Topological Quantum Computing with Only One Mobile Quasiparticle

S. H. Simon,[1] N. E. Bonesteel,[2] M. H. Freedman,[3] N. Petrovic,[1] and L. Hormozi[2]
[1]Bell Laboratories, Lucent Technologies, 700 Mountain Avenue, Murray Hill, New Jersey 07974, USA
[2]Department of Physics and NHMFL, Florida State University, Tallahassee, Florida 32310, USA
[3]Microsoft Research, One Microsoft Way, Redmond, Washington 98052, USA
(Received 23 September 2005; revised manuscript received 5 December 2005; published 23 February 2006)

In a topological quantum computer, universal quantum computation is performed by dragging quasiparticle excitations of certain two dimensional systems around each other to form braids of their world lines in 2 + 1 dimensional space-time. In this Letter we show that any such quantum computation that can be done by braiding n identical quasiparticles can also be done by moving a single quasiparticle around $n - 1$ other identical quasiparticles whose positions remain fixed.

DOI: 10.1103/PhysRevLett.96.070503 PACS numbers: 03.67.Lx, 03.65.Vf, 03.67.Pp, 73.43.−f

A remarkable recent theoretical advance in quantum computation is the idea of topological computation [1–7]. Using exotic two dimensional quantum systems, including certain fractional quantum Hall states [8–10], rotating Bose condensates [11], and certain spin systems [12,13], it has been shown [1,2] that universal quantum computations can be performed by simply dragging identical quasiparticle excitations around each other to form particular braids in the quasiparticles' world lines in 2 + 1 dimensions. Because the resulting quantum gate operations depend only on the topology of the braids formed by these world lines, the computation is intrinsically protected from decoherence due to small perturbations to the system. Realization of such a topological quantum computer has previously appeared prohibitively difficult in part because one would have to be able to manipulate many quasiparticles individually so as to braid them around each other in arbitrary patterns. In this Letter we show that universal quantum computation is possible using a very restricted subset of braid topologies (''weaves'') where only a single quasiparticle moves and all the other identical quasiparticles remain stationary. This simplification may greatly reduce the technological difficulty in realizing topological quantum computation.

We note that there are several different proposed schemes for topological quantum computation [1–5]. In this Letter we focus on systems of the so-called Chern-Simons-Witten type [2,6]. In these systems the topological properties are described by a gauge group and a ''level'' k which we write as a subscript. The cases of $SU(2)_k$ are known to correspond to the properties of certain quantum Hall states [8,9]. The $SU(2)_3$ case, which is thought to have been observed experimentally [8,10], is the simplest such model capable of universal quantum computation [2] and is very closely related to the Fibonacci anyon model, $SO(3)_3$ [6,12]. It may also be possible to realize theories of this type in rotating Bose condensates [11] and quantum spin systems [12,13].

The braid group B_n on n strands is a group generated by the $(n - 1)$ elements τ_1 through τ_{n-1} and their inverses. As shown in Fig. 1, The generator τ_p switches the strand at position number p with the strand at position $p + 1$ in a clockwise manner, whereas the inverse τ_p^{-1} switches these strands in a counterclockwise manner (we count strand positions from bottom to top). By multiplying these generators, any braid on n strands can be built (see Fig. 1). Reading an expression left to right such as $\tau_3\tau_2\tau_3^{-1}$ means one should do τ_3 first followed by τ_2 followed by τ_3^{-1}. We thus express a general braid as

$$\tau_{s(1)}^{r(1)}\tau_{s(2)}^{r(2)}\tau_{s(3)}^{r(3)}\ldots\tau_{s(p)}^{r(p)} \quad (1)$$

with p the total number of generators required to express the braid. Here each $s(i)$ takes a value in $1\ldots n - 1$ and each $r(i)$ is either ± 1.

