Topological quantum computing and SU (2) braid group representations

Article *in* Proceedings of SPIE - The International Society for Optical Engineering · May 2008

DOI: 10.1117/12.778068

2 authors:

Louis Kauffman
University of Illinois at Chicago

Jr. Samuel J. Lomonaco
University of Maryland, Baltimore County

Topological Quantum Computing and $SU(2)$ Braid Group Representations

Louis H. Kauffman[a] and Samuel J. Lomonaco Jr.[b]

[a] Department of Mathematics, Statistics and Computer Science (m/c 249), 851 South Morgan Street, University of Illinois at Chicago, Chicago, Illinois 60607-7045, USA

[b] Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, 1000 Hilltop Circle, Baltimore, MD 21250, USA

ABSTRACT

We study representations of the braid group to $SU(2)$ and their relationships with topological quantum computation.

Keywords: braiding, knotting, linking, spin network, Temperley – Lieb algebra, unitary representation.

1. INTRODUCTION

This paper describes relationships between quantum topology and quantum computing. Quantum topology is, roughly speaking, that part of low-dimensional topology that interacts with statistical and quantum physics. Many invariants of knots, links and three dimensional manifolds have been born of this interaction, and the form of the invariants is closely related to the form of the computation of amplitudes in quantum mechanics. Consequently, it is fruitful to move back and forth between quantum topological methods and the techniques of quantum information theory. In this paper we concentrate on represeentations of the braid group to $SU(2)$ and $U(2)$ with applications to the Fibonacci model for topological quantum computing and to quantum algorithms for computing the Jones polynomial. The present paper is intended as a clarification of material on $SU(2)$ representations of the braid group that we have published elsewhere,[22] and to provide background for the representations used in our paper on a three stranded quantum algorithm for the Jones polynomial.[24]

In quantum computing, the application of topology is most interesting because the simplest non-trivial example of the Temperley–Lieb recoupling Theory gives the so-called Fibonacci model. The recoupling theory yields representations of the Artin braid group into unitary groups $U(n)$ where n is a Fibonacci number. These representations are *dense* in the unitary group, and can be used to model quantum computation universally in terms of representations of the braid group. Hence the term: topological quantum computation.

Here is a very condensed presentation of how unitary representations of the braid group are constructed via topological quantum field theoretic methods. One has a mathematical particle with label P that can interact with itself to produce either itself labeled P or itself with the null label $*$. We shall denote the interaction of two particles P and Q by the expression PQ, but it is understood that the "value" of PQ is the result of the interaction, and this may partake of a number of possibilities. Thus for our particle P, we have that PP may be equal to P or to $*$ in a given situation. When $*$ interacts with P the result is always P. When $*$ interacts with $*$ the result is always $*$. One considers process spaces where a row of particles labeled P can successively interact, subject to the restriction that the end result is P. For example the space $V[(ab)c]$ denotes the space of interactions of three particles labeled P. The particles are placed in the positions a, b, c. Thus we begin with $(PP)P$. In a typical sequence of interactions, the first two P's interact to produce a $*$, and the $*$ interacts with P to produce P.

$$(PP)P \longrightarrow (*)P \longrightarrow P.$$

Further author information: L.H.K. E-mail: kauffman@uic.edu, S.J.L. Jr.: E-mail: lomonaco@umbc.edu

Quantum Information and Computation VI, edited by Eric J. Donkor, Andrew R. Pirich,
Howard E. Brandt, Proc. of SPIE Vol. 6976, 69760M, (2008) · 0277-786X/08/$18 · doi: 10.1117/12.778068

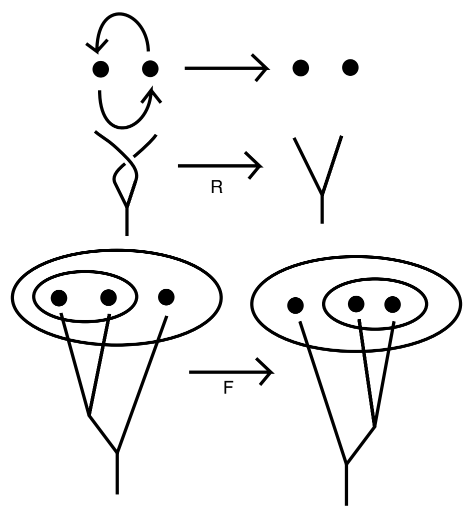

Figure 1. Braiding Anyons

In another possibility, the first two P's interact to produce a P, and the P interacts with P to produce P.

$$(PP)P \longrightarrow (P)P \longrightarrow P.$$

It follows from this analysis that the space of linear combinations of processes $V[(ab)c]$ is two dimensional. The two processes we have just described can be taken to be the qubit basis for this space. One obtains a representation of the three strand Artin braid group on $V[(ab)c]$ by assigning appropriate phase changes to each of the generating processes. One can think of these phases as corresponding to the interchange of the particles labeled a and b in the association $(ab)c$. The other operator for this representation corresponds to the interchange of b and c. This interchange is accomplished by a *unitary change of basis mapping*

$$F : V[(ab)c] \longrightarrow V[a(bc)].$$

If

$$A : V[(ab)c] \longrightarrow V[(ba)c]$$

is the first braiding operator (corresponding to an interchange of the first two particles in the association) then the second operator

$$B : V[(ab)c] \longrightarrow V[(ac)b]$$

is accomplished via the formula $B = F^{-1}RF$ where the R in this formula acts in the second vector space $V[a(bc)]$ to apply the phases for the interchange of b and c. These issues are illustrated in Figure 1, where the parenthesization of the particles is indicated by circles and by also by trees. The trees can be taken to indicate patterns of particle interaction, where two particles interact at the branch of a binary tree to produce the particle product at the root.

