An Introduction to the Theory of Topological Quantum Computing

Michael K. Spillane
University of Washington

Abstract

Topological quantum computing offers an excellent method to create fault-tolerant, quantum computers while using fewer qubits than other fault-tolerant methods. In this paper I will discuss the most popular form, the use of nonabelian anyons, which occur in 2D systems. In particular I will discuss Fibonacci Anyons and braids that simulate quantum gates to arbitrary accuracy.

Introduction

Topological invariants present a potentially effective way to prevent error in quantum computing. Topological invariants are those attributes of a system, which remain unchanged by small, local changes. This is exactly what is needed to perform fault-tolerant quantum computations. What still remains to be determined is what topological invariants can be used. There are ideas on how to use topology to prevent computation errors for trapped-ions, superconducting qubits. There are also techniques using superfluids ($p_x + ip_y$) combined with flying qubits and finally using braided anyons. Anyons have been shown to occur in certain types of 2D superfluids and are believed to occur also in fractional quantum Hall systems[1]. In this paper I will present an introduction to braid theory, anyons, and how the combination of these two theories may be used to perform quantum computations. It has been shown that for some anyon models topological quantum computing is capable of completing quantum computation with the same power as other forms of quantum computers, an important result[2]. Except where noted, all the references for the next four sections are from Professor John Preskill's lecture notes[2].

Braid Theory

Knots, links and braids have been of interest to humans since at least the time of Alexander the Great in the 4th century BCE. Knots became of interest to physicists when Lord Kelvin purposed the idea that atoms where each distinct knots [3]. Following this there was a large effort made by mathematicians and physicists to determine the fundamental knots. A representation of a knot was defined to be a closed polygonal curve in space. Links are then a combination of knots that are intertwined. It was not until later (1920s) that mathematicians became interested in representations of braids which were defined to be a set of n polygonal curves stretching from z = 0 plane (in $\mathbf{R}^3$) to the z = 1 plane where the k^{th} curve stretches from (1/2, k/n, 0) to (1/2, k/n, 1) and the z value is strictly increasing and the curves do not intersect[3].

Braids clearly have some algebraic properties. There is a clear identity braid, which is just formed by connecting the start and end points with straight lines. We can imagine "adding" two braids with the same number of strands. This addition will be associative" a(bc) = (ab)c. Similarly, we could imagine by exactly reversing the way we did the braiding, that we could add two braids which could be manipulated to obtain the identity (an inverse braid). Finally, if we add many braids together it is clear it will still remain a braid. So we now have a group.

Let us now think about how we would generate this group and what equalities we require of combinations of those generators so that we can determine if two braids are equivalent. Let us define σ_k to be the exchange of the k^{th} curve with $(k+1)^{st}$ curve where the k^{th} curve passes over the $(k+1)^{st}$ (see Figure 1). We then get the following set of identities:

$$\sigma_i \, \sigma_j = \sigma_j \, \sigma_I \text{ for } |i - j| < 3 \qquad (1)$$

$$\sigma_i \, \sigma_{i+1} \sigma_i = \sigma_{i+1} \, \sigma_i \, \sigma_{i+1} \, . \qquad (2)$$

The first of these equations is relatively obvious - two disjoint exchanges are commutative and the second can be seen in Figure 1. What is rather surprising is that these conditions are all which are required to define our braid group. We will use the second of these equalities (Eq. 2) later to talk about abelian anyons.

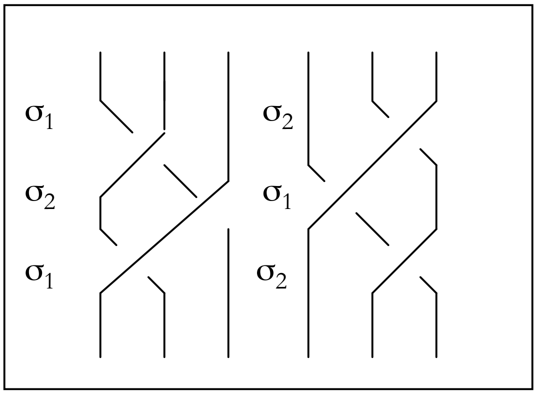

Figure 1. If you look closely you can see the two braids can be continuously deformed into each other without cutting any of the strands. This demonstrates the equality in Equation 2.

Anyons

Anyons are quasiparticles that occur in 2D systems. Unlike 1 and 3 dimensional systems, particles do not necessarily fall into the categories of fermions or bosons. This is a result of the topology of SO(2), the set of rotations in 2 space [2]. Anyons are able to carry charges that are fractions of the fundamental charge of the electron. The spin of these quasiparticles can take on any real value. This is of course related to their statistics and the fact that they are neither fermions nor bosons.

While anyons appear very different from bosons and fermions they do have some very important similarities. There are no physical processes that can create or destroy isolated anyons. This is important if we intend to use them in a quantum computer. If the anyons could spontaneously appear or disappear any quantum operation using them would fail. They also have antiparticles, which they can interact with to combine or annihilate. Anyons can also combine with other anyons that are not their antiparticle, which will be useful later.

