A modular functor which is universal for quantum computation

Michael Freedman†, Michael Larsen‡, and Zhenghan Wang‡

February 1, 2008

† *Microsoft Research, One Microsoft Way, michaelf@microsoft.com*
‡ *Indiana Univ., larsen@math.indiana.edu and zhewang@indiana.edu*

Abstract

We show that the topological modular functor from Witten-Chern-Simons theory is universal for quantum computation in the sense a quantum circuit computation can be efficiently approximated by an intertwining action of a braid on the functor's state space. A computational model based on Chern-Simons theory at a fifth root of unity is defined and shown to be polynomially equivalent to the quantum circuit model. The chief technical advance: the density of the irreducible sectors of the Jones representation, have topological implications which will be considered elsewhere.

1 Introduction

The quantum computer was Feynman's [Fey] last great idea. He understood that local "quantum gates", the basis of his model, can efficiently simulate the evolution of any finite dimensional quantum system and by extension any renormalizable system. The details of the argument are given in [Ll]. Topological quantum field theories (TQFTs), although possessing a finite dimensional Hilbert space, lack a Hamiltonian—the derivative of time evolution on which the Feynman-Lloyd argument is based. In [FKW], we provide a different argument for the poly-local nature of TQFTs showing that quantum computers efficiently simulate these as well. Here we give a converse to this simulation result. The Feynman-Lloyd argument is reversible, so we may summarize the situation as:

(1) finite dimensional quantum systems,

(2) quantum computers (meaning the quantum circuit model QCM [D][Y]),

(3) certain topological modular functors (TMFs).

Each can efficiently simulate the others. We wrote TMF above instead of TQFT because we use only the conformal blocks and the action of the mapping class groups on these—not the general morphisms associated to 3-dimensional non-product bordisms.

We would like to thank Alexei Kitaev for conversations on our approach.

2 A universal quantum computer

The strictly 2-dimensional part of a TQFT is called a *topological modular functor* (TMF). The most interesting examples of TMFs are given by the SU(2) Witten-Chern-Simons theory at roots of unity [Wi]. These examples are mathematically constructed in [RT] using quantum groups (See also [T][Wa]). A modular functor assigns to a compact surface Σ (with some additional structures detailed below) a complex vector space $V(\Sigma)$ and to a diffeomorphism of the surface (preserving structures) a linear map of $V(\Sigma)$. In the cases considered here $V(\Sigma)$ always has a positive definite Hermitian inner product $<,>_h$ and the induced linear maps preserve $<,>_h$, i.e. are unitary. The usual additional structures are fixed parameterizations of each boundary component, a labeling of each boundary component by an element of a finite label set $\mathcal{L}$ with an involution $\hat{}: \mathcal{L} \to \mathcal{L}$, and a Lagrangian subspace L of $H_1(\Sigma, \mathbb{Q})$ ([T][Wa]). Since our quantum computer is built from quantum-$SU(2)$-invariants of braiding, and the intersection pairing of a planar surface is 0, $L = H_1(\Sigma; \mathbb{Q})$ and can be ignored. The parameterization of boundary components can be dropped. (The essential information which enhances the Kauffman bracket to the Jones polynomial is remembered by the "blackboard framing" of the braid.) The involution $\hat{}$ is simply the identity since the $SU(2)$-theory is self-dual. In fact, we can manage by only considering the $SU(2)$-Chern-Simons theory at $q = e^{\frac{2\pi i}{r}}, r = 5$ and so our label set will be the symbols $\{0, 1, 2, 3\}$. Note that in our notation, 0 labels the trivial representation, not 1. Since we are suppressing boundary parameterizations, we may work in the disk with n marked points-thought of crushed boundary components. Because we only need the "uncolored theory" to make a universal model, each marked point is assigned the label 1, and the boundary of the disk is assigned the label 0. We consider the action of the braid group $B(n)$ which consists of diffeomorphisms of the disk which leave the n marked points and the boundary set-wise invariant modulo those isotopic to the identity. The braid group has the well-known presentation:

$$\begin{aligned} B(n) = \{\sigma_1, \cdots, \sigma_{n-1} | \quad & \sigma_i \sigma_j \sigma_i^{-1} \sigma_j^{-1} = id \text{ if } |i-j| > 1 \\ & \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \text{ if } |i-j| = 1\}, \end{aligned}$$

where σ_i is the half right twist of the i-th marked point about the $i+1$-st marked point.

To describe our fault-tolerant computational model "Chern-Simons5" **CS5**, we must deal with the usual error arising from decoherence as well as a novel "qubit smearing error" resulting from imbedding the computational qubits within a modular functor super-space. To explain our approaches we initially ignore all errors; in particular formula (1) is a simplification valid only in the error-free context.

The state space $S_k = (\mathbb{C}^2)^{\otimes k}$ of our quantum computer consists of k qubits, that is the disjoint union of k spin$=\frac{1}{2}$ systems which can be described mathematically as the tensor product of k copies of the state space $\mathbb{C}^2$ of the basic 2-level system, $\mathbb{C}^2 = \text{span}(|0>, |1>)$. For each even integer k, we will choose an inclusion $S_k \overset{i}{\hookrightarrow} V(D^2, \text{ 3k marked points}) = V(D^2, 3k)$ and show how to use the action of the braid group $B(3k)$ on the modular functor to (approximately) induce the action of any poly-local unitary operator $\mathbf{U} : S_k \to S_k$. That is we will give an (in principle) efficient procedure for constructing a braid $b = b(\mathbf{U})$ so that

$$i \circ \mathbf{U} = V(b) \circ i. \qquad (1)$$

To see that this allows us to simulate the QCM, we need to explain: (i) what we mean by the hypothesis "poly-local" on $\mathbf{U}$, (ii) what "efficient" means, (iii) what the effect of the two types of errors are on line (1), and (iv) what measurement consists of within our model.

We begin by explaining how to map S_k into V and how to perform 1 and 2 qubit gates.

Let D be the unit 2-dimensional disk and

$$\left\{\frac{11}{100k}, \frac{12}{100k}, \frac{13}{100k}, \frac{21}{100k}, \frac{22}{100k}, \frac{23}{100k}, \dots, \frac{10k+1}{100k}, \frac{10k+2}{100k}, \frac{10k+3}{100k}\right\}$$

be a subset of $3k$ marked points on the x-axis. Without giving formulae the reader should picture k disjoint sub-disks $D_i, 1 \leq i \leq k$, each containing one clump of 3 marked points in its interior (these will serve as qubits) and further $\begin{pmatrix} k \\ 2 \end{pmatrix}$ disks $D_{i,j}, 1 \leq i < j \leq k$, containing D_i and D_j, but with $D_{ij} \cap D_l = \emptyset, l \neq i$ or j (which will allow 2-qubit gates). Strictly speaking, among the larger subdisks, we only need to consider $D_{i,i+1}, 1 \leq i, i+1 < k$, and could choose a standard (linear) arrangement for these but there is no cost in the exposition to considering all $D_{i,j}$ above which will correspond in the model to letting any two qubits interact. Also, curiously, we will see that any of the numerous topologically distinct arrangements for the $\{D_{i,j}\}$ within D may be selected without prejudice.

