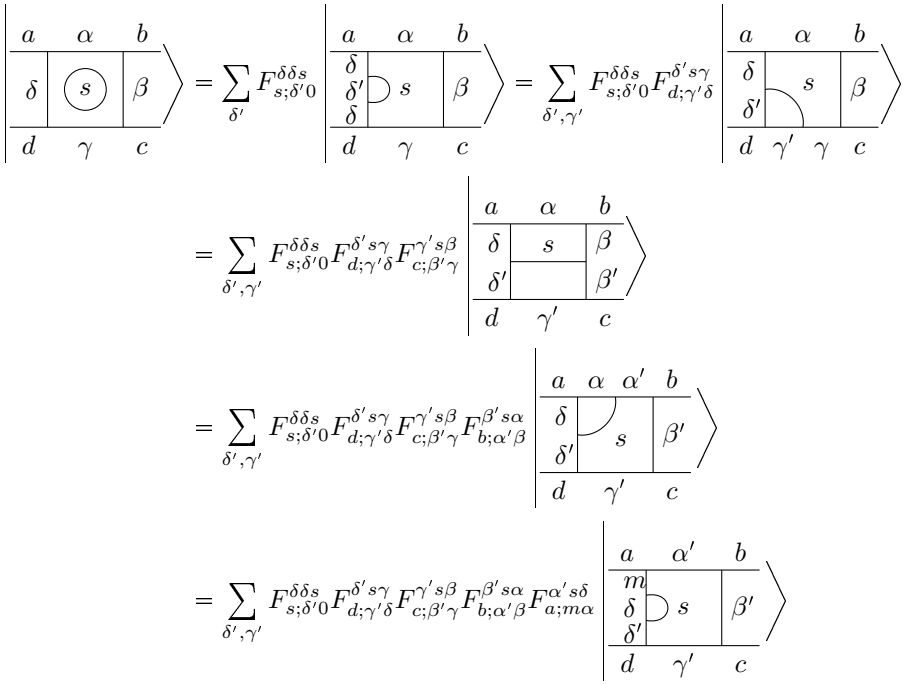
The boundary ∂N_Γ is a new surface S_Γ, to which $\mathcal{C}$'s TQFT assigns a vector space $V_{\mathcal{C}}(S_\Gamma)$, isomorphic to the subspace of L_Γ spanned by all ground states with vertex terms enforced, i.e. all admissible edge-labelings. A plaquette p in Y intersects S_Γ in a circle:



Zero total flux through p is enforceable with the S-matrix: each row corresponds to a label c, to which the formal combination $w_c = D^{-2} \sum_a \tilde{s}_{c,a} a$ projects the flux. The Levin-Wen plaquette term B_p is just the projection enforcing trivial flux through p. An explicit formula is straightforward, but complicated. Here is the procedure for a square:



The s-loop insertion is performable by sequential F-moves:



Proposition 1.19(7) then yields the final expression:

$$B_p \left| \begin{array}{ccc} a & \alpha & b \\ \delta & & \beta \\ d & \gamma & c \end{array} \right\rangle = \sum_{\alpha',\beta'\gamma',\delta',s} \frac{d_s}{D^2} F^{\delta' s\gamma}_{d;\gamma'\delta} F^{\gamma' s\beta}_{c;\beta'\gamma} F^{\beta' s\alpha}_{b;\alpha'\beta} F^{\alpha' s\delta}_{a;\delta'\alpha} \left| \begin{array}{ccc} a & \alpha' & b \\ \delta' & & \beta' \\ d & \gamma' & c \end{array} \right\rangle \tag{8.6}$$

While the general conclusion is clear—everything should be parallel to the toric code—the detailed mathematical analysis is much harder and not yet complete.

If $\mathcal{C}$ is not multiplicity-free, each vertex of Γ must be labeled by an orthonormal basis of the fusion space. More complicated is how to normalize the 6j symbols so that the Levin-Wen Hamiltonian H is Hermitian. For this we assume $\mathcal{C}$ is unitary. Since unitarity implies sphericity, we need only assume $\mathcal{C}$ is a unitary fusion category. The sufficient normalization conditions in [**LW1**], improved in [**H**], are unachievable in general.

The most interesting example is probably when $\mathcal{C}$ is the Fibonacci theory. Then the Levin-Wen model is a qubit model. On a torus, the ground state degeneracy is fourfold, like the toric code. But the double-Fibonacci braiding is much richer: it is universal for quantum computation.

8.1.3. DFib and the golden identity. Given a trivalent graph G on the sphere, the amplitude $\langle G\rangle_{\mathrm{DFib}}$ is the evaluation of G using Fibonacci F-matrices. It differs from the Yamada polynomial of G by a factor of $\phi^{\frac{5}{4}V(G)}$. Tutte discovered the following golden identity for the chromatic polynomial:

$$\phi^{3V(G)-10}(\phi+2)\chi_G^2(\phi+1) = \chi_G(\phi+2).$$

THEOREM 8.7 ([**FFNWW**]). $\langle G\rangle^2_{\mathrm{DFib}} = \frac{1}{\phi+2}\chi_{\hat{G}}(\phi+2)$.

8.1.4. DYL. The Fibonacci theory has a Galois conjugate, the Yang-Lee theory. This is a rank=2 MTC with the same fusion rule, but nonunitary. In particular, the quantum dimension of τ is $d = \frac{1-\sqrt{5}}{2}$. Using $F = \left(\begin{smallmatrix} d-1 & 1+d \\ 2d-3 & 1-d \end{smallmatrix}\right)$ and Eqn. (8.6), we can still define a Levin-Wen model for DYL, but the plaquette term is no longer Hermitian. There are various ways to make the resulting Hamiltonian Hermitian, but all are gapless [**Fr3**]. It will be interesting to know if this gapless system is a critical phase. Generally, is a Hermitian version of the Levin-Wen model of a nonunitary theory always gapless?