A subset of the braid group B_n is the set of all braids that move only a single strand (the ''warp'' strand in the nomenclature of weaving) around $n - 1$ stationary strands (the ''weft''). We will call this subset weaves with $n - 1$ weft strands. An example of a weave is shown in Fig. 2. A braid that is a nonweave is shown in Fig. 1.

In topological quantum computation, qubits are encoded in clusters of quasiparticles. Dragging quasiparticles around each other to form braids in 2 + 1 dimensional space-time performs quantum operations in the Hilbert space of the system. Each braid generator corresponds to a particular unitary operation, and performing one braid followed by another corresponds to performing one quan-

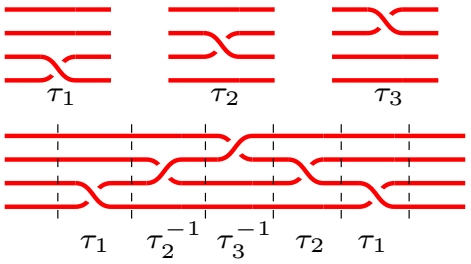

FIG. 1 (color online). Braids on four strands. Top: The three braid generators. Bottom: An arbitrary braid on four strands can be made by multiplying together the generators and their inverses. This braid shown here, $\tau_1\tau_2^{-1}\tau_3^{-1}\tau_2\tau_1$, is not a weave.

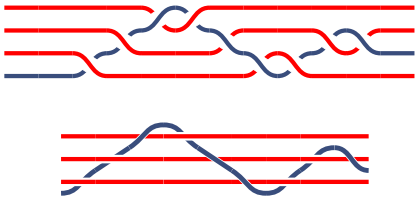

FIG. 2 (color online). The same weave with 3 weft strands drawn two different ways. In both pictures the warp strand is blue (dark gray) while the weft strands are red (light gray). In the lower picture it is clear that the three weft strands remain stationary.

tum operation followed by another. In this way, complicated gate operations can be built up from simple ones in the same way that complicated braids are built from the generators.

To build such a quantum computer it has previously been thought that one would have to be able to control the motion of n quasiparticles separately (with n proportional to the number of qubits in the system) such that arbitrary braids can be created. This amount of control of a (typically microscopic) quantum system is daunting technologically. To address this problem, in this work we will show that the set of weaves is also sufficient to perform universal quantum computation, and further that such a weaving computer is "efficient" in the computational sense. This result greatly simplifies the challenge of actually building a topological quantum computer. Now, instead of having to manipulate n quasiparticles, we need only fix the position of $n-1$ (weft) quasiparticles and control the motion of a single (warp) quasiparticle.

By definition, in a topological quantum computer, any quantum operation on the computational Hilbert space can be approximated arbitrarily accurately with a braid [2]. We will show (in part I below) that any quantum operation can also be approximated arbitrarily accurately with a weave. Then, given any braid on n quasiparticles made of p generators [Eq. (1)] we show (in part II below) one way to explicitly construct a weave that performs the same quantum operation as the given braid to within any desired accuracy ϵ. Further we show that the particular weave we construct is longer than the original braid by a factor of at most $Cnp|\log(\epsilon/(np))|^{\alpha}$ with C a constant depending on the particular topological theory and $\alpha \simeq 4$. Thus we demonstrate explicitly that our construction is computationally efficient (since such polynomial and log increases are acceptable for most quantum computational applications).

Part I: Dense Image of Pure Weaves. We define the group PB_n, known as the "pure braid group on n strands," to be the subgroup of the braid group on n strands, B_n, where each strand begins and ends in the same position. A subgroup of the pure braids on n strands is the "pure weaves" on $n-1$ weft strands, PW_{n-1}. These are analogously the weaves on $n-1$ weft strands where the warp particle begins and ends at the bottom position.