We define V_k^l to be the $SU(2)$ Hilbert space of k marked points in the interior with labels equal 1 and l label on ∂D. We need to understand the many ways in which V_m^0 arises via the "gluing axiom" ([Wa]) from smaller pieces. The axiom provides an isomorphism:

$$V(X \cup_\gamma Y) = \oplus_{\text{all consistent labelings } l} V(X,l) \otimes V(Y,l), \tag{2}$$

where the notation suppress all labels not on the 1-manifold γ along which X and Y are glued. The sum is over all labelings of the components of γ satisfying the conditions that matched components have equal labels. According to $SU(2)$-Chern-Simons theory [KL], for three-punctured spheres with boundary labels a, b, c, the Hilbert space $V_{abc} \cong \mathbb{C}$ if

$$(i) : a + b + c = \text{even},$$

$$(ii) : a \leq b + c, b \leq a + b, c \leq a + b \ \ \text{(triangle inequalities)} \tag{3}$$

$$(iii) : a + b + c \leq 2(r - 2);$$

and $V_{abc} = 0$ otherwise. The gluing axiom together with the above information allows an inductive calculation of V_k^l, where the superscript denotes the label on ∂D. We easily calculate that

$$\dim V_3^1 = 2, \;\; \dim V_3^3 = 1, \dim V_6^0 = 5, \;\; \dim V_6^2 = 8. \tag{4}$$

Line (4) motivates taking $V(D_i, \text{its 3 pts}, \text{boundary label 1}) =: V_i \cong \mathbb{C}^2$ as our fundamental unit of computation, *the qubit*. We fix the choice of an arbitrary "complementary vector" v in the state space of $D \setminus \cup_{i=1}^k D_i$ $v \in V(D \setminus \cup_{i=1}^k D_i$, all boundary labels $= 1$ except boundary of $D = 0)$ $=: V_{\text{complement}}$ (To keep this space nontrivial, we have taken k even.) Using v, the gluing axiom defines an injection:

$$i_v : (\mathbb{C}^2)^{\otimes k} \cong \otimes_{i=1}^k V_i \overset{\otimes v}{\to} (\otimes_{i=1}^k V_i) \otimes V_{\text{complement}} \overset{\text{as summand}}{\hookrightarrow} V_{3k}^0 \tag{5}$$

This composition i_v determines what we will serve as our computational qubits within the modular functor V_{3k}^0. The reader familiar with [FKW] will notice that we use here a dual approach. In that paper, we imbedded the modular functor into a larger Hilbert space that is a tensor power; here we imbedded a tensor power into the modular functor.

The action of $B(3)$ on D_i yields 1-qubit gates, whereas two qubit gates will be constructed using the action of $B(6)$ on $D_{i,j}$. Supposing our quantum computer S_k is in state s, a given v as above determines a state $i_v(s) = s \otimes v \in V_{3k}^0$. Now suppose we wish to evolve s by a 2-qubit gate g acting unitarily on $\mathbb{C}_i^2 \otimes \mathbb{C}_j^2$ and by id on $\mathbb{C}_l^2, l \neq i$ or j. Using gluing axiom (2) and the inclusion (5), we may write

$$s = \sum_h t_h \otimes u_h, \tag{6}$$

where $\{t_h\}$ is a basis or partial basis for $\mathbb{C}_i^2 \otimes \mathbb{C}_j^2$ and $u_h \in \otimes_{l \neq i,j} \mathbb{C}_l^2$, so $s \otimes v = \sum_h (t_h \otimes u_h) \otimes v$. Decomposing along $\gamma = \partial D_{i,j}$, we may write $v = \alpha_0 \otimes \beta_0 + \alpha_2 \otimes \beta_2$, where $\alpha_\epsilon \in V\big(D_{i,j} \setminus (D_i \cup D_j), \epsilon \text{ on } \gamma\big)$, $\epsilon = 0$ or 2 and $\beta_\epsilon \in V\big(D \setminus (\cup_{l \neq i,j} D_l \cup D_{ij}), \epsilon \text{ on } \gamma, \text{ and } 0 \text{ on } \partial D\big)$. Thus

$$s \otimes v = \sum_h t_h \otimes u_h \otimes \alpha_0 \otimes \beta_0 + \sum_h t_h \otimes u_h \otimes \alpha_2 \otimes \beta_2, \tag{7}$$

An element of $B(6)$ applied to the 6 marked points in $D_i \cup D_j \subset D_{ij}$ acts via a representation $\rho^0 \oplus \rho^2 =: \rho$ on $V^0(D_{ij}, 6\text{ pts}) \oplus V^2(D_{ij}, 6\text{ pts})$, where the superscript denotes the label appearing when the surface is cut along γ. In particular $B(6)$ acts on each factor $t_h \otimes \alpha_0$ and $t_h \otimes \alpha_2$ in (7). Note $t_h \otimes \alpha_0$ belongs to the summand of $V^0(D_{ij}, 6\text{ pts})$ corresponding to boundary labels on $\partial\big(D_{ij} \backslash (D_i \cup D_j)\big) = 0, 1, 1$. There is an additional 1-dimensional summand corresponding to boundary labels 0,3,3-with 0,1,3 and 0,3,1 excluded by the triangle inequality (ii) in (3) above. Similarly $t_h \otimes \alpha_2$ belongs to the summand of $V^2(D_{ij}, 6\text{ pts})$ with boundary labels=2,1,1. There are additional summands corresponding to (2,1,3), and (2,3,1) of dimensions 2 each.

Ideally we would find a braid $b = b(g) \in B(6)$ so that $\rho^0(b)(t_h \otimes \alpha_0) = gt_h \otimes \alpha_0$ and $\rho^2(b)(t_h \otimes \alpha_2) = gt_h \otimes \alpha_2$. Then referring to (7) we easily check that

$$\rho(b)(s \otimes v) = \sum_h \big((gt_h) \otimes u_h\big) \otimes v, \tag{8}$$

i.e. $\rho(b)$ implements the gate g on the state space S_k of our quantum computer. In practice there are two issues: (i) we cannot control the phase of the output of either ρ^0 or ρ^2, and (ii) these outputs will be only approximations of the desired gate g. The phase issue (i) leads to a change of the complimentary vector $v \to v'$ as follows as seen on line (9) below. This is harmless since ultimately we only measure the qubits.

$$s \otimes v = \sum_h t_h \otimes u_h \otimes \alpha_0 \otimes \beta_0 + \sum_h t_h \otimes u_h \otimes \alpha_2 \otimes \beta_2$$

$$\Downarrow \text{gate}$$

$$\begin{aligned} s \otimes v &= \omega_0 \sum_h gt_h \otimes u_h \otimes \alpha_0 \otimes \beta_0 + \omega_2 \sum_h gt_h \otimes u_h \otimes \alpha_2 \otimes \beta_2 \\ &= \sum_h \omega_0 gt_h \otimes u_h \otimes \alpha_0 \otimes \beta_0 + \sum_h \omega_2 gt_h \otimes u_h \otimes \alpha_2 \otimes \beta_2 \\ &= \sum_h (gt_h \otimes u_h) \otimes (\omega_0\alpha_0 \otimes \beta_0 + \omega_2\alpha_2 \otimes \beta_2) \\ &=: \sum_h (gt_h \otimes u_h) \otimes v' \end{aligned} \tag{9}$$

The approximation issue is addressed by Theorem 2.1 below.

Theorem 2.1. *There is a constant $C > 0$ so that for all unitary $g : \mathbb{C}_i^2 \otimes \mathbb{C}_j^2 \to \mathbb{C}_i^2 \otimes \mathbb{C}_j^2$, there is a braid b_l of length $\leq l$ in the generators σ_i and their inverses $\sigma_i^{-1}, 1 \leq i \leq n-1$, so that:*

$$||\omega_0 \rho^0(b_l) - g \oplus id_1|| + ||\omega_2 \rho^2(b_l) - g \oplus id_4|| \leq \epsilon (> 0) \tag{10}$$

for some unit complex numbers (phases) $\omega_i, i = 0, 2$ whenever ϵ satisfies

$$l \leq C \cdot \left(\frac{1}{\epsilon}\right)^2. \tag{11}$$

We use $||\quad||$ to denote the operator norms and the subscripts on id indicate the dimension of the orthogonal component in which we are trying *not* to act.