8.2. Chiral quantum liquids

Models of FQH liquids are the other extreme of topological phases of matter: maximally chiral in the sense that they are as far as possible from quantum doubles. In Chap. 6, we saw that a defining feature of FQH states is a plateau at certain filling fractions. Each plateau is in some topological state, though a filling fraction alone cannot uniquely determine the state. An interesting question is how to model the electron liquid at a plateau. The electrons at a plateau are doing their own collective dance. Unfortunately their quantum world is well-separated from our classical world. We can only imagine what is happening in an electron dance. Significant insight has been derived from wave functions which describe the electron liquid. For $\nu = 1/3$, an answer is given by Laughlin. For N electrons in the positions $z_1, \dots, z_N$, their distribution is given by the (unnormalized) wave function without the Gaussian factor

$$\psi(z_1, \dots, z_N) = \prod_{i<j} (z_i - z_j)^3$$

Using this formula, we can deduce the following rules:

(1) Electrons avoid each other as much as possible.
(2) Every electron is in its own constant cyclotron motion.
(3) Each electron takes three steps to go around another electron.

The first rule is due to Fermi statistics, encoded in ψ by the vanishing of ψ when $z_i = z_j$. The second follows from Landau's solution of a single electron in a magnetic field. The third is encoded in the exponent of the Laughlin wave function. These strict rules force the electrons to organize themselves into a nonlocal, internal, dynamical pattern—topological order. While $\nu = 1/3$ is a topological state of matter, it supports only abelian anyons. Therefore it is not very useful for TQC. A more interesting plateau is $\nu = 5/2$. It is believed, with less confidence than $\nu = 1/3$, to be modeled by the Pfaffian wave function in the so-called Moore-Read (MR) state. The MR state supports non-abelian anyons. Its bosonic version is modeled by the Jones-Kauffman TQFT for $A = \pm ie^{\pm 2\pi i/16}$—the Ising TQFT. Unfortunately, the braiding of the non-abelian anyons is not complicated enough to be universal for QC. The Pfaffian wave function is defined as follows. Recall that given a $2n \times 2n$ skew-symmetric matrix $A = (a_{ij})_{1 \leqslant i,j \leqslant 2n}$, up to an overall factor $\mathrm{Pf}(A) = \mathrm{Pf}(a_{ij})$ is defined to be the scalar in front of $dx^1 \wedge \cdots \wedge dx^{2n}$ in ω_A^n (we form a 2-form $\omega_A = \sum_{i<j} a_{ij} dx^i \wedge dx^j$). Then for $2n$ electrons at $z_1, \dots, z_{2n}$, the Pfaffian wave function is

$$\mathrm{Pf}\left(\frac{1}{z_i - z_j}\right) \prod_{i<j} (z_i - z_j)^2$$

We will continue to drop the Gaussian factor. An important difference between the Pfaffian and Laughlin is that the Pfaffian has off-particle zeros: fixing all but one variable, say z_1, then as a polynomial of z_1, the zeros are not all of the form $z_1 = z_j$ for some j.

8.2.1. Pattern of zeros in wave functions. It is not obvious that the Pfaffian is related to a TQFT. We will explain this connection in the next two subsections.

It is an elementary fact that any nonconstant antisymmetric polynomial in $z_1, \dots, z_N$ is divisible by $\prod_{i<j}(z_i - z_j)$. Since we will be studying only polynomials, we will focus on symmetric rather than antisymmetric ones. Summarizing, we will consider nonconstant wave functions with the following properties:

- Chirality: the wave function $\psi(z_1, \dots, z_N)$ is a polynomial.
- Statistics: $\psi(z_1, \dots, z_N)$ is fully symmetric in z_i.
- Translation invariance: $\psi(z_1 + c, \dots, z_N + c) = \psi(z_1, \dots, z_N)$ for any constant c.
- Filling fractions: for physical relevance, we need to consider the limit when $N \to \infty$ through a sequences of integers. So we study a sequence of polynomials $\{\psi(z_1, \dots, z_N)\}$. For a fixed variable z_i, the maximal degree N_ϕ of z_i has a physical interpretation as the flux quantum number. We assume $\lim_{N\to\infty} {}^{N}/_{N_\phi}$ exists and is a rational number ν, called the filling fraction.

Now the idea is as follows. Two electrons repel each other, so the amplitude of their coincidence should be zero (we ignore spin since electrons in a FQH liquid are believed to be spin polarized along the magnetic field, and numerically the spin polarized case is energetically more favorable, as pointed out to me by X. Wan). Since our wave function is divided by $\prod_{i<j}(z_i - z_j)$, this is not strictly true. When $\psi(z_1, \dots, z_N) \neq 0$ at $z_i = z_j$, we say $\psi(z_1, \dots, z_N)$ vanishes at 0th order. If we bring a electrons together, i.e., let $z_1, \dots, z_a$ approach a common value, what is the order of the vanishing of the wave function? We denote it by S_a. These vanishing powers $\{S_a\}_{a=1,2,,\dots,\infty}$ should be consistent to represent the same local physics of a topological phase, and encode many topological properties of the FQH liquid. More precisely:

DEFINITION 8.8. *Let $\psi(z_1, \dots, z_N) = \sum_I c_I z^I$ for a sequence of integers $N \to \infty$, where $I = (i_1, \dots, i_N)$. Then*

$$S_a = \min_I \sum_{j=1}^{a} i_j \quad \text{for } a < N.$$

This sequence of integers will be called the pattern of zeros.

For the bosonic Laughlin $\prod_{i<j}(z_i - z_j)^2$, $\nu = 1/2$ and $S_a = \frac{a(a-1)}{2}$, the triangular numbers. For the bosonic Pfaffian $\mathrm{Pf}\left(\frac{1}{z_i - z_j}\right) \prod_{i<j}(z_i - z_j)$, $\nu = 1$ and $S_a = \frac{a(a-1)}{2} - \lfloor a/2 \rfloor$. Our program for classifying FQH states is:

- Find necessary and sufficient conditions for a pattern of zeros
  - to be realized by polynomials.
  - to represent a topological state.
- If it were a topological state, which one?

- Are there non-abelian anyons in the state? If so, are their braidings universal for TQC?

THEOREM 8.9. *If a pattern of zeros $\{S_a\}$ is realized by wave functions satisfying the so-called unique-fusion and and n-cluster conditions, then the sequence $\{S_a\}$ is determined by $\{S_1, \dots, S_n\}$ and $m = S_{n+1} - S_n$. Moreover,*

- $S_1 = 0$.
- $S_{a+kn} = S_a + kS_n + \frac{k}{2}(k-1)mn + kma$.
- S_{2a} *and* mn *are even.*
- $2S_n = 0 \mod n$.
- $\Delta_2(a,b) = S_{a+b} - S_a - S_b \geqslant 0$.
- $\Delta_3(a,b,c) = S_{a+b+c} - S_{a+b} - S_{b+c} - S_{a+c} + S_a + S_b + S_c \geqslant 0$.
- *The filling fraction of the state is* $\nu = {}^{n}\!/_{m}$.

