New Journal of Physics
The open–access journal for physics

Braiding operators are universal quantum gates

Louis H Kauffman[1] **and Samuel J Lomonaco Jr**[2]

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

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

E-mail: kauffman@uic.edu and lomonaco@umbc.edu

New Journal of Physics **6** (2004) 134
Received 21 May 2004
Published 19 October 2004
Online at http://www.njp.org/
doi:10.1088/1367-2630/6/1/134

Abstract. This paper explores the role of unitary braiding operators in quantum computing. We show that a single specific solution R (the Bell basis change matrix) of the Yang–Baxter equation is a universal gate for quantum computing, in the presence of local unitary transformations. We show that this same R generates a new non-trivial invariant of braids, knots and links. Other solutions of the Yang–Baxter equation are also shown to be universal for quantum computation. The paper discusses these results in the context of comparing quantum and topological points of view. In particular, we discuss quantum computation of link invariants, the relationship between quantum entanglement and topological entanglement, and the structure of braiding in a topological quantum field theory.

PII: S1367-2630(04)81066-8

Contents

1. Introduction

It is a challenge to unravel the relationships among quantum entanglement, topological entanglement and quantum computation. In this paper, we show some of the pieces in this puzzle and how they fit together. In no way do we claim to have assembled the entire puzzle! That is a challenge for futher work. In order to introduce our problems, and explain what we have done with them, the next few paragraphs will give capsule summaries of each of the major points of view taken in this study. We then describe in more detail what is contained in each separate section of the paper. The paper strives to be self-contained, and to describe carefully the issues involved, particularly with topological structures that may be unfamiliar to a physics audience.

Quantum computing can be regarded as a study of the structure of the preparation, evolution and measurement of quantum systems. In the quantum computation model, an evolution is a composition of unitary transformations (finite dimensional over the complex numbers). The unitary transformations are applied to an initial state vector that has been prepared for this process. Measurements are projections to elements of an orthonormal basis of the space upon which the evolution is applied. The result of measuring a state $|\psi\rangle$, written in the given basis, is probabilistic. The probability of obtaining a given basis element from the measurement is equal to the absolute square of the coefficient of that basis element in the state being measured.

It is remarkable that the above lines constitute an essential summary of quantum theory. All applications of quantum theory involve filling in details of unitary evolutions and specifics of preparations and measurements.

One hopes to build powerful quantum computers. Such hopes would be realized if there were reliable ways to implement predetermined patterns of unitary evolution and measurement. In the course of trying to understand the potential for quantum computing, it became apparent that arbitrary finite dimensional unitary transformations can be built from a relatively small set of primitives. A standard set of primitives consists in all two-dimensional unitary transformations, together with a choice of one sufficiently robust four-dimensional transformation such as the *CNOT* gate discussed in the first section of this paper. One says that *CNOT*, together with single qubit gates (two-dimensional unitary transformations) is *universal* for quantum computation.

Probability in quantum mechanics acts quite differently from classical probability. Entangled quantum states embody this difference. An example of an entangled state is the two-qubit state $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. This state is not decomposable as a tensor product of single-qubit states, and a measurement in one of its tensor factors will determine the outcome in the other factor. Implicit in entanglement is the phenomenon of quantum non-locality: physical access to the measurement of one tensor factor or the other may be separated by an arbitrary spatial interval. The result of a measurement can have the appearance of instantaneous determination across an arbitrary distance.

Entanglement and quantum computing are related in a myriad of ways, not the least of which is the fact that one can replace the *CNOT* gate by another gate R and maintain universality (as described above) just so long as R can entangle quantum states. That is, R can be applied to some unentangled state to produce an entangled state. It is of interest to examine other sets of universal primitives that are obtained by replacing *CNOT* by such an R.

Contemplating the inherent non-locality of entangled states, it is natural to ask whether there are relationships between topological entanglement and quantum entanglement. Topology studies global relationships in spaces, and how one space can be placed within another, such as knotting and linking of curves in three-dimensional space. One way to study topological entanglement and quantum entanglement is to try making direct correspondences between patterns of topological linking and entangled quantum states. One approach of this kind was initiated by Aravind as we discuss in section 8 of this paper and also in [1, 2]. A deeper method (we believe) is to consider unitary gates R that are both universal for quantum computation and are also solutions to the condition for topological braiding. Such matrices R are unitary solutions to the Yang–Baxter equation, as explained in section 2. We are then in a position to compare the topological and quantum properties of these transformations. In this way, we can explore the apparently complex relationship among topological entanglement, quantum entanglement, and quantum computational universality. It is this exploration that is the theme of this paper.

In this paper, we prove that certain solutions of the Yang–Baxter equation together with local unitary two-dimensional operators form a universal set of quantum gates. In the first version of this result, we generate *CNOT* using a solution to the algebraic Yang–Baxter equation. In the second version, we generate *CNOT* using versions of the braiding Yang–Baxter equation. Results of this kind follow from general results of the Brylinskis [3] about universal quantum gates. Here, we give explicit proofs by expressing the *CNOT* gate in terms of solutions to the Yang–Baxter equation (and local unitary transformations).

Section 2 of the paper defines the Yang–Baxter equation, gives unitary examples and proves the results about universal gates. We regard these results as a significant elementary step in relating quantum topology and quantum computing. The results say that quantum computing can be framed in the context of quantum topology. They also say that quantum computing can be

framed in those statistical mechanics contexts where the solutions to the Yang–Baxter equation are natural structures.

Certainly the Yang–Baxter equation is a natural structure in thinking about the topology of braids, knots and links. In section 3, we formalize an extension of the Artin braid group that can accomodate local operators so that this extended braid group can represent any unitary transformantion. Section 3 shows how to use solutions to the Yang–Baxter equation to obtain such representations. The section ends with a discussion of the role of the algebraic Yang–Baxter equation in configuring quantum circuit diagrams.

In section 4, we work out details of the invariant of knots and links that is associated with the universal gate R, and give a number of examples. In particular, we show that this invariant measures the linking of the Borromean Rings and the Whitehead Link, both examples of links with zero linking numbers.

In section 5, we indicate how to formulate a quantum computation of a quantum link invariant in terms of a preparation, a unitary evolution and a measurement. We include in this context a process that quantum computes the absolute value of the trace of an arbitrary unitary transformation. These ideas are applied in section 7 first to a unitary representation of the three strand braid group that will produce a good chunk of the Jones polynomial for three strand braids when configured as a quantum computer, and then to the invariant discussed in section 4.

Entanglement is an integral ingredient in certain communications procedures such as the teleportation of quantum states. In section 6 we digress on the structure of teleportation, using the ideas presented in the previous section for obtaining the trace of a unitary transformation. By associating a matrix M to a measurement state $\langle \mathcal{M}|$ and using the entangled state $|\delta\rangle$ used for preparation in the trace calculation of the previous section, we show that for unitary M there is a full teleportation procedure for obtaining $M|\psi\rangle$ from a given state $|\psi\rangle$. This discussion will be expanded in subsequent papers to deal with the question of quantum computation in general, and the specific problem of computing knot invariants that are based on non-unitary solutions to the Yang–Baxter equation. The approach to teleportation given here is inherently topological (in the diagrammatic sense) and we shall take up its applications in subsequent papers [4].

In section 8 we discuss the relationship between topological entanglement and quantum entanglement. We recall an invariant of links associated with the solution to the Yang–Baxter equation used for theorem 1. This solution, R', makes an invariant that detects linking numbers of two-component links exactly when R' is capable of entangling quantum states. Examples like this, and invariants like the one constructed via the matrix R, indicate relationships between topological entanglement and quantum entanglement. Other examples, such as the braid group representation representing the Jones polynomial of section 4, do not exhibit such behaviour. The question remains open. In this section we give an example that effectively destroys the hope of continuing an analogy of Aravind that would identify the cutting of a link component with an observation of a state. Aravind himself showed that his notion was not invariant under basis change. We point out that it is easy to build states whose entanglement or lack of it after an observation is a matter of probability obtained from a probability amplitude. Since linking of classical links is not a matter of probability, this destroys the possibility of a direct relationship between classical linking and quantum entanglement. Of course, there may be more subtle avenues. We are in the process of working on such ideas.

Section 9 is a capsule summary of topological quantum field theory from the point of view of anyonic models for quantum computation. We have included this section to indicate how

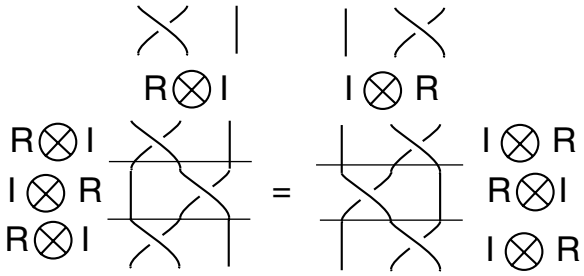

Figure 1. The Yang–Baxter equation $(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I) \times (I \otimes R)$.

braiding gates fit into a wider context. In section 10, we carry on a philosophical discussion about the relationship of quantum and topological entanglement, speculating that a spin network pregeometry of the right kind could enlighten us in our quest.

2. Braiding operators and universal gates

We shall assume that the reader is familiar with the notions of knots, links and braids in Euclidean three-dimensional space. Recall that a knot is an embedding of a circle, taken up to topological equivalence, and that a link is an embedding of a collection of circles, taken up to topological equivalence. Braids form a group under concatenation, where the concatenation of two braids is obtained by attaching the bottom strands of the first braid to the top strands of the second braid.

A class of invariants of knots and links called quantum invariants can be constructed by using representations of the Artin braid group, and more specifically by using solutions to the Yang–Baxter equation [5], first discovered in relation to (1 + 1)-dimensional quantum field theory, and two-dimensional statistical mechanics. Braiding operators feature in constructing representations of the Artin braid group, and in the construction of these invariants of knots and links.

A key concept in the construction of quantum link invariants is the association of a Yang–Baxter operator R to each elementary crossing in a link diagram. The operator R is a linear mapping

$$R : V \otimes V \longrightarrow V \otimes V$$

defined on the 2-fold tensor product of a vector space V, generalizing the permutation of the factors (i.e., generalizing a swap gate when V represents one qubit). Such transformations are not necessarily unitary in topological applications. It is a motivation for our research to understand when they can be replaced by unitary transformations for the purpose of quantum computing. Such unitary R-matrices can be used to make unitary representations of the Artin braid group.

A solution to the Yang–Baxter equation, as described in the last paragraph, is a matrix R, regarded as a mapping of a two-fold tensor product of a vector space $V \otimes V$ to itself that satisfies the equation

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R).$$

From the point of view of topology, the matrix R is regarded as representing an elementary bit of braiding represented by one string crossing over another. In figure 1 below, we have illustrated

the braiding identity that corresponds to the Yang–Baxter equation. Each braiding picture with its three input lines (below) and output lines (above) corresponds to a mapping of the three-fold tensor product of the vector space V to itself, as required by the algebraic equation quoted above. The pattern of placement of the crossings in the diagram corresponds to the factors $R \otimes I$ and $I \otimes R$. This crucial topological move has an algebraic expression in terms of such a matrix R. Our main approach to relate topology, quantum computing, and quantum entanglement is through the use of the Yang–Baxter equation. In order to accomplish this aim, *we need to study solutions of the Yang–Baxter equation that are unitary.* Then the R matrix can be seen *either* as a braiding matrix *or* as a quantum gate in a quantum computer.

The problem of finding solutions to the Yang–Baxter equation that are unitary turns out to be surprisingly difficult. Dye [6] has classified all such matrices of size 4×4. A rough summary of her classification is that all 4×4 unitary solutions to the Yang–Baxter equation are similar to one of the following types of matrix:

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

$$R' = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & 0 & d \end{pmatrix}, \qquad R'' = \begin{pmatrix} 0 & 0 & 0 & a \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ d & 0 & 0 & 0 \end{pmatrix},$$

where a, b, c and d are unit complex numbers.

For the purpose of quantum computing, one should regard each matrix as acting on the standard basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ of $H = V \otimes V$, where V is a two-dimensional complex vector space. Then, for example, we have

$$R|00\rangle = (1/\sqrt{2})|00\rangle - (1/\sqrt{2})|11\rangle, \qquad R|01\rangle = (1/\sqrt{2})|01\rangle + (1/\sqrt{2})|10\rangle,$$

$$R|10\rangle = -(1/\sqrt{2})|01\rangle + (1/\sqrt{2})|10\rangle, \qquad R|11\rangle = (1/\sqrt{2})|00\rangle + (1/\sqrt{2})|11\rangle.$$

The reader should note that R is the familiar change-of-basis matrix from the standard basis to the Bell basis of entangled states.