The main work in proving Theorem 2.1 is to show that the closure of the image of the representation $\rho : B(6) \to \mathbf{U}(5) \times \mathbf{U}(8)$ contains $SU(5) \times SU(8)$. Once this is accomplished the estimate (10) follows with some exponent ≥ 2 from [Ki] and the refinement to exponent=2 which will appear in [CN] following a suggestion of the first author of the present paper. Also as explained in [Ki] there is a $poly(\frac{1}{\epsilon})$ time classical algorithm which can be used to construct the approximating braid b_l as a word in $\{\sigma_i\}$ and $\{\sigma_i^{-1}\}$. The density theorem is the substance of Section 4.

The action $\rho(b)$ "approximately" executes the gate g on S_k but not in the usual sense of approximation since the state space $i_v(S_k)$ itself is only approximately g invariant. To convert this "smearing of qubits" to errors of the type considered in the fault tolerant literature, after each g is approximately executed by $\rho(b)$ we measure the labels around $\cup_{i=1}^k \partial D_i$ to project the new state $\rho(b)(s \otimes v)$ into the form $s' \otimes v, s' \in S_k$, with probability $1 - \mathcal{O}(\epsilon^2), |s' - s| \leq \mathcal{O}(\epsilon)$. With probability $\mathcal{O}(\epsilon^2)$ the label measurement around ∂D_i does not yield one; in this case $V^1(D_i; 3 \text{ pts}) =: V_{1,1,1,1} \cong \mathbb{C}^2$ has collapsed to $V_{1,1,1,3} \cong \mathbb{C}$ and it is as if a qubit has been "traced out" of our state space. More specifically, if the label 3 is measured on ∂D_i, we replace $V^3(D_i, \text{its 3 marked pts})$ with a freshly cooled qubit $V^1(D', 3 \text{ pts})$ with a completely random initial state—an ancilli—which we have been saving for such an occasion. The reader may picture dragging D_i off to the edge of the disk D and dragging the ancilli D_i' in as its replacement (and then renaming D' by D_i.) The hypothesis that such ancilli are available is discussed below. The error model of [AB] is precisely suited to this situation; Aharanov and Ben-Or show in Chapter 8 that a calculation on the level of "logical" qubits can be kept precisely on track with a probability $\geq \frac{2}{3}$ provided the ubiquitous errors at the level of "physical" qubits are of norm $\leq \mathcal{O}(\epsilon)$ (even if they are systematic and not random) and the large errors (in our case tracing a qubit) have probability also $\leq \mathcal{O}(\epsilon)$ for some threshold constant $\epsilon > 0$. For this, and all other fault tolerant models, entropy must be kept at bay by ensuring a "cold" stream of ancilli $|0>$'s. In the context of our model we must now explain both the role of measurement and ancilla.

Given any essential simple closed curve γ on a surface Σ, the gluing formula reads:

$$V(\Sigma) = \oplus_{l \in \mathcal{L}} V(\Sigma_{cut_\gamma}, l) \tag{12}$$

so "measuring a label" means that we posit for every γ a Hermitian operator H_γ with eigenvalues distinguishing the summands of the r.h.s. of (12) above. For a more comprehensive computational study, we would wish to posit that if γ has length $= L$, then H_γ can be computed in poly(L) time. For the present purpose we only need that $H_\gamma, \gamma = \partial D_i$ or $\partial D_{i,j}$ can be computed in constant time. Beyond measuring labels, we hypothesize that there is some way of probing the quantum state of the smallest nontrivial building blocks in the theory. For us these are the qubits $= V_{1,1,1,1} \cong \mathbb{C}^2$. Fix a basis $\{|0>, |1>\}$ for $V_{1,1,1,1}$ and posit for each $D_i, 1 \leq i \leq k$, with label 1 on its boundary, an observable Hermitian operator $\sigma_z^i : V_{3k}^0 \to V_{3k}^0$ which acts as the Pauli matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in a fixed basis $\{|0>, |1>\}$ for that qubit. This is our repertoire of measurement: H_γ is used to "unsmear physical qubits" after each gate and the σ_z's to read out the final state (according to von Neumann's statistical postulate on measurement) after the computation is completed.

In fault tolerant models of computation it is essential to have available a stream of "freshly cooled" ancilli qubits. If these are present from the start of the computation, even if untouched, they will decohere from errors in employing the identity operator. In the physical realization of a quantum computer unless stored zeros were extremely stable there would have to be some device (inherently not unitary!) for resetting ancilli to $|0>$, e.g. a polarizing magnetic field. As a theoretical matter unbounded computation requires such resetting. In a topological model such as $V(\Sigma)$ it is not unreasonable to postulate that $|0> \in V_{1,1,1,1} = V^1(D_i, 3 \text{ pts})$ is stable if not involved in any gates. An alternative hypothesis is that there is some mechanism outside the system analogous to the polarizing magnetic field above which can "refrigerate" ancilli in the state $|0>$ until they are to be used. We refer below to either of these as the "fresh ancilli" hypothesis. To correct the novel qubit smearing errors, we already encountered the need for ancilli in a random state $\rho = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$. This state, of course, is easier to maintain.

Let us now return to line (1). Let $\mathbf{U}$ be the theoretical output of a quantum circuit $\mathcal{C}$ of (i.e. composition of) gates to be executed on the physical qubit level so as to fault-tolerantly solve a problem instance of length n. We assume the problem is in BQP and that the above composition has length $\leq poly(n)$. Actually, due to error, $\mathcal{C}$ will output a completely positive trace preserving super-operator $\mathcal{O}$, called a physical operator. Now simulate $\mathcal{C}$ in the modular functor V a gate at a time by a succession of braidings and H_γ-measurements. With regard to parallelism (necessary in all fault tolerant schemes), notice that disjoint 2 qubit gates can be performed simultaneously if $D_{i,j} \cap D_{i',j'} = \emptyset$. For example this can always be arranged in the linear QCM for gates acting in $D_{i,i+1}$ and $D_{j,j+1}$ provided $i+1 \neq j, j+1 \neq i$, and $i \neq j$, and even this model is shown to be fault tolerant [AB]. As noted above, the complementary vector $v \in V_{\text{complement}}$ evolves probabilistically as the simulation progresses . Different v's will occur as a tensor factor in a growing number of probabilistically weighted terms. These new v-values are in the end unimportant; they simply label a computational state (to be observed with some probability) and are never read by the output measurements σ_z^i.

