Resources required for topological quantum factoring

M. Baraban,[1] N. E. Bonesteel,[2] and S. H. Simon[3]

[1]*Department of Physics, Yale University, 217 Prospect Street, New Haven, Connecticut 06511, USA*
[2]*Department of Physics and National High Magnetic Field Laboratory, Florida State University, Tallahassee, Florida 32310, USA*
[3]*Rudolf Peierls Centre for Theoretical Physics, Oxford University, 1 Keble Road, Oxford OX1 3NP, United Kingdom*

(Received 24 March 2010; published 16 June 2010)

We consider a hypothetical topological quantum computer composed of either Ising or Fibonacci anyons. For each case, we calculate the time and number of qubits (space) necessary to execute the most computationally expensive step of Shor's algorithm, modular exponentiation. For Ising anyons, we apply Bravyi's distillation method [S. Bravyi, Phys. Rev. A **73**, 042313 (2006)] which combines topological and nontopological operations to allow for universal quantum computation. With reasonable restrictions on the physical parameters we find that factoring a 128-bit number requires approximately 10^3 Fibonacci anyons versus at least 3×10^9 Ising anyons. Other distillation algorithms could reduce the resources for Ising anyons substantially.

DOI: 10.1103/PhysRevA.81.062317 PACS number(s): 03.67.Lx, 73.43.−f

I. INTRODUCTION

Shor's algorithm is at the center of much of the excitement surrounding quantum computation. Classically, the time to factor a number of length $\mathcal{L}$ grows exponentially in $\mathcal{L}$, but given a sufficiently large quantum computer, Shor's algorithm could be used to factor in polynomial time [1]. Specifically, the most computationally expensive step of Shor's algorithm is modular exponentiation which scales as $\mathcal{L}^3$. Since internet security is based on the near impossibility of factoring large numbers, the ability to factor in polynomial time, or in other words, the existence of a sufficiently large quantum computer, would be of monumental importance. In this article, we will address the question of what *sufficiently large* means for a topological quantum computer.

Many different systems have been proposed as the building blocks for a quantum computer known as quantum bits or qubits, but we will focus on topologically protected qubits which are created using non-Abelian particles [2]. Topological systems are particularly attractive candidates for quantum computation because of their natural resistance to decoherence. Non-Abelian particles have the property that topological operations, or braiding the particles around each other at large distances, can rotate the system between its degenerate ground states. The ground-state degeneracy grows exponentially with the number of particles allowing groups of particles to store quantum information in the form of qubits [2,3].

The most commonly considered non-Abelian particle is the Majorana fermion, or Ising anyon, where it is most convenient to use four Ising anyons to form a single qubit. Ising anyons are expected to be the excitations of the $\nu = 5/2$ fractional quantum Hall state [4]. Additionally, there have been proposals to create Ising anyons in Sr_2RuO_4 thin films [5], cold atoms [6], and most recently in several varieties of strongly coupled spin orbit systems involving superconducting junctions [7]. While Ising anyons are the simplest example of a non-Abelian particle, braiding Ising anyons is not sufficient for universal quantum computation (UQC). Bravyi has suggested a method for combining topological and nontopological operations to allow for UQC with Ising anyons [8]. We will explore this method in detail below, but the basic strategy is to create entangled states using nontopological operations and then braid these states with the target qubits to perform gates that are not allowed topologically. We find that when the time to prepare these entangled states is large compared to the time to run the algorithm, the number of qubits required to perform the algorithm scales approximately as the number of gates, $\mathcal{N}$, which is proportional to $\mathcal{L}^3$.

A second type of non-Abelian particle are Fibonacci anyons which are expected to be the excitations of the $\nu = 12/5$ fractional quantum Hall state [9] and exist in certain toy lattice models [10]. Here it is convenient to use three Fibonacci anyons to form a single qubit. Since braiding Fibonacci anyons is sufficient for UQC, the number of Fibonacci anyons needed to factor a number of length $\mathcal{L}$ scales as $\mathcal{L}$ rather than $\mathcal{L}^3$. Practically, this means that factoring a 128-bit number requires approximately 10^3 Fibonacci anyons rather than 3×10^9 Ising anyons. While 10^9 is a huge number, Ising anyons remain attractive as a possible platform for quantum computation because, as shown by Bravyi [8], and seen explicitly below, there is a high error tolerance for the nontopological operations necessary to prepare the states.

To estimate the number of particles necessary for modular exponentiation, we will assume that all braid operations can be performed perfectly and that error only results from the error intrinsic in the gates themselves. For Ising anyons, the error stems from the nontopological operations needed to prepare the entangled states, while for Fibonacci anyons, the length of the braid determines the accuracy of the gate. In this paper, all errors will be stated as error probabilities (the *square* of the amplitude), and for both Ising and Fibonacci anyons, the error per gate must be less than or on the order of $1/\mathcal{N}$ where $\mathcal{N}$ is the total number of gates [11]. Additionally, we assume that the state of the qubit can be measured efficiently and with negligible error (which can always be achieved by repetitive measurements). The number of NOT, CNOT (controlled-NOT), and CCNOT (controlled-controlled-NOT) gates required for efficient modular exponentiation is proportional to $\mathcal{L}^3$ and was calculated precisely in Ref. [12]. For $\mathcal{L} = 128$, the total number of gates is $\mathcal{N} \approx 10^9$.