In the case of R', we have

$$R'|00\rangle = a|00\rangle, \qquad R'|01\rangle = c|10\rangle, \qquad R'|10\rangle = b|01\rangle, \qquad R'|11\rangle = d|11\rangle.$$

Note that R' can be regarded as a diagonal phase gate P, composed with a swap gate S.

$$P = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Compositions of solutions of the (braiding) Yang–Baxter equation with the swap gate S are called *solutions to the algebraic Yang–Baxter equation*. Thus the diagonal matrix P is a solution to the algebraic Yang–Baxter equation.

2.1. Universal gates

A *two-qubit gate* G is a unitary linear mapping $G : V \otimes V \longrightarrow V$ where V is a two complex dimensional vector space. We say that the gate G is *universal for quantum computation* (or just *universal*) if G together with local unitary transformations (unitary transformations from V to V) generates all unitary transformations of the complex vector space of dimension 2^n to itself. It is well known [7] that *CNOT* is a universal gate.

A gate G, as above, is said to be *entangling* if there is a vector

$$|\alpha\beta\rangle = |\alpha\rangle \otimes |\beta\rangle \in V \otimes V$$

such that $G|\alpha\beta\rangle$ is not decomposable as a tensor product of two qubits. Under these circumstances, one says that $G|\alpha\beta\rangle$ is *entangled*.

In [3], the Brylinskis give a general criterion of G to be universal. They prove that *a two-qubit gate G is universal if and only if it is entangling*.

The reader will also be interested in the paper [8] and the url http://www.physics.uq.edu.au/gqc/, wherein the practical algorithm in [8], for expressing entangling gates in terms of *CNOT* and local transformations, is implemented online.

It follows at once from the Brylinski theorem that the matrices R, R', and R'' are universal gates, except for certain specific choices of parameters in R' and R''. In a sequel to this paper [9] we will give a complete catalogue of universality for two-qubit gates that are solutions to the Yang–Baxter equation. In this paper, we shall concentrate on specific examples and their properties.

Remark. A two-qubit pure state

$$|\phi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

is entangled exactly when $(ad - bc) \neq 0$. It is easy to use this fact to check when a specific matrix is, or is not, entangling.

Theorem 0. *Let D denote the phase gate shown below. D is a solution to the algebraic Yang–Baxter equation (see the earlier discussion in this section). Then D given by*

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

is a universal gate.

Proof. It follows at once from the Brylinski theorem that D is universal. For a more specific proof, note that $CNOT = QDQ^{-1}$, where $Q = H \otimes I$, H is the 2×2 Hadamard matrix. The

conclusion then follows at once from this identity and the discussion above. We illustrate the matrices involved in this proof below:

$$H = \left(\frac{1}{\sqrt{2}}\right)\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad Q = \left(\frac{1}{\sqrt{2}}\right)\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{pmatrix}, \qquad D = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{pmatrix},$$

$$QDQ^{-1} = QDQ = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} = CNOT.$$

This completes the proof of the theorem. □

Remark. We thank Martin Roetteles [10] for pointing out the specific factorization of *CNOT* used in this proof.

Theorem 1. *The matrix solutions R' and R'' to the Yang–Baxter equation, described above, are universal gates exactly when $ad - bc \neq 0$ for their internal parameters a, b, c, d. In particular, let R_0 denote the solution R' (above) to the Yang–Baxter equation with $a = b = c = 1$, $d = -1$. Then*

$$R_0 = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & -1\end{pmatrix}.$$

Then R_0 is a universal gate.

Proof. The first part follows at once from the Brylinski theorem. In fact, letting H be the Hadamard matrix as before, and

$$\sigma = \begin{pmatrix}1/\sqrt{2} & \mathrm{i}/\sqrt{2}\\ \mathrm{i}/\sqrt{2} & 1/\sqrt{2}\end{pmatrix}, \qquad \lambda = \begin{pmatrix}1/\sqrt{2} & 1/\sqrt{2}\\ \mathrm{i}/\sqrt{2} & -\mathrm{i}/\sqrt{2}\end{pmatrix}, \qquad \mu = \begin{pmatrix}(1-\mathrm{i})/2 & (1+\mathrm{i})/2\\ (1-\mathrm{i})/2 & (-1-\mathrm{i})/2\end{pmatrix}.$$

Then

$$CNOT = (\lambda \otimes \mu)(R_0(I \otimes \sigma)R_0)(H \otimes H).$$

This gives an explicit expression for *CNOT* in terms of R_0 and local unitary transformations (for which we thank Ben Reichardt in response to an early version of the present paper). □

Remark. Let *SWAP* denote the Yang–Baxter solution R' with $a = b = c = d = 1$. Then

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

SWAP is the standard swap gate. Note that *SWAP* is not a universal gate. This also follows from the Brylinski theorem, since *SWAP* is not entangling. Note also that R_0 is the composition of the phase gate D with this swap gate.

Theorem 2. *Let*

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

be the unitary solution to the Yang–Baxter equation discussed above. Then R is a universal gate. The proof below gives a specific expression for CNOT in terms of R.

Proof. This result follows at once from the Brylinksi theorem, since R is highly entangling. For a direct computational proof, it suffices to show that *CNOT* can be generated from R and local unitary transformations. Let

$$\alpha = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}, \qquad \beta = \begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \\ \mathrm{i}/\sqrt{2} & \mathrm{i}/\sqrt{2} \end{pmatrix},$$

$$\gamma = \begin{pmatrix} 1/\sqrt{2} & \mathrm{i}/\sqrt{2} \\ 1/\sqrt{2} & -\mathrm{i}/\sqrt{2} \end{pmatrix}, \qquad \delta = \begin{pmatrix} -1 & 0 \\ 0 & -\mathrm{i} \end{pmatrix}.$$

Let $M = \alpha \otimes \beta$ and $N = \gamma \otimes \delta$. Then it is straightforward to verify that

$$CNOT = MRN.$$

This completes the proof. □

Remark. We take both theorems 1 and 2 as suggestive of fruitful interactions between quantum topology and quantum computing. It is worth comparing these theorems with the results in [11], a comparison that we shall leave to a future paper.

Remark. We thank Stephen Bullock for his help in obtaining this result. On showing him the Yang–Baxter solution R used in the above proof, he showed us the paper [12] in which he and his co-authors give a criterion for determining if a 4×4 unitary matrix can be generated by local unitary transformations and a single *CNOT*. We then calculated that criterion and found

that R passes the test. Bullock then showed us how to apply their theory to obtain the specific transformations needed in this case. Thus the above result is a direct application of their paper. The criterion also shows that the solutions of type R' and R'' listed above require two applications of *CNOT*. We will discuss their structure elsewhere; but for the record, it is of interest here to record the Shende, Bullock and Markov criterion.

Theorem [12]. *We shall say that a matrix can be* simulated *using k CNOT gates if it can be expressed by that number k of CNOT gates plus local unitary transformations. Let E be the following matrix:*

$$E = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Let U be a matrix in SU(4). *Let* $\gamma(U)$ *be defined by the formula*

$$\gamma(U) = UEUE.$$

Let tr(M) *denote the trace of a square matrix M. Then*

1. *U can be simulated using zero CNOTS if and only if* $\gamma(U) = I$, *where I denotes the identity matrix.*
2. *U can be simulated using one CNOT gate if and only if tr*$[\gamma(U)] = 0$ *and* $\gamma(U)^2 = -I$.
3. *U can be simutated using two CNOT gates if and only if tr*$[\gamma(U)]$ *is real.*

Note that in applying this criterion, the matrix in question must be in the special unitary group. We leave it to the reader to show that matrices of type R' and R'' require two *CNOTS*, and that the matrix R is picked by this criterion to require only one *CNOT*, just as we have shown explicitly above. Note that since R^8 is the identity, we have $R^{-1} = R^7$, as well as the fact that R^{-1} can be expressed in terms of local transformations and a single application of *CNOT*.

3. Generalizing and representing the Artin braid group

Let B_n denote the Artin braid group on n strands [13]. We recall here that B_n is generated by elementary braids $\{s_1, \ldots, s_{n-1}\}$ 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 $i = 1, \ldots, n - 2$.

See figure 2 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 ith and $(i + 1)$th strands wind around one another by a single half-twist

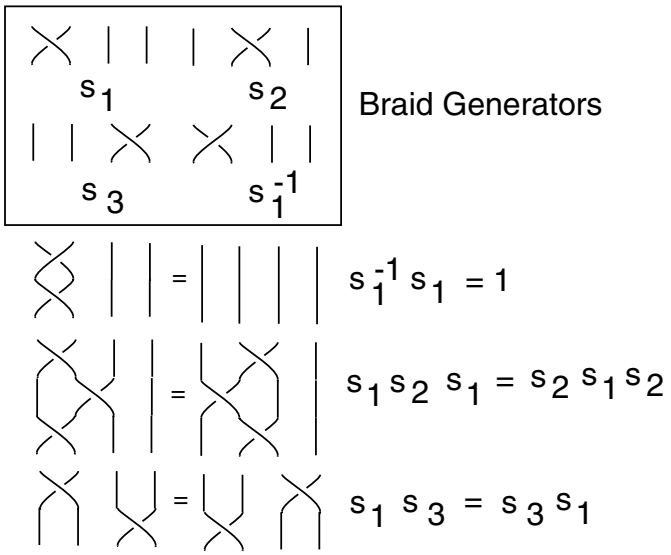

Figure 2. Braid generators and relations.

(the sense of this turn is shown in figure 2) and all other strands drop straight to the bottom. Braids are diagrammed vertically as in figure 2, 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 2 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 $s_1 s_3 = s_3 s_1$. With this interpretation, it is apparent from figures 1 and 2 that the second braiding relation (above) is formally the same as the Yang–Baxter equation.

In fact, if V denotes the basic vector space (the space for one qubit in our context), and R is an invertible solution to the Yang–Baxter equation as described in section 2, then we obtain a representation of the n strand braid group into the vector space of automorphisms of the nth tensor power of V:

$$rep_n : B_n \longrightarrow Aut(V^{\otimes n})$$

by defining

$$rep_n(s_i) = I^{\otimes i-1} \otimes R \otimes I^{\otimes n-i-1},$$

where I denotes the identity mapping on V. Note that since R is a unitary matrix, it follows that this representation is unitary. We shall call this the *standard* method for making a representation of the braid group from an invertible solution to the Yang–Baxter equation. Note that $rep_n(s_i)$ is supported by R on the ith and $(i+1)$th tensor factors and is the identity mapping on the other factors.

We now wish to generalize the classical Artin braid group to a larger group whose representations can include compositions of the elements $rep_n(s_i)$ constructed in the last paragraph with local unitary transfomations. A diagrammatic example of such a composition

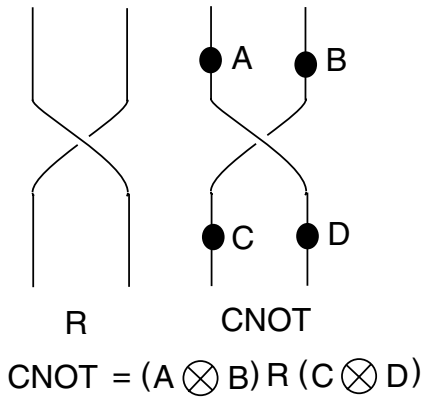

Figure 3. $CNOT = (A \otimes B)R(C \otimes D)$.

is given in figure 3, where we illustrate (as in theorem 2) the expression of *CNOT* in terms of *R* and local unitary transfomations. In this diagram, the local unitary transformations are inicated by nodes on single braiding lines. This corresponds to the fact that the local unitary operations act on single tensor factors. Thus we shall generalize the braid group so that the new group generators are represented on single tensor factors while the elementary braids are represented on two essential tensor factors. This is formalized in the next paragraph.

Let G be any group, and let $G^{\otimes n}$ denote the n-fold tensor product of G with itself, where by this tensor product we mean the group whose elements are of the form $g_1 \otimes g_2 \otimes \cdots \otimes g_n$, with $g_i \in G$, satisfying

$$(g_1 \otimes g_2 \otimes \cdots \otimes g_n)(g'_1 \otimes g'_2 \otimes \cdots \otimes g'_n) = g_1 g'_1 \otimes g_2 g'_2 \otimes \cdots \otimes g_n g'_n.$$

We articulate $G^{\otimes n}$ in tensor language, because we wish to consider representations of the group where individual members of G go to matrices and the elements $g_1 \otimes g_2 \otimes \cdots \otimes g_n$ are sent to tensor products of these matrices. Let $h_i(g) = e \otimes e \cdots \otimes g \otimes e \cdots \otimes e$, where e is the identity element in G, and the element g is in the ith place in this tensor product string. Then

$$g_1 \otimes g_2 \otimes \cdots \otimes g_n = h_1(g_1) \cdots h_n(g_n),$$

and $G^{\otimes n}$ is generated by the elements $h_i(g)$ where i ranges from 1 to n and g ranges over elements of G. Note that for $i \neq j$, and for any $g, g' \in G$, the elements $h_i(g)$ and $h_j(g')$ commmute. Note that h_i is an isomorphism of G to the subgroup $h_i(G)$ of $G^{\otimes n}$.