Now the two main theorems:

Theorem 2.2. *Let QCM denote the exact quantum circuit model. Suppose M is a problem instance in BQP solved by a circuit $\mathcal{C}$ of length poly(L) where L is length(M). Let* **CS5** *denote the model based on the SU(2)-Chern-Simons modular functor of braids at the fifth root of unity $e^{\frac{2\pi i}{5}}$ which we have described in this section: uncolored 3k-strand braids, H_γ and σ_z^i measurements, and "fresh ancilli". The braid group acts on the modular functor and within the functor one may identify k-qubits S_k. These actions together with label measurement H_γ's define a probabilistic evolution of the initial (possibly mixed) state $\alpha \in S_k$. This evolution, defined gate-wise, evolves the mixed state $\alpha \otimes v \in V_{3k}$ of the modular functor to a new (probabilistic mixture of) state(s) β. Performing σ_z^i-measurements on β samples from the mixture drawing out a state $\beta_l = \alpha_l \otimes v_l$ and observing (according to von Neumann measurement) only the α_l factor. With probability $\geq \frac{3}{4}$ the observations correctly solve the problem instance M. The number of marked points to be* *braided (=3k) and the length of the braiding exceed the size of the original circuit $\mathcal{C}$ by at most a multiplicative poly(log(L)) factor. Taken in triples, they represent the "physical qubits" of the [AB] fault tolerant model, thus* **CS5** *provides a model which efficiently and fault tolerantly simulates the computations of QCM. We note that the use of label measurements H_γ introduces non-unitary steps in the middle of our simulation.*

Proof: The structure of the proof relies heavily on Chapter 8 [AB] to reduce the QCM to a linear quantum circuit (with state space S_k) enjoying a very liberal error model (small systematic errors plus rare trace over qubit). In the final state $\beta = \sum p_l \beta_l$, each β_l admits a tensor decomposition according to the geometry: $D = (\cup_i D_i) \cup$ (complement), but along the k boundary components $\cup_i \partial D_i$ all choices of labels 1 or 3 may appear. So if we write $\beta_l = \alpha_l \otimes v_l$ we must remember that associated to l is an element $[l] \in \{1,3\}^k$ which defines the subspaces in which α_l and v_l lie and that β_l lies in the corresponding $[l]$ sector of the modular functor. All occurrences of the label 3 correspond to a $\mathbb{C}$ tensor factor, $\mathbb{C} \cong V^3(D_i, 3\text{ pts}) \subset V(D_i, 3\text{ pts})$ whereas the label 1 corresponds to a $\mathbb{C}^2$ factor. Thus in the [AB] framework each label 3 corresponds to a "lost" or averaged qubit according to our replacement procedure $D_i \longleftrightarrow D'$. Losing an occasional qubit from the computational space S_k is the price we pay to "unsmear" S_k within the modular functor. Theorem 2.1 implies that for a braid length $= \mathcal{O}(\frac{1}{\epsilon^2})$ a qubit will be lost with probability $\mathcal{O}(\epsilon^2)$ and if no qubit is lost the gate will be performed with error $\mathcal{O}(\epsilon)$ on pure states. Factoring a mixed state as a probabilistic combination of pure states and passing the error estimate across the probabilities we see that the $\mathcal{O}(\epsilon)$ error bound holds on the super-operator trace norm as well. Thus for ϵ sufficiently small (estimated $< 10^{-6}$ in Chapter 8 [AB]), observing (at random) α_l amounts to sampling from an error prone implementation of the quantum circuit $\mathcal{C}$. The error model is not entirely random in that the approximation procedure used to construct b_L will have systematic biases. This implies that the $\mathcal{O}(\epsilon)$ errors introduced in the functioning of each gate are not random and must be treated as "malicious". Fortunately the error model explained in Chapter 8 [AB] permits the small error to be arbitrary as long as the large error, e.g. qubit losses, occurs with a probability dominated by a small constant independent of the qubit and the computational history, as they do in our **CS5** model. This completes the proof of Theorem 2.2 modulo the proof of the density Theorem 4.1.

We may define a variant of our model **CS5**, "exact Chern-Simons at $e^{\frac{2\pi i}{5}}$",

ECS5, in which we assume that all the braid groups act exactly (no error) on the modular functor V. Such a hypothesis is not outrageous since a physical implementation of a topological theory may itself confer fault tolerance, in that topological phenomena are inherently discrete. The only difference in the algorithm for modeling the QCM in **ECS5** is the simplification that H_γ measurements are not performed in the middle of the simulation, but only at the very end, prior to reading out the qubits S_k with σ_z^k measurements.

Theorem 2.3. *There is an efficient and strictly unitary simulation of QCM by* **ECS5**. *Thus given a problem instance M of length L in BQP, there is a classical poly(L) time algorithm for constructing a braid b as a word of length poly(L) in the generators $\sigma_i, 1 \leq i \leq$ poly(L)=3k. Applying b to a standard initial state, $\psi_{initial} \in V^0(D, 3k)$, results in a state $\psi_{final} \in V^0(D, 3k)$, so that the results of H_γ on ∂D_i followed by σ_z^i measurements on ψ_{final} correctly solve the problem instance M with probability ≥ 6.*

Proof: In the quantum circuit model $\mathcal{C}$ for M (implied by the problem lying in BQP) count the number n of gates to be applied. Use line (11) to approximate each gate g by a braid b of length l so that the operator norm error $||\rho(b) - g||$ of the approximating gate will be less than $\frac{1}{10n}$. The composition of n braids which gate-wise simulate the quantum circuit introduces an error on operator norm < 0.1. It follows that our two measurement steps will return an answer (nearly) as reliable as the original quantum circuit $\mathcal{C}$: H_γ projects to $V^1(D, 3 \text{ pts})$ with (more than) 90% probability and the subsequent probabilities of σ_z^1 measuring $|0>$ or $|1>$ differ from $\mathcal{C}$ by less than 10%.

Remark: Theorem 2.2 and 2.3 are complementary. One provided additional fault tolerance—fault tolerance beyond what might be inherent in a topological model—but at the cost of introducing intermediate non-unitary steps (i.e. measurements). The other eschews intermediate measurements by and so gives a strictly unitary simulation, but cannot confer additional fault tolerance. It is an interesting open problem whether fault tolerance and strictly unitary can be combined in a universal model of computation based on topological modular functors.

3 Jones' representation of the braid groups

A TMF gives a family of representations of the braid groups and mapping class groups. In this section, we identify the representations of the braid groups from the SU(2) modular functor at primitive roots of unity with the irreducible sectors of the representation discovered by Jones whose weighted trace gives the Jones polynomial of the closure link of the braid [J1][J2]. To prove universality of the modular functor for quantum computation, we only use this portion of the TMF. Therefore, we will focus on these representations.

First let us describe the Jones representation of the braid groups explicitly following [We]. To do so, we need first to describe the representation of the Temperley-Lieb-Jones algebras $A_{\beta,n}$. Fix some integer $r \geq 3$ and $q = e^{\frac{2\pi i}{r}}$. Let $[k]$ be the quantum integer defined as $[k] = \frac{q^{\frac{k}{2}} - q^{\frac{-k}{2}}}{q^{\frac{1}{2}} - q^{\frac{-1}{2}}}$. Note that $[-k] = -[k]$, and $[2] = q^{\frac{1}{2}} + q^{\frac{-1}{2}}$. Then $\beta := [2]^2 = q + \bar{q} + 2 = 4cos^2(\frac{\pi}{r})$. The algebras $A_{\beta,n}$ are the finite dimensional C^*-algebras generated by 1 and projectors $e_1, \cdots, e_{n-1}$ such that

1. $e_i^2 = e_i$, and $e_i^* = e_i$,
2. $e_i e_{i\pm 1} e_i = \beta^{-1} e_i$,
3. $e_i e_j = e_j e_i$ if $|i-j| \geq 2$,

and there exists a positive trace $tr : \cup_{n=1}^{\infty} A_{\beta,n} \to \mathbb{C}$ such that $tr(xe_n) = \beta^{-1} tr(x)$ for all $x \in A_{\beta,n}$.