Given a group G with a subgroup H, we say that H is a "normal" subgroup of G if for each $g \in G$ and $h \in H$, we have $ghg^{-1} \in H$. We now show that PW_{n-1} is a normal subgroup of PB_n. Choosing any pure braid b and any pure weave w, we claim that bwb^{-1} is topologically equivalent to a pure weave (See Fig. 3). To see that this is true, we erase the warp strand as shown in Fig. 3, so b maps to a pure braid b' on $n-1$ strands, w maps to the identity on $n-1$ strands, and b^{-1} maps to b'^{-1}. Thus bwb^{-1} maps to $b'b'^{-1}$ meaning that we obtain the identity once we erase the warp strand. This implies that the original braid bwb^{-1} must have been a pure weave, proving that the pure weaves PW_{n-1} are a normal subgroup of the pure braids PB_n.

We now consider a topological system with n identical quasiparticles and a Hilbert space of dimension M. We assume that the pure braids PB_n have a dense image in $PU(M)$. Here $PU(M) = SU(M)/\mathbb{Z}_M$. [The $\mathbb{Z}_M$ subgroup of $SU(M)$ is generated by $e^{2\pi i/M}$ times the identity. Since this is just an overall phase factor, it is irrelevant for quantum computation.] The statement that PB_n has a dense image in $PU(M)$ means essentially that given an element $a \in PU(M)$ there exists a braid in PB_n corresponding to some element $\tilde{a} \in PU(M)$ in the Hilbert space whose value is arbitrarily close to a. This statement is necessarily true if one can do universal quantum computation with quasiparticles of the theory (which is what we are assuming). We note that for $SU(2)_k$ Chern-Simons-Witten theories it has been shown [2,14] that the pure braids on n strands do indeed have a dense image in $PU(M)$ for $k > 2$ and $k \neq 4, 8$ when $n = 3$, and for $k > 2$ and $k \neq 4$ when $n > 3$.

Since the group PB_n has a dense image in $PU(M)$, the normal subgroup PW_{n-1} of PB_n must then have an image which is dense in some normal subgroup of $PU(M)$. However, it is a well-known result [2] that $PU(M)$ has no normal subgroups except for the identity and the entire group $PU(M)$ itself. Since it is easy to show [15] that the pure weaves PW_{n-1} do not all map to the identity, PW_{n-1} must also have a dense image in all of $PU(M)$. Thus we

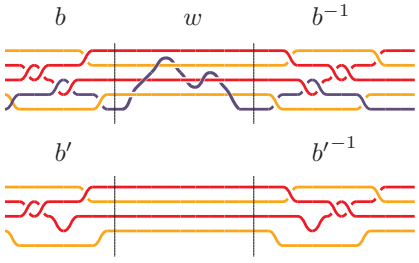

FIG. 3 (color online). Graphical proof that PW_{n-1}, the pure weaves with $n-1$ weft strands, is a normal subgroup of PB_n, the pure braids with n strands. In the top we construct a pure braid b on 5 strands followed by a pure weave w with 4 weft strands [the warp strand is blue (dark gray)] followed by the pure braid b^{-1}. To see that the resulting braid bwb^{-1} is a pure weave, we erase the warp strand as shown in the bottom. Since the remaining braid is the identity, bwb^{-1} must have been a weave.

have shown that any quantum operation can be approximated arbitrarily accurately with a weave.

To be more precise about the key piece of this argument we can state the following:

Lemma:—If a group H (such as PW_{n-1}) is a normal subgroup of G (such as PB_n) and G is mapped by a group homomorphism ρ densely into a compact topological group T [such as $PU(M)$] then $S = \text{closure}(\text{image}(H))$ is a normal subgroup of T.

Proof:—Assume S is not normal in T, so that there must exist a $t \in T$ such that tSt^{-1} is some subgroup S' different from S. Since G is mapped densely into T, there must exist a sequence of $t_i \in T$ which converges to t where each $t_i = \rho(g_i)$ for some $g_i \in G$. The limit of the sequence $\text{closure}(\text{image}(g_i H g_i^{-1}))$ must then be $\lim[t_i(\text{closure}(\text{image}(H))t_i^{-1}] = \lim t_i S t_i^{-1} = tSt^{-1} = S'$. But since H is normal in G, we must have $g_i H g_i^{-1} = H$ for any g_i so each element of the sequence must give S, contradicting our assumption that $S' \neq S$. (Q.E.D.)