We define an extension GB_n of the braid group B_n by the group $G^{\otimes n}$ as follows: GB_n is freely generated by $G^{\otimes n}$ and B_n modulo the relations

$$h_i(g)s_j = s_j h_i(g)$$

for all g in G and all choices of i and j such that $i < j$ or $i > j + 1$.

Just as there is a diagrammatic interpretation of the braid group B_n in terms of strings that entangle one another, there is a diagrammatic intepretation of GB_n. Think of a braid diagram and suppose that on the lines of the diagram there is a collection of labelled dots, with each dot labelled by an element of the group G. Let it be given that if two dots occur consecutively on one of the strings of the braid diagram, then they can be replaced by a dot labelled by the product

of these two elements. We make no assumptions about moving dots past elementary braiding elements (which have the appearance of one string passing over or under the other). It is easy to see that this diagrammatic description also defines a group extending the braid group, and that this diagrammatic group is isomorphic to GB_n.

We apply this description of GB_n by taking $G = U(2)$, the 2×2 unitary matrices, viewing them as local unitary transformations for quantum computing. Then we let UB_n denote $U(2)B_n$ and take the representation of UB_n to $Aut(V^{\otimes n})$ that is obtained by the mapping

$$\Gamma : UB_n \longrightarrow Aut(V^{\otimes n})$$

defined by $\Gamma(h_i(g)) = h_i(g)$ for g in $U(2)$ and $\Gamma(s_i) = I^{\otimes i-1} \otimes R \otimes I^{\otimes n-i-1}$, where R is the Yang–Baxter solution discussed in theorem 2.

Recall that a quantum computer is an n-qubit unitary transformation U coupled with rules/apparatus for preparation and measurement of quantum states to which this transformation is applied. We then conclude from theorem 2 that

Theorem 3. *Any quantum computer has its basic unitary transformation U in the image of Γ.*

Remark. This theorem means that, in principle, one can draw a circuit diagram for a quantum computer that is written in the language of the extended braid group UB_n. In particular, this means that braiding relations will apply for sectors of the circuitry that are not encumbered by local unitary transformations. Typically, there will be many such local unitary transformations. We will investigate this braid algebraic structure of quantum computers in a sequel to this paper. A key illustration of theorem 3 is the diagrammatic interpretation of theorem 2. This is shown in figure 3 where we have written in diagrams an equation of the form

$$CNOT = (A \otimes B)R(C \otimes D).$$

Here A, B, C and D represent the local unitary matrices that are used in theorem 2 (with different names) to express $CNOT$ in terms of R.

In general, a unitary transformation can be written as an extended braiding diagram, with appearances of R occupying two adjacent strands, and of local transformations occupying single strands. Note that since R^8 is the identity, theorem 3 actually says that a unitary transformation can be built via a representation of the extension of a quotient B'_n of the braid group B_n, where each braid generator s'_i in B'_n has order eight. It is worth investigating the algebraic structure of B'_n. This is a topic for further research.

3.1. The algebraic Yang–Baxter equation

If R denotes a solution to the Yang–Baxter equation (not neccessarily the R of theorem 2), then we can consider the composition $r = SR$, where S is the swap gate defined in section 2. If we think of r as supported on two tensor lines, and write r_{ij} for the same matrix, now supported on tensor lines i and j (all other lines carrying the identity matrix), then we find that the Yang–Baxter equation for R is equivalent to the following equations for r_{ij}:

$$r_{i,i+1}r_{i,i+2}r_{i+1,i+2} = r_{i+1,i+2}r_{i,i+2}r_{i,i+1}.$$

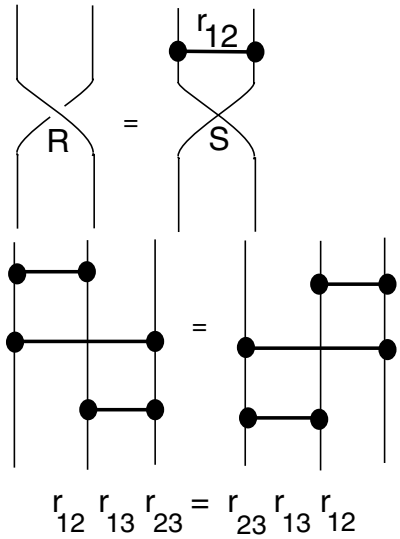

Figure 4. Algebraic Yang–Baxter equation.

The above equation is called the *algebraic Yang–Baxter equation*. See figure 4 for an illustration of this relationship. In making circuit diagrams to apply theorem 1, it is useful to use the formalism of the algebraic Yang–Baxter equation since we can then think of the phase gate D as such a solution and use the above relation to relocate compositions of D on diffferent tensor lines. Given a solution to the algebraic Yang–Baxter equation, plus the swap gate S, we can again define a generalization of the braid group that includes local unitary transformations on the single tensor lines. We will leave detailed application of this point of view to a sequel to this paper.

4. An invariant of knots and links associated with the matrix *R*

A well-known relationship between braids and knots and links allows the construction of invariants of knots and links from representations of the Artin braid group. We give here a quick summary of these relationships and then apply them to the quantum universal matrix R, showing that it gives rise to an interesting invariant of knots and links. The reader should note that this section is concerned only with the classical braid group. It does not use the extensions of the braid group that are discussed in the previous section.

At this point it is worth making a digression about the Reidemeister moves. In the 1920s Kurt Reidemeister proved an elementary and important theorem that translated the problem of determining the topological type of a knot or link to a problem in combinatorics. Reidemeister observed that any knot or link could be represented by a *diagram*, where a diagram is a graph in the plane with four edges locally incident to each node, and with extra structure at each node that indicates an over-crossing of one local arc (consisting in two local edges in the graph) with another. See figure 5. The diagram of a classical knot or link has the appearance of a sketch of the knot; but it is a rigorous and exact notation that represents the topological type of the knot. Reidemeister showed that two diagrams represent the same topological type (of knottedness or linkedness) if and only if one diagram can be obtained from another by planar

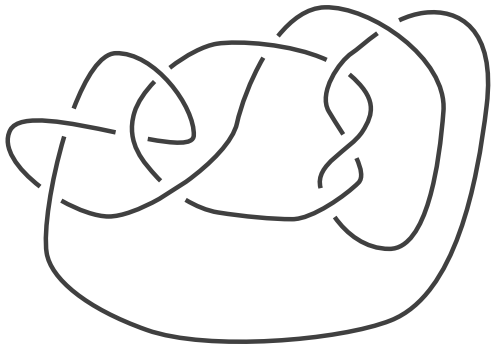

Figure 5. A knot diagram.

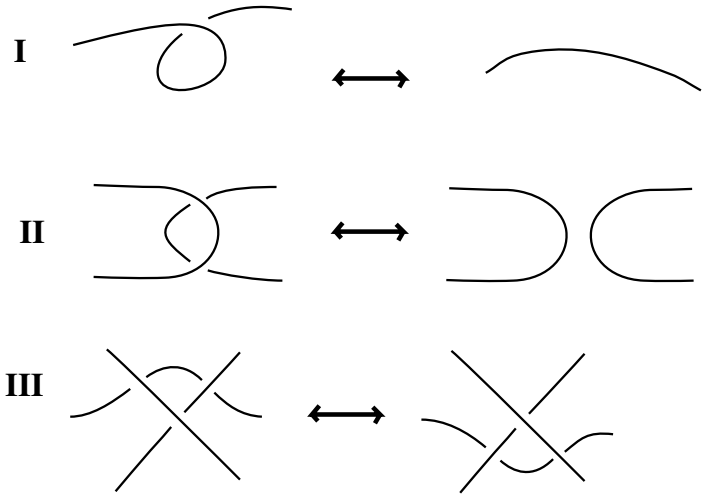

Figure 6. Reidemeister moves.

homeomorphisms coupled with a finite sequence of the *Reidemeister moves* illustrated in figure 6. Each of the Reidemeister moves is a local change in the diagram that is applied as shown in this figure.

We say that two knots or links are *isotopic* if one can be obtained from the other by a sequence using any of the three Reidemeister moves (plus global topological mappings of the diagram plane to itself).

The first significant fact relating links and braids is the

Theorem of Alexander. *Every knot or link is isotopic to the closure of a braid.*

The closure of a braid b, here denoted $CL(b)$, is obtained by attaching each top strand to the corresponding bottom strand in the fashion shown in figure 7. The closed braid is a weave that proceeds circularly around a given axis. There are many proofs of Alexander's theorem. The interested reader should consult [13].

Given that every knot or link can be represented by a closed braid, it is natural to wonder whether the classification of braids will effect a classification of the topological types of all knots and links. The situation is more complicated than one might have expected. There are many braids whose closure is isotopic to any given knot or link. Here are two basic methods for

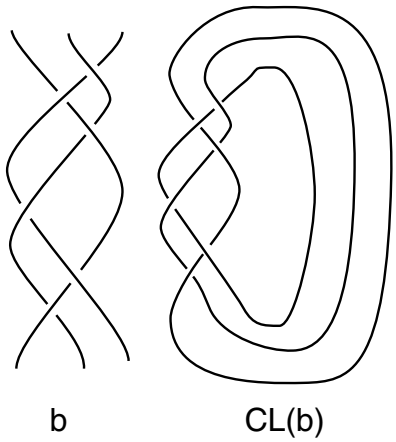

Figure 7. Closing a braid to form the Borromean rings.

modifying a braid b in B_n so that the topological type of its closure does not change:

1. Let g be any braid in B_n. Then

$$CL(gbg^{-1}) = CL(b),$$

   where we use equality to denote isotopy of knots and links as described above.
2. Note that if b is in B_n, then bs_n is in B_{n+1}. It is easy to see that

$$CL(b) = CL(bs_n) \quad \text{and} \quad CL(b) = CL(bs_n^{-1}).$$

In the light of the equivalences we have just indicated, the following two moves on braids are called the *Markov moves* (after Markov who enunciated the theorem we state below):

1. **Markov Move 1.** Replace a braid b by gbg^{-1}, where g is another braid with the same number of strands.
2. **Markov Move 2.** Replace a braid $b \in B_n$ by either bs_n or by bs_n^{-1} or vice versa, replace $bs_n^{\pm 1}$ with b.

Markov theorem. *Suppose that b and b' are two braids (of possibly different numbers of strands) with $CL(b) = CL(b')$. Then b' can be obtained from b by a series of braid equivalences coupled with applications of the Markov moves).*

Remark. For proofs of the Markov theorem, see [14, 15]. See figure 9 for an illustration of the second Markov move. Notice that in making this move we promote the braid $b \in B_n$ to a braid in B_{n+1} by adding a right-most strand. Then we multiply by $s_n \in B_{n+1}$. The closure of the resulting braid differs by a single first Reidemeister move from the closure of b. The upshot of this theorem is that it is *possible* for a trace function on a representation of the braid group to give rise to topological information about the closure of the braid. For example, suppose that we have

a unitary representation of the braid group arising from a unitary solution of the Yang–Baxter equation, as described in section 3. Let the representation be denoted by

$$rep_n : B_n \longrightarrow Aut(V^{\otimes n}).$$

Let

$$\tau(b) = tr(rep_n(b)),$$

where $tr(M)$ denotes the trace of a square matrix M. Then, since the trace of any linear mapping satisfies $tr(AB) = tr(BA)$, it follows that $\tau(gbg^{-1}) = \tau(b)$, and hence τ gives the same values on braids that differ by Markov moves of type 1. We would like τ to be invariant under Markov moves of type 2, but this is usually too much to ask. It is standard practice in the literature of link invariants to search for a matrix η mapping V to V such that the modified trace $TR(b) = tr(\eta^{\otimes n} rep_n(b))$ has a multiplicative property under the second Markov move in the sense that $TR(bs_n) = \alpha TR(b)$ and $TR(bs_n^{-1}) = \alpha^{-1} TR(b)$, where α is a invertible constant in the ring of values for the trace. Such a function TR is called a *Markov trace*, and one can normalize it to obtain a function that is an invariant of isotopy of links by defining $I(b) = \alpha^{-w(b)} TR(b)$, where $w(b)$ is the sum of the signs of the crossings of the braid b.

In the case of our computationally universal matrix R, the bare trace $\tau(b) = tr(rep_n(b))$ behaves in a very simple way under the second Markov move. We find (and will show the details below) that

$$\tau(bs_n) = \sqrt{2}\tau(b)$$

and

$$\tau(bs_n^{-1}) = \sqrt{2}\tau(b).$$

Note that the multiplicative factor is the same for both types of second Markov move. Instead of making a normalizing factor from this, we can say that if two links $CL(b)$ and $CL(b')$ are isotopic, then $\tau(b)$ and $\tau(b')$ will differ by a multiplicative factor that is some power of the square root of two. In particular, this means that if $\tau(b)$ and $\tau(b')$ have different signs, or if one is zero and the other not zero, then we know that the closures of b and b' are not isotopic.