The Jones representation of $A_{\beta,n}$ is the representation corresponding to the G.N.S construction with respect to the above trace. An important feature of the Jones representation is that it splits as a direct sum of irreducible representations indexed by some 2-row Young diagrams, which we will refer to as *sectors*. A Young diagram $\lambda = [\lambda_1, \cdots \lambda_s], \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s$ is called a $(2,r)$ diagram if $s \leq 2$ (at most two rows) and $\lambda_1 - \lambda_2 \leq r-2$. Let $\wedge_n^{(2,r)}$ denote all $(2,r)$ diagrams with n nodes. Given $\lambda \in \wedge_n^{(2,r)}$, let $T_\lambda^{(2,r)}$ be all standard tableaus $\{t\}$ with shape λ satisfying the inductive condition which is the analogue of (iii) in (3): when $n, n-1, \cdots, 2, 1$ are deleted from t one at a time, each tableau appeared is a tableau for some $(2,r)$ Young diagram. The representation of $A_{\beta,n}$ is a direct sum of irreducible representations $\pi_\lambda^{(2,r)}$ over all $(2,r)$ Young diagrams λ. The representation

$\pi_\lambda^{(2,r)}$ for a fixed $(2,r)$ Young diagram λ is given as follows: let $V_\lambda^{(2,r)}$ be the complex vector space with basis $\{\vec{v}_t,\ t\in T_\lambda^{(2,r)}\}$. Given a generator e_i in the Temperley-Lieb-Jones algebra and a standard tableau $t\in V_\lambda^{(2,r)}$. Suppose i appears in t in row r_1 and column c_1, $i+1$ in row r_2 and column c_2. Denote by $d_{t,i}=c_1-c_2-(r_1-r_2)$, $\alpha_{t,i}=\frac{[d_{t,i}+1]}{[2][d_{t,i}]}$, and $\beta_{t,i}=\sqrt{\alpha_{t,i}(1-\alpha_{t,i})}$. They are both non-negative real numbers and satisfy the equation $\alpha_{t,i}=\alpha_{t,i}^2+\beta_{t,i}^2$. Then we define

$$\pi_\lambda^{(2,r)}(e_i)(\vec{v}_t)=\alpha_{t,i}\vec{v}_t+\beta_{t,i}\vec{v}_{g_i(t)}, \tag{13}$$

where $g_i(t)$ is the tableau obtained from t by switching i and $i+1$ if $g_i(t)$ is in $T_\lambda^{(2,r)}$. If $g_i(t)$ is not in $T_\lambda^{(2,r)}$, then $\alpha_{t,i}$ is 0 or 1 given by its defining formula. This can occur in several cases. It follows that $\pi_\lambda^{(2,r)}$ with respect to the basis $\{\vec{v}_t\}$ is a matrix consisting of only of 2×2 and 1×1 blocks. Furthermore, the 1×1 blocks are either 0 or 1, and the 2×2 blocks are

$$\begin{pmatrix} \alpha_{t,i} & \beta_{t,i} \\ \beta_{t,i} & 1-\alpha_{t,i} \end{pmatrix}. \tag{14}$$

The identity $\alpha_{t,i}=\alpha_{t,i}^2+\beta_{t,i}^2$ implies that (14) is a projector. So all eigenvalues of e_i are either 0 or 1.

The Jones representation of the braid groups is defined by

$$\rho_{\beta,n}(\sigma_i)=q-(1+q)e_i. \tag{15}$$

Combining (15) with the above representation of the Temperley-Lieb-Jones algebra, we get Jones' representation of the braid groups, denoted still by $\rho_{\beta,n}$:

$$\rho_{\beta,n}: B_n\to A_{\beta,n}\to \mathbf{U}(N_{\beta,n}),$$

where the dimension $N_{\beta,n}=\sum_{\lambda\in\wedge_n^{(2,r)}}\dim V_\lambda^{(2,r)}$ grows asymptotically as β^n.

When $|q|=1$, as we have seen already, Jones' representation $\rho_{\beta,n}$ is unitary. To verify that $\rho(\sigma_i)\rho^*(\sigma_i)=1$, note $\rho^*(\sigma_i)=\bar{q}-(1+\bar{q})e_i^*$. So we have $\rho(\sigma_i)\rho^*(\sigma_i)=q\bar{q}+(1+q)(1+\bar{q})e_ie_i^*-(1+q)e_i-(1+\bar{q})e_i^*=1$. We use the fact $e_i^*=e_i$ and $e_i^2=e_i$ to cancel out the last 3 terms.

From the definition, $\rho_{\beta,n}$ also splits as a direct sum of representations over $(2,r)$-Young diagrams. A sector corresponding to a particular Young diagram λ will be denoted by $\rho_{\lambda,\beta,n}$.

Now we collect some properties about the Jones representation of the braid groups into the following:

Theorem 3.1. *(i) For each $(2,r)$-Young diagram λ, the representation $\rho_{\lambda,\beta,n}$ is irreducible.*

(ii) The matrices $\rho_{\lambda,\beta,n}(\sigma_i)$ for $i=1,2$ generate an infinite subgroup of $\mathbf{U}(2)$ *modulo center for $r \neq 3,4,6,10$.*

(iii) Each matrix $\rho_{\lambda,\beta,n}(\sigma_i), 1 \leq i \leq n-1$, has exactly two distinct eigenvalues $-1, q$.

(iv) For the (2,5)-Young diagram $\lambda=[4,2]$, $n=6$, the two eigenvalues $-1, q$ of every $\rho_{\lambda,\beta,6}(\sigma_i)$ have multiplicity of 3 and 5, respectively.

The proofs of (i) and (ii) are in [J2]. For (iii), first note that the matrix $\rho_{\lambda,\beta,n}(\sigma_1)$ is a diagonal matrix with respect to the basis $\{\vec{v}_t\}$ with only two distinct eigenvalues $-1, q$. Now (iii) follows from the fact that all braid generators σ_i are conjugate to each other. For (iv), simply check the explicit matrix for $\rho_{\lambda,\beta,6}(\sigma_1)$ at the end of this section.

Now we identify the sectors of the Jones representation with the representations of the braid groups coming from the $SU(2)$ Chern-Simons modular functor. The $SU(2)$ Chern-Simons modular functor **CSr** of level r has been constructed several times in the literature (for example, [RT][T][Wa][G]). Our construction of the modular functor **CSr** is based on skein theory [KL]. The key ingredient is the substitute of Jones-Wenzl idempotents for the intertwiners of the irreducible representations of quantum groups [RT][T][Wa]. This is the same $SU(2)$ modular functor as constructed using quantum groups in [RT] (see [T]) which is regarded as a mathematical realization of the Witten-Chern-Simons theory. All formulae we need for skein theory are summarized in Chapter 9 of [KL] with appropriate admissible conditions. Fix an integer $r \geq 3$. Let $A = \sqrt{-1} \cdot e^{-\frac{2\pi i}{4r}}$, and $s = A^2$, and $q = A^4$. (Note the confusion caused by notations. The q in [KL] is A^2 which is our s here. But in Jones' representation of the braid groups [J2], q is A^4. In all formulae in [KL], q should be interpreted as s in our notation.) The label set $\mathcal{L}$ of the modular functor **CSr** will be $\{0, 1, \cdots, r-2\}$ and the involution is the identity. We are interested in a unitary modular functor and the one in [G] is not unitary. We claim that if we follow the same construction of [G] using our choice of A and endow all state spaces of the modular functor with the following Hermitian inner product, the resulting modular functor **CSr** is unitary.