Part II: Explicit Construction. Our construction is based on the "injection weave" first discussed in Ref. [7]. This is a weave on three strands (two weft strands), approximating the identity operation on the Hilbert space, which starts with the warp strand as the bottom of the three strands and ends with the warp strand as the top of the three strands. We can similarly define the inverse of the injection weave which moves the warp from the top to the bottom of the three strands.

The Kitaev-Solovay theorem [16] along with our above Lemma [17] guarantee that for any system of Chern-Simons-Witten type capable of topological quantum computation it is possible to efficiently find an injection weave of length $C|\log\epsilon|^{\alpha}$ where ϵ is a measure of the distance of the resulting gate from the identity, $\alpha \simeq 4$, and C is a constant depending on the particular topological theory we are considering. Thus, with linearly increasing complexity of the injection weave, the identity can be approximated exponentially more accurately [7,18].

In Ref. [7], examples of injection weaves were explicitly constructed for Fibonacci anyons [2,6]. One such example is shown in Fig. 4. [The same injection weave applies for the elementary quasiparticles of the experimentally observed [10] $SU(2)_3$ system.] It is useful to think back to the Fibonacci anyon case as a concrete example, although our construction is much more general.

FIG. 4 (color online). An example of an injection weave for the Fibonacci anyon model [$SO(3)_3$ or $SU(2)_3$]. This injection was first discussed in Ref. [7] and approximates the identity operation on the Hilbert space to better than one part in 10^2, while transferring the warp quasiparticle from the bottom to the top. Longer weaves will approximate the identity exponentially more closely with the weave becoming longer only linearly [7,16]. The box on the left establishes the notation used in Fig. 5 below.

We now consider multiple injections. Suppose the warp is strand number m at a given point in time and we would like to move the warp until it is strand number $m + 2q$ (with q an integer) without disturbing the state of the system. We do this by repeating the injection weave

$$M_{m;m+2q} = \begin{cases} I_{m,m+2} I_{m+2,m+4} \cdots I_{m+2q-2,m+2q} & q > 0 \\ I^{-1}_{m-2,m} I^{-1}_{m-4,m-2} \cdots I^{-1}_{m+2q,m+2q+2} & q < 0. \end{cases} \quad (2)$$

Here, $I_{a,a+2}$ is an injection weave acting on strands a, $a+1$, and $a+2$ where the warp starts at position a and ends at position $a+2$. Similarly, $I^{-1}_{a-2,a}$ is an injection acting on strands $a-2$, $a-1$, and a which moves the warp from position a to position $a-2$. Thus, the multiple injection $M_{m;m+2q}$ moves the warp from position m to position $m+2q$ while performing only (approximately) the identity operation on the Hilbert space. Note that $M_{m,m}$ is defined to be the identity, since no braiding is needed to move the warp from position m to position m.

We consider an arbitrary braid expressed as in (1) above. Starting with the warp on the bottom at position 1, we do multiple injections until the warp is in a position to make the first desired braid operation $\tau^{r(1)}_{s(1)}$. Defining $[a]_2 = a \bmod 2$, our first step is then $M_{1;s(1)-[s(1)]_2+1}$ which performs (approximately) the identity on the Hilbert space, but moves the warp an even number of strands over, placing it in position to do the desired $\tau^{r(1)}_{s(1)}$. After performing $\tau^{r(1)}_{s(1)}$, the warp is occupying an even numbered position. We then make multiple injections to move the warp to a position where it can do the next braid operation $\tau^{r(2)}_{s(2)}$, after which the warp occupies an odd number position again, and so forth. Generally, let us define