This theorem is from [**WW1**].

It follows that such a pattern of zeros can be labeled by $m, S_2, \dots, S_n$, denoted $[m; S_2, \dots, S_n]$. For Laughlin, $n = 1$ and m comes from $\prod_{i<j}(z_i - z_j)^m$. For Pfaffian, $n = 2$ and $m = 2$, and $[m; S_2] = [2; 0]$.

8.2.2. From pattern of zeros to UMTC. The theory is elementary, but encouraging progress has been made. With reasonable assumptions, from the pattern of zeros we can determine

- number of quasiparticle types, i.e., rank of the UMTC,
- quasiparticle charge,
- fusion matrix,
- S-matrix,
- T-matrix partially.

These results are from [**WW2, BaW1**]. But the question of when a pattern of zeros represents a topological state is completely out of reach. From $\{S_a\}_{a=1,2,\dots}$ we can construct a model Hamiltonian whose ground state is our wave function [**RR, WW1, SRR**]. But we do not know whether this is the unique ground state of highest density, or whether this Hamiltonian has a gap when $N \to \infty$.

8.3. CFT and holo=mono

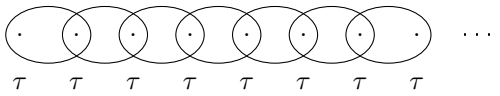
The pattern of zeros approach to FQH wave functions is inspired by an earlier sophisticated approach based on CFTs [**MR**]. In the CFT approach to FQH liquids, wave functions of electrons and quasiholes are conformal blocks. There are two natural braid group representations associated to such a theory: the physical holonomy representation from the projectively flat Berry connection, and the monodromy representation from branch cuts of quasihole wave functions. Moore and Read conjectured that they are the same if the CFT is unitary. It is an important question since combined with the Drinfeld-Kohno theorem (see [**Kas**]) it would imply that the unitary TQFT braid group representation is the same as the physical braiding of anyons. This holo=mono conjecture has been demonstrated physically for certain abelian phases, Blok-Wen states, and the Pfaffian [**ASW, BlW, NW, R2**]. But it is open in general and challenging.

8.4. Bulk–edge correspondence

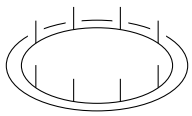
Real samples of topological states of matter, e.g., FQH liquids, are confined to a planar compact region R with boundary. The interior of R is referred to as the bulk and the boundary as the edge in physical jargon. In the simplest case, R is a disk. As time evolves, the physical system lives on $R \times [t_0, t_1]$. For a fixed time slice, e.g., at $t = t_0$ or t_1, the physical system is 2-dimensional, hence described by a 2-dimensional QFT. Similarly, if we restrict our discussion to the cylinder $\partial R \times [t_0, t_1]$, we have another (1+1)-QFT. A priori, these two 2-dimensional QFTs might not even be related after Wick rotations. In a FQH liquid they are believed to be the same CFT, but in general the bulk–edge correspondence is complicated. In the extreme case of quantum doubles, there are no gapless edge excitations. See [**Wen5, R3**].

8.5. Interacting anyons and topological symmetry

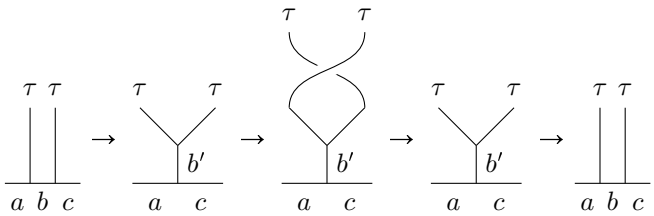
When many anyons in a topological liquid are well-separated, they have degenerate ground states and interact mainly through statistics. But when they are brought closer, their interaction starts to split the degeneracy and potentially might drive the liquid into another phase. As a simple example, consider a chain of Fibonacci anyons and posit that they interact through fusion:



Two neighboring anyons fuse either to 1 or τ, and we penalize the τ channel. Let V_n^i be the ground states of n Fibonacci anyons, where i is the total charge, 1 or τ. Then $H = \sum_i P_i$, where $P_i|e_B\rangle = 0$ if the $(i, i+1)$ anyons fuse to 1 and $P_i|e_B\rangle = |e_B\rangle$ if they fuse to τ. Physicists like to work with a periodic boundary condition, hence the anyons live on a circle.



Consider two τ anyons in a chain of Fibonacci anyons,



The combined operation of a basis transformation F before applying the R-matrix is often denoted by the braid-matrix $B = F_a^{\tau\tau c} R^{\tau\tau} F_c^{a\tau\tau}$. Using a basis $\{|abc\rangle\}$ for the lower labels, the bases before and after the transformation are

$$\{|1\tau 1\rangle, |\tau\tau 1\rangle, |1\tau\tau\rangle, |\tau 1\tau\rangle, |\tau\tau\tau\rangle\}, \qquad \{|111\rangle, |\tau\tau 1\rangle, |1\tau\tau\rangle, |\tau 1\tau\rangle, |\tau\tau\tau\rangle\}.$$

In this representation the F-move is given by

$$F = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \phi^{-1} & \phi^{-1/2} \\ & & & \phi^{-1/2} & -\phi^{-1} \end{pmatrix}$$

and the R-matrix is $R = \mathrm{diag}(e^{4\pi i/5}, e^{-3\pi i/5}, e^{-3\pi i/5}, e^{4\pi i/5}, e^{-3\pi i/5})$. We finally obtain for the braid-matrix

$$B = FRF^{-1} = \begin{pmatrix} e^{4\pi i/5} & & & & \\ & e^{-3\pi i/5} & & & \\ & & e^{-3\pi i/5} & & \\ & & & \phi^{-1}e^{-4\pi i/5} & -\phi^{-1/2}e^{-2\pi i/5} \\ & & & -\phi^{-1/2}e^{-2\pi i/5} & -\phi^{-1} \end{pmatrix}$$

In the $L \to \infty$ limit, this theory becomes gapless and has a conformal symmetry. The model can be solved exactly and the CFT for the gapless phase is the $c = 7/10$ $M(3,4)$ minimal model. The gapless phase is protected by a topological symmetry operator given by driving a τ anyon around the hole: the operator obtained from fusing τ into the circle of anyons [**FTLTKWF**].