Here is the matrix R:

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

We have

$$R|ab\rangle = R_{ab}^{00}|00\rangle + R_{ab}^{01}|01\rangle + R_{ab}^{10}|10\rangle + R_{ab}^{11}|11\rangle.$$

Let

$$tr_2(R) = \Sigma_k R^{bk}_{ak}$$

be the partial trace of R with respect to the second tensor factor. Then

$$tr_2(R) = (1/\sqrt{2} + 1/\sqrt{2})I = \sqrt{2}I,$$

where I denotes the 2×2 identity matrix and

$$tr_2(R^{-1}) = \sqrt{2}I.$$

Recall from the previous section that

$$rep_n : B_n \longrightarrow Aut(V^{\otimes n})$$

is defined on braid generators by the equation

$$rep_n(s_i) = I^{\otimes i-1} \otimes R \otimes I^{\otimes n-i-1},$$

where I denotes the identity mapping on V. Now suppose that $b \in B_n$. We want to compute $\tau(bs_n)$. This expression requires interpretation. When we write bs_n, we are taking b in B_n and regarding it as an element of B_{n+1} by adding an extra right-most strand to b. In general, by adding strands in this way, we have standard embeddings of B_n in B_m when $m \geqslant n$. Working in B_{n+1}, we have

$$rep_{n+1}(b) = rep_n(b) \otimes I$$

and

$$rep_{n+1}(s_n) = I^{\otimes(n-1)} \otimes R.$$

Thus

$$\tau(bs_n) = tr(rep_{n+1}(bs_n)) = tr((rep(b) \otimes I)(I^{\otimes(n-1)} \otimes R)).$$

From this it is easy to see that in tracing $rep_{n+1}(bs_n)$, the rightmost indices of the matrix R (in the $n+1$ tensor factor) are contracted directly with one another (since b is supported on the first n strands). Thus the partial trace is applied to the R that appears in the representation of bs_n corresponding to s_n. It follows from this that

$$\tau(bs_n) = tr(rep_n(b))tr_2(R) = \tau(b)\sqrt{2}.$$

Hence, for the tensor representation built from R as described in section 3, we have

$$\tau(bs_n) = \sqrt{2}\tau(b)$$

and in like manner, we have

$$\tau(bs_n^{-1}) = \sqrt{2}\tau(b).$$

This proves the assertions we have made about the properties of τ for this R.

Remark. In figure 10, we illustrate diagrammatically the above argument at the index level. In this illustration, we have placed a shaded box around a braid to indicate the application of the representation of the braid group. Thus a shaded braided box represents a matrix with upper indices correpsponding to the upper strands on the box, and lower indices corresponding to the lower strands on the box. The simplest instance of such a matrix is a single vertical line which represents the identity matrix, and iconically indicates the identity of the top index with the bottom index (hence representing the identity as a Kronecker delta).

It is a fact that shaded boxes so placed on the braids give a correct picture of the contractions of the corresponding matrices via the convention that *we contract the indices along lines that connect free index ends between diagrammatic matrices.* The figure then illustrates directly via these diagrammatic matrices how we obtain the formula

$$tr(rep_{n+1}(bs_n)) = \sqrt{2}tr(rep_n(b)).$$

Note that the trace of a diagrammatic matrix has exactly the same form as the closure of a braid, since the connection of two open lines corresponds to the identification and contraction over their respective indices.

Finally, here is the same argument using matrix algebra with indices. We use the Einstein summation convention: summation is taken over repeated upper and lower indices. Suppose that $rep_n(b) = (M^{a,i}_{b,j})$ where a and b are vectors of indices for the the first $n-1$ factors of the tensor product, and i and j are individual indices with values 0 or 1. Then

$$rep_{n+1}(b) = (M^{a,i}_{b,j}\delta^r_s),$$

where δ^r_s is the 2×2 identity matrix. Furthermore,

$$rep_{n+1}(s_n) = \delta^a_b R^{t,u}_{v,w}.$$

Hence

$$rep_{n+1}(bs_n) = (M^{a,i}_{b,j}R^{j,u}_{k,w})$$

from which it follows that

$$tr(rep_{n+1}(bs_n)) = tr(M^{a,i}_{b,j}R^{j,u}_{k,w}) = tr(M^{a,i}_{b,j}R^{j,u}_{k,u}),$$

where *in the last equality we have contracted the last indices of R.* Since

$$R^{j,u}_{k,u} = \sqrt{2}\delta^j_k,$$

it follows that

$$tr(rep_{n+1}(bs_n)) = tr(M^{a,i}_{b,j}\sqrt{2}\delta^j_k) = \sqrt{2}tr(M^{a,i}_{b,k}) = \sqrt{2}tr(rep_n(b)).$$

This completes the explicit index verification of the behaviour of τ under the second Markov move.

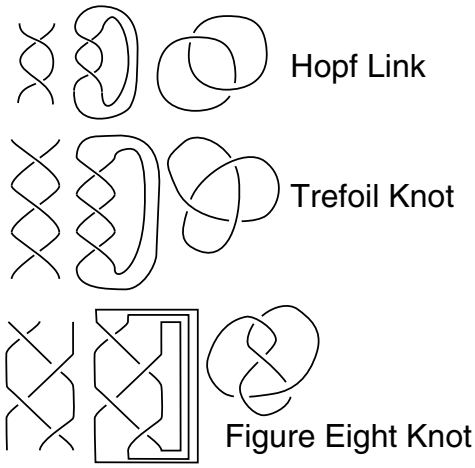

Figure 8. Closing braids to produce Hopf link, trefoil knot and figure eight knot.

This invariant of knots and links turns out to be quite interesting. For example, it detects the linkedness of the Borromean rings (depicted in figures 7 and 16). It gives the following values:

1. τ (unlink of three components) $= 8 > 0$;
2. τ (Hopf link) $= 0$;
3. τ (trefoil knot) $= -2\sqrt{2} < 0$;
4. τ (figure-eight knot) $= -4 < 0$;
5. τ (Borromean rings) $= -8 < 0$.

Note that τ does not detect the difference between the trefoil knot, the figure-eight knot and the Borromean rings, but it does show that the Hopf link is linked, that the Borromean rings are linked, and that the trefoil knot and the figure-eight knot are knotted. See figure 8 for illustrations of these knots and links. It remains to be seen how the quantum entangling properties of the matrix R are related to the behaviour of this link invariant.

Remark on a Skein relation. In this subsection, we point out that there is a *skein relation* that helps in the computation of the trace $\tau(b)$ for a braid b. A skein relation is an equation about an invariant involving local changes at the site of a single crossing in corresponding braid or link diagrams. The first skein relation in knot theory was discovered and utilized for the Alexander polynomial by Conway in his remarkable paper [16]. (Conway used an idea that was implicit in Alexander's original paper of 1928.) The Jones polynomial and many other knot polynomial invariants satisfy such relations.

The matrix R satisfies the equation

$$R + R^{-1} = \sqrt{2} I_2,$$

where I_n denotes the $2^n \times 2^n$ identity matrix. We leave it to the reader to check this fact. It is also easy to check that

$$R^8 = I_2$$

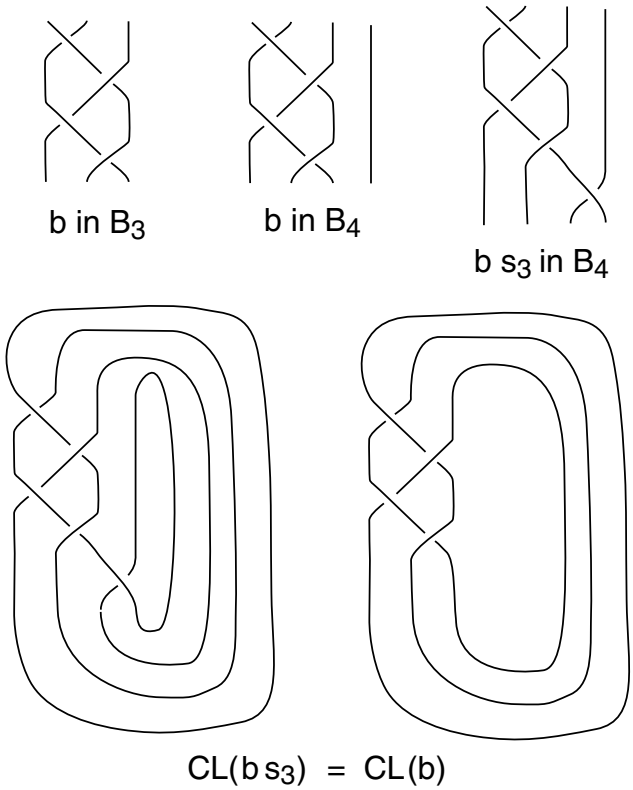

Figure 9. Illustration of the second Markov move.

and that all the lower powers are non-trivial. The fact that R has finite order certainly limits its power as a link or braid invariant. For example, we have the eight-fold periodicity

$$\tau(s_i^{n+8}) = \tau(s_i^n)$$

as a direct consequence of the finite order of R. On the other hand, the identity $R + R^{-1} = \sqrt{2}I_2$ can be viewed as a method for simplifying the calculations for a braid. This implies the skein relation

$$\tau(b) + \tau(b') = \sqrt{2}\tau(b'')$$

when b and b' are elements of the n-strand braid group that differ at a single crossing and b'' is the result of replacing this crossing by an identity braid. The crossing can be interpreted as a single instance of s_i for some i, and we then use $rep_n(\alpha s_i \beta) + rep_n(\alpha s_i^{-1}\beta) = \sqrt{2}\, rep_n(\alpha\beta)$.

Example 1. Here is the simplest example of this sort of computation. We work in B_2 and let $s = s_1$:

$$\tau(ss) + \tau(ss^{-1}) = \sqrt{2}\tau(s).$$

Here we have $\tau(ss^{-1}) = \tau(I_2) = 4$ and $\tau(s) = \sqrt{2}\tau(I_1) = 2\sqrt{2}$. Hence $\tau(ss) = 0$, as we remarked earlier with ss the braid representative for the Hopf link (see figure 8). More generally,

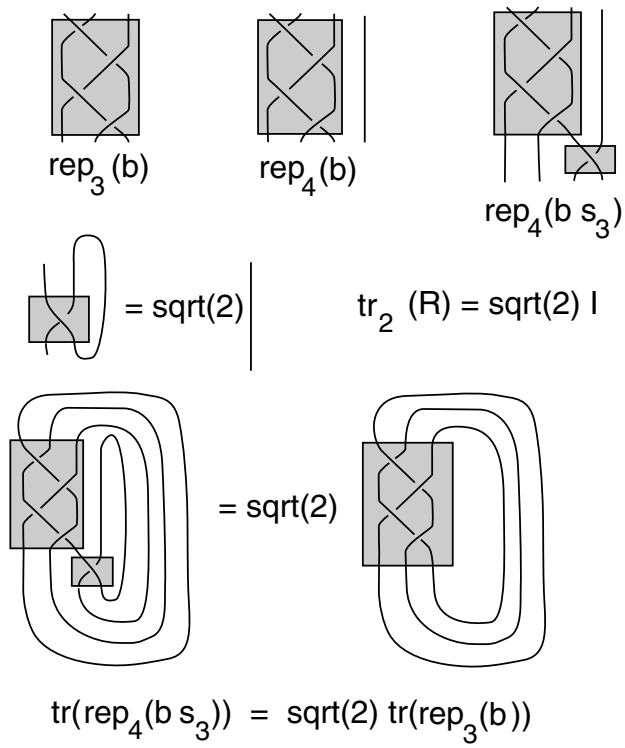

Figure 10. Illustration of the behaviour of the trace on the second Markov move.

we have

$$\tau(s^{n+1}) + \tau(s^{n-1}) = \sqrt{2}\tau(s^n)$$

so that

$$\tau(s^{n+1}) = \sqrt{2}\tau(s^n) - \tau(s^{n-1}).$$

Letting 1 denote the identity braid in B_2, we then have

$$\tau(1) = 4, \qquad \tau(s) = 2\sqrt{2}, \qquad \tau(s^2) = 0, \qquad \tau(s^3) = -2\sqrt{2},$$
$$\tau(s^4) = -4, \qquad \tau(s^5) = -2\sqrt{2}, \qquad \tau(s^6) = 0, \qquad \tau(s^7) = 2\sqrt{2}$$

with the periodicity

$$\tau(s^{n+8}) = \tau(s^n).$$

Since s^7 and s^3 close to knots, we see that this invariant can distinguish these two knots from one another, but cannot tell that the closure of s^7 is knotted.