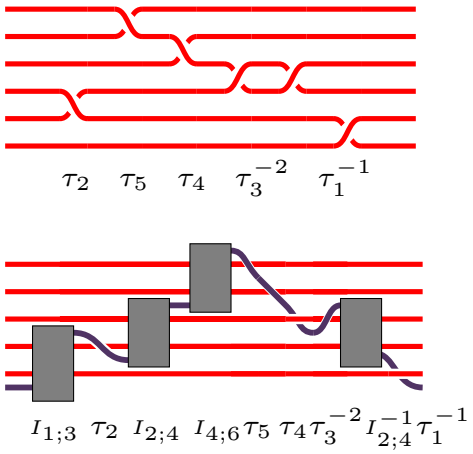

FIG. 5 (color online). We construct a weave (bottom) which produces the same quantum operation on the Hilbert space as some desired arbitrary braid (top). In the bottom, the shaded boxes represent injection weaves which have (approximately) no effect on the Hilbert space. This construction shows that, so long as an injection weave exists, weaves are just as capable as braids at performing efficient universal quantum computation.

$$\tilde{M}(i) = \begin{cases} M_{s(i-1)+[s(i-1)]_2;s(i)+[s(i)]_2} & \text{even } i \\ M_{s(i-1)-[s(i-1)]_2+1;s(i)-[s(i)]_2+1} & \text{odd } i \end{cases}. \quad (3)$$

Thus, defining $s(0) = 0$, we can write out the full weave that performs the same quantum operation as the braid written in expression (1) above

$$\tilde{M}(1)\tau_{s(1)}^{r(1)}\tilde{M}(2)\tau_{s(2)}^{r(2)}\tilde{M}(3)\ldots\tilde{M}(p)\tau_{s(p)}^{r(p)}. \quad (4)$$

Figure 5 shows this construction graphically. By construction, to the extent that $\tilde{M}$ correctly performs the identity on the Hilbert space, this weave performs the same operation on the Hilbert space as any given braid in expression (1). The constructed weave is longer than the given braid by no more than np times the length of the needed injection weave. Further, if we want to approximate the quantum operation of the original braid to within some accuracy ϵ, each $\tilde{M}$ need only be equal to the identity to within ϵ/p. Thus, each injection weave need only be equivalent to the identity to within $\epsilon/(np)$ which requires the injection to be length $C|\log(\epsilon/(np))|^{\alpha}$. Note that since the constant C is determined entirely from the injection weave on three strands, it is independent of n and p. Thus the total length of the constructed weave need be no longer than $Cnp|\log(\epsilon/(np))|^{\alpha}$ as claimed. This length estimate should be viewed as an upper bound and proof of principle. In fact, we expect that weaves may be efficiently found which are significantly shorter than those constructed here. Nonetheless, the concept of injection can also be used to design more practical weaves, as will be discussed in forthcoming work.

Further Comments: In this Letter we have nowhere discussed the initialization or readout steps required for quantum computation. This is a difficult problem that has not been satisfactorily answered anywhere in the literature for this type of topological quantum computer. It has been proposed that measurements and initialization could be achieved in principle using interference experiments [19,20], or by fusion of quasiparticles [1,2]. However, the precise initialization and measurement schemes will depend heavily on the particular nature of the realization of the computer when it is built.

The authors acknowledge G. Zikos for helpful conversations, and I. Berdnikov for his careful proofreading of this manuscript. N. E. B. and L. H. acknowledge support from US DOE Grant No. DE-FG02-97ER45639.