In this scheme, vector spaces corresponding to associated strings of particle interactions are interrelated by *recoupling transformations* that generalize the mapping F indicated above. A full representation of the Artin braid group on each space is defined in terms of the local interchange phase gates and the recoupling transformations. These gates and transformations have to satisfy a number of identities in order to produce a well-defined representation of the braid group. These identities were discovered originally in relation to topological quantum field theory. In our approach the structure of phase gates and recoupling transformations arise naturally from the structure of the bracket model for the Jones polynomial. Thus we obtain[22] a knot-theoretic basis for topological quantum computing.

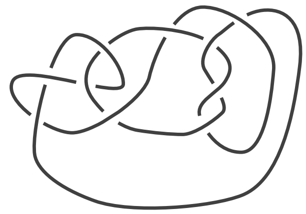

Figure 2. A Knot Diagram

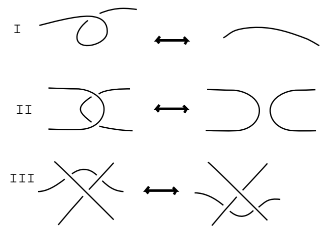

Figure 3. The Reidemeister Moves

In modeling the quantum Hall effect,[3–5, 34] the braiding of quasi-particles (collective excitations) leads to non-trival representations of the Artin braid group. Such particles are called *Anyons*. The braiding in these models is related to topological quantum field theory.

In this paper we concentrate just on those unitary braid representations that arise for $SU(2)$ and we show by elementary means that they all have the form $\{R, F^{-1}RF\}$ although not necessarily coming from a recoupling theory. It is of fundamental interest to see this source of representations and to place it in the context of anyonic quantum computing.

2. KNOTS AND BRAIDS

The purpose of this section is to give a quick introduction to the diagrammatic theory of knots, links and braids. A *knot* is an embedding of a circle in three-dimensional space, taken up to ambient isotopy. The problem of deciding whether two knots are isotopic is an example of a *placement problem*, a problem of studying the topological forms that can be made by placing one space inside another. In the case of knot theory we consider the placements of a circle inside three dimensional space. There are many applications of the theory of knots. Topology is a background for the physical structure of real knots made from rope of cable. As a result, the field of practical knot tying is a field of applied topology that existed well before the mathematical discipline of topology arose. Then again long molecules such as rubber molecules and DNA molecules can be knotted and linked. There have been a number of intense applications of knot theory to the study of DNA[32] and to polymer physics.[25] Knot theory is closely related to theoretical physics as well with applications in quantum gravity[18, 31, 33] and many applications of ideas in physics to the topological structure of knots themselves.[13]

Quantum topology is the study and invention of topological invariants via the use of analogies and techniques from mathematical physics. Many invariants such as the Jones polynomial are constructed via partition functions and generalized quantum amplitudes. As a result, one expects to see relationships between knot theory and physics. In this paper we will study how knot theory can be used to produce unitary representations of the braid group. Such representations can play a fundamental role in quantum computing.

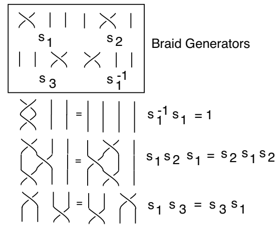

Figure 4. Braid Generators

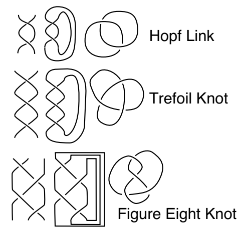

Figure 5. Closing Braids to Form Knots and Links

That is, two knots are regarded as equivalent if one embedding can be obtained from the other through a continuous family of embeddings of circles in three-space. A *link* is an embedding of a disjoint collection of circles, taken up to ambient isotopy. Figure 2 illustrates a diagram for a knot. The diagram is regarded both as a schematic picture of the knot, and as a plane graph with extra structure at the nodes (indicating how the curve of the knot passes over or under itself by standard pictorial conventions).