Example 2. Let $b = s_1^2 s_2^{-1} s_1 s_2^{-1}$. See figure 11. The closure of b is W, a link of two components, with linking number equal to zero. W is called the *Whitehead link*, after the topologist, J H C Whitehead, who first studied its properties. We shall check that $\tau(b) = -4\sqrt{2}$, showing that our invariant detects the linkedness of the Whitehead link.

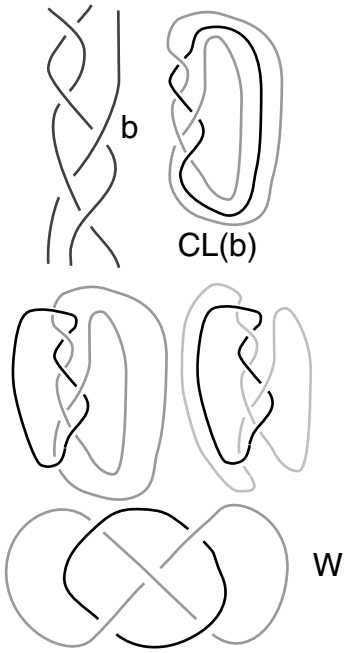

Figure 11. Whitehead link, $W = CL(b = s_1^2 s_2^{-1} s_1 s_2^{-1})$.

We use skein relation for the first appearance of s_2^{-1} from the left on the word for b. This gives

$$\tau(b) = -\tau(s_1^2 s_2 s_1 s_2^{-1}) + \sqrt{2}\tau(s_1^2 s_1 s_2^{-1}).$$

Note that

$$s_1^2 s_2 s_1 s_2^{-1} = s_1(s_1 s_2 s_1)s_2^{-1} = s_1(s_2 s_1 s_2)s_2^{-1} = s_1 s_2 s_1.$$

Then

$$\tau(s_1 s_2 s_1) = \tau((s_1 s_2)s_1) = \tau(s_1(s_1 s_2)) = \tau(s_1^2 s_2) = \sqrt{2}\tau(s_1^2) = 0.$$

Hence

$$\tau(b) = \sqrt{2}\tau(s_1^2 s_1 s_2^{-1}) = \sqrt{2}\tau(s_1^3 s_2^{-1}) = \sqrt{2}^2\tau(s_1^3) = 2(-2\sqrt{2}) = -4\sqrt{2}.$$

5. Quantum computation of knot invariants

Can the invariants of knots and links such as the Jones polynomial be configured as quantum computers? This is an important question because the algorithms to compute the Jones polynomial are known to be *NP*-hard, and so corresponding quantum algorithms may shed light on the relationship of this level of computational complexity with quantum computing (see [17]). Such models can be formulated in terms of the Yang–Baxter equation [18]–[21]. The next paragraph explains how this comes about.

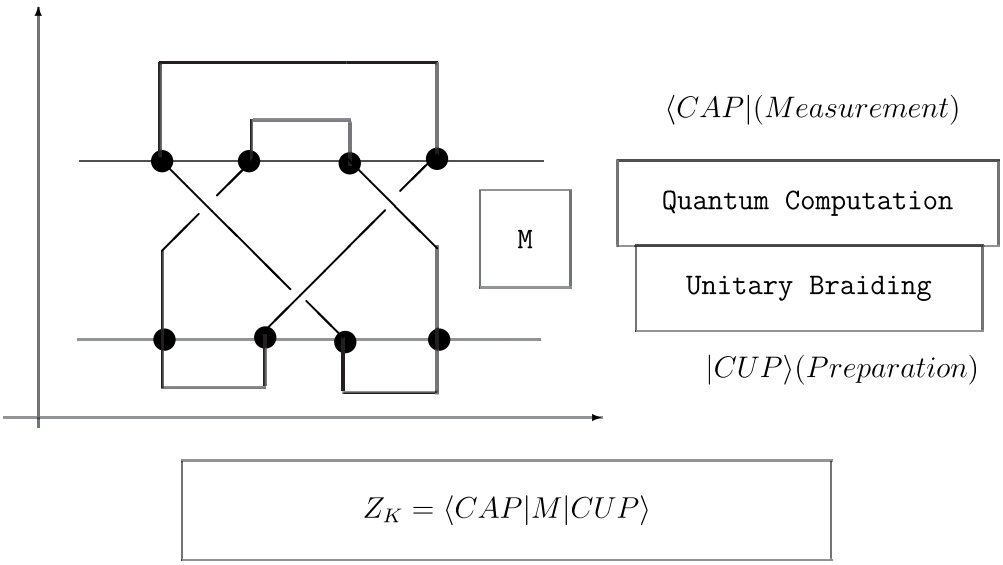

Figure 12. A knot quantum computer.

In figure 12, we indicate how topological braiding plus maxima (caps) and minima (cups) can be used to configure the diagram of a knot or link. This also can be translated into algebra by the association of a Yang–Baxter matrix R (not necessarily the R of the previous sections) to each crossing and other matrices to the maxima and minima. There are models of very effective invariants of knots and links such as the Jones polynomial that can be put into this form [21]. In this way of looking at things, the knot diagram can be viewed as a picture, with time as the vertical dimension, of particles arising from the vacuum, interacting (in a two-dimensional space) and finally annihilating one another. The invariant takes the form of an amplitude for this process that is computed through the association of the Yang–Baxter solution R as the scattering matrix at the crossings and the minima and maxima as creation and annihilation operators. Thus we can write the amplitude in the form

$$Z_K = \langle CUP|M|CAP\rangle,$$

where $\langle CUP|$ denotes the composition of cups, M is the composition of elementary braiding matrices, and $|CAP\rangle$ is the composition of caps. We regard $\langle CUP|$ as the preparation of this state, and $|CAP\rangle$ as the measurement of this state. In order to view Z_K as a quantum computation, M must be a unitary operator. This is the case when the R-matrices (the solutions to the Yang–Baxter equation used in the model) are unitary. Each R-matrix is viewed as a quantum gate (or possibly a composition of quantum gates), and the vacuum–vacuum diagram for the knot is interpreted as a quantum computer. This quantum computer will probabilistically (via quantum amplitudes) compute the values of the states in the state sum for Z_K.

The form of the model proposed for translating the Jones polynomial to a quantum computation is also the form of models for anyonic quantum computation (see [11], [22]–[25]). In an anyonic model, the braiding corresponds to the motion of configurations of particles in a two-dimensional space. These theories are directly related to quantum link invariants and to topological quantum field theories [26]. It is hoped that quantum computing placed in the anyonic context can be made resistant to the effects of decoherence due, in part, to the invariance of topological structures under perturbation.

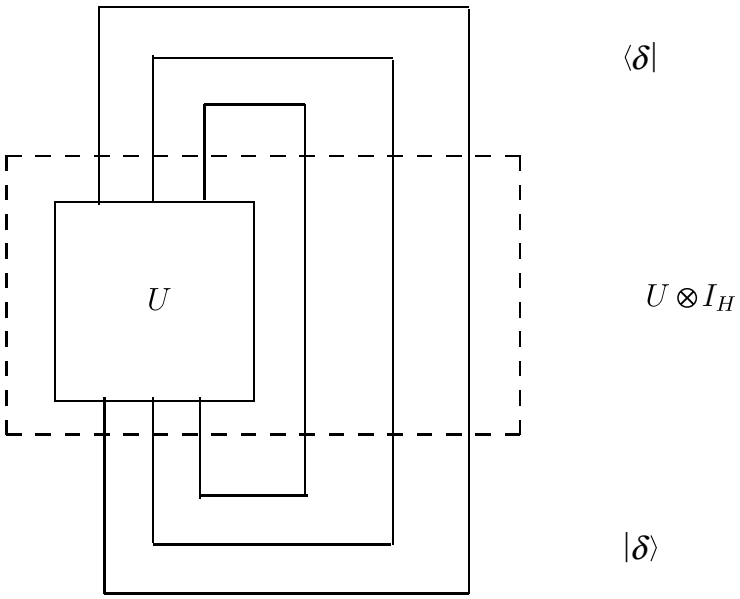

Figure 13. A quantum process to obtain $|tr(U)|$.

The formalism of configuring a computation in terms of preparation and measurement in the pattern of figure 12 can be used in very general quantum computational contexts. For example, let U be a unitary transformation on $H = V^{\otimes n}$, where V is the complex two-dimesional space for a single qubit. Represent U as a box with n input lines at the bottom and n output lines at the top, each line corresponding to a single qubit in an element of the tensor product H with basis $\{|\alpha\rangle | \alpha$ is a binary string of length $n\}$. Let $|\delta\rangle = \Sigma_\alpha |\alpha, \alpha\rangle \in H \otimes H$, where α runs over all binary strings of length n. Note that $\langle\delta|$ is the following covector mapping $H \otimes H$ to the complex numbers C:

$$\langle\delta|\alpha, \beta\rangle = 1 \quad \text{if } \alpha = \beta \quad \text{and} \quad \langle\delta|\alpha, \beta\rangle = 0 \text{ otherwise.}$$

Now let $W = U \otimes I_H$, where I_H denotes the identity transformation of H to H. Then

$$\langle\delta|W|\delta\rangle = \langle\delta|U \otimes I_H|\delta\rangle = \langle\delta|\Sigma_\gamma U_\alpha^\gamma|\gamma, \alpha\rangle = \Sigma_\alpha U_\alpha^\alpha = tr(U).$$

For example, $\langle\delta|\delta\rangle = 2^n = tr(I_H)$. See figure 13 for an illustration of this process.

Thus we see that we can, for any unitary matrix U, produce a quantum computational process with preparation $|\delta\rangle$ and measurement $\langle\delta|$ such that *the amplitude of this process is the trace of the matrix U divided by* $(\sqrt{2})^n$. This means that the corresponding quantum computer computes the probability associated with this amplitude. This probability is the absolute square of the amplitude and so the quantum computer will have $|tr(U)|^2/2^n$ as the probability of success and hence one can find $|tr(U)|$ by successive trials. We have proved the

Lemma. *With the above notation, the absolute value of the trace of a unitary matrix U,* $|tr(U)|$, *can be obtained to any desired degree of accuracy from the quantum computer corresponding to* $U \otimes I_H$ *with preparation* $|\delta\rangle$ *and measurement* $\langle\delta|$, *where* $|\delta\rangle = \Sigma_\alpha |\alpha, \alpha\rangle \in H \otimes H$.

The proof of the lemma is in the discussion above its statement.

6. Unitary representations and teleportation

The formalism we used at the end of the last section to describe the (absolute value of the) trace of a unitary matrix contains a hidden teleportation. It is the purpose of this section to bring forth that hidden connection.

First consider the state

$$|\delta\rangle = \Sigma_\alpha |\alpha, \alpha\rangle \in H \otimes H$$

from the last section, where $H = V^{\otimes n}$ and V is a single-qubit space. One can regard $|\delta\rangle$ as a generalization of the EPR state $\langle 00| + \langle 11|$.

Let $|\psi\rangle \in H$ be an arbitrary pure state in H. Let $\langle \mathcal{M}|$ be an abitrary element of the dual of $H \otimes H$ and consider the possibility of a successful measurement via $\langle \mathcal{M}|$ in the first two tensor factors of

$$|\psi\rangle|\delta\rangle \in H \otimes H \otimes H.$$

The resulting state from this measurement will be

$$\langle \mathcal{M}|[|\psi\rangle|\delta\rangle].$$

If

$$\langle \mathcal{M}| = \Sigma_{\alpha,\beta} M_{\alpha,\beta} \langle\alpha|\langle\beta|,$$

then

$$\begin{aligned}\langle \mathcal{M}|[|\psi\rangle|\delta\rangle] &= \Sigma_{\alpha,\beta} M_{\alpha,\beta} \langle\alpha|\langle\beta|\Sigma_{\gamma,\lambda}\psi_\gamma|\gamma\rangle|\lambda\rangle|\lambda\rangle \\ &= \Sigma_{\alpha,\beta} M_{\alpha,\beta}\Sigma_{\gamma,\lambda}\psi_\gamma\langle\alpha|\gamma\rangle\langle\beta|\lambda\rangle|\lambda\rangle = \Sigma_{\alpha,\beta} M_{\alpha,\beta}\psi_\alpha|\beta\rangle \\ &= \Sigma_\beta[\Sigma_\alpha M_{\alpha,\beta}\psi_\alpha]|\beta\rangle = \Sigma_\beta (M^{\mathrm{T}}\psi)_\beta|\beta\rangle = M^{\mathrm{T}}|\psi\rangle.\end{aligned}$$

Thus we have proved the

Teleportation lemma. *Successful measurement via $\langle \mathcal{M}|$ in the first two tensor factors of*

$$|\psi\rangle|\delta\rangle \in H \otimes H \otimes H$$

results in the state $M^{\mathrm{T}}|\psi\rangle$ where the matrix M represents the measurment state $\langle \mathcal{M}|$ in the sense that

$$\langle \mathcal{M}| = \Sigma_{\alpha,\beta} M_{\alpha,\beta} \langle\alpha|\langle\beta|,$$

and M^{T} denotes the transpose of the matrix M.