8.6. Topological phase transition

In Landau's theory of phases of matter, phase transitions are described by group symmetry breaking. In topological phases of matter, there are no group symmetries in general. But the UMTC can be viewed as some kind of symmetry. Then we may ask if a similar theory can be developed. In particular, we are interested in phase transitions from abelian to non-abelian phases. In Kitaev's honeycomb model, the toric code and Ising are examples of such phase transitions. One observation is that those two topological phases have the same entanglement entropy $\ln 2$. It will be interesting to know under what conditions topological entanglement entropy stays the same across a phase transition. The global quantum dimension D is a very special algebraic number. If the entropy crosses the phase transition continuously, the entanglement entropy $\ln D$ will stay the same.

Among FQH liquids of the same filling fraction, different phases might be connected by phase transitions. As pointed out to me by X.-G. Wen, the transition from 331 to Pfaffian indeed preserves the topological entanglement entropy [**RG, Wen6**]. But in general, topological entanglement entropy is not preserved by continuous topological phase transitions, e.g., 330 to $\mathbb{Z}_4$-parafermion [**BaW2**].

8.7. Fault tolerance

An error-correcting code is an embedding of $(\mathbb{C}^2)^{\otimes n}$ into $(\mathbb{C}^2)^{\otimes m}$ such that information in the image of $(\mathbb{C}^2)^{\otimes n}$ is protected from local errors on $(\mathbb{C}^2)^{\otimes m}$. We call the encoded qubits the logical qubits and the raw qubits $(\mathbb{C}^2)^{\otimes n}$ the constituent qubits. Let V, W be logical and constituent qubit spaces.

THEOREM 8.10. *The pair (V, W) is an error-correcting code if there exists an integer $k \geqslant 0$ such that the composition*

$$V \xhookrightarrow{\ i\ } W \xrightarrow{\ O_k\ } W \xrightarrow{\ \pi\ } V$$

is $\lambda \cdot \mathrm{id}_V$ for any k-local operator O_k on W, where i is inclusion and π projection.

This theorem can be found in [**G**].

When $\lambda \neq 0$, O_k does not degrade the logical qubits. But when $\lambda = 0$, it rotates logical qubits out of the code subspace, introducing errors. But it always rotates a state to an orthogonal state, so errors are detectable and correctable.

The possibility of fault-tolerant QC was a milestone. The smallest number of constituent qubits fully protecting one logical qubit is 5. This error-correcting code is generated by the content Hamiltonian $H = \sum_{i=1}^{4} H_i$ on $(\mathbb{C}^2)^{\otimes 5}$, where

$$H_1 = \sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x \otimes \sigma_0 \qquad H_2 = \sigma_0 \otimes \sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x$$
$$H_3 = \sigma_x \otimes \sigma_0 \otimes \sigma_x \otimes \sigma_z \otimes \sigma_z \qquad H_4 = \sigma_z \otimes \sigma_x \otimes \sigma_0 \otimes \sigma_x \otimes \sigma_z$$

where σ_x, σ_z are Pauli matrices and $\sigma_0 = \mathrm{id}$. The ground state space is isomorphic to $\mathbb{C}^2$. The unitary matrices $X = \sigma_x^{\otimes 5}$, $Z = \sigma_z^{\otimes 5}$ are symmetries of the Hamiltonian, hence act on the ground states. Therefore X and Z can be used to process encoded information. They are called logical gates. An error basis can be detected using measurements and then corrected.

Topological phases of matter are natural error-correcting codes. Indeed the disk axiom of TQFT implies local errors are phases: if an operator is supported on a disk, then splitting the disk off induces a decomposition of the modular functor space $V(\Sigma) \cong V(\Sigma') \otimes V(D^2)$, where $V(D^2) \cong \mathbb{C}$ and Σ' is the punctured surface. This can be made rigorous in the Levin-Wen model, but the details have not been worked out.

CONJECTURE 8.11. *The ground states of the Levin-Wen model form an error-correcting code.*

This is known for the toric code, but I don't know an explicit proof even for DFib.

CHAPTER 9

Outlook and Open Problems

Machines always make me uneasy. Thinking more about machines, I realize that my insecurity comes from a fundamental distrust of machines. What will happen if powerful machines take over our world?

I believe quantum information science will enable us to "see" the colorful quantum world and will bring us exciting new technologies. Elaborating on an idea of M. Freedman and X.-G. Wen, we can consider wave functions as new numbers. While place values provide a linear array of holders for a fixed number of digits, wave functions have Hilbert space bases as holders and complex numbers as digits. In principle a Hilbert space basis can form any shape of any dimension, though bases for qubits are linear arrays. It is bound that we can count more efficiently with wave functions. Science makes a leap when we can count more things efficiently. Before we start to count things with wave functions, we have to be able to control them. Take one qubit as an example: we need to reach every point on the Bloch sphere with arbitrary precision. This might be difficult, but seems not impossible. As a reminder to ourselves, I consider this endeavor as analogous to mountaineering: reach every point on our sphere, such as the daunting K2. K2 has been conquered; qubit states $\mathbb{C}P^{2^n-1}$ are the new frontier.

There are many open problems and new directions. Some of them are mentioned in the earlier chapters. Here we list a few more.

9.1. Physics

The central open problem in TQC is to establish the existence of non-abelian anyons. The current proposal is to use the candidate materials to build a small topological quantum computer [**DFN**]. More theoretical questions include:

- Define topological phases of matter so that they are in 1–1 correspondence with pairs $(\mathcal{C}, c)$, where $\mathcal{C}$ is a unitary MTC and c is a positive rational number such that $c_{\text{top}} = c \mod 8$.
- Develop a theory of phase transitions between topological phases of matter, especially to understand the transition from an abelian phase to a non-abelian one.
- Study stability of topological phases of matter under realistic conditions such as thermal fluctuations or finite temperatures.
- Develop tools to decide whether a given Hamiltonian has a gap in the thermodynamical limit. There are many interesting model Hamiltonians for wave functions in FQH states.
- Formulate mathematically and prove the Moore-Read conjecture holo=mono.
- More speculatively, extend Landau's theory from group symmetry to fusion category symmetry.

9.2. Computer science

Different computing models usually have different favorite problems to solve. QCM is convenient for solving number-theoretic problems with Fourier transforms, while TQC is natural for approximating link invariants. Quantum programming is a black art of extracting useful information from certain unitary matrices such as Fourier transforms. In TQC, there is no preferred role for the Fourier transform. Then where is the magic? One possibility is the algebraic structure of UMTCs, which endows quantum invariants of links with algorithmic structures.

