Large quantum Fourier transforms are never exactly realized by braiding conformal blocks

Michael H. Freedman[1] and Zhenghan Wang[1,2]
[1]*Microsoft Project Q, Kavli Institute for Theoretical Physics, University of California, Santa Barbara, California 93106-4030, USA*
[2]*Department of Mathematics, Indiana University, Bloomington, Indiana 47405, USA*
(Received 14 August 2006; published 15 March 2007)

Fourier transform is an essential ingredient in Shor's factoring algorithm. In the standard quantum circuit model with the gate set $\{\mathbb{U}(2)$, controlled-NOT$\}$, the discrete Fourier transforms $F_N=(\omega^{ij})_{N\times N}$, $i,j=0,1,\ldots,N-1$, $\omega=e^{2\pi i/N}$, can be realized exactly by quantum circuits of size $O(n^2)$, $n=\ln N$, and so can the discrete sine or cosine transforms. In topological quantum computing, the simplest universal topological quantum computer is based on the Fibonacci (2+1)-topological quantum field theory (TQFT), where the standard quantum circuits are replaced by unitary transformations realized by braiding conformal blocks. We report here that the large Fourier transforms F_N and the discrete sine or cosine transforms can never be realized exactly by braiding conformal blocks for a fixed TQFT. It follows that an approximation is unavoidable in the implementation of Fourier transforms by braiding conformal blocks.

DOI: 10.1103/PhysRevA.75.032322 PACS number(s): 03.67.Lx, 02.40.−k

I. INTRODUCTION

The simplest topological model for quantum computing which can approximate any quantum circuit efficiently by braiding conformal blocks is based on the Fibonacci topological quantum field theory (TQFT) [1]. The corresponding conformal field theories (CFTs) for the Fibonacci TQFT include the level=1 WZW G_2 CFT. TQFTs are low-energy effective theories for topological phases of matter such as fractional quantum Hall (FQH) liquids, where quasiparticles can be anyons, even non-Abelian anyons theoretically. We will use the term anyon loosely here to include also the non-Abelian anyons. On theoretical and numerical grounds it is believed that the Fibonnaci TQFT is an essential part of an effective theory for the FQH liquids at filling fraction $\nu=12/5$ [2,3]. Moore and Read proposed that the ground-state wave functions for anyons localized at fixed positions are given by the conformal blocks of the corresponding conformal field theory [4]. Thus quantum gates in topological quantum computers are the braiding matrices of the conformal blocks, which are also the braiding statistics of anyons.

A decade ago, Shor discovered the polynomial-time quantum algorithm for factoring integers. A key component of Shor's algorithm is the application of the discrete Fourier transforms F_N. It is known that a Fibonacci topological quantum computer can simulate Shor's algorithm efficiently, but the simulation requires approximations of the Fourier transforms [1]. In this paper we present a "no-go" theorem by showing that an approximation is unavoidable. Closely related to the Fourier transforms are the discrete sine or cosine transforms which are also useful for signal processing. Our discussion of Fourier transforms applies equally to those transforms.

As the prospect of a topological quantum computer has attracted increased attention, examination of the programming and compiling issues attendant to this design has begun [5]. Even an accurate (10^{-5}) NOT gate requires several hundred elementary braids according to the known approximation scheme [6]. Audiences seeing such compilations always ask, "yes, but isn't there a better way? Can't the arithmetic properties of Fibonacci anyons be matched to the number theory of factoring?" While efficient factoring is still a theoretical possibility, we show no arithmetic wizardry will create the all-important Fourier, sine, or cosine transforms inside TQFTs.

A TQFT has a finite label set $L=\{a,b,c,\ldots\}$, which physically represents the anyon types in the theory. Then a TQFT is a consistent rule to assign each two-dimensional oriented compact space Σ a vector space $V(\Sigma)$ and each cobordism (M,Σ_1,Σ_2) a linear map $Z(M,\Sigma_1,\Sigma_2):V(\Sigma_1)\to V(\Sigma_2)$—in particular, a projective representation of the mapping class group $\mathbb{M}(\Sigma)$ on $V(\Sigma)$. When Σ has boundaries, the boundaries will be labeled by anyons.