Ambient isotopy is mathematically the same as the equivalence relation generated on diagrams by the *Reidemeister moves*. These moves are illustrated in Figure 3. Each move is performed on a local part of the diagram that is topologically identical to the part of the diagram illustrated in this figure (these figures are representative examples of the types of Reidemeister moves) without changing the rest of the diagram. The Reidemeister moves are useful in doing combinatorial topology with knots and links, notably in working out the behaviour of knot invariants. A *knot invariant* is a function defined from knots and links to some other mathematical object (such as groups or polynomials or numbers) such that equivalent diagrams are mapped to equivalent objects (isomorphic groups, identical polynomials, identical numbers). The Reidemeister moves are of great use for analyzing the structure of knot invariants and they are closely related to the *Artin braid group*, which we discuss below.

A *braid* is an embedding of a collection of strands that have their ends in two rows of points that are set one above the other with respect to a choice of vertical. The strands are not individually knotted and they are disjoint from one another. See Figures 4 and 5 for illustrations of braids and moves on braids. Braids can be multiplied by attaching the bottom row of one braid to the top row of the other braid. Taken up to ambient isotopy, fixing the endpoints, the braids form a group under this notion of multiplication. In Figure 4 we illustrate the form of the basic generators of the braid group, and the form of the relations among these generators. Figure 5 illustrates how to close a braid by attaching the top strands to the bottom strands by a collection of parallel arcs. A key theorem of Alexander states that every knot or link can be represented as a closed braid. Thus the theory of braids is critical to the theory of knots and links.

Let B_n denote the Artin braid group on n strands. We recall here that B_n is generated by elementary braids $\{s_1, \cdots, s_{n-1}\}$ with relations

1. $s_i s_j = s_j s_i$ for $|i - j| > 1$,

2. $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ for $i = 1, \cdots n-2$.

See Figure 4 for an illustration of the elementary braids and their relations. Note that the braid group has a diagrammatic topological interpretation, where a braid is an intertwining of strands that lead from one set of n points to another set of n points. The braid generators s_i are represented by diagrams where the i-th and $(i+1)$-th strands wind around one another by a single half-twist (the sense of this turn is shown in Figure 4) and all other strands drop straight to the bottom. Braids are diagrammed vertically as in Figure 4, and the products are taken in order from top to bottom. The product of two braid diagrams is accomplished by adjoining the top strands of one braid to the bottom strands of the other braid.

In Figure 4 we have restricted the illustration to the four-stranded braid group B_4. In that figure the three braid generators of B_4 are shown, and then the inverse of the first generator is drawn. Following this, one sees the identities $s_1 s_1^{-1} = 1$ (where the identity element in B_4 consists in four vertical strands), $s_1 s_2 s_1 = s_2 s_1 s_2$, and finally $s_1 s_3 = s_3 s_1$.

Braids are a key structure in mathematics. It is not just that they are a collection of groups with a vivid topological interpretation. From the algebraic point of view the braid groups B_n are important extensions of the symmetric groups S_n. Recall that the symmetric group S_n of all permutations of n distinct objects has presentation as shown below.

1. $s_i^2 = 1$ for $i = 1, \cdots n-1$,
2. $s_i s_j = s_j s_i$ for $|i-j| > 1$,
3. $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ for $i = 1, \cdots n-2$.

Thus S_n is obtained from B_n by setting the square of each braiding generator equal to one. We have an exact sequence of groups

$$1 \longrightarrow B_n \longrightarrow S_n \longrightarrow 1$$

exhibiting the Artin braid group as an extension of the symmetric group.

In the next sections we shall show how representations of the Artin braid group are rich enough to provide a dense set of transformations in the unitary groups. Thus the braid groups are *in principle* fundamental to quantum computation and quantum information theory.

3. $SU(2)$ REPRESENTATIONS OF THE ARTIN BRAID GROUP

The purpose of this section is to determine all the representations of the three strand Artin braid group B_3 to the special unitary group $SU(2)$ and concomitantly to the unitary group $U(2)$. One regards the groups $SU(2)$ and $U(2)$ as acting on a single qubit, and so $U(2)$ is usually regarded as the group of local unitary transformations in a quantum information setting. If one is looking for a coherent way to represent all unitary transformations by way of braids, then $U(2)$ is the place to start. Here we will show that there are many representations of the three-strand braid group that generate a dense subset of $U(2)$. Thus it is a fact that local unitary transformations can be "generated by braids" in many ways.

We begin with the structure of $SU(2)$. A matrix in $SU(2)$ has the form

$$M = \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix},$$

where z and w are complex numbers, and $\bar{z}$ denotes the complex conjugate of z. To be in $SU(2)$ it is required that $Det(M) = 1$ and that $M^{\dagger} = M^{-1}$ where Det denotes determinant, and $M^{\dagger}$ is the conjugate transpose of M. Thus if $z = a + bi$ and $w = c + di$ where a, b, c, d are real numbers, and $i^2 = -1$, then

$$M = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

with $a^2 + b^2 + c^2 + d^2 = 1$. It is convenient to write

$$M = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

and to abbreviate this decomposition as

$$M = a + bi + cj + dk$$

where

$$1 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i \equiv \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j \equiv, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k \equiv \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

so that

$$i^2 = j^2 = k^2 = ijk = -1$$

and

$$ij = k, jk = i, ki = j$$
$$ji = -k, kj = -i, ik = -j.$$

The algebra of $1, i, j, k$ is called the *quaternions* after William Rowan Hamilton who discovered this algebra prior to the discovery of matrix algebra. Thus the unit quaternions are identified with $SU(2)$ in this way. We shall use this identification, and some facts about the quaternions to find the $SU(2)$ representations of braiding. First we recall some facts about the quaternions.