This lemma contains the key to teleportation. Let $|\psi\rangle$ be a state held by Alice, where Alice and Bob share the generalized EPR state $|\delta\rangle$. Alice measures the combined state $|\psi\rangle|\delta\rangle$ and reports to Bob that she has succeeded in measuring via $\langle \mathcal{M}|$ (from some list of shared transformations that they have in common) by a classical transmission of information. By the lemma, Bob knows that he now has access to the state $M^{\mathrm{T}}|\psi\rangle$. In this generalized version of teleportation, we imagine that Alice and Bob have a shared collection of matrices M, each coded by a bit-string that can be

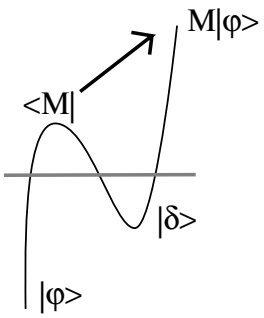

Figure 14. Matrix teleportation.

transmitted in a classical channel. By convention, Alice and Bob might take the zero bit-string to denote lack of success in measuring in one of the desired matrices. Then Alice can send Bob by the classical channel the information of success in one of the matrices, or failure. For success, Bob knows the identity of the resulting state without measuring it. See figure 14 for a schematic of this process.

In the case of success, and if the matrix M is unitary, Bob can apply $(M^{\mathrm{T}})^{-1}$ to the transmitted state and know that he now has the original state $|\psi\rangle$ itself. The usual teleportation scenario is actually based on a list of unitary transformations sufficient to form a basis for the measurement states. Let us recall how this comes about.

First take the case where M is a unitary 2×2 matrix and let $\sigma_1, \sigma_2, \sigma_3$ be the three Pauli matrices

$$\sigma_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad \sigma_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \sigma_2 = \begin{bmatrix} 0 & \mathrm{i} \\ -\mathrm{i} & 0 \end{bmatrix}.$$

We replace σ_3 by $-\mathrm{i}\sigma_3$ (for ease of calculation) and obtain the three matrices X, Y, Z:

$$X = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Basis lemma. *Let M be a 2×2 matrix with complex entries. Let the* measuring state for *M be the state*

$$\langle \mathcal{M}| = M_{00}|00\rangle + M_{01}|01\rangle + M_{10}|10\rangle + M_{11}|11\rangle.$$

Let $\langle \mathcal{X}M|$ denote the measuring state for the matrix XM (similarly for YM and ZM). Then the vectors

$$\{\langle \mathcal{M}|, \langle \mathcal{X}M|, \langle \mathcal{Y}M|, \langle \mathcal{Z}M|\}$$

are orthogonal in the complex vector space $V \otimes V$ if and only if M is a multiple of a unitary matrix$U$ of the form

$$U = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}$$

with complex numbers z and w as generating entries.

Proof. We leave the proof of this lemma to the reader. It is a straightforward calculation. □

This lemma contains standard teleportation procedure when one takes $M = I$ to be the identity matrix. Then the four measurement states

$$\{\langle \mathcal{I}|, \langle \mathcal{X}|, \langle \mathcal{Y}|, \langle \mathcal{Z}|\}$$

form an orthogonal basis and by the teleportation lemma, they successfully transmit $\{|\psi\rangle, X^{\mathrm{T}}|\psi\rangle, Y^{\mathrm{T}}|\psi\rangle, Z^{\mathrm{T}}|\psi\rangle\}$ respectively. Bob can rotate each of these received states back to $|\psi\rangle$ by a unitary transformation. (Remember that states are determined up to phase.) In this form, the lemma shows that we can, in fact, teleport any 2×2 unitary matrix transformation U. We take $M = U$, and take the othogonal basis provided by the lemma. Then a 2-qubit classical transmission from Alice to Bob will enable Bob to identify the measured state and he can rotate it back to $U|\psi\rangle$.

Note that for $H = V^{\otimes n}$ we can consider the matrices

$$T_{\alpha,\beta} = T_{\alpha(1),\beta(1)} \otimes \cdots \otimes T_{\alpha(n),\beta(n)},$$

where $\alpha = (\alpha(1), \ldots, \alpha(n))$ and $\beta = (\beta(1), \ldots, \beta(n))$ are bit-strings of length n and $T_{0,0} = I$, $T_{0,1} = X$, $T_{1,0} = Y$, $T_{1,1} = Z$ are the modified Pauli matrices discussed above. Then just as in the above lemma, if U is a unitary matrix defined on H, then the set of measurement states $\langle \mathcal{T}_{\alpha,\beta}\mathcal{U}|$ for the matrices $T_{\alpha,\beta}U$ are an orthogonal basis for $H \otimes H$. Hence we can teleport the action of the arbitrary unitary matrix U from Alice to Bob, at the expense of a transmission of 2^n classical bits of information. This means that, we can construct an arbitrary unitary transformation (hence an idealized quantum computer) almost entirely by using quantum measurments. This result should be compared with the results of [27, 28], which we shall do in a forthcoming paper. If Alice and Bob coincide as observers, then there is no need to transmit the classical bits. The result of a given measurement is an instruction to perform one of a preselected collection of unitary transformations on the resulting state.

There are a number of lines that we will follow in susequent papers related to the points made in this section. In particular, it is certainly of interest that one can partially teleport transformations M that are not unitary, at the cost of having only partial information beforehand of the success of any given measurement. In particular, this means that we could consider computing results such as traces or generalized traces of matrices that are not unitary. In this way we could examine computations of knot and link invariants that are based on non-unitary solutions to the Yang–Baxter equation. All of this will be the subject of another paper. In the next section we turn to the subject of quantum computation of link invariants based on unitary solutions to the Yang–Baxter equation.

7. Unitary representations of the braid group and the corresponding quantum computers

Many questions are raised by the formulation of a quantum computer associated with a given link diagram configured as preparation, unitary transformation and measurement. Unitary solutions to the Yang–Baxter equation (or unitary representations of the Artin braid group) that also give link invariants are not so easy to come by. Here we give a unitary representation that computes the Jones polynomial for closures of 3-braids. This representation provides a test case for the

corresponding quantum computation. We now analyse this representation by making explicit how the bracket polynomial [18]–[21] is computed from it.

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

$$P^2 = |v|^2 P, \qquad Q^2 = |w|^2 Q,$$

$$PQP = |\langle v|w\rangle|^2 P, \qquad QPQ = |\langle v|w\rangle|^2 Q.$$

P and Q generate a representation of the Temperley–Lieb algebra [21]. One can adjust parameters to make a representation of the three-strand braid group in the form

$$s_1 \longmapsto rP + sI, \qquad s_2 \longmapsto tQ + uI,$$

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 that it is possible for the representation to be unitary even though its mathematical 'parts' P and Q are not unitary. Note also that the resulting representation is made entirely from local unitary transformations, so that while there is measurement of topological entanglement, there is no quantum entanglement of any of the corresponding quantum states.

The representation depends on two symmetric but non-unitary matrices U_1 and U_2 with

$$U_1 = \begin{bmatrix} d & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad U_2 = \begin{bmatrix} d^{-1} & \sqrt{1-d^{-2}} \\ \sqrt{1-d^{-2}} & d-d^{-1} \end{bmatrix}.$$

Note that $U_1^2 = dU_1$ and $U_2^2 = dU_2$. 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 [18, 21]. The desired representation of the Artin braid group is given on the two braid generators for the three-strand braid group by the equations:

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

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 $d = -2\cos(2\theta)$. We find a specific range of angles $|\theta| \leqslant \pi/6$ and $|\theta - \pi| \leqslant \pi/6$ *that give unitary representations of the three-strand braid group.* Thus a specialization of a more general representation of the braid group gives rise to a continuum family of unitary representations of the braid group.

Note that $tr(U_1) = tr(U_2) = d$ 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 $\langle \bar{b} \rangle$, can be calculated directly from the trace of this representation, except for the part involving the identity matrix. The result is the equation

$$\langle \bar{b} \rangle = A^{I(b)}d^2 + tr(\Pi(b)),$$

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

$$\langle \bar{b} \rangle = tr(\Phi(b)) + A^{I(b)}(d^2 - 2).$$

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 matrix $\Phi(b)$. To what extent can our quantum computer determine the trace of this matrix? We have seen just before this subsection that a quantum computation can determine the absolute value of the trace by repeated trials. This shows that a major portion of the Jones polynomial for three-strand braids can be done by quantum computation.

7.1. The invariant based on R

A second example is given by the invariant discussed in the previous section. In that case, we have the formula

$$\tau(b) = tr(rep_n(b))$$

taken up to multiples of the square root of 2, and the matrix $rep_n(b)$ is unitary for any braid b in an n-strand braid group for arbitrary positive integer n. This invariant can be construed as the trace of a unitary matrix for a quantum computation. Since, as we have seen, knowledge of the invariant often depends upon knowing the global sign of the trace of $rep_n(b)$, it is not enuough to just compute the absolute value of this trace. Nevertheless, some topological information is available just from the absolute value.

8. Quantum entanglement and topological entanglement

The second question about unitary solutions to the Yang–Baxter equation is the matter of understanding their capabilities in entangling quantum states. We use the criterion that

$$\phi = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

is entangled if and only if $ad - bc \neq 0$. This criterion is generalized to higher dimensional pure states in our papers [1, 2], [29]–[31].

In [1, 2, 21], we discovered families of unitary solutions to the Yang–Baxter equation that detect topological linking if and only if the gates corresponding to these solutions can entangle quantum states.

Is there a deeper connection between topological entanglement and quantum entanglement? We believe that more exploration is called for before a definitive answer to this question can be formulated. We need more bridges between quantum topology and quantum computation.

The matrix

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

is a unitary solution of the Yang–Baxter equation; and it is highly entangling for quantum states. It takes the standard basis for the tensor product of two single qubit spaces to the Bell basis. On the topological side, R generates a new and non-trivial invariant of knots and links. On the quantum side, R is a universal gate at the same level as *CNOT*, as we showed in theorems 2 and 3. Thus R is a good example of a transformation that can be examined fruitfully in both the quantum and the topological contexts.

8.1. Linking numbers and the matrix R'

The unitary R' matrix that we have considered in this paper gives rise to a non-trivial invariant of links. The discussion in this section summarizes our treatement of this invariant in [1]. Here we discuss the invariant associated with the specialization of R' with

$$R' = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & 0 & a \end{bmatrix}.$$

The invariant is calculated from a state summation associated with the matrix R' and can be shown to have the form

$$Z_K = 2(1 + (c^2/a^2)^{lk(K)})$$

for two-comonent links K, where $lk(K)$ denotes the linking number of the two components of K. We show that *for this specialization of the R' matrix the operator R' entangles quantum states exactly when it can detect linking numbers in the topological context.*

Here is a description of the state sum: label each component of the diagram with either 0 or 1. Take vertex weights of a or c for each local labelling of a positive crossing as shown in figure 15. For a negative crossing (obtained by interchanging over-crossing and under-crossing segments at a positive crossing) the corresponding labels are $1/a$ and $1/c$ (which are the complex conjugates of a and c repsectively, when a and c are unit complex numbers). Let each state (labelling of the diagram by zeros and ones) contribute the product of its vertex weights. Let $\Sigma(K)$ denote the sum over all the states of the products of the vertex weights. Then one can verify that $Z(K) = a^{-w(K)}\Sigma(K)$, where $w(K)$ is the sum of the crossing signs of the diagram K.

For example, view figure 16. Here we show the zero–one states for the Hopf link H. The 00 and 11 states each contribute a^2, while the 01 and 10 states contribute c^2. Hence

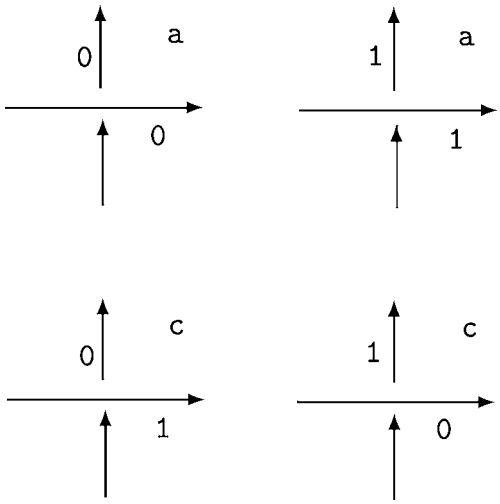

Figure 15. Positive crossing weights.