- Are there known interesting gates in QCM algorithms that can be exactly implemented by braiding non-abelian anyons?
- Ground states in Levin-Wen models are believed to be error-correcting codes. What are their properties?
- Computationally easy TQFTs seem to be rare. The associated braid representations have finite images in the unitary groups. The resulting quantum invariants for links form a lattice in the complex plane. Are they always computable in polynomial time classically for links?
- The Tutte polynomial of graphs includes many graph problems as special cases. Can quantum approximation algorithms help find a quantum algorithm for the graph isomorphism problem?

9.3. Mathematics

- Finiteness conjecture of MTCs and classification of low rank MTCs [**RSW**].
- Arithmetic properties of MTCs [**FW**].
- Property F conjecture [**NR**].
- Existence of exotic MTCs [**HRW**].
- Structure of the Witt group of MTCs. A related question is classification of MTCs up to Morita equivalence [**DMNO**].
- Categorical formulation of topological phase transitions using tensor functors.
- Spin MTCs/TQFTs [**BM**].
- Patterns of zeros [**WW1, WW2, BaW1, LWWW**].
- Lattice models of chiral topological liquids [**YK**].
- Nonunitary and irrational (2+1)-TQFTs, e.g., quantized CS theory with gauge group $\mathrm{SL}(2,\mathbb{R})$ or $\mathrm{SL}(2,\mathbb{C})$.
- (3+1)-TQFTs.
- Quantified Ocneanu rigidity: fixing a rank=n fusion rule, are there subexponential estimates of the number of fusion categories, or polynomial estimates of the number of UMTCs?

Bibliography

[AAEL] D. Aharonov, I. Arad, E. Eban, and Z. Landau, *Polynomial quantum algorithms for additive approximations of the Potts model and other points of the Tutte plane*, arXiv:quant-ph/0702008.

[AJL] D. Aharonov, V. Jones, and Z. Landau, *A polynomial quantum algorithm for approximating the Jones polynomial*, STOC '06: Proceedings of the 38th Annual ACM Symposium on Theory of Computing, ACM, New York (2006), 427–436, arXiv:quant-ph/0511096.

[ASW] D. Arovas, J. Schrieffer, and F. Wilczek, *Fractional statistics and the quantum Hall effect*, Phys. Rev. Lett. **53**, 7 (1984), 722–723.

[AS] A. Altland and B. Simons, *Condensed Matter Field Theory*, Cambridge University Press, 2006.

[A] M. Atiyah, *On framings of* 3*-manifolds*, Topology **29**, 1 (1990), 1–7.

[BK] B. Bakalov and A. Kirillov, Jr., *Lectures on Tensor Categories and Modular Functors*, University Lecture Series **21**, Amer. Math. Soc., 2001.

[Ba] P. Bantay, *The Frobenius-Schur indicator in conformal field theory*, Phys. Lett. B **394**, 1–2 (1997), 87–88, arXiv:hep-th/9610192.

[Ba2] P. Bantay, *The kernel of the modular representation and the Galois action in RCFT*, Comm. Math. Phys. **233**, 3 (2003), 423–438, arXiv:math/0102149.

[BaW1] M. Barkeshli and X.-G. Wen, *Structure of quasiparticles and their fusion algebra in fractional quantum Hall states*, Phys. Rev. B **79**, 19 (2009), 195132, arXiv:0807.2789.

[BaW2] M. Barkeshli and X.-G. Wen, *Effective field theory and projective construction for the Z_k parafermion fractional quantum Hall states*, arXiv:0910.2483.

[BM] D. Belov and G. Moore, *Classification of abelian spin Chern-Simons theories*, arXiv:hep-th/0505235.

[BHMV] C. Blanchet, N. Habegger, G. Masbaum, and P. Vogel, *Topological quantum field theories derived from the Kauffman bracket.* Topology **34**, 4 (1995), 883–927.

[BlW] B. Blok and X.-G. Wen, *Many-body systems with non-abelian statistics*, Nuc. Phys. B **374** (1992), 615–646.

[Bo] P. Bonderson, *Non-abelian anyons and interferometry*, Caltech Ph.D. thesis, 2007.

[BFN] P. Bonderson, M. Freedman, and C. Nayak, *Measurement-only topological quantum computation via anyonic interferometry*, Annals Phys. **324**, 14 (2009), 787–826, arXiv:0808.1933.

[BHZS] N. Bonesteel, L. Hormozi, G. Zikos, and S. Simon, *Braid topologies for quantum computation*, Phys. Rev. Lett. **95** (2005), 140503.

[BFLW] M. Bordewich, M. Freedman, L. Lovász, and D. Welsh, *Approximate counting and quantum computation*, Combin. Probab. Comput. **14**, 5–6 (2005), 737–754, arXiv:0908.2122.

[Brav] S. Bravyi, *Universal quantum computation with the nu=5/2 fractional quantum Hall state*, Phys. Rev. A **73** (2006), 042313, arXiv:quant-ph/0511178.

[BrK] S. Bravyi and A. Kitaev, *Quantum invariants of* 3*-manifolds and quantum computation*, unpublished (2001).

[Bru] A. Bruguières, *Catégories prémodulaires, modularisations et invariants des variétés de dimension 3*, (French) Math. Ann. **316**, 2 (2000), 215–236.

[BXMW] M. Burrello, H. Xu, G. Mussardo, and X. Wan, *Topological quantum hashing with icosahedral group*, arXiv:0903.1497.

[CF] C. Caves and C. Fuchs, *Quantum information: How much information in a state vector?*, arXiv:quant-ph/9601025.

[DLL] O. Dasbach, T. Le, and X.-S. Lin, *Quantum morphing and the Jones polynomial*, Comm. Math. Phys. **224**, 2 (2001), 427–442.

[DFN] S. Das Sarma, M. Freedman, and C. Nayak, *Topologically protected qubits from a possible non-abelian fractional quantum Hall state*, Phys. Rev. Lett. **94**, 16 (2005), 166802, arXiv:cond-mat/0412343.

[DMNO] A. Davydov, M. Müger, D. Nikshych, and V. Ostrik, *Étale algebras in braided fusion categories*, in preparation.