Anyons come in two types, abelian and nonabelian. By braiding two anyons, they acquire up a topological phase similar to that found in the Aharonov-Bohm effect – that is the phase given to a charged particle accumulates when it travels around a solenoid. Just like the phase obtained in Aharonov-Bohm effect, the phase only depends on how many times the anyons wrap around each other and not the path they follow. In the one-dimensional representation of the braid group, we obtain $\sigma_j = e^{i\,\theta_j}$ for identical anyons. From Equation 2, we then get

$$e^{i\,\theta_j} = e^{i\,\theta_{j+1}} = e^{i\,\theta} \qquad (3)$$

where θ_j is the topological phase added by the σ_j operation and i is the imaginary number. So all exchanges of identical anyons have the same phase. Note if we let $\theta = 0$ we get bosons and if $\theta = \pi$ we get fermions. We see that in this one-dimensional representation of the braid group the exchanges are commutative so anyons that follow this form are called abelian anyons. Alternatively, we could have a multidimensional representation, which allow us to have nonabelian anyons (sometimes called nonabelions) as well. These nonabelian anyons are more useful for quantum computing than abelian anyons.

We now must consider how anyons can combine and split. Each model of anyons will have different fusion rules. The fusion rules determine the total charge, c, when a and b combine. These are written as

$$a \times b = \sum_c N^c_{ab} \qquad (3).$$

where N^c_{ab} is a nonnegative integer and the sum is over the complete set of labels of the composite. The composition rules are symmetric (a x b = b x a) so the possible charges do not depend on which side the anyon came from. Note that if N^c_{ab} is zero the charge, c, cannot be formed, while if it is one there is a unique way of obtaining c, and N^c_{ab} can also be greater than one. So N^c_{ab} represents the number of distinguishable ways that a charge c can be obtained. The distinguishable ways that a and b can be combined to form c then represents an orthonormal basis for a Hilbert space V^c_{ab}. V^c_{ab} is then called a fusion space and we denote the basis elements as

$$\{|ab; c, \mu>, \ \ \mu = 1,2,\ldots, N^c_{ab}\}.$$

There are isomorphisms between different spaces, which will not be discussed here since we will only be considering a specific case (the simplest one) and the formalism would get in the way. The next idea that is introduced is the R matrix, which is the braid operator, and the F matrix, which is the fusion operator. These are each specific to a given model. The last result of the formalism of anyons that should be noted is that the Hilbert space can be shown to be exponential in size making it a good space to do quantum computations.

The final important aspect we want our system to have is a mass gap. This means that the anyons are not massless. Because they are not massless, it takes more energy to create a pair of anyons (this is of course not the case with massless particles) so that if we cool the system down sufficiently there will be a low probability of anyons spontaneously forming and then wrapping around the anyons we are using for computation, which would effectively form an undesired gate or simply causing decoherence.

Fibonacci Anyons

Before talking about creating a quantum circuit using Fibonacci anyons a brief introduction is required. The Fibonacci model of anyons is the simplest nonabelian model. It also goes by the name "Yang-Lee model", but Fibonacci is more natural. The only nontrivial fusion rule is 1 x 1 = 0 + 1 where 1 is the trivial label (no anyon) and the only nontrivial label is 1 which is its own antiparticle. The statement then means that two anyons can either annihilate or fuse into a single anyon. This model is nonabelian because the two anyons can fuse in distinguishable ways. The name comes from the fact that the dimension of the Hilbert space of n anyons is the $(n+1)^{st}$ Fibonacci number (1, 1, 2, 3, 5, 8…). The total charge of a collection of Fibonacci anyons (fusing them all together) is either 0 or 1. This charge is also called "q-deformed" spin quantum number (q-spin)[4]. Fibonacci anyons are believed to exist in experimentally observed quantum Hall states as well as in rotating Bose condensates and quantum spin systems [4].

Quantum Computations with Fibonacci Anyons

Let us now consider how we might braid a quantum gate. We first must start by defining our qubits. Looking at the Fibonacci numbers we see that the fusion space for two anyons is 2 dimensional with the basis $|(\bullet,\bullet)_0>$ and $|(\bullet,\bullet)_1>$ where the 0 and 1 represent the total q-spin. After we add a third anyon the 3 dimensional space is spanned by $|((\bullet,\bullet)_0,\bullet)_1>$, $|((\bullet,\bullet)_1,\bullet)_1>$ and $|((\bullet,\bullet)_1,\bullet)_0>$. It is then customary to take $|0> = |((\bullet,\bullet)_0,\bullet)_1>$ and $|1> = |((\bullet,\bullet)_1,\bullet)_1>$ and the remaining is considered a noncomputational state. We can then measure the qubits by measuring the q-spin of the first two anyons. This could be done by doing local measurements when they are close together or using interference[4]. The R matrices for the two braids that can be formed using three qubits are shown in Figure 2 with an image the operation. We can for any possible braiding of these three qubits using these two matrices. The fact that the matrices are block diagonal means that only the phase of the noncomputational qubit is changed so we will not have leakage error into that state. Bonesteel et. al. (2005) searched through the braids with up to 46 exchanges to find approximate quantum gates to within $\varepsilon \sim 1 - 2 \times 10^{-3}$. Where the distance between to matrices $||U\text{-}V|| = O$ is defined as the square root of the largest eigenvaule of $O^{\dagger}O$. Unfortunately to increase the accuracy the number of braids too be analyzed grows exponential. However, there is a theorem by Solovay and Kitaev[5] that guaranties that a set of gates can be generated by finite braids to within a certain accuracy with the length of the braid increasing $\sim |\log \varepsilon|^c$ where c ~4.