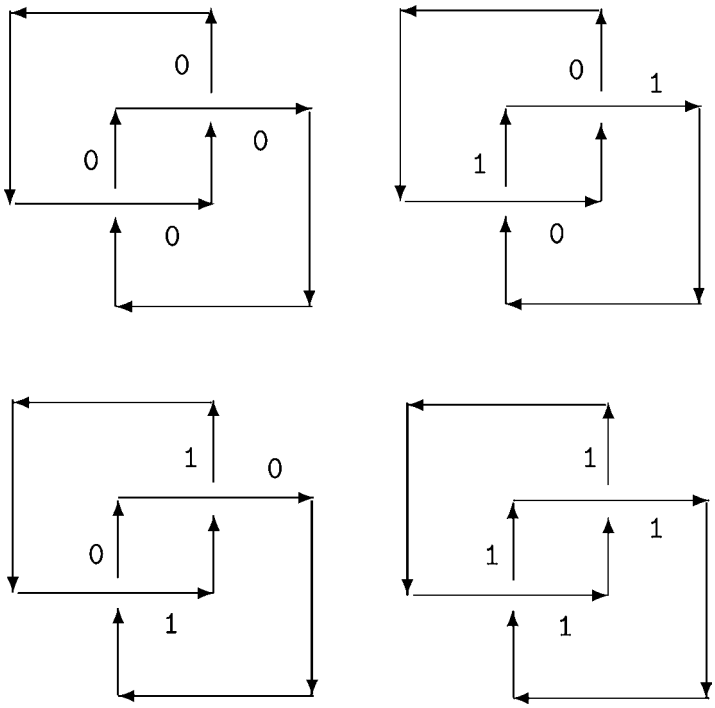

Figure 16. Zero–one states for the Hopf link.

$\Sigma(H) = 2(a^2 + c^2)$ and

$$a^{-w(H)}\Sigma(H) = 2(1 + (c^2/a^2)^1) = 2(1 + (c^2/a^2)^{lk(H)}),$$

as expected.

The calculation of the invariant in this form is an analysis of quantum networks with cycles in the underlying graph. In this form of calculation we are concerned with those states of the

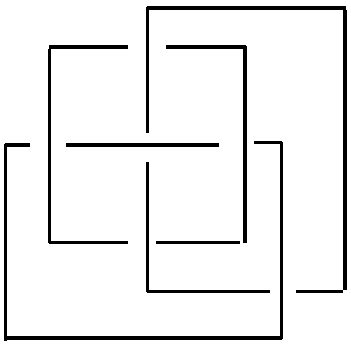

Figure 17. Borromean rings.

network that correspond to labellings by qubits that are compatible with the entire network structure. One considers only quantum states that are compatible with the interconnectedness of the network as a whole.

8.2. The question about invariants and entanglement

We have seen that there are examples, such as the one given above, where topological entanglement measures, and measures of quantum entanglement are related to one another. In that example we found the solution R' to the Yang–Baxter equation would, as an operator on states, entangle quantum states exactly when the invariant could measure linking numbers. We have also discussed the invariant assoicated with the universal gate R and shown that it detects many topological situations that are quite subtle. For example, it can measure the linkedness of the Borromean rings and the linkedness of the Whitehead link, both of which are situations where the linking numbers are zero. And yet, we have also given an example, in the previous section, of a representation of the braid group on three strands, B_3 (not constructed from a solution to the Yang–Baxter equation), that produces the Jones polynomial for closures of three-stranded braids, but is defined on a single qubit. Since this last representation acts only on one qubit, there is no entanglement associated with it. Therefore it remains, at this writing, unclear just what is the relationship between the quantum entangling properties of braid group representations and their ability to measure topological entanglement. In a sequel to this paper we will concentrate this analysis just on invariants assoicated with solutions to the Yang–Baxter equation.

8.3. The Aravind hypothesis

Link diagrams can be used as graphical devices and holders of information. In this vein Aravind [32] proposed that the entanglement of a link should correspond to the entanglement of a state. *Observation of a link would be modelled by deleting one component of the link.* A key example is the Borromean rings. See figures 7 and 17.

Deleting any component of the Boromean rings yields a remaining pair of unlinked rings. The Borromean rings are entangled, but any two of them are unentangled. In this sense, the Borromean rings are analogous to the GHZ state $|GHZ\rangle = (1/\sqrt{2})(|000\rangle + |111\rangle)$. Observation in any factor of the GHZ yields an unentangled state. Aravind points out that this property is basis dependent. We point out that *there are states whose entanglement after an observation is*

a matter of probability (via quantum amplitudes). Consider for example the state

$$|\psi\rangle = (1/2)(|000\rangle + |001\rangle + |101\rangle + |110\rangle).$$

Observation in any coordinate yields an entangled or an unentangled state with equal probability. For example,

$$|\psi\rangle = (1/2)(|0\rangle(|00\rangle + |01\rangle) + |1\rangle(|01\rangle + |10\rangle)),$$

so that projecting to $|0\rangle$ in the first coordinate yields an unentangled state, while projecting to $|1\rangle$ yields an entangled state, each with equal probability.

New ways to use link diagrams must be invented to map the properties of such states. *We take seriously the problem of classifying the topological entanglement patterns of quantum states*. We are convinced that such a classification will be of practical importance to quantum computing, distributed quantum computing and relations with quantum information protocols.

9. Braiding and topological quantum field theory

The purpose of this section is to discuss in a very general way how braiding is related to topological quantum field theory and to the enterprise [24] of using this sort of theory as a model for anyonic quantum computation. The ideas in the subject of topological quantum field theory are well expressed in the book [33] by Michael Atiyah and the paper [26] by Edward Witten. The simplest case of this idea is C N Yang's original interpretation of the Yang–Baxter equation [34]. Yang articulated a quantum field theory in one dimension of space and one dimension of time in which the R-matrix (meaning here any matrix satisfying the Yang–Baxter equation) was regarded as giving the scattering ampitudes for an interaction of two particles whose (let us say) spins corresponded to the matrix indices so that R_{ab}^{cd} is the amplitude for particles of spin a and spin b to interact and produce particles of spin c and d. Since these interactions are between particles in a line, one takes the convention that the particle with spin a is to the left of the particle with spin b, and the particle with spin c is to the left of the particle with spin d. If one follows the braiding diagram for a concatenation of such interactions, then there is an underlying permutation that is obtained by following the braid strands from the bottom to the top of the diagram (thinking of time as moving up the page). Yang designed the Yang–Baxter equation so that *the amplitudes for a composite process depend only on the underlying permutation corresponding to the process and not on the individual sequences of interactions.* The simplest example of this is the diagram for the Yang–Baxter equation itself as we have shown it in figure 1.

In taking over the Yang–Baxter equation for topological purposes, we can use the same intepretation, but think of the diagrams with their under- and over-crossings as modelling events in a spacetime with two dimensions of space and one dimension of time. The extra spatial dimension is taken in displacing the woven strands perpendicular to the page, and allows us to use both braiding operators R and R^{-1} as scattering matrices. Taking this picture to heart, one can add other particle properties to the idealized theory. In particular, one can add fusion and creation vertices where in fusion two particles interact to become a single particle and in creation one particle changes (decays) into two particles. Matrix elements corresponding to trivalent vertices can represent these interactions. See figure 18.

Once one introduces trivalent vertices for fusion and creation, there is the question of how these interactions will behave with respect to the braiding operators. There will be a matrix

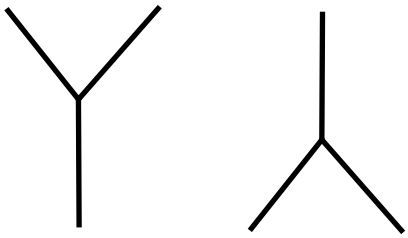

Figure 18. Creation and fusion.

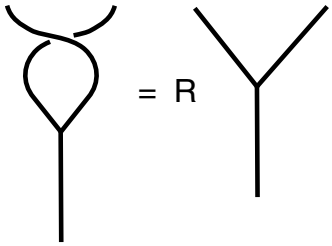

Figure 19. Braiding.

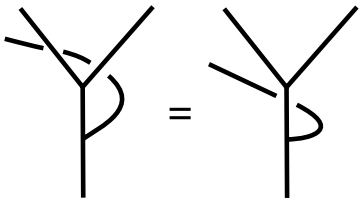

Figure 20. Intertwining.

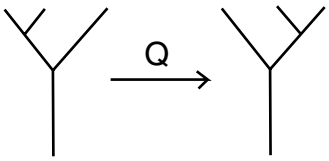

Figure 21. Recoupling.

expression for the compositions of braiding and fusion or creation as indicated in figure 19. Here we will restrict ourselves to showing the diagrammatics with the intent of giving the reader a flavour of these structures. It is natural to assume that braiding intertwines with creation as shown in figure 20 (similarly with fusion). This intertwining identity is clearly the sort of thing that a topologist will love, since it indicates that the diagrams can be interpreted as embeddings of graphs in three-dimensional space. Thus the intertwining identity is an assumption like the Yang–Baxter equation itself, that simplifies the mathematical structure of the model.

It is to be expected that there will be an operator that expresses the recoupling of vertex interactions as shown in figure 21 and labelled by Q. The actual formalism of such an operator will parallel the mathematics of recoupling for angular momentum. See for example [35]. If one just considers the abstract structure of recoupling, then one sees that for trees with four branches (each with a single root) there is a cycle of length five as shown in figure 22. One can start with

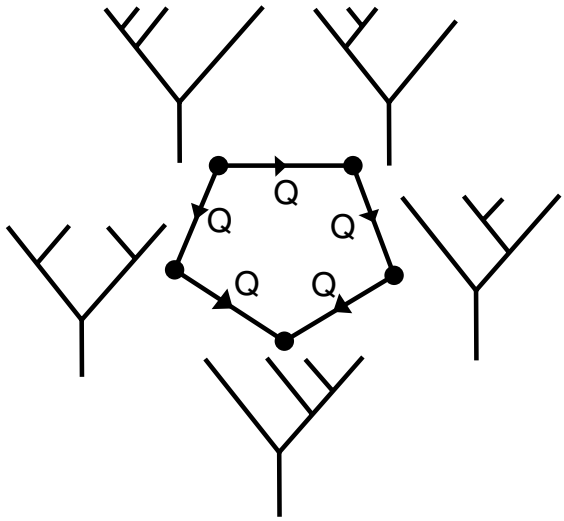

Figure 22. Pentagon identity.

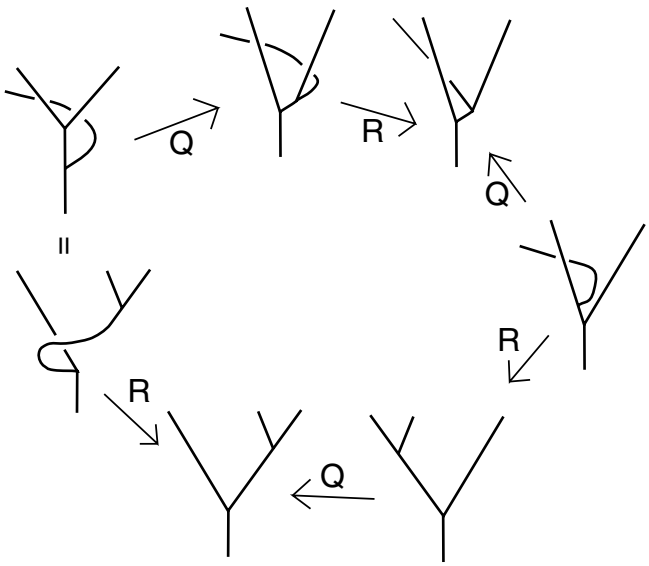

Figure 23. Hexagon identity.

any pattern of three vertex interactions and go through a sequence of five recouplings that bring one back to the same tree from which one started. *It is a natural simplifying axiom to assume that this composition is the identity mapping*. This axiom is called the *pentagon identity*.

Finally, there is a hexagonal cycle of interactions between braiding, recoupling and the intertwining identity as shown in figure 23. One says that the interactions satisfy the *hexagon identity* if this composition is the identity.

A *three-dimensional topological quantum field theory* is an algebra of interactions that satisfies the Yang–Baxter equation, the intertwining identity, the pentagon identity and the hexagon identity. There is no room in this summary to detail the remarkable way that these properties fit into the topology of knots and three-dimensional manifolds. As the reader can see, a three-dimensional *TQFT* is a highly simplified theory of point particle interactions in

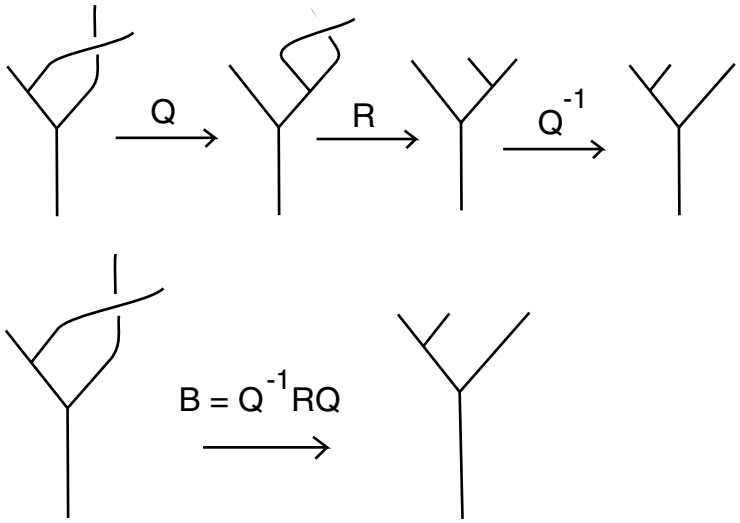

Figure 24. A more complex braiding operator.