A TQFT is unitary if each vector space $V(\Sigma)$ has a positive definite Hermitian inner product $\langle\cdot,\cdot\rangle_\Sigma$ satisfying the following conditions.

(1) The Hermitian inner product is multiplicative with respect to disjoint union of surfaces, and the inner product on $V(\emptyset)$ for the empty surface $\emptyset$ is 1.

(2) The Hermitian inner product is natural with respect to the mapping class group action.

(3) For any cobordism (M,Σ_1,Σ_2) and any $x\in V(\Sigma_1)$ and $y\in V(\Sigma_2)$, we have

$$\langle Z(M,\Sigma_1,\Sigma_2)(x),y\rangle_{\Sigma_2}=\langle x,Z(\bar{M},\Sigma_2,\Sigma_1)(y)\rangle_{\Sigma_1}.$$

These conditions imply that the projective representations of the mapping class groups are unitary. Furthermore, according to [7] for any TQFT and any surface Σ (if $\partial\Sigma\neq\emptyset$, then $\partial\Sigma$ should be labeled) a spanning set for $V(\Sigma)$ is obtained by the functor V applied to 3-manifolds M containing a labeled trivalent graph with $\partial M=\Sigma$. Thus, for any $x,y\in V(\Sigma)$ with $x=Z(M)$, we have $\langle Z(M),y\rangle_\Sigma=\langle Z(M,\emptyset,\partial M)(1),y\rangle_\Sigma=\langle 1,Z(\bar{M},\partial M,\emptyset)(y)\rangle_\emptyset$. It follows from this identity that any Hermitian structure obeying (1)–(3) above is determined by the operators $Z(\bar{M},\partial M,\emptyset)$, hence unique. We can use the gluing axiom to reduce the computation of the Hermitian inner products for all surfaces to the computation for annuli and pairs of pants. It follows that if all the

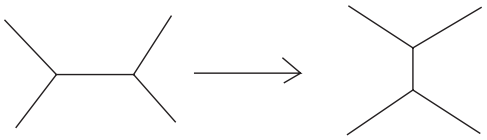

FIG. 1. F moves: the free ends are labeled by anyons.

quantum dimensions of an Hermitian TQFT are positive and the Hermitian products on all pairs of pants are positive definite, then the TQFT is unitary.

II. F MATRICES

Given a unitary TQFT and a four-punctured sphere $S^2_{a,b,c,d}$, where the four punctures are labeled by anyons of types a, b, c, and d. The four-punctured sphere can be divided into two pairs of pants (= three-punctured spheres) in two different ways. In Fig. 1, the four-punctured sphere is the boundary of a thickened neighborhood of the graph in either side and the two graphs encode the two different pants decompositions of the four-punctured sphere. The F move is just the change of the two pants decompositions.

By the axioms of a TQFT, each pants decomposition of $S^2_{a,b,c,d}$ determines an orthonormal basis of $V(S^2_{a,b,c,d})$. Therefore the F move gives rise to a change of orthonormal bases of the same Hilbert space $V(S^2_{a,b,c,d})$, hence induces a unitary matrix $F_{a,b,c,d}$, which is called the F matrix.

From the definition the F matrices are unitary, but it is not obvious that the entries of the F matrices are always algebraic. One of our goals is to show that the entire unitary structure, including the F matrices, is compatible with algebraic choices for all unitary TQFTs. The difficulty lies in the choices of the F matrices as they are basis dependent. The obvious "solution"—solve all complex equations in a TQFT such as the pentagon and hexagon equations for their real and imagine parts independently plus the unitarity constraints for the F matrices—is not sufficient for the compatibility as the condition of being purely real or purely imaginary is not algebraic. Our approach instead is to satisfy the algebraic conditions first for the F matrices with certain normalization and then to deduce unitarity from the normalization.

III. FIBONACCI TQFT

First we recall the data for the Fibonacci TQFT, our chief example. There is only one nontrivial anyon type τ in the theory. We will also use τ to denote the golden ratio $\tau = \frac{1+\sqrt{5}}{2}$, and no confusions should arise.

There are two unitary TQFTs with anyon types $\{1,\tau\}$ and the fusion rule: $\tau \otimes \tau = 1 \oplus \tau$. One is the mirror (or parity reversed) theory of the other. We list the data for one theory and refer to the resulting theory as the Fibonacci TQFT. The data for the other theory are obtained by complex conjugate all the data below.