1. Note that if $q = a + bi + cj + dk$ (as above), then $q^{\dagger} = a - bi - cj - dk$ so that $qq^{\dagger} = a^2 + b^2 + c^2 + d^2 = 1$.
2. A general quaternion has the form $q = a + bi + cj + dk$ where the value of $qq^{\dagger} = a^2 + b^2 + c^2 + d^2$, is not fixed to unity. The *length* of q is by definition $\sqrt{qq^{\dagger}}$.
3. A quaternion of the form $ri + sj + tk$ for real numbers r, s, t is said to be a *pure* quaternion. We identify the set of pure quaternions with the vector space of triples (r, s, t) of real numbers R^3.
4. Thus a general quaternion has the form $q = a + bu$ where u is a pure quaternion of unit length and a and b are arbitrary real numbers. A unit quaternion (element of $SU(2)$) has the addition property that $a^2 + b^2 = 1$.
5. If u is a pure unit length quaternion, then $u^2 = -1$. Note that the set of pure unit quaternions forms the two-dimensional sphere $S^2 = \{(r, s, t) | r^2 + s^2 + t^2 = 1\}$ in R^3.
6. If u, v are pure quaternions, then
$$uv = -u \cdot v + u \times v$$
whre $u \cdot v$ is the dot product of the vectors u and v, and $u \times v$ is the vector cross product of u and v. In fact, one can take the definition of quaternion multiplication as
$$(a + bu)(c + dv) = ac + bc(u) + ad(v) + bd(-u \cdot v + u \times v),$$
and all the above properties are consequences of this definition. Note that quaternion multiplication is associative.

7. Let $g = a + bu$ be a unit length quaternion so that $u^2 = -1$ and $a = cos(\theta/2), b = sin(\theta/2)$ for a chosen angle θ. Define $\phi_g : R^3 \longrightarrow R^3$ by the equation $\phi_g(P) = gPg^\dagger$, for P any point in R^3, regarded as a pure quaternion. Then ϕ_g is an orientation preserving rotation of R^3 (hence an element of the rotation group $SO(3)$). Specifically, ϕ_g is a rotation about the axis u by the angle θ. The mapping

$$\phi : SU(2) \longrightarrow SO(3)$$

is a two-to-one surjective map from the special unitary group to the rotation group. In quaternionic form, this result was proved by Hamilton and by Rodrigues in the middle of the nineteeth century. The specific formula for $\phi_g(P)$ as shown below:

$$\phi_g(P) = gPg^{-1} = (a^2 - b^2)P + 2ab(P \times u) + 2(P \cdot u)b^2 u.$$

We want a representation of the three-strand braid group in $SU(2)$. This means that we want a homomorphism $\rho : B_3 \longrightarrow SU(2)$, and hence we want elements $g = \rho(s_1)$ and $h = \rho(s_2)$ in $SU(2)$ representing the braid group generators s_1 and s_2. Since $s_1 s_2 s_1 = s_2 s_1 s_2$ is the generating relation for B_3, the only requirement on g and h is that $ghg = hgh$. We rewrite this relation as $h^{-1}gh = ghg^{-1}$, and analyze its meaning in the unit quaternions.

Suppose that $g = a + bu$ and $h = c + dv$ where u and v are unit pure quaternions so that $a^2 + b^2 = 1$ and $c^2 + d^2 = 1$. then $ghg^{-1} = c + d\phi_g(v)$ and $h^{-1}gh = a + b\phi_{h^{-1}}(u)$. Thus it follows from the braiding relation that $a = c$, $b = \pm d$, and that $\phi_g(v) = \pm\phi_{h^{-1}}(u)$. However, in the case where there is a minus sign we have $g = a + bu$ and $h = a - bv = a + b(-v)$. Thus we can now prove the following Theorem.

Theorem. If $g = a + bu$ and $h = c + dv$ are pure unit quaternions,then, without loss of generality, the braid relation $ghg = hgh$ is true if and only if $h = a + bv$, and $\phi_g(v) = \phi_{h^{-1}}(u)$. Furthermore, given that $g = a + bu$ and $h = a + bv$, the condition $\phi_g(v) = \phi_{h^{-1}}(u)$ is satisfied if and only if

$$bu \cdot bv = a^2 - \frac{1}{2}$$

when $u \neq v$. If $u = v$ then then $g = h$ and the braid relation is trivially satisfied.