[DGG] P. Di Francesco, O. Golinelli, and E. Guitter, *Meanders and the Temperley-Lieb algebra*, Comm. Math. Phys. **186** (1997), 1–59, arXiv:hep-th/9602025.

[DMS] P. Di Francesco, P. Mathieu, and D. Senechal, *Conformal Field Theory*, Graduate Texts in Contemporary Physics, Springer; 1st ed. 1997. Corr. 2nd printing edition (January 18, 1999).

[D] H. Dye, *Unitary solutions to the Yang-Baxter equation in dimension four*, Quantum Inf. Process. **2**, 1–2 (2002), 117–151 (2003), arXiv:quant-ph/0211050.

[ENO] P. Etingof, D. Nikshych, and V. Ostrik, *On fusion categories*, Ann. of Math. (2) **162**, 2 (2005), 581–642, arXiv:math/0203060.

[FTLTKWF] A. Feiguin, S. Trebst, A. Ludwig, M. Troyer, A. Kitaev, Z. Wang, and M. Freedman, *Interacting anyons in topological quantum liquids: The golden chain*, Phys. Rev. Lett. **98** (2007), 160409, arXiv:cond-mat/0612341.

[Fe82] R. Feynman, *Simulating physics with computers*, International Journal of Theor. Physics **21**, 6 (1982), 467–488.

[FFNWW] L. Fidkowski, M. and Freedman, C. Nayak, K. Walker, and Z. Wang, *From string nets to nonabelions*, Comm. Math. Phys. **287**, 3 (2009), 805–827, arXiv:cond-mat/0610583.

[Fi] M. Finkelberg, *An equivalence of fusion categories*, Geom. Funct. Anal. **6**, 2 (1996), 249–267.

[FNTW] E. Fradkin, C. Nayak, A. Tsvelik, and F. Wilczek, *A Chern-Simons effective field theory for the pfaffian quantum Hall state*, Nucl. Phys. B **516**, 3 (1998), 704–718, arXiv:cond-mat/9711087.

[FRW] J. Franko, E. Rowell, and Z. Wang, *Extraspecial 2-groups and images of braid group representations*, J. Knot Theory Ramifications **15**, 4 (2006), 413–427, arXiv:math.RT/0503435.

[Fr1] M. Freedman, *P/NP, and the quantum field computer*, Proc. Natl. Acad. Sci. USA **95**, 1 (1998), 98–101.

[Fr2] M. Freedman, *A magnetic model with a possible Chern-Simons phase*, with an appendix by F. Goodman and H. Wenzl, Comm. Math. Phys. **234**, 1 (2003), 129–183, arXiv:quant-ph/0110060.

[Fr3] M. Freedman, Station Q seminar (2007).

[FKLW] M. Freedman, A. Kitaev, M. Larsen, and Z. Wang, *Topological quantum computation*, Bull. Amer. Math. Soc. (N.S.) **40**, 1 (2003), 31–38, arXiv:quant-ph/0101025.

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

[FLW1] M. Freedman, M. Larsen, and Z. Wang, *A modular functor which is universal for quantum computation*, Comm. Math. Phys. **227**, 3 (2002), 605–622, arXiv:quant-ph/0001108.

[FLW2] M. Freedman, M. Larsen, and Z. Wang, *The two-eigenvalue problem and density of Jones representation of braid groups*, Comm. Math. Phys. **228**, 1 (2002), arXiv:math.GT/0103200.

[FNSWW] M. Freedman, C. Nayak, K. Shtengel, K. Walker, and Z. Wang, *A class of P,T-invariant topological phases of interacting electrons*, Ann. Phys. **310**, 2 (2004), 428–492, arXiv:cond-mat/0307511.

[FNW] M. Freedman, C. Nayak, and K. Walker, *Towards universal topological quantum computation in the $\nu = 5/2$ fractional quantum Hall state*, Phys. Rev. B **73**, 24 (2006), 245307, arXiv:cond-mat/0512066.

[FNWW] M. Freedman, C. Nayak, K. Walker, and Z. Wang, *On picture (2+1)-TQFTs*, in Topology and Physics, Nankai Tracts Math. **12**, World Sci. Publ., Hackensack, NJ, 2008, 19–106, arXiv:0806.1926.

[FWW] M. Freedman, K. Walker, and Z. Wang, *Quantum* SU(2) *faithfully detects mapping class groups modulo center*, Geom. Topol. **6** (2002), 523–539, arXiv:math.GT/0209150.

[FW] M. Freedman and Z. Wang, *Large quantum Fourier transforms are never exactly realized by braiding conformal blocks*, Phys. Rev. A (3) **75**, 3 (2007), 032322, arXiv:cond-mat/0609411.

[FG] J. Fröhlich and F. Gabbiani, *Braid statistics in local quantum theory*, Rev. Math. Phys. **2**, 3 (1990), 251–353.

[FM] J. Fröhlich and P. Marchetti, *Quantum field theory of anyons*, Lett. Math. Phys. **16**, 4 (1988), 347–358.

[GW] F. Goodman and H. Wenzl, *The Temperley-Lieb algebra at roots of unity*, Pacific J. Math. **161**, 2 (1993), 307-334.

[G] D. Gottesman, *Theory of fault-tolerant quantum computation*, Phys. Rev. Lett. A **57** (1998), 127–137.

[GWW] M. Greiter, X.-G. Wen, and F. Wilczek, *Paired Hall state at half filling*, Phys. Rev. Lett. **66**, 24 (1991), 3205–3208.

[Hag] T. Hagge, *Graphical calculus for fusion categories and quantum invariants for 3-manifolds*, Indiana University Ph.D. thesis, 2008.

[HH] T. Hagge and S. Hong, *Some non-braided fusion categories of rank 3*, Commun. Contemp. Math. **11**, 4 (2009), 615–637, arXiv:0704.0208.

[Hal] B. Halperin, *Statistics of quasiparticles and the hierarchy of fractional quantized Hall states*, Phys. Rev. Lett. **52**, 18 (1984), 1583–1586.

[H] S.-M. Hong, *On symmetrization of 6j-symbols and Levin-Wen Hamiltonian*, arXiv:0907.2204.

[HRW] S.-M. Hong, E. Rowell, and Z. Wang, *On exotic modular categories*, Commun. Contemp. Math. **10** (2008), suppl. 1, 1049–1074, arXiv:0710.5761.