Anyon types: $\{1,\tau\}$.

Fusion rule: $1 \otimes \tau = \tau \otimes 1 = \tau$, $\tau \otimes \tau = 1 \oplus \tau$.

Quantum dimensions: $\{1,\tau\}$.

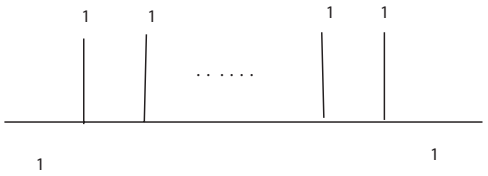

FIG. 2. The basis is in one-to-one correspondence to admissible labelings of the internal edges with 1 or τ subject to the fusion rules at each trivalent vertex. In all figures, label 0 represents type 1, and label 1 represents τ.

Twists: $\theta_1 = 1$, $\theta_\tau = e^{4\pi i/5}$.

Braidings: $R_1^{\tau\tau} = e^{4\pi i/5}$, $R_\tau^{\tau\tau} = e^{7\pi i/5}$.

S matrices: $S_1 = \frac{1}{\sqrt{2+\tau}}\begin{pmatrix} 1 & \tau \\ \tau & -1 \end{pmatrix}$, $S_\tau = (e^{3\pi i/10})$.

Topological degeneracy:

Let $\Sigma_{g,n}$ be the genus$=g$ oriented surface with n boundaries labeled by τ; then, $\dim V(\Sigma_{g,n}) = \frac{\tau^n + (-1)^n \tau^{2-2g-n}}{(\tau+2)^{1-g}}$.

Topological inner product:

The Hilbert space $V(\Sigma_{g,n})$ is spanned by labeled unitrivalent graphs $\{G\}$ in a bounding handlebody $H_{g,n}$ (for simplicity we ignore the framing subtlety.) Given two vectors in $v,w \in V(\Sigma_{g,n})$ represented by two graphs G_v, G_w, then the inner product of v,w is the topological invariant of the 3-manifold M with a trivalent graph G inside obtained from doubling the handlebodies and unitrivalent graphs G_v, G_w: glue the orientation reversed handlebody containing G_v with the handlebody containing G_w by the identity map on their boundaries.

Conformal block basis (Fig. 2):

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

We will refer to this choice of the F matrix as the unitary normalization. Experts know that there is a phase ubiquity in the off-diagonal entry of F if F is only required to be unitary. But the above choice of F is determined if the conformal block basis is further required to be orthogonal to each other with the same norm. To see this, we consider the four-punctured sphere. Computations of the norms of the two basis vectors lead to the value of the θ symbol equal to $\tau^{3/2}$. But the θ symbol can also be calculated directly using the F move. Setting the value to $\tau^{3/2}$ shows that the off-diagonal entry of F is real, hence the unitary normalization.

The braiding of two anyons in a conformal block basis state is represented by the graph in Fig. 3.

To find the matrix elements, we form the inner products of this braided basis with all bases. The topological inner product in the conformal block basis is given by flipping over the first argument and stacking on top of the second argument. Hence the matrix element is an invariant of a trivalent graph

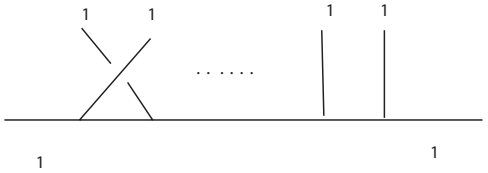

FIG. 3. The braiding is obtained by stacking the braid on top of a conformal block basis, and the braiding matrix is computed by using the graphical calculus.

with certain braidings. Now we observe that the invariant of any such graph is a complex number in the number field $\mathbb{Q}(\sqrt{\tau},\xi_{20})$, where $\xi_{20}=e^{2\pi i/20}$ and $\mathbb{Q}(\sqrt{\tau},\xi_{20})$, an example of a number field, consists of all complex numbers which are rational polynomials in $\sqrt{\tau},\xi_{20}$ with integer coefficients. Therefore, we have the following.