Given a surface Σ, a pants decomposition of Σ determines a basis of $V(\Sigma)$: each basis element is a tensor product of the basis elements of the constituent pants. The desired inner products are determined by axiom (2.14) [Wa] if we specify an inner product on each space V_{abc}. Our choice of A makes all constants $S(a)$ appearing in the axiom (2.14) [Wa] positive. Consequently, positive definite Hermitian inner products on all spaces V_{abc} determine a positive definite Hermitian inner product on $V(\Sigma)$. The vector space V_{abc} of the three punctured sphere P_{abc} is defined to be the skein space of the disk D_{abc} enclosed by the seams of the punctured sphere P_{abc}. The numbering of the three punctures induces a numbering of the three boundary "points" of the disk D_{abc} labeled by $\{a, b, c\}$. Suppose t is a tangle on D_{abc} in the skein space of D_{abc}, and let $\bar{t}$ be the tangle on D_{abc} obtained by reflecting the disk D_{abc} through the first boundary point and the origin. Then the inner product $<,>_h$: $V_{abc} \times V_{abc} \to \mathbb{C}$ is as follows: given two tangles s and t on D_{abc}, their product $< s, t >_h$ is the Kauffman bracket evaluation of the resulting diagram on S^2 obtained by gluing the two disks with s and $\bar{t}$ on them respectively, along their common boundaries with matching numberings. Extending $<,>_h$ on the skein space of D_{abc} linearly in the first coordinate and conjugate linearly in the second coordinate, we obtain a positive definite Hermitian inner product on V_{abc}. It is also true that the mapping class groupoid actions in the basic data respect this Hermitian product, and the fusion and scattering matrices F and S also preserve this product. So **CSr** is indeed a unitary modular functor.

This modular functor **CSr** defines representations of the central extension of the mapping class groups of labeled extended surfaces, in particular for n-punctured disks D_n^m with all interior punctures labeled 1 and boundary labeled m. If $m \neq 1$, then the mapping class group is the braid group B_n. If $m = 1$, then the mapping class group is the spherical braid group $\mathcal{S}B_{n+1} = \mathcal{M}(0, n+1)$. Recall that we suppress the issues of framing and central extension as they are inessential in our discussion. Also the representation of the mapping class groups coming from **CSr** will be denoted simply by ρ_r.

Theorem 3.2. *Let D_n^m be as above.*

(1): If $m + n$ is even, and $m \neq 1$, then ρ_r is equivalent to the irreducible sector of the Jones representation $\rho_{\lambda,\beta,n}$ for the Young diagram $\lambda = [\frac{m+n}{2}, \frac{m-n}{2}]$ up to phase.

(2): If n is odd, and $m = 1$, then the composition of ρ_r with the natural map $\iota : B_n \to \mathcal{S}B_{n+1}$ is equivalent to the irreducible sector of the Jones representation $\rho_{\lambda,\beta,n}$ for the Young diagram $\lambda = [\frac{n+1}{2}, \frac{n-1}{2}]$ up to phase.

The equivalence of these two representations was first established in a non-unitary version [Fu]. A computational proof of this theorem can be obtained following [Fu]. So we will be content with giving some examples for $r = 5$.

For the $(2,5)$ Young diagram $\lambda = [2,1]$, $n = 3$ with an appropriate ordering of the basis:

$$\rho_{[2,1],\beta,3}(\sigma_1) = \begin{pmatrix} -1 & 0 \\ 0 & q \end{pmatrix},$$

$$\rho_{[2,1],\beta,3}(\sigma_2) = \begin{pmatrix} \frac{q^2}{q+1} & -\frac{q\sqrt{[3]}}{q+1} \\ -\frac{q\sqrt{[3]}}{q+1} & -\frac{1}{q+1} \end{pmatrix}, \text{ where quantum } [3] = q + \bar{q} + 1.$$

For the $(2,5)$ Young diagram $\lambda = [3,3]$, $n = 6$, the representation is 5-dimensional. With an appropriate ordering of the basis, we have:

$$\rho_{[3,3],\beta,6}(\sigma_1) = \begin{pmatrix} -1 & & & & \\ & q & & & \\ & & -1 & & \\ & & & q & \\ & & & & q \end{pmatrix},$$

$$\rho_{[3,3],\beta,6}(\sigma_2) = \begin{pmatrix} \frac{q^2}{q+1} & -\frac{q\sqrt{[3]}}{q+1} & & & \\ -\frac{q\sqrt{[3]}}{q+1} & -\frac{1}{q+1} & & & \\ & & \frac{q^2}{q+1} & -\frac{q\sqrt{[3]}}{q+1} & \\ & & -\frac{q\sqrt{[3]}}{q+1} & -\frac{1}{q+1} & \\ & & & & q \end{pmatrix}.$$

For the $(2,5)$ Young diagram $\lambda = [4,2]$, $n = 6$, the representation is 8-dimensional. Here the inductive condition on basis elements make one standard tableau illegal, so the representation is not 9-dimensional as it would be if $r > 5$. This is the restriction analogous to (iii) in (3) for the modular functor. With an appropriate ordering of the basis:

$$\rho_{[4,2],\beta,6}(\sigma_1) = \begin{pmatrix} -1 & & & & & & & \\ & q & & & & & & \\ & & -1 & & & & & \\ & & & q & & & & \\ & & & & -1 & & & \\ & & & & & q & & \\ & & & & & & q & \\ & & & & & & & q \end{pmatrix}.$$

4 A Density theorem

In this section, we prove the density theorem.

Theorem 4.1. *Let* $\rho := \rho_{[3,3]} \oplus \rho_{[4,2]} : B_6 \to \mathbf{U}(5) \times \mathbf{U}(8)$ *be the Jones representation of* B_6 *at the 5-th root of unity* $q = e^{\frac{2\pi i}{5}}$. *Then the closure of the image of* $\rho(B_6)$ *in* $\mathbf{U}(5) \times \mathbf{U}(8)$ *contains* $SU(5) \times SU(8)$.

By Theorem 3.2, this is the same representation $\rho := \rho^0 \oplus \rho^2 : B_6 \to \mathbf{U}(5) \times \mathbf{U}(8)$ in the $SU(2)$ Chern-Simons modular functor at the 5-th root of unity used in Section 2 to build a universal quantum computer. In the following, a key fact used is that the image matrix of each braid generator under the Jones representation has exactly two eigenvalues $\{-1, q\}$ whose ratio is not ± 1. This strong restriction allows us to identify both the closed image and its representation.

Proof: First it suffices to show that the images of $\rho_{[3,3]}$ and $\rho_{[4,2]}$ contain $SU(5)$ and $SU(8)$, respectively. Supposing so, if $K = \overline{\rho(B_6)} \cap (SU(5) \times SU(8))$, then the two projections $p_1 : K \to SU(5)$ and $p_2 : K \to SU(8)$ are both surjective. Let N_2 (respectively N_1) be the kernel of p_1 (respectively p_2). Then N_1 (respectively N_2) can be identified as a normal subgroup of $SU(5)$ (respectively $SU(8)$). By Goursat's Lemma (page 54, [La]), the image of K in $SU(5)/N_1 \times SU(8)/N_2$ is the graph of some isomorphism $SU(5)/N_1 \cong SU(8)/N_2$. As the only nontrivial normal subgroups of $SU(n)$ are finite groups, this is possible only if $N_1 = SU(5)$ and $N_2 = SU(8)$. Therefore, $K = SU(5) \times SU(8)$.

The proofs of the density for $\rho_{[3,3]}$ and $\rho_{[4,2]}$ are similar. So we prove both cases at the same time and give separate argument for the more complicated case $\rho_{[4,2]}$ when necessary.