Proof. We have proved the first sentence of the Theorem in the discussion prior to its statement. Therefore assume that $g = a + bu, h = a + bv$, and $\phi_g(v) = \phi_{h^{-1}}(u)$. We have already stated the formula for $\phi_g(v)$ in the discussion about quaternions:

$$\phi_g(v) = gvg^{-1} = (a^2 - b^2)v + 2ab(v \times u) + 2(v \cdot u)b^2 u.$$

By the same token, we have

$$\phi_{h^{-1}}(u) = h^{-1}uh = (a^2 - b^2)u + 2ab(u \times -v) + 2(u \cdot (-v))b^2(-v)$$
$$= (a^2 - b^2)u + 2ab(v \times u) + 2(v \cdot u)b^2(v).$$

Hence we require that

$$(a^2 - b^2)v + 2(v \cdot u)b^2 u = (a^2 - b^2)u + 2(v \cdot u)b^2(v).$$

This equation is equivalent to

$$2(u \cdot v)b^2(u - v) = (a^2 - b^2)(u - v).$$

If $u \neq v$, then this implies that $u \cdot v = \frac{a^2 - b^2}{2b^2}$ and this (since $a^2 + b^2 = 1$) is equivalent to

$$bu \cdot bv = a^2 - \frac{1}{2}.$$

This completes the proof of the Theorem.

An Example. Let

$$g = e^{i\theta} = a + bi$$

where $a = cos(\theta)$ and $b = sin(\theta)$. Let

$$h = a + b[(c^2 - s^2)i + 2csk]$$

where $c^2 + s^2 = 1$ and $c^2 - s^2 = \frac{a^2-b^2}{2b^2}$. Then we can rewrite g and h in matrix form as the matrices G and H. Instead of writing the explicit form of H, we write $H = FGF^{\dagger}$ where F is an element of $SU(2)$ as shown below.

$$G = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

$$F = \begin{pmatrix} ic & is \\ is & -ic \end{pmatrix}$$

This representation of braiding where one generator G is a simple matrix of phases, while the other generator $H = FGF^{\dagger}$ is derived from G by conjugation by a unitary matrix, has the possibility for generalization to representations of braid groups (on greater than three strands) to $SU(n)$ or $U(n)$ for n greater than 2. In fact we shall see just such representations constructed later in this paper, by using a version of topological quantum field theory. The simplest example is given by

$$g = e^{7\pi i/10}$$

$$f = i\tau + k\sqrt{\tau}$$

$$h = frf^{-1}$$

where $\tau^2 + \tau = 1$. Then g and h satisfy $ghg = hgh$ and generate a representation of the three-strand braid group that is dense in $SU(2)$. We shall call this the *Fibonacci* representation of B_3 to $SU(2)$.

Density. Consider representations of B_3 into $SU(2)$ produced by the method of this section. That is consider the subgroup $SU[G, H]$ of $SU(2)$ generated by a pair of elements $\{g, h\}$ such that $ghg = hgh$. We wish to understand when such a representation will be dense in $SU(2)$. By finding two elements A and B in the representation such that the powers of A are dense in the rotations about its axis, and the powers of B are dense in the rotations about its axis, and such that the axes of A and B are linearly independent in R^3, one can verify the density of the representation. The set of elements $A^{a+c}B^bA^{a-c}$ are dense in $SU(2)$. It follows for example, that the Fibonacci representation described above is dense in $SU(2)$, and indeed the generic representation of B_3 into $SU(2)$ will be dense in $SU(2)$.

3.1. A Special Unitary Representation of B_3 from Dirac Ket-Bras

The idea behind the construction of this representation depends upon the algebra generated by two single qubit density matrices (ket-bras). Let $|v\rangle$ and $|w\rangle$ be two qubits in V, a complex vector space of dimension two over the complex numbers. Let $P = |v\rangle\langle v|$ and $Q = |w\rangle\langle w|$ be the corresponding ket-bras. Note that

$$P^2 = |v|^2 P,$$

$$Q^2 = |w|^2 Q,$$

$$PQP = |\langle v|w\rangle|^2 P,$$

$$QPQ = |\langle v|w\rangle|^2 Q.$$

P and Q generate a representation of the Temperley-Lieb algebra. One can adjust parameters to make a representation of the three-strand braid group in the form

$$s_1 \longmapsto rP + sI,$$

$$s_2 \longmapsto tQ + uI,$$

where I is the identity mapping on V and r, s, t, u are suitably chosen scalars. In the following we use this method to adjust such a representation so that it is unitary. Note also that this is a local unitary representation of B_3 to $U(2)$. We leave it as an exersise for the reader to verify that it fits into our general classification of such representations as given in section 3 of the present paper.

Here is a specific representation depending on two symmetric matrices U_1 and U_2 with

$$U_1 = \begin{bmatrix} d & 0 \\ 0 & 0 \end{bmatrix} = d|w\rangle\langle w|$$

and

$$U_2 = \begin{bmatrix} d^{-1} & \sqrt{1-d^{-2}} \\ \sqrt{1-d^{-2}} & d-d^{-1} \end{bmatrix} = d|v\rangle\langle v|$$

where $w = (1, 0)$, and $v = (d^{-1}, \sqrt{1-d^{-2}})$, assuming the entries of v are real. Note that $U_1^2 = dU_1$ and $U_2^2 = dU_1$. Moreover, $U_1U_2U_1 = U_1$ and $U_2U_1U_2 = U_1$. This is an example of a specific representation of the Temperley-Lieb algebra.[9, 11] The desired representation of the Artin braid group is given on the two braid generators for the three strand braid group by the equations:

$$\Phi(s_1) = AI + A^{-1}U_1,$$
$$\Phi(s_2) = AI + A^{-1}U_2.$$

Here I denotes the 2×2 identity matrix.