Observation. All matrix entries of the braiding matrices with the above choices of data for the Fibonacci TQFT lie inside the number field $\mathbb{Q}(\sqrt{\tau},\xi_{20})$ whose Galois group is the non-Abelian dihedral group D_4. Furthermore, only (1,2,4,5,10,20)th roots of unity exist in $\mathbb{Q}(\sqrt{\tau},\xi_{20})$.

We will now see that there are only finitely many roots of unity in $\mathbb{Q}(\sqrt{\tau},\xi_{20})$. But to realize all the discrete Fourier transforms F_N, we need infinitely many root of unity; therefore, discrete Fourier transforms F_N for large N cannot be realized exactly by braiding conformal blocks. The roots of unity in $\mathbb{Q}(\sqrt{\tau},\xi_{20})$ determine which Fourier transform can be potentially realized by braiding conformal blocks in the Fibonacci TQFT. The notation below is clarified in below. Notice that $[\mathbb{Q}(\sqrt{\tau},\xi_{20}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{\tau},\xi_{20}):\mathbb{Q}(\xi_{20})][\mathbb{Q}(\xi_{20}):\mathbb{Q}]$. For a primitive mth root of unity ξ_m, $[\mathbb{Q}(\xi_m):\mathbb{Q}]=\phi(m)$, where $\phi(m)$ is the Euler function whose value is the number of integers from 1 to $m-1$, which is relatively prime to m. Since $\tau\in\mathbb{Q}(\xi_{20})$, so $[\mathbb{Q}(\sqrt{\tau},\xi_{20}):\mathbb{Q}(\xi_{20})]=2$ and $[\mathbb{Q}(\xi_{20}):\mathbb{Q}]=\phi(20)=8$. Hence we have $[\mathbb{Q}(\sqrt{\tau},\xi_{20}):\mathbb{Q}]=16$. It follows that there are only finitely many roots of unity in $\mathbb{Q}(\sqrt{\tau},\xi_{20})$ since there are only finitely m such that $\phi(m)\leqslant 16$.

Another consequence of this observation is that the Fibonacci TQFT with the unitary normalization cannot be realized in an Abelian extension of $\mathbb{Q}$ because the Galois group of $\mathbb{Q}(\sqrt{\tau},\xi_{20})$ is non-Abelian. It suffices to show that the Galois group of $\mathbb{Q}(\sqrt{\tau},i)\subset\mathbb{Q}(\sqrt{\tau},\xi_{20})$ is non-Abelian, which is the same as the Galois group for the minimal polynomial of $\sqrt{\tau}\,f(x)=x^4-x^2-1$. To determine the Galois group of $f(x)$, we use the following fact: let $g(x)=x^4+ax^2+b\in\mathbb{Q}(x)$ be irreducible. If neither b nor $b(a^2-4b)$ is a square in $\mathbb{Q}$, then the Galois group of $g(x)$ is the non-Abelian dihedral group D_4. For a proof, see Proposition 4.11 of [8] on p. 273 and Ex. 9 on p. 277. Now it is obvious that the Galois group of $f(x)$ is D_4.

Finally let us determine all the possible roots of unity in $\mathbb{Q}(\sqrt{\tau},\xi_{20})$. If a primitive mth root of unity ξ_m is in $\mathbb{Q}(\sqrt{\tau},\xi_{20})$, then $\phi(m)$ is a factor of 16 because $[\mathbb{Q}(\sqrt{\tau},\xi_{20}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{\tau},\xi_{20}):\mathbb{Q}(\xi_m)][\mathbb{Q}(\xi_m):\mathbb{Q}]=16$. If m is relatively prime to 20 and $\geqslant 7$, then ξ_{20m} would be in $\mathbb{Q}(\sqrt{\tau},\xi_{20})$. But $\phi(20m)=8\phi(m)>16$, a contradiction. It follows that if $\xi_m\in\mathbb{Q}(\sqrt{\tau},\xi_{20})$, then m is of the form $2^k\times 3\times 5$ for possibly $k=1,2,3$. But the first three cannot be a factor m because, otherwise, $\xi_{60}\in\mathbb{Q}(\sqrt{\tau},\xi_{20})$. Since $\mathbb{Q}(\xi_{60})$ would be a subfield of $\mathbb{Q}(\sqrt{\tau},\xi_{20})$, which are both a degree-16 extension of Q, we will have $\mathbb{Q}(\xi_{60})=\mathbb{Q}(\sqrt{\tau},\xi_{20})$. But this is impossible since the Galois group of $\mathbb{Q}(\xi_{60})$ is Abelian, while the Galois group of $\mathbb{Q}(\sqrt{\tau},\xi_{20})$ is non-Abelian. Exactly the same argument will rule out $k=3$ with ξ_{40} replacing ξ_{60}. So the only possible primitive roots of unity in $\mathbb{Q}(\sqrt{\tau},\xi_{20})$ are $\xi_m, m=1,2,4,5,10,20$ and their powers.