Bonesteel *et. al* (2005) also considered the problem of creating a two qubit gate. The problem that immediately arises is the fact that the Hilbert Space is now 13 dimensional. The R-matrices are still block diagonal with blocks

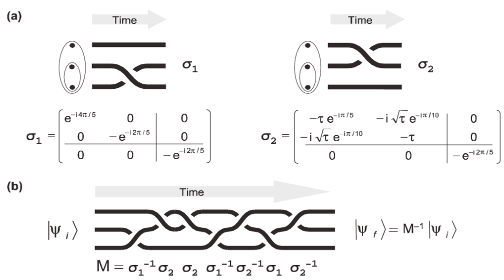

Figure 2.a) shows the basic braids with there matrices. b) This is an entangling of a single qubit. These are only representations in reality the anyons would have to remain far apart when not being braided to prevent lifting the topological protection (from 4).

of size 5 x 5 (total spin 0) and 8 x 8 (total spin 1). The theorem of Solovay and Kitaev again guaranties that in principle we can find gates to arbitrary accuracy. Bonesteel *et. al.* (2005) were able to construct braids to approximate controlled rotation gates, which only require finding a finite number of 3 quasiparticle braids. They do this by moving two control quasiparticle in unison around only two of the target quasiparticles (Figure 3). If the q-spin of the pair of quasiparticles is zero then this braiding is the identity while if the total q-spin is one it is not. By moving the two control quasiparticles in unison this method reduces the problem to finding three quasiparticle braids, which is what they had already done for single qubit gates. Solovay and Kitaev also created a method for reducing the error in a braid, known as construction[5]. Using this it is then possible to feasibly create two qubit gates to arbitrary accuracy.

Conclusion

There is a great deal of progress that has been made in the theory of topological quantum computing. There is still a significant amount of work to be done on the experimental side to find systems that contain anyons of the desired type and in learning how to manipulate them. Research also continues in the use of alternate techniques an interesting one being braid in superfluids (p_x+ip_y) combined with flying qubits.

[1] Chuanwei Zhang, Sumanta Tewari and S. Das Samra, Bells Inquality and Universal Quantum Gates in a Cold-Atom Chiral Fermionic p-Wave Superfluid. Phys. Rev. Lett. **99**, p. 220502 (2007). (In print)

[2] John Preskill, California Institute of Technology, Lecture Notes for Physics 219: Quantum Computation. ,http://www.theory.caltech.org/~preskill/ph219/topological.pdf/ (2004).

[3] Alexei Sossinsky, *Knots* (Harvard University Press, Cambridge, Mass., 2002), 1, **Vol. 1**, p. 127.

[4] N. E. Bonesteel, L. Hormozi, G. Zikos and S. H. Simon, Braid Topologies for Quantum Computation. Phys. Rev. Lett. **95**, p. 140503 (2005). (In print)

[5] A. Yu. Kitaev, A. H. Shen and M. N. Vyalyi, *Classical and Quantum Computation.* American Mathematical Society, Providence, 1999.

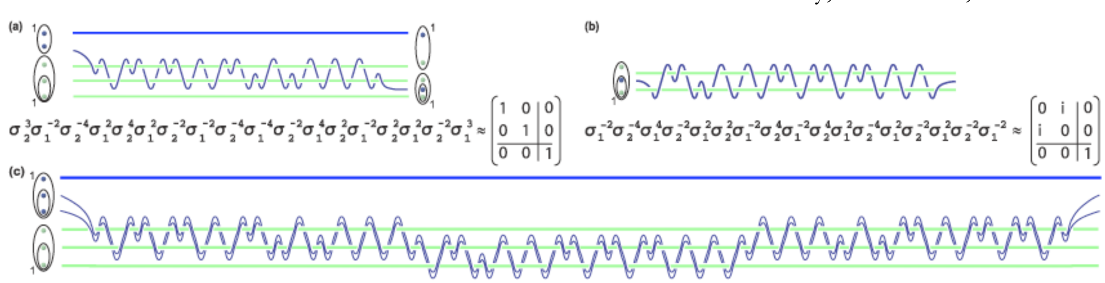

Figure 3.a) This braid is called an injection. It takes the two control quasiparticles and puts them inside the target qubit without changing any of the q-spins. b) This is then a controlled not operation once the two control quasiparticles are in the target qubit. c) This a combination of a and b and then the inverse of a to remove it safely from the target. This is then a control not gate with ε ~ $1.2x10^{-3}$(from 4).