For any A with $d = -A^2 - A^{-2}$ these formulas define a representation of the braid group. With $A = e^{i\theta}$, we have $d = -2cos(2\theta)$. We find a specific range of angles θ in the following disjoint union of angular intervals

$$\theta \in [0, \pi/6] \sqcup [\pi/3, 2\pi/3] \sqcup [5\pi/6, 7\pi/6] \sqcup [4\pi/3, 5\pi/3] \sqcup [11\pi/6, 2\pi]$$

that give unitary representations of the three-strand braid group. Thus a specialization of a more general represention of the braid group gives rise to a continuous family of unitary representations of the braid group.

Remark. We can now see how this representation via ket-brass fits into the quaternionic analysis with which we began this section. We will work with the specific matrix representation above, but it is easy to see that there is no loss in generality. First note that $Det(\Phi(s_1)) = Det(\Phi(s_2)) = -A^{-2}$, where $Det(M)$ denotes the determinant of the matrix M. This means that if we define $G = iA\Phi(s_1)$ and $H = iA\Phi(s_2)$, then G and H will be elements of $SU(2)$ that satisfy the braiding relation $GHG = HGH$, under the above assumptions about the range of θ. It is then easy to see that, in our notation for $g = a + bu$ and $h = a + bv$ we have $bu \cdot bv = (d + cos(2\theta))(d^{-1} + cos(2\theta))$ while $a = -sin(2\theta)$. Thus, with $d = -2cos(2\theta)$ we indeed have the relation $bu \cdot bv = a^2 - \frac{1}{2}$. This shows how this relation fits into our general scheme. In the next sections we recall how this ket-bra representation is related to a quantum algorithm for the Jones polynonmial.

4. THE BRACKET POLYNOMIAL AND THE JONES POLYNOMIAL

We now discuss the Jones polynomial. We shall construct the Jones polynomial by using the bracket state summation model.[9] The bracket polynomial, invariant under Reidmeister moves II and III, can be normalized to give an invariant of all three Reidemeister moves. This normalized invariant, with a change of variable, is the Jones polynomial.[7, 8] The Jones polynomial was originally discovered by a different method than the one given here.

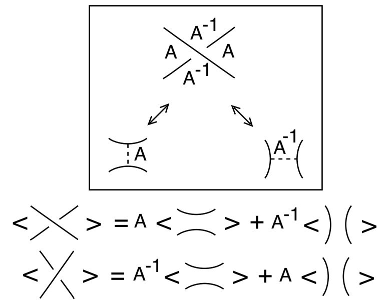

Figure 6. Bracket Smoothings

The *bracket polynomial* , $< K > = < K > (A)$, assigns to each unoriented link diagram K a Laurent polynomial in the variable A, such that

1. If K and K' are regularly isotopic diagrams, then $< K > = < K' >$.
2. If $K \sqcup O$ denotes the disjoint union of K with an extra unknotted and unlinked component O (also called 'loop' or 'simple closed curve' or 'Jordan curve'), then
$$< K \sqcup O > = \delta < K >,$$
where
$$\delta = -A^2 - A^{-2}.$$
3. $< K >$ satisfies the following formulas
$$< \chi > = A < \asymp > + A^{-1} <)(>$$
$$< \overline{\chi} > = A^{-1} < \asymp > + A <)(>,$$

where the small diagrams represent parts of larger diagrams that are identical except at the site indicated in the bracket. We take the convention that the letter chi, χ, denotes a crossing where *the curved line is crossing over the straight segment.* The barred letter denotes the switch of this crossing, where *the curved line is undercrossing the straight segment.* See Figure 6 for a graphic illustration of this relation, and an indication of the convention for choosing the labels A and A^{-1} at a given crossing.

It is easy to see that Properties 2 and 3 define the calculation of the bracket on arbitrary link diagrams. The choices of coefficients (A and A^{-1}) and the value of δ make the bracket invariant under the Reidemeister moves II and III. Thus Property 1 is a consequence of the other two properties.

In computing the bracket, one finds the following behaviour under Reidemeister move I:
$$< \gamma > = -A^3 < \smile >$$
and
$$< \overline{\gamma} > = -A^{-3} < \smile >$$
where γ denotes a curl of positive type as indicated in Figure 7, and $\overline{\gamma}$ indicates a curl of negative type, as also seen in this figure. The type of a curl is the sign of the crossing when we orient it locally. Our convention of signs is also given in Figure 7. Note that the type of a curl does not depend on the orientation we choose. The small arcs on the right hand side of these formulas indicate the removal of the curl from the corresponding diagram.