Using the relation $\frac{p_+}{D}=e^{2\pi i(c/8)}$, we deduce that the central charges of the corresponding CFTs are $c=14/5$ mod 8, which is realized by the level=1 G_2 CFT. Because the central charges $c\neq 0$, we have to either work with projective representations rather than linear representations of the mapping class groups or work with some central extension of the mapping class groups for extended surfaces. For the torus case, the projective representation can always be lifted to a linear representation as follows: direct computation shows that $(st)^3=\frac{p_+}{D}s^2$, so if we set $\tilde{t}=t\left(\frac{p_+}{D}\right)^{-1/3}$, then $(s\tilde{t})^3=s^2$. It has been shown that a third root of unity of $\frac{p_+}{D}$ is sufficient to lift all projective representations of the mapping class groups to linear representations of the extended mapping class groups [7]. Hence there are at least three different normalizations for a given TQFT, which lead to successively larger number fields.

(1) Arbitrary choice for the F matrices and projective representations for the mapping class groups

(2) Unitary normalization for the F matrices and projective representations for the mapping class groups

(3) Unitary normalization for the F matrices and linear representations for the extended mapping class groups.

For the Fibonacci TQFT, with normalization (1), the Fibonacci TQFT can be described in $\mathbb{Q}(\xi_{20})$; with normalization (2), $\mathbb{Q}(\sqrt{\tau},\xi_{20})$; with normalization (3) $\mathbb{Q}(\sqrt{\tau},\xi_{60})$. Note this field contains ξ_m for all $m|60$ by an argument similar to the one above.

IV. UNITARY TQFTs

Let $\mathbb{Q}$ be the field of the rational numbers (a field here is not in the sense field theory in physics, but as in number theory. A field is a generalization of the number systems $\mathbb{Q},\mathbb{R},\mathbb{C}$.) A number field is a finitely dimensional vector space K over $\mathbb{Q}$ which is a field: a vector space with a compatible multiplication. The field K is called an extension field of $\mathbb{Q}$, and the dimension of K as a vector space over $\mathbb{Q}$ is called the degree of the extension, denoted by $[K:\mathbb{Q}]$. Given a complex number x, $\mathbb{Q}(x)$ is the field of all complex numbers of the form $p(x)/q(x)$, where $p(x),q(x)$ are polynomials in x with coefficients in $\mathbb{Q}$ and $q(x)\neq 0$. For example, $\mathbb{Q}(\sqrt{\tau})$ is a degree=4 extension of $\mathbb{Q}$. Fields can be extended repeatedly as follows: let K be an extension of $\mathbb{Q}$ and y a complex number; then, $K(y)$ is the field of all complex numbers of the form $p(y)/q(y)$, where $p(y),q(y)$ are polynomials in y with coefficients in K and $q(y)\neq 0$. Given two complex numbers x,y, the number field $\mathbb{Q}(x,y)$ is the extension of first $\mathbb{Q}$ to $\mathbb{Q}(x)=K$ or $\mathbb{Q}(y)=K$, then K to $K(y)$ or $K(x)$, which both are $\mathbb{Q}(x,y)$. The degree of the extension is $[\mathbb{Q}(x,y):\mathbb{Q}]=[\mathbb{Q}(x,y):\mathbb{Q}(x)][\mathbb{Q}(x):\mathbb{Q}]=[\mathbb{Q}(x,y):\mathbb{Q}(y)][\mathbb{Q}(y):\mathbb{Q}]$.

V. MAIN RESULTS

(1) Given a unitary TQFT, there is a normalization so that all the entries of the F matrices are in a number field K, and the F matrices associated to the F moves are unitary.