[1] A. Yu. Kitaev, Ann. Phys. (N.Y.) **303**, 2 (2003).
[2] M. Freedman, M. Larsen, and Z. Wang, Commun. Math. Phys. **227**, 605 (2002); **228**, 177 (2002); M. Freedman, A. Kitaev, M. Larsen, and Z. Wang, Bull. Am. Math. Soc. **40**, 31 (2003).
[3] R. W. Ogburn and J. Preskill, Lect. Notes Comput. Sci. **1509**, 341 (1999).
[4] C. Mochon, Phys. Rev. A **67**, 022315 (2003).
[5] C. Mochon, Phys. Rev. A **69**, 032306 (2004).
[6] J. Preskill, Quantum Computation, Lecture Notes for Physics Vol. 219, http://www.theory.caltech.edu/~preskill/ph219/ph219_2004.html.
[7] N. E. Bonesteel, L. Hormozi, G. Zikos, and S. H. Simon, Phys. Rev. Lett. **95**, 140503 (2005).
[8] N. Read and E. Rezayi, Phys. Rev. B **59**, 8084 (1999).
[9] J. K. Slingerland and F. A. Bais, Nucl. Phys. **B612**, 229 (2001).
[10] J. S Xia *et al.*, Phys. Rev. Lett. **93**, 176809 (2004).
[11] N. R. Cooper, N. K. Wilkin, and J. M. F. Gunn, Phys. Rev. Lett. **87**, 120405 (2001).
[12] P. Fendley and E. Fradkin, Phys. Rev. B **72**, 024412 (2005).
[13] M. Freedman, C. Nayak, K. Shtengel, K. Walker, and Z. Wang, Ann. Phys. (N.Y.) **310**, 428 (2004).
[14] Regarding our assumption that the image of PB_n is dense in $PU(M)$, if the image of the braid group B_n is dense in $PU(M)$ then since PB_n is a normal subgroup of B_n, and the image of PB_n is clearly not the identity, by using the same Lemma proved in this work PB_n is also dense in $PU(M)$ for these theories.
[15] To show that the image of PW_{n-1} is not the identity, we assume the converse. This would imply that the square of a braid generator is the identity. However, when the square of the braid generator is the identity, the representation of the braid group must be the finite symmetric group, which therefore contradicts the assumption that we started with a dense representation of PB_n.
[16] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation* (American Mathematical Society, Providence, 1999).
[17] In order to show that an injection weave can approximate the identity in the full Hilbert space of 3 strands, we consider a pure weave with zero total winding number times $\tau_1\tau_2^{-1}$. Such weaves have an image in $SU(2) \oplus \mathbf{1}$ and we need only find the identity in $SU(2)$ [2,7]. The pure weaves with zero winding number are a normal subgroup of PB_3 so the Lemma implies a dense image in $PU(2)$. In fact, the image is dense in $SU(2)$ since the only proper normal subgroup of $SU(2)$ is $\mathbb{Z}_2$ and the reasoning of [15] can be applied to exclude the possibility that $\mathbb{Z}_2$ is the image.
[18] For all $SU(2)_k$ models with $k > 2$ we have numerically found approximate injection weaves similar to those found for $k = 3$ in Ref. [7] and we have shown that they can be systematically improved to any desired accuracy [16]. Note that for $k = 4m$, the weave τ_i^{2m+1} provides an exact injection of finite length which transfers the warp over a single weft particle [9]. To perform arbitrary single qubit rotations it is necessary to efficiently find a sequence of elementary braiding operations which yield a matrix V which approximates a desired matrix U to whatever accuracy is required. The accuracy of a given approximation V to U can be measured by the trace distance $\epsilon = \|U - V\|$, where $\|A\| = \mathrm{tr}\sqrt{A^{\dagger}A}$. We find that brute force numerical searches of braiding patterns for three quasiparticles with $\sim$60 crossings can produce gates for which the trace distance to any desired single qubit gate is $\epsilon \sim 10^{-3}$.
[19] B. J. Overbosch and F. A. Bais, Phys. Rev. A **64**, 062107 (2001).
[20] S. Das Sarma, M. Freedman, and C. Nayak, Phys. Rev. Lett. **94**, 166802 (2005); A. Stern and B. I. Halperin, cond-mat/0508447; P. Bonderson, A. Kitaev, and K. Shtengel, cond-mat/0508616.