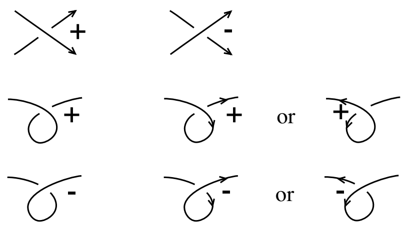

Figure 7. Crossing Signs and Curls

The bracket is invariant under regular isotopy and can be normalized to an invariant of ambient isotopy by the definition

$$f_K(A) = (-A^3)^{-w(K)} < K > (A),$$

where we chose an orientation for K, and where $w(K)$ is the sum of the crossing signs of the oriented link K. $w(K)$ is called the *writhe* of K. The convention for crossing signs is shown in Figure 7.

Remark. By a change of variables one obtains the original Jones polynomial, $V_K(t)$, for oriented knots and links from the normalized bracket:

$$V_K(t) = f_K(t^{-\frac{1}{4}}).$$

4.1. Quantum Computation of the Jones Polynomial

Quantum algorithms for computing the Jones polynomial have been discussed elsewhere. See.[1, 2, 14, 21, 23] Here, as an example, we give a local unitary representation that can be used to compute the Jones polynomial for closures of 3-braids. We analyze this representation by making explicit how the bracket polynomial is computed from it, and showing how the quantum computation devolves to finding the trace of a unitary transformation.

We now use the ket-bra construction for a unitary braid group representation that was discussed in Section 3. Recall that this representation depends on two symmetric matrices U_1 and U_2 with

$$U_1 = \begin{bmatrix} d & 0 \\ 0 & 0 \end{bmatrix} = d|w\rangle\langle w|$$

and

$$U_2 = \begin{bmatrix} d^{-1} & \sqrt{1-d^{-2}} \\ \sqrt{1-d^{-2}} & d-d^{-1} \end{bmatrix} = d|v\rangle\langle v|$$

where $w = (1, 0)$, and $v = (d^{-1}, \sqrt{1-d^{-2}})$, assuming the entries of v are real. The representation of the Artin braid group is given by the equations:

$$\Phi(s_1) = AI + A^{-1}U_1,$$
$$\Phi(s_2) = AI + A^{-1}U_2.$$

Here I denotes the 2×2 identity matrix.

Lemma. Note that the traces of these matrices are given by the formulas $tr(U_1) = tr(U_2) = d$ while $tr(U_1U_2) = tr(U_2U_1) = 1$. If b is any braid, let $I(b)$ denote the sum of the exponents in the braid word that expresses b. For b a three-strand braid, it follows that

$$\Phi(b) = A^{I(b)}I + \Pi(b)$$

where I is the 2×2 identity matrix and $\Pi(b)$ is a sum of products in the Temperley-Lieb algebra involving U_1 and U_2.

Since the Temperley-Lieb algebra in this dimension is generated by I,U_1, U_2, U_1U_2 and U_2U_1, it follows that the value of the bracket polynomial of the closure of the braid b, denoted $<\overline{b}>$, can be calculated directly from the trace of this representation, except for the part involving the identity matrix. The result is the equation

$$<\overline{b}>= A^{I(b)}d^2 + tr(\Pi(b))$$

where $\overline{b}$ denotes the standard braid closure of b, and the sharp brackets denote the bracket polynomial. From this we see at once that

$$<\overline{b}>= tr(\Phi(b)) + A^{I(b)}(d^2 - 2).$$

It follows from this calculation that the question of computing the bracket polynomial for the closure of the three-strand braid b is mathematically equivalent to the problem of computing the trace of the unitary matrix $\Phi(b)$.

For more information about the corresponding algorithm for computing the Jones polynomial, see.[24] Our purpose, in this paper, has been to place the representation structure for our three-stranded algorithm in the context of all possible unitary representations of B_3 to $U(2)$. In a sequel to this paper, we shall study these relations with the unitary groups in more depth.