Let G be the closure of the image of $\rho_{[3,3]}$ (or $\rho_{[4,2]}$) in $\mathbf{U}(5)$ (or $\mathbf{U}(8)$) which we will try to identify. By Theorem 3.1, G is a compact subgroup of $\mathbf{U}(m)$ ($m = 5$ or 8) of positive dimension. Denote by V the induced m-dimensional faithful, irreducible complex representation of G. The representation V is faithful since G is a subgroup of $\mathbf{U}(m)$. Let H be the identity component of G. What we actually show is that the derived group of H, $Der(H) = [H, H]$, is actually $SU(m)$. We will divide the proof into several steps.

Claim 1: The restriction of V to H is an isotypic representation, i.e. a direct sum of several copies of a single irreducible representation of H.

Proof: As G is compact, $V = \oplus_P V_P$, where P runs through some irreducible representations of H, and V_P is the direct sum of all the copies of P contained in V. Since H is a normal subgroup, and the braid generators σ_i topologically generate G, the σ_i's permute transitively the isotypic components V_P [CR, Section 49]. If there is more than 1 such component, then some σ_i acts nontrivially, so it must permute these blocks.

Now we need a linear algebra lemma:

Lemma 4.2. *Suppose W is a vector space with a direct sum decomposition $W = \oplus_{i=1}^n W_i$, and there is a linear automorphism T such that $T : W_i \to W_{i+1}$ $1 \leq i \leq n$ cyclically. Then the product of any eigenvalue of T with any n-th root of unity is still an eigenvalue of T.*

Proof: Choose a basis of W consisting of bases of $W_i, i = 1, 2, \cdots, n$. If k is not a multiple of n, then $\mathrm{tr}T^k = 0$, as all diagonal entries are 0 with respect to the above basis. Let $\{\lambda_i\}$ be all eigenvalues of T. (They may repeat.) Consider all values of $\mathrm{tr}T^m = \sum \lambda_i{}^m$ $(m = 1, 2, \cdots)$ which are sums of m-th powers of all eigenvalues of T. These sums of m-th powers of $\{\lambda_i\}$ are invariant if we simultaneously multiply all the eigenvalues $\{\lambda_i\}$ by an n-th root of unity ω: $\sum (\omega\lambda_i)^m = \sum \omega^m \lambda_i{}^m = \omega^m \sum \lambda_i{}^m$ which is equal to $\mathrm{tr}T^m = \sum \lambda_i{}^m$ because when m is not a multiple of n, they are both 0, and when m is, $\omega^m = 1$. These values $\mathrm{tr}T^m$ uniquely determine the eigenvalues of T, and therefore the set of the eigenvalues of T is invariant under multiplication by any n-th root of unity.

Back to claim 1, if there is more than one isotypic component, then some σ_i will have an orbit of length at least 2. It is impossible to have an orbit of length 3 or more by the above lemma as this will lead to at least 3 eigenvalues. If the orbit is of length 2 and as $\rho(\sigma_i)$ has only two eigenvalues $\{a, b\}$, by the lemma, $\{-a, -b\}$ are also eigenvalues. It follows that $a = -b$ which is impossible when $q \neq -1$.

Claim 2: The restriction of V to H is an irreducible representation.

Proof: By claim 1, $V|_H$ has only one isotypic component. If $V|_H$ is reducible, then the isotypic component is a tensor product $V_1 \otimes V_2$, where V_1 is the irreducible representation of H in the isotypic component and V_2 is a trivial representation of H with $\dim V_2 \geq 2$. If V_1 is 1-dimensional, then $\rho(\sigma_i), i = 1, 2$ generate a finite subgroup of $\mathbf{U}(m)$ modulo center which is excluded by Theorem 3.1. So we have $\dim V_1 \geq 2$. Now we recall a fact in representation theory: a representation of a group $\rho : G \to GL(V)$ is irreducible if and only if the image $\rho(G)$ of G generates the full matrix algebra $\mathrm{End}(V)$. As V_1 is an irreducible representation of H, the image $\rho(H)$ generates $\mathrm{End}(V_1) \otimes \mathrm{id}_2$, where the subscript of id indicate the tensor factor. As the elements σ_i normalize H, they also normalize the subalgebra $\mathrm{End}(V_1) \otimes \mathrm{id}_2$ in $\mathrm{End}(V_1 \otimes V_2)$. Consequently they act as automorphisms of the full matrix algebra $\mathrm{End}(V_1)$. Any automorphism of a full matrix algebra is a conjugation by a matrix, so the braid generators σ_i act via conjugation (up to a scalar multiple) as invertible matrices in $\mathrm{End}(V_1) \otimes \mathrm{id}_2$ modulo its centralizer. It is not hard to see the centralizer of $\mathrm{End}(V_1) \otimes \mathrm{id}_2$ in $\mathrm{End}(V_1 \otimes V_2)$ is $\mathrm{id}_1 \otimes \mathrm{End}(V_2)$. Therefore, the braid generators σ_i act via conjugation as invertible matrices in $\mathrm{End}(V_1) \otimes \mathrm{End}(V_2)$, i.e. they preserve the tensor decomposition. This is impossible by the following eigenvalue analysis. Consider a braid generator σ_i, its image $\rho(\sigma_i)$ is a tensor product of two matrices each of sizes at least 2. Since $\rho(\sigma_i)$ has only two eigenvalues, neither factor matrix can have 3 or more eigenvalues. If both factor matrices have two eigenvalues, the fact that $\rho(\sigma_i)$ has 2 eigenvalues in all implies that the ratio of these two eigenvalues is ± 1 which is forbidden. If one factor matrix is trivial, then $\rho(\sigma_i)$ acts trivially on this factor. As all braid generators are conjugate to each other, so the whole group G will act trivially on this factor which implies that V is a reducible representation of G. This case cannot happen either, as V is an irreducible representation of G.

Claim 3: The derived group, $Der(H) = [H, H]$, of H is a semi-simple Lie group, and the further restriction of V to $Der(H)$ is still irreducible.

Proof: By claim 2, $V|_H$ is a faithful, irreducible representation, so H is a reductive Lie group [V, Theorem 3.16.3]. It follows that the derived group of H is semi-simple. It also follows that the derived group and the center of H generate H. By Schur's lemma, the center act by scalars. So $V|_{Der(H)}$ is still irreducible.

Claim 4: Every outer automorphism of $Der(H)$ has order 1, 2, or 3.

First we recall a simple fact in representation theory. If V is an irreducible representation of a product group $G_1 \times G_2$, then V splits as an outer tensor product of irreducible representations of $G_i, i = 1, 2$. The restriction of V to G_1 has only one isotypic component, and the restriction of V to G_2 lies in the centralizer of the image of G_1. So the representation splits.

Proof: It suffices to prove the same statement for the universal covering $Der^{uc}(H)$ of $Der(H)$, as the automorphism group of $Der(H)$ is a subgroup of the automorphism group of $Der^{uc}(H)$.

For the 5-dimensional case: as 5 is a prime, $Der^{uc}(H)$ is a simple group. It is well-known that any outer automorphism of a simple Lie group is of order 1, 2, or 3.

For the 8-dimensional case, if $Der^{uc}(H)$ is a simple group, it can be handled as above, so we need only to consider the split cases. If $Der^{uc}(H)$ splits into two simple factors, then one factor must be $SU(2)$: of all simply connected simple Lie groups, only $SU(2)$ has a 2-dimensional irreducible representation. So the outer automorphism group is either Z_2 when both factors are $SU(2)$, or the same as the outer automorphism group of the other simple factor. Our claim holds. If there are three simple factors, they must all be $SU(2)$. The outer automorphism group is the permutation group on three letters S_3. Again our claim is true.