(2 + 1)-dimensional spacetime. It can be used to articulate invariants of knots and links and invariants of three manifolds. The reader interested in the $SU(2)$ case of this structure and its implications for invariants of knots and three manifolds can consult [20], [35]–[38]. One expects that physical situations involving 2 + 1 spacetime will be approximated by such an idealized theory. It is thought for example that aspects of the quantum Hall effect will be related to topological quantum field theory [39]. One can imagine a physics where the space is two-dimensional and the braiding of particles corresponds to their exchanges as though circulating around one another in the plane. Such particles that, unlike fermions, do not just change the amplitude by a sign under interchange, but rather by a complex phase or even a linear combination of states, are called *anyons*. It is hoped that *TQFT* models will describe applicable physics. One can think about the possible applications of anyons to quantum computing. The *TQFT*s then provide a class of anyonic models where the braiding is essential to the physics and to the quantum computation. We have given a sketch of this approach here to give the reader a picture of one of the possibilities of using braiding in quantum computing.

The key point in the application and relationship of *TQFT* and quantum information theory is, in our opinion, contained in the structure illustrated in figure 24. There we show a more complex braiding operator, based on the composition of recoupling with the elementary braiding at a vertex. (This structure is implicit in the Hexagon identity of figure 23.) The new braiding operator is a source of unitary representations of braid group in situations (which exist) where the recoupling transformations are themselves unitary. This kind of pattern is implicitly utilized in the work of Freedman and collaborators [11], [22]–[25] and in the case of classical angular momentum formalism has been dubbed a 'spin-network quantum simulator' by Marzuoli and Rasetti [40].

10. Discussion

It is natural to expect relationships between topology and quantum mechanics. For example, Dirac [41] described the relationship between an observer and a fermion by using the properties

of twisted belts embedded in three-dimensional space. These properties vividly portray the consequences of the fact that $SU(2)$ double covers $SO(3)$. The rotation group $SO(3)$ and the unitary group $SU(2)$ are involved since a rotation of the observer is mapped to a unitary transformation of the wave function. The topology of the belt gives a direct way to image the properties of this connection, with one full rotation changing the sign of the wave function, while two full rotations do not change that sign. In the topological picuture, that relationship between one object and another object rotated relative to the first object is depicted by a belt connecting them. Topological properties of the belt mimic the orientation–entanglement relation.

How might such relationships between topology and quantum mechanics impinge upon quantum computing? The Dirac string trick suggests that topology may enter in the structure of non-locality and entanglement. On the quantum computing side, we know many uses for entangled states (e.g. teleportation protocols); and one wants to understand the role of entanglement in the efficiency of computing procedures. Entanglement in quantum mechanics and entanglement (linking and knotting) in topology can be related in a number of ways that give rise to a host of research questions.

We would like to state some general properties of this quest for relationship between topology and quantum mechanics: it is normally assumed that one is given the background space over which quantum mechanics appears. In fact, it is the already given nature of this space that can make non-locality appear mysterious. In writing $|\phi\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, we indicate the entangled nature of this quantum state without giving any hint about the spatial separation of the qubits that generate the first and second factors of the tensor product for the state. This split between the properties of the background space and properties of the quantum states is an artifact of the rarefied form given to the algebraic description of states, but it also points out that it is exactly the separation properties of the topology on the background space that are implicated in a discussion of non-locality.

Einstein, Podolsky and Rosen might have argued that if two points in space are separated by disjoint open sets containing them, then they should behave as though physically independent. Such a postulate of locality is really a postulate about the relationship of quantum mechanics to the topology of the background space. The Dirac string trick can be understood in a similar manner. In this way, we see that discussions of non-locality in quantum mechanics are in fact discussions of the relationship between properties of the quantum states and properties of the topology of the background space. Subtle questions related to metric and change of metric give rise to the well-known problems of quantum gravity (since general relativity must take into account the subtleties of the spacetime metric and the topology of spacetime).

Approaches such as Roger Penrose's spin networks and the more recent work of John Baez, John Barrett, Louis Crane, Lee Smolin, and others suggest that spacetime structure should emerge from networks of quantum interactions occurring in a pregeometric or process phase of physicality. In such a spin network model, there would be no separation between topological properties and quantum properties. We intend to carry this discussion to the spin network or to the spin foam level. It is our aim to deepen the discussion of topology and quantum computing to a level where this can be done in a uniform manner.

The spin network level is already active in topological models such as the Jones polynomial, the so-called quantum invariants of knots, links and three-manifolds, topological quantum field theories [26, 33], and related anyonic models for quantum computing [11, 22, 23]. For example, the bracket model [18]–[21] for the Jones polynomial can be realized by generalization of the Penrose $SU(2)$ spin nets to the quantum group $SU(2)_q$.

Since the advent of knot invariants such as the Jones polynomial, spin network studies have involved q-deformations of classical spin networks and the corresponding topological properties. These q-deformations are, in turn, directly related to properties of q-deformed Lie algebras (quantum groups, Hopf algebras) containing solutions to the Yang–Baxter equation. Solutions to the Yang–Baxter equation are maps $R : V \otimes V \longrightarrow V \otimes V$ on the tensor product of two vector spaces that represent topological braiding.

A direct question important for us is the determination of unitary solutions to the Yang–Baxter equation, and the investigation of both their topological properties and their quantum information properties. For the latter we want to know what role such solutions (matrices) can play in quantum computing. Specific questions are how such a matrix can be used in a quantum computational model for a link invariant, and can the matrix in question map unentangled states to entangled states. Some of these specific phenomena have been discussed in this paper. For the reader interested in pursuing these ideas further, we recommend the following as additional reading: [42]–[52].

Acknowledgments

Most of this effort was sponsored by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory, Air Force Materiel Command, USAF, under agreement F30602-01-2-05022. Some of this effort was also sponsored by the National Institute for Standards and Technology (NIST). The US Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright annotations thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Defense Advanced Research Projects Agency, the Air Force Research Laboratory, or the US Government. (Copyright 2004.) It gives the first author great pleasure to acknowledge support from NSF Grant DMS-0245588, and to give thanks to the University of Waterloo and the Perimeter Institute in Waterloo, Canada for their hospitality during the preparation of this research. It gives both authors pleasure to thank Michael Nielson for very useful comments on an early version of this paper. We thank Ferando Souza, Hilary Carteret and Niel de Beaudrap for helpful conversations.

References

[1] Kauffman L H and Lomonaco S J Jr 2002 *New J. Phys.* **4** 73
[2] Kauffman L H and Lomonaco S J Jr 2003 *Quantum Information and Computation, SPIE Proc., April 2003, Orlando, FL* ed E Donkor, A R Pinch and H E Brandt, vol 5105, pp 51–8
[3] Brylinski J L and Brylinski R 2002 *Mathematics of Quantum Computation* ed R Brylinski and G Chen (Boca Raton, FL: Chapman and Hall/CRC Press)
[4] Carteret H, Kauffman L and Lomonaco S, in preparation
[5] Baxter R J 1982 *Exactly Solved Models in Statistical Mechanics* (New York: Academic)
[6] Dye H 2003 *Quantum Inform. Process.* **2** 117 (*Preprint* quant-ph/0211050v3, August)
[7] Nielsen M and Chuang I 1999 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[8] Bremmer M J, Dawson C M, Dodd J L, Gilchrist A, Harrow A W, Mortimer D, Nielsen M A and Osborne T J 2002 *Phys. Rev. Lett.* **89** 247902
[9] Dye H, Kauffman L, Lomonaco S and Souza F, in preparation

[10] Roetteles M 2003 Private conversation
[11] Freedman M, Larsen M and Wang Z 2000 *Preprint* quant-ph/0001108v2, February
[12] Shende V V, Bullock S S and Markov I L 2003 *Preprint* quant-ph/030845v2, August
[13] Prasolov V V and Sossinsky A B 1997 *Knots, Links, Braids and 3-Manifolds* American Mathematical Society (Translations of Mathematical Monographs, vol 154)
[14] Birman J 1976 *Braids, Links and Mapping Class Groups, Ann. Math. Studies No. 82* (Princeton, NJ: Princeton University Press)
[15] Lambropoulou S and Rourke C P 1997 *Topol. Appl.* **78** 95
[16] Conway J H 1967 *Computational Problems in Abstract Algebra* (Oxford: Pergamon) pp 329–58
[17] Bordewich M, Freedman M, Lovasz L and Welsh D 2004 *Combin. Probab. Comput.* in press
[18] Kauffman L H 1987 *Topology* **26** 395
[19] Kauffman L H 1989 *AMS Contemp. Math.* **78** 263
[20] Kauffman L H 1991 *Knots and Physics* (Singapore: World Scientific) (2nd edn 1993, 3rd edn 2002)
[21] Kauffman L H 2002 *Quantum Computation and Information* ed S Lomonaco Jr (Providence, RI: AMS) pp 101–37
[22] Freedman M 2001 *Preprint* quant-ph/0110060v1, October
[23] Freedman M 1998 *Topological Views on Computational Complexity* Documenta Mathematica—Extra Volume ICM, pp 453–64
[24] Freedman M H, Kitaev A and Wang Z 2002 *Commun. Math. Phys.* **227** 587 (*Preprint* quant-ph/0001071)
[25] Freedman M 2000 *Preprint* quant-ph/0003128
[26] Witten E 1989 *Commun. Math. Phys.* **121** 351
[27] Gottesman D and Chuang I 1999 *Preprint* quant-ph/9908010v1, August
[28] Raussendorf R and Briegel H J 2002 *Preprint* quant-phys/0207183v1, July
[29] Lomonaco S 2002 *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium* PSAPM vol 58 (Providence, RI: AMS) pp 3–65
[30] Lomonaco S 2002 *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium* PSAPM vol 58 (Providence, RI: AMS) pp 305–49
[31] Lomonaco Jr S and Brandt H (ed) 2002 *Quantum Computation and Information* (Providence, RI: AMS)
[32] Aravind P K 1997 *Potentiality, Entanglement and Passion-at-a-Distance* ed R S Cohen, M Horne and J Stachel (Boston: Kluwer Academic) pp 53–9
[33] Atiyah M F 1990 *The Geometry and Physics of Knots* (Cambridge: Cambridge University Press)
[34] Yang C N 1967 *Phys. Rev. Lett.* **19** 1312
[35] Kauffman L H and Lins S 1994 *Temperley–Lieb Recoupling Theory and Invariants of Three-Manifolds, Ann. Studies* vol 114 (Princeton, NJ: Princeton University Press)
[36] Kohno T 1998 *Conformal Field Theory and Topology* (*AMS Trans. Math. Monographs* vol 210)
[37] Crane L 1991 *Commun. Math. Phys.* **135** 615
[38] Moore G and Seiberg N 1989 *Commun. Math. Phys.* **123** 177
[39] Wilczek F 1990 *Fractional Statistics and Anyon Superconductivity* (Singapore: World Scientific)
[40] Marzuoli A and Rasetti M 2002 *Phys. Lett.* A **306** 79
[41] Dirac P A M 1958 *Principles of Quantum Mechanics* (Oxford: Oxford University Press)
[42] Deutsch D 1985 *Proc. R. Soc.* A **400** 97
[43] Jones V F R 1985 *Bull. Am. Math. Soc.* **129** 103
[44] Kauffman L H and Baadhio R 1993 *Quantum Topology* (Singapore: World Scientific)
[45] Kauffman L H (ed) 1996 *The Interface of Knots and Physics* PSAPM vol 51 (Providence, RI: AMS)
[46] Kauffman L H 2002 *Quantum Computation* PSAPM vol 58, ed S Lomonaco, pp 273–303
[47] Lidar D A and Biham O 1997 *Preprint* quant-ph/9611038v6, September
[48] Linden N and Popescu S 1997 *Preprint* quant-ph/9711016
[49] Linden N, Popescu S and Sudbery A 1998 *Preprint* quant-ph/9801076
[50] Lomonaco Jr S (ed) 2002 *Quantum Computation* PSAPM vol 58 (Providence, RI: AMS)
[51] Meyer D A 1992 *Knots 90* (New York: Walter de Gruyter)
[52] Wootters W K 1997 *Preprint* quant-ph/9709029