[HBS] L. Hormozi, N. Bonesteel, and S. Simon, *Topological quantum computing with Read-Rezayi states*, Phys. Rev. Lett. **103** (2009), 160501, arXiv:0903.2239.

[I] D. Ivanov, *Non-abelian statistics of half-quantum vortices in p-wave superconductors*, Phys. Rev. Lett. **86**, 2 (2001), 268–271, arXiv:cond-mat/0005069.

[Ja] F. Jaeger, *Tutte polynomials and link polynomials*, Proc. Amer. Math. Soc. **103**, 2 (1988), 647–654, arXiv:0902.1162.

[Jo1] V. Jones, *Index for subfactors*, Invent. Math. **72**, 1 (1983), 1–25.

[Jo2] V. Jones, *A polynomial invariant for knots via von Neumann algebras*, Bull. Amer. Math. Soc. (N.S.) **12**, 1 (1985), 103–111.

[Jo3] V. Jones, *Braid groups, Hecke algebras and type* II_1 *factors*, in Geometric Methods in Operator Algebras (Kyoto, 1983), Pitman Res. Notes Math. Ser. **123**, Longman Sci. Tech., Harlow, 1986, 242–273. Harlow, 1986.

[Jo4] V. Jones, *Hecke algebra representations of braid groups and link polynomials*, Ann. of Math. (2) **126**, 2 (1987), 335–388.

[Kas] C. Kassel, *Quantum Groups*, Graduate Texts in Mathematics **155**, Springer-Verlag, New York, 1995.

[Ki1] A. Kitaev, *Fault-tolerant quantum computation by anyons*, Ann. Physics **303**, 1 (2003), 2–30, arXiv:quant-ph/9707021.

[Ki2] A. Kitaev, *Anyons in an exactly solved model and beyond*, Ann. Physics **321**, 1 (2006), 2–111, arXiv:cond-mat/0506438.

[KP] A. Kitaev and J. Preskill, *Topological entanglement entropy*, Phys. Rev. Lett. **96**, 11 (2006), 110404, arXiv:hep-th/0510092.

[KSV] A. Kitaev, A. Shen, and V. Vyalyi, *Classical and Quantum Computation*, translated from the 1999 Russian original by L. Senechal, Graduate Studies in Mathematics **47**, American Mathematical Society, Providence, RI, 2002.

[Kau] L. Kauffman, *State models and the Jones polynomial*, Topology **26**, 3 (1987), 395–407.

[KL] L. Kauffman and S. Lins, *Temperley-Lieb recoupling theory and invariants of* 3*-manifolds*, Annals of Mathematics Studies **134**, Princeton University Press, Princeton, NJ, 1994.

[KM1] R. Kirby and P. Melvin, *The* 3*-manifold invariants of Witten and Reshetikhin-Turaev for* $\mathrm{sl}(2, C)$. Invent. Math. **105**, 3 (1991), 473–545.

[KM2] R. Kirby and P. Melvin, *Local surgery formulas for quantum invariants and the Arf invariant*, Proceedings of the Casson Fest, Geom. Topol. Monogr. **7**, Geom. Topol. Publ., Coventry, 2004, 213–233, arXiv:math.GT/0410358.

[LRW] M. Larsen, E. Rowell, and Z. Wang, *The N-eigenvalue problem and two applications*, Int. Math. Res. Not. **2005**, 64, 3987–4018, arXiv:math/0506025.

[LM] J. Leinaas and J. Myrheim, *On the theory of identical particles*, Il Nuovo Cimento B **37**, 1 (1977), 1–23.

[LW1] M. Levin and X.-G. Wen, *String-net condensation: A physical mechanism for topological phases*, Phys. Rev. B **71**, 4 (2005), 045110, arXiv:cond-mat/0404617.

[LW2] M. Levin and X.-G. Wen, *Detecting topological order in a ground state wave function*, Phys. Rev. Lett. **96**, 11 (2006), 110405, arXiv:cond-mat/0510613.

[Li] J. Liptrap, *Generalized Tambara-Yamagami categories*, in preparation.

[Ll] S. Lloyd, *Universal quantum simulators*, Science **273**, 5278 (1996), 1073–1078.

[LWWW] Y.-M. Lu, X.-G. Wen, Z. Wang, and Z. Wang, *Non-abelian quantum Hall states and their quasiparticles: from the pattern of zeros to vertex algebra*, arXiv:0910.3988.

[Ma] S. MacLane, *Categories for the working mathematician*, Graduate Texts in Mathematics **5**, Springer-Verlag, New York-Berlin, 1971.

[MW] D. Meyer and N. Wallach, *Global entanglement in multiparticle systems*, J. Math. Phys. **43**, 9 (2002), 4273–4278, arXiv:quant-ph/0108104.

[MR] G. Moore and N. Read, *Nonabelions in the fractional quantum Hall effect*, Nuclear Phys. B **360**, 2–3 (1991), 362–396.

[Mu1] M. Müger, *From subfactors to categories and topology I, Frobenius algebras in and Morita equivalence of tensor categories*, J. Pure Appl. Algebra **180**, 1-2 (2003), 81–157, arXiv:math.CT/0111204.

[Mu2] M. Müger, *From subfactors to categories and topology II, The quantum double of tensor categories and subfactors*, J. Pure Appl. Algebra **180**, 1–2 (2003), 159–219, arXiv:math.CT/0111205.

[NSSFD] C. Nayak, S. Simon, A. Stern, M. Freedman, and S. Das Sarma, *Non-abelian anyons and topological quantum computation*, Rev. Mod. Phys. **80**, 3 (2008), 1083–1159, arXiv:0707.1889.

[NR] D. Naidu and E. Rowell, *A finiteness property for braided fusion categories*, arXiv:0903.4157.

[NW] C. Nayak and F. Wilczek, *2n-quasihole states realize 2^{n-1}-dimensional spinor braiding statistics in paired quantum Hall states*, Nucl. Phys. B **479**, 3 (1996), 529–553, arXiv:cond-mat/9605145.

[NS] S.-H. Ng and P. Schauenburg, *Congruence subgroups and generalized Frobenius-Schur indicators*, arXiv:0806.2493.

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

[P] J. Preskill, *Physics 219 Quantum Computing lecture notes*, Chapter 9, http://www.theory.caltech.edu/∼preskill/ph229/.

[R1] N. Read, *Non-abelian braid statistics versus projective permutation statistics*, J. Math. Phys. **44** (2003), 558–563, arXiv:hep-th/0201240.