Claim 5: For each braid generator σ_i, we can choose a corresponding element $\tilde{\sigma_i}$ lying in the derived group $Der(H)$ which also has exactly two eigenvalues, whose ratio is not ± 1. The multiplicity of each eigenvalue of $\tilde{\sigma_i}$ is the same as that of σ_i. (The choice of $\tilde{\sigma_i}$ is not unique, but its two eigenvalues have ratio q.)

Proof: Since $Der(H)$ is still a normal subgroup of G, and the braid generators σ_i normalize $Der(H)$, so they determine outer-automorphisms of $Der(H)$. By claim 4, an outer-automorphism of $Der(H)$ is of order 1, 2, or 3. Hence σ_i^6 acts as an inner automorphism of $Der(H)$. By Schur's lemma, each σ_i^6 is the product of an element in $Der(H)$ with a scalar, though the decomposition is not unique. Fix a choice for an element $\tilde{\sigma_i}$ in $Der(H)$. Then it has exactly two desired eigenvalues.

To complete the proof of Theorem 4.1, we summarize our situation: we have a nontrivial semi-simple group $Der^{uc}(H)$ with an irreducible unitary representation. Furthermore, it has a special element x whose image under the representation has exactly two distinct eigenvalues whose ratio is not ± 1.

For the 5-dimensional case, $Der^{uc}(H)$ is a simple Lie group. Going through the list [MP] of pairs (G, ϖ), where G is a simply connected Lie group and ϖ a dominant weight. The only possible 5-dimensional irreducible representations are as follows: rank=1, $(SU(2), 4\varpi_1)$, rank=2, $(Sp(4), \varpi_2)$, and rank=4, $(SU(5), \varpi_i), i = 1, 4$. By examining the possible eigenvalues, we can exclude the first two cases as follows: for the first case, suppose α, β are the two eigenvalues of the above element x in $SU(2)$, then under the representation $4\varpi_1$ the eigenvalues of the image of x are $\alpha^i\beta^j, i + j = 4$, where i and j both are non-negative integers. The only possibility is two eigenvalues whose ratio is ± 1. For the second case, since 5 is an odd number, any element in the image has a real eigenvalue. Other eigenvalues come in mutually reciprocal pairs. Again the only possibility is two eigenvalues whose ratio is ± 1. Therefore, the only possible pair is the third case which gives $Der^{uc}(H) = SU(5)$. As V is a faithful representation of $Der(H)$, the image of $Der(H)$ is the same as that of $Der^{uc}(H)$ which is $SU(5)$.

The 8-dimensional case for $\rho_{[4,2]}$ is similar. By [MP], we see the possible pairs for simply connected simple groups are $\big(SU(2), 7\varpi_1\big)$, $\big(SU(3), \varpi_1 + \varpi_2\big)$, $\big(Spin(7), \varpi_3\big)$, $\big(Sp(8), \varpi_1\big)$, $\big(Spin(8), \varpi_i\big), i = 1, 3, 4$ and $\big(SU(8), \varpi_i\big), i = 1, 7$, where ϖ_i is the fundamental weight. The same eigenvalue analysis will exclude all but the $\big(SU(8), \varpi_i\big)$ case. The proof follows the same pattern as above with the following novelties. Case 2 is the adjoint representation of $SU(3)$, if the special element $x \in SU(3)$ has eigenvalues $\{\alpha, \beta, \gamma\}$, the image matrix of x will have eigenvalue 1 with multiplicity 2 and all six pair-wise ratios of $\{\alpha, \beta, \gamma\}$, so they are ± 1. For case 4, recall that if λ is an eigenvalue of a symplectic matrix, so is λ^{-1} with the same multiplicity, thus there are candidates for the special element x, but all such elements have the property that the multiplicity for both eigenvalues is 4. Notice by Theorem 3.1 (iv), the multiplicity of the two distinct eigenvalue in $\tilde{\rho}(\sigma_i)$ is 3 and 5, respectively. Case 5 is done just as case 4. This excludes all the unwanted simple groups. We have to consider also the product cases. For product of two or three simple factors, the same analysis of eigenvalues as at the end of the proof of claim 2 excludes them. Actually, there are only four cases here: $SU(2) \times SU(2)$, $SU(2) \times SU(4)$, $SU(2) \times Sp(4)$ and $SU(2) \times SU(2) \times SU(2)$. This completes the proof of our density theorem.

References

[AB] D. Aharanov and M. Ben-Or, *Fault tolerant quantum computation with constant error*, quant-ph/9906129.

[CN] I. Chuang and M. Nielsen, Quantum computation and Quantum information, Cambridge Univ. Press (a book to appear).

[CR] C. Curtis and I. Reiner, *Representation theory of finite groups and associate algebras*, Pure and Applied Math., vol XI, Interscience Publisher, 1962.

[D] D. Deutsch, *Quantum computational networks,* Proc. Roy. Soc. London, **A425**(1989), 73-90.

[Fey] R. Feynman, *Simulating physics with computers,* Int. J. Theor. Phys. **21**(1982), 467-488.

[FKW] M. Freedman, A. Kitaev, and Z. Wang, *Simulation of topological field theories by quantum computers*, quant-ph/0001071.

[Fu] L. Funar, *On the TQFT representations of the mapping class groups*, Pac. J. Math., **188**(1999), 251-274.

[G] R. Gelca, *Topological quantum field theory with corners based on the Kauffmann bracket*, Comment. Math. Helv., **72**(1997), 210-243.

[J1] V.F.R. Jones, *Hecke algebra representations of braid groups and link polynomial,* Ann. Math., **126**(1987), 335-388.

[J2] V.F.R. Jones, *Braid groups, Hecke algebras and type II_1 factors*, Geometric methods in operator algebras, Proc. of the US-Japan Seminar, Kyoto, July 1983.

[KL] L. Kauffmann and S. Lins, *Temperley-Lieb recoupling theory and invariants of 3-manifolds*, Ann. Math. Studies, vol 134, Princeton Univ. Press, 1994.

[Ki] A. Kitaev, *Quantum computations: algorithms and error correction,* Russian Math. Survey, **52:61**(1997), 1191-1249.

[La] S. Lang, *Algebra*, 2nd edition, Addison-Wesley Publishing Company, 1984.

[Ll] S. Lloyd, *Universal quantum simulators,* Science, **273**(1996), 1073-1078.

[MP] W. Mckay and J. Patera, *Tables of dimensions, indices, and branching rules for representations of simple Lie algebras*, Lecture Notes in Pure and Applied Math., vol 69.

[RT] N. Reshetikhin, and V.G. Turaev, *Invariants of* 3*-manifolds via link polynomials and quantum groups*, Invent. Math. **103** (1991), no. 3, 547–597.

[T] V. Turaev, *Quantum invariants of knots and 3-manifolds*, de Gruyter Studies in Math., vol 18, 1994.

[V] V.S. Varadarajan,*Lie groups, Lie algebras and their representaions*, Graduate Texts in Math., vol 102, Springer-Verlag, 1984.

[Wa] K. Walker, *On Witten's 3-manifold invariants,* preprint, 1991.

[We] H. Wenzl, *Hecke algebras of type A_n and subfactors*, Invent. Math. **92**(1988), 349-383.

[Wi] E. Witten, *Quantum field theory and the Jones polynomial,* Comm. Math. Phys., **121**(1989), 351-399.

[Y] A. Yao, *Quantum circuit complexity,* Proc. 34th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 352-361.