(2) Each Hilbert space $V(\Sigma)$ has an orthonormal basis so that every representation matrix of the mapping class group has entries in the number field K. Warning the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is not necessarily Abelian.

(3) Large Fourier transforms, the discrete sine or cosine transforms cannot be realized exactly in any fixed TQFT by braiding conformal blocks.

Part (3) follows from part (2) as follows. We recall that the number of roots of unity in a number field K is always finite. To see this, the degree of the extension of $\mathbb{Q}(\xi_m), \xi_m = e^{2\pi i/m}$ is $\phi(m)$, where $\phi(m)$ is the Euler function. Therefore if $[K:\mathbb{Q}]=n$ and $\phi(m)>n$, then ξ_m cannot be in K because otherwise the extension degree will be $>n$. Similarly for $\mathbb{Q}[\sin(2\pi/m)]$, $\mathbb{Q}[\cos(2\pi/m)]$.

Part (2) follows from part (1). Given a unitary TQFT, there is a unique way to construct compatible topological inner products for $V(\Sigma)$'s ([7];, Chap. IV, Sec. 10), and we need an explicit orthonormal basis for each $V(\Sigma)$ to compute the braiding matrices. To do this one sets up a graphical calculus so that each matrix entry is an invariant of a certain trivalent graph, which depends on our choices of the F matrices and θ symbols. The theorem is reduced to the careful choices of F matrices and θ symbols which are compatible with the topological inner product. The invariants of such graphs are polynomial of certain roots of unity and $6j$ symbols F_{ijk}^{lmn}. There are three kinds of contributions of roots of unity: the braiding eigenvalues, the twists, and the higher Frobenius-Schur indicators resulting from bending anyon trajectories. They are in some fixed extension of $\mathbb{Q}$ whose degree is determined by the fusion rules through Vafa's theorem. The $6j$ symbols are constrained by the pentagon identities. To have a consistent set of $6j$ symbols F_{ijk}^{lmn} with graphical calculus, it is sufficient to solve the following set of polynomial equations (for easiness of notation we drop the dependence on trivalent vertices):

$$F_{j^*i^*0}^{ijk} = \sqrt{\frac{d_k}{d_i d_j}}\delta_{ijk}, \tag{1}$$

$$F_{\mathrm{kln}}^{ijm} = F_{ijn^*}^{klm^*} = F_{nk^*l^*}^{mij}\sqrt{\frac{d_m d_n}{d_j d_l}}, \tag{2}$$

$$\sum_n F_{kp^*n}^{mlq} F_{mns^*}^{jip} F_{lkr^*}^{js^*n} = F_{q^*kr^*}^{jip} F_{mls^*}^{riq^*}. \tag{3}$$

Any solution of this set of equations will be a consistent choice of $6j$ symbols for the unitary TQFT. Now we cite a theorem in algebraic geometry: the solution to the polynomial equations above is an algebraic variety over $\mathbb{Q}(\sqrt{d_i})$, $i=1,2,\ldots,R$, where R is the number of anyon types. Since this variety has at least one point which gives rise to the TQFT, then there will be also an algebraic point by Theorem 7 on p. 32 of [9]. It follows that every graph invariant will be inside a fixed finite extension of $\mathbb{Q}(\sqrt{d_i})$ and hence in a number field over $\mathbb{Q}$.

The resulting graphical calculus from the solution of the the pentagon equations with the above normalization has very nice properties. The conformal block basis is an orthogonal basis. The θ symbols $\theta(a,b,c)=\sqrt{d_a d_b d_c}$, where d_a, d_b, and d_c are the quantum dimensions of the anyons a, b, and c. One consequence of the θ symbol values is that the conformal block basis elements have the same length, independent of the internal labelings. So the F matrices are a change of basis for two orthonormal bases up to overall scalars, hence are unitary.

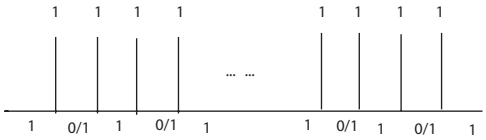

FIG. 4. The edges labeled by 0 or 1 correspond to standard qubits, and other basis span the non-computational subspace which should be evolved by the identity operator ideally in the computational process. Again 0 represents 1 and 1 represents τ.