[R2] N. Read, *Non-abelian adiabatic statistics and Hall viscosity in quantum Hall states and $p_x + ip_y$ paired superfluids*, Phys. Rev. B **79** (2009), 045308, arXiv:arXiv:0805.2507.

[R3] N. Read, *Conformal invariance of chiral edge theories*, Phys. Rev. B **79** (2009), 245304, arXiv:0711.0543.

[RG] N. Read and D. Green, *Paired states of fermions in two dimensions with breaking of parity and time-reversal symmetries and the fractional quantum Hall effect*, Phys. Rev. B **61**, 15 (2000), 10267-10297, arXiv:cond-mat/9906453.

[RR] N. Read and E. Rezayi, *Beyond paired quantum Hall states: Parafermions and incompressible states in the first excited Landau level*, Phys. Rev. B **59**, 12 (1999), 8084–8092, arXiv:cond-mat/9809384.

[RT] N. Reshetikhin and V. Turaev, *Invariants of 3-manifolds via link polynomials and quantum groups*, Invent. Math. **103**, 3 (1991), 547–597.

[Ro] E. Rowell, *From quantum groups to unitary modular tensor categories*, Contemp. Math. **413** (2006), 215–230, arXiv:math.QA/0503226.

[RSW] E. Rowell, R. Stong, and Z. Wang, *On classification of modular tensor categories*, Communications in Mathematical Physics **292**, 2 (2009), 343–389, arXiv:0712.1377.

[RW] E. Rowell and Z. Wang, in preparation.

[S] P. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, in 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994), IEEE Comput. Soc. Press, Los Alamitos, CA, 1994, 124–134.

[SJ] P. Shor and S. Jordan, *Estimating Jones polynomials is a complete problem for one clean qubit*, Quantum Inf. Comput. **8**, 8–9 (2008), 681–714, arXiv:0707.2831.

[SRR] S. Simon, E. Rezayi, and N. Regnault, *S3 quantum Hall wavefunctions*, arXiv:0908.0947.

[TY] D. Tambara and S. Yamagami, *Tensor categories with fusion rules of self-duality for finite abelian groups*, J. Algebra **209**, 2 (1998), 692–707.

[Tu] V. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, De Gruyter Studies in Mathematics **18**, Walter de Gruyter & Co., Berlin, 1994.

[TV] V. Turaev and O. Viro, *State sum invariants of* 3*-manifolds and quantum 6j-symbols*, Topology **31**, 4 (1992), 865–902.

[V] D. Vertigan, *The computational complexity of Tutte invariants for planar graphs*, SIAM J. Comput. **35**, 3 (2005), 690–712.

[Wal1] K. Walker, *On Witten's 3-manifold Invariants*, 1991 notes at http://canyon23.net/math/.

[Wal2] K. Walker, *TQFTs*, 2006 notes at http://canyon23.net/math/.

[Wel] D. Welsh, *Complexity: Knots, Colourings and Counting*, London Mathematical Society Lecture Note Series **186**, Cambridge University Press, Cambridge, 1993.

[Wenz] H. Wenzl, *On sequences of projections*, C. R. Math. Rep. Acad. Sci. Canada **9**, 1 (1987), 5–9.

[Wen1] X.-G. Wen, *Topological orders in rigid states*, Internat. J. Mod. Phys. B **4**, 2 (1990), 239–271.

[Wen2] X.-G. Wen, *Non-abelian statistics in the fractional quantum Hall states*, Phys. Rev. Lett. **66**, 6 (1991), 802–805.

[Wen3] X.-G. Wen, *Mean-field theory of spin-liquid states with finite energy gap and topological orders*, Phys. Rev. B **44**, 6 (1991), 2664–2672.

[Wen4] X.-G. Wen, *Theory of the edge states in fractional quantum Hall effects*, Internat. J. Mod. Phys. B **6**, 10 (1992), 1711–1762.

[Wen5] X.-G. Wen, *Topological orders and edge excitations in FQH states*, Advances in Physics **44**, 5 (1995), 405–473, arXiv:cond-mat/9506066.

[Wen6] X.-G. Wen, *Continuous topological phase transitions between clean quantum Hall states*, Phys. Rev. Lett. **84**, 17 (2000), 3950–3953, arXiv:cond-mat/9908394.

[Wen7] X.-G. Wen, *Quantum Field Theory of Many-Body Systems*, Oxford University Press, 2004.

[WW1] X.-G. Wen and Z. Wang, *Classification of symmetric polynomials of infinite variables: Construction of abelian and non-abelian quantum Hall states*, Phys. Rev. B. **77**, 23 (2008), 235108, arXiv:0801.3291.

[WW2] X.-G. Wen and Z. Wang, *Topological properties of abelian and non-abelian quantum Hall states classified using patterns of zeros*, Phys. Rev. B. **78**, 15 (2008), 155109, arXiv:0803.1016.

[Wi1] F. Wilczek, *Quantum mechanics of fractional-spin particles*, Phys. Rev. Lett. **49**, 14 (1982), 957–959.

[Wi2] F. Wilczek, *Fractional Statistics and Anyon Superconductivity*, World Scientific Publishing Co., Inc., Teaneck, NJ, 1990.

[Witt] E. Witten, *Quantum field theory and the Jones polynomial*, Comm. Math. Phys. **121**, 3 (1989), 351–399.

[WY] P. Wocjan and J. Yard, *The Jones polynomial: quantum algorithms and applications in quantum complexity theory*, Quantum Inf. Comput. **8**, 1-2 (2008), 147–180, arXiv:quant-ph/0603069.

[Wu] Y.-S. Wu, *General theory for quantum statistics in two dimensions*, Phys. Rev. Lett. **52**, 24 (1984), 2103–2106.

[YK] H. Yao and S. Kivelson, *Exact chiral spin liquid with non-abelian anyons*, Phys. Rev. Lett. **99**, 24 (2007), 247203, arXiv:0708.0040.

[Y1] S. Yamagami, *Polygonal presentations of semisimple tensor categories*, J. Math. Soc. Japan **54**, 1 (2002), 61–68.

[Y2] S. Yamagami, *Frobenius reciprocity in tensor categories*, Math. Scand. **90**, 1 (2002), 35–56.

[Y] D. Yetter, *Markov algebras*, in Braids (Santa Cruz, CA, 1986), Contemp. Math. **78**, Amer. Math. Soc., Providence, RI, 1988, 705–730.