REFERENCES

1. D. Aharonov, V. Jones, Z. Landau, A polynomial quantum algorithm for approximating the Jones polynomial, quant-ph/0511096.
2. D. Aharonov, I. Arad, The BQP-hardness of approximating the Jones polynomial, quant-ph/0605181.
3. N. E. Bonesteel, L. Hormozi, G. Zikos and S. H. Simon, Braid topologies for quantum computation, quant-ph/0505665.
4. S. H. Simon, N. E. Bonesteel, M. H. Freedman, N. Petrovic and L. Hormozi, Topological quantum computing with only one mobile quasiparticle, quant-ph/0509175.
5. E. Fradkin and P. Fendley, Realizing non-abelian statistics in time-reversal invariant systems, Theory Seminar, Physics Department, UIUC, 4/25/2005.
6. V.F.R. Jones, A polynomial invariant for links via von Neumann algebras, Bull. Amer. Math. Soc. **129** (1985), 103–112.
7. V.F.R.Jones. Hecke algebra representations of braid groups and link polynomials. Ann. of Math. 126 (1987), pp. 335-338.
8. V.F.R.Jones. On knot invariants related to some statistical mechanics models. Pacific J. Math., vol. 137, no. 2 (1989), pp. 311-334.
9. L.H. Kauffman, State models and the Jones polynomial, Topology **26** (1987), 395–407.
10. L.H. Kauffman, Statistical mechanics and the Jones polynomial, AMS Contemp. Math. Series **78** (1989), 263–297.
11. L.H. Kauffman, *Temperley-Lieb Recoupling Theory and Invariants of Three-Manifolds*, Princeton University Press, Annals Studies **114** (1994).
12. L.H.Kauffman, New invariants in the theory of knots, *Amer. Math. Monthly*, Vol.95,No.3,March 1988. pp 195-242.
13. L.H. Kauffman, *Knots and Physics*, World Scientific Publishers (1991), Second Edition (1993), Third Edition (2002).
14. L.H. Kauffman, Quantum computing and the Jones polynomial, math.QA/0105255, in *Quantum Computation and Information*, S. Lomonaco, Jr. (ed.), AMS CONM/305, 2002, pp. 101–137.
15. L.H. Kauffman and S. J. Lomonaco Jr., Quantum entanglement and topological entanglement, New Journal of Physics **4** (2002), 73.1–73.18 (http://www.njp.org/).
16. L. H. Kauffman, Teleportation Topology, quant-ph/0407224, (in the Proceedings of the 2004 Byelorus Conference on Quantum Optics), *Opt. Spectrosc.* 9, 2005, 227-232.

17. L. H. Kauffman, math.GN/0410329, Knot diagrammatics. "Handbook of Knot Theory“, edited by Menasco and Thistlethwaite, 233–318, Elsevier B. V., Amsterdam, 2005.
18. L. H. Kauffman and T. Liko, hep-th/0505069, Knot theory and a physical state of quantum gravity, *Classical and Quantum Gravity*, Vol 23, ppR63 (2006).
19. L.H. Kauffman and S. J. Lomonaco Jr., Entanglement Criteria - Quantum and Topological, in *Quantum Information and Computation - Spie Proceedings, 21-22 April, 2003, Orlando, FL*, Donkor, Pinch and Brandt (eds.), Volume 5105, pp. 51–58.
20. L. H. Kauffman and S. J. Lomonaco Jr., Quantum knots, in *Quantum Information and Computation II, Proceedings of Spie, 12 -14 April 2004* (2004), ed. by Donkor Pirich and Brandt, pp. 268-284.
21. L. H. Kauffman and S. J. Lomonaco, Braiding Operators are Universal Quantum Gates, New Journal of Physics 6 (2004) 134, pp. 1-39.
22. L. H. Kauffman and S. J. Lomonaco Jr., q - Deformed Spin Networks, Knot Polynomials and Anyonic Topological Quantum Computation, *J. Knot Theory Ramifications* 16 (2007), no. 3, 267–332. quant-ph/0606114.
23. L. H. Kauffman and S. J. Lomonaco Jr., Topological quantum computing and the Jones polynomial, quant-ph/0605004.
24. L. H. Kauffman and S. J. Lomonaco Jr., A Three-stranded quantum algorithm for the Jones polynonmial, to appear in "Quantum Information and Quantum Computation V", (Proceedings of Spie, April 2007) edited by E.J. Donkor, A.R. Pirich and H.E. Brandt, Intl Soc. Opt. Eng. quant-ph/0706.0021.
25. L. H. Kauffman (editor), "Knots and Applications", (1996) World Scientific Pub. Co.
26. A. Kitaev, Anyons in an exactly solved model and beyond, *arXiv.cond-mat/0506438 v1 17 June 2005.*
27. G. Moore and N. Seiberg, Classical and quantum conformal field theory, *Comm. Math. Phys.* **123** (1989), no. 2, 177-254.
28. M. A. Nielsen and I. L. Chuang, " Quantum Computation and Quantum Information," Cambrige University Press, Cambridge (2000).
29. R. Penrose, Angular momentum: An approach to Combinatorial Spacetime, In *Quantum Theory and Beyond*, edited by T. Bastin, Cambridge University Press (1969).
30. J. Preskill, Topological computing for beginners, (slide presentation), Lecture Notes for Chapter 9 - Physics 219 - Quantum Computation. *http://www.iqi.caltech.edu/ preskill/ph219*
31. C. Rovelli and L. Smolin, Spin networks and quantum gravity, *Phys Rev. D* 52 (1995), 5743-5759.
32. C. Ernst, D.W. Sumners, A calculus for rational tangles: Applications to DNA Recombination, *Math. Proc. Camb. Phil. Soc.*, **108** (1990), 489-515.
33. Lee Smolin, Link polynomials and critical points of the Chern-Simons path integrals, *Mod. Phys. Lett. A*, Vol. 4,No. 12, 1989, pp. 1091-1112.
34. F. Wilczek, *Fractional Statistics and Anyon Superconductivity,* World Scientific Publishing Company (1990).
35. E. Witten, Quantum field Theory and the Jones Polynomial, *Commun. Math. Phys.*,vol. 121, 1989, pp. 351-399.