VI. APPROXIMATION BY A FIBONACCI QUANTUM COMPUTER

Since the exact realization of the Fourier transforms is impossible in the Fibonacci TQFT, we would like to approximate them using braiding matrices. Given a prescribed accuracy, it will be interesting to find the explicit approximations. We will only outline an approximation here.

To simulate a standard n-qubit quantum circuit $U_L:(\mathbb{C}^2)^{\otimes n}\to(\mathbb{C}^2)^{\otimes n}$, we embed $(\mathbb{C}^2)^{\otimes n}$ into the conformal blocks on $2n+2$ Fibonacci anyons at fixed positions. Since $\dim(V_{2n+2})=F_{2n+2}>2^n$ except for $n=1$, we need to choose an efficiently computable subspace of the conformal blocks. One way to do this is to choose the following subspace $(\mathbb{C}^2)^{\otimes n}$ of V_{2n+2} with the conformal block basis (Fig. 4).

Then we look for a braid b so that the following diagram commutes up to the prescribed error, where $\rho(b)$ is the braiding matrix of conformal blocks:

$$\begin{array}{ccc} (\mathbb{C}^2)^{\otimes n} & \to & V_{2n+2} \\ U_L\downarrow & & \downarrow\rho(b) \\ (\mathbb{C}^2)^{\otimes n} & \to & V_{2n+2} \end{array}$$

The standard quantum circuits for the exact realization of the Fourier transforms are given on p. 219 of [6]. Given a precision $\epsilon>0$, then one finds a braid that approximates F_N by using the approximations of the single-qubit gates and controlled-NOT in [5].

VII. CONCLUSION

TQFTs are effective theories for topological phases of matter such as the fractional quantum Hall liquids. Specifically, the braiding matrices of conformal blocks are unitary transformations of the degenerate ground states when anyons are fixed at certain positions. Because polynomial time approximation schemes exist [6], the reported obstruction to exact realization of the Fourier transforms will not impose a fundamental physical constraint on topological quantum computing. However, as a practical matter there is an important distinction between billions as opposed to millions of braid generators to factor a large number.

The Jones braid representation(s) that we get from Fibonacci anyons can be described as a regularized Fourier transform (FTB) of the braid group(s) B_n. The braid genera-

tors correspond to "position" coordinates and the path basis of conformal blocks is a regularized momentum basis for the group algebra of the braid group $\mathbb{C}[B_n]$. The chosen regularization consists of passing to an appropriate semisimple quotient, the Temperley-Lieb algebra $\mathrm{TL}_q^n = \mathbb{C}[B_n]/\sim, q = e^{2\pi i/5}$. We have shown that one cannot find the FT of large cyclic groups inside these FTB. The most direct application of FTB is to the estimation of Jones polynomial evaluations [10,11]. The possibility of harnessing FTB for number theoretic application such as factoring should be explored.

ACKNOWLEDGMENT

This research has been supported by the NSF under Grants Nos. DMR-0130388 and DMR-0354772 (Z.W.).

[1] M. H. Freedman, M. J. Larsen, and Z. Wang, Commun. Math. Phys. **227**, 605 (2002).
[2] E. H. Rezayi and N. Read, e-print cond-mat/0608346.
[3] J. S. Xia *et al.*, Phys. Rev. Lett. **93**, 176809 (2004).
[4] G. Moore and N. Read, Nucl. Phys. B **360**, 362 (1991).
[5] N. E. Bonesteel *et al.*, Phys. Rev. Lett. **95**, 140503 (2005).
[6] M. A. Niesen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[7] V. Turaev, *Quantum Invariants of Knots and 3-manifolds, de Gruyter Studies in Mathematics*, Vol. 18 (Water De Gruyter, Berlin, 1994).
[8] T. W. Hungerford, *Algebra, GTM* (Springer, New York, 1974), Vol. 73.
[9] S. Lang, *Introduction to Algebraic Geometry* (Interscience, New York, 1958).
[10] M. H. Freedman, A. Kitaev, M. Larsen, and Z. Wang, Bull., New Ser., Am. Math. Soc. **40**, 31 (2003).
[11] M. Bordewich, M. Freedman, L. Lovsz, and D. Welsh, Combinatorics, Probab. Comput. **14**, 737 (2005).