II. ISING ANYONS

Bravyi's method to achieve UQC with Ising anyons uses nontopological operations to poorly approximate the one- and two-qubit states $|a_4\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$ and $|a_8\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$. These states are then distilled in a process that takes many states with large error to a single state with smaller error using only topological operations and measurements [8,14]. States with arbitrarily small error can be produced by repeating the distillation process. The purified $|a_4\rangle$ and $|a_8\rangle$ states are then braided with the target qubits to implement the controlled $\pi/4$ phase gate, $\Lambda(e^{i\pi/4})$, and CNOT gates. The combination of CNOT and $\Lambda(e^{i\pi/4})$ allows for UQC with Ising anyons [13].

We will calculate how many qubits and how many operations are necessary to first distill the states and then execute the modular exponentiation algorithm. Reference [8] carried out a similar calculation and found that to distill $\mathcal{N}$ states, the number of operations and qubits necessary scaled as $\mathcal{N}(\ln\mathcal{N})^3$. This calculation assumed that the error in the initial states was asymptotically small, and in this limit, the distillation procedure is successful nearly 100% of the time. Since the probability of a successful distillation vanishes as the initial error approaches an upper bound, the number of qubits required to distill one state depends strongly on the initial error. Additionally, the calculation did not account for the possibility of reusing qubits or performing distillation rounds in parallel. In theory, one could imagine starting with enough qubits to distill all $\mathcal{N}$ states simultaneously without qubit reuse and then performing the modular exponentiation. This would minimize the time; however, as we will see, it would also require a gigantic number of qubits. In our calculation, we will not assume asymptotically small initial error and we will explore the balance between the time and space requirements by combining parallel operations with reusing qubits. Initially, since $\mathcal{N}$ distilled states are required to perform the algorithm, let us assume we have at least $\mathcal{N}$ qubits to work with (which is already a large number) and we will attempt to perform the full distillation and algorithm with no more than this number (we will further examine this requirement below).

The number of qubits necessary to distill a single $|a_8\rangle$ state is shown in Fig. 1(a) where $|a_8\rangle$ distillation is only successful when the initial error is less than 0.38. Notice that even for a relatively large initial error, the number of qubits to distill one $|a_8\rangle$ state is small compared to $\mathcal{N}$ for $\mathcal{L} = 128$. Given our attempt to limit the number of qubits, we choose to create $\mathcal{N}$ $|a_8\rangle$ states using $O(\mathcal{N})$ qubits. Specifically, we will start with about $\mathcal{N}$ poorly approximated $|a_8\rangle$ states and perform the distillation algorithm in parallel on all these initial states. This will result in a small fraction of the initial qubits being converted into fully distilled $|a_8\rangle$ states. The remainder of the qubits can be reinitialized to poor approximations of $|a_8\rangle$ and again distilled in parallel to purified $|a_8\rangle$ states. By repeating this process, nearly all the initial qubits can be converted into fully distilled $|a_8\rangle$ states. Note that the distillation process ends by measuring the qubits which are not part of the distilled state. Since these qubits are no longer entangled with the purified state, they can easily be reused in a subsequent distillation.

$|a_4\rangle$ distillation has an added complication because $|a_8\rangle$ states are required in the distillation process. At each level of distillation, the $|a_8\rangle$ states must have an error at least as small as the final $|a_4\rangle$ states. The number of qubits to distill a single $|a_4\rangle$ state is shown in Fig. 1(b), where the qubits needed for the $|a_4\rangle$ and $|a_8\rangle$ states are plotted separately, and the maximum error for the initial $|a_4\rangle$ state is 0.14. Notice the number of qubits needed for $|a_8\rangle$ states sometimes decreases as the initial error increases. These decreases result from a technicality where less exact $|a_8\rangle$ states are required within the $|a_4\rangle$ distillation round. To avoid confusion, we will not plot these nonmonotonicities in the future as the distillation can always be run assuming the larger error.

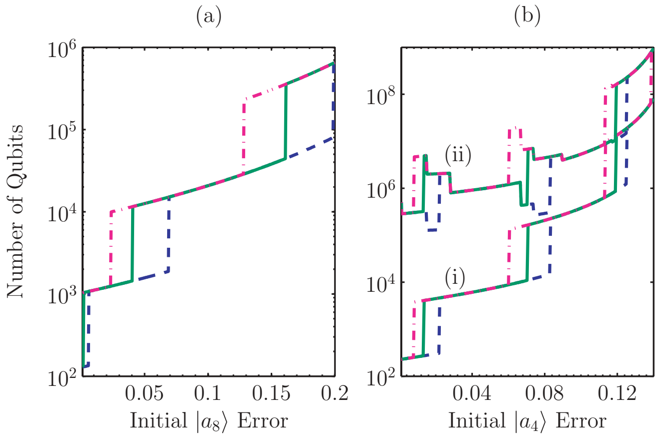

FIG. 1. (Color online) Plot (a) shows the number of qubits required to create a single $|a_8\rangle$ state with final error of 10^{-9} (dashed), 10^{-11} (solid), and 10^{-13} (dash-dot). The jumps indicate where the number of distillation levels increases by one, with plateau at 0.1 being four purification rounds. Plot (b) shows the number of qubits to create a single $|a_4\rangle$ state where (i)/(ii) is the qubits to make $|a_4\rangle/|a_8\rangle$ states. The initial error of the $|a_8\rangle$ states is taken to be 0.01, and the final errors for $|a_4\rangle$ are the same as plot (a).

To distill many $|a_4\rangle$ states, we will again choose to minimize the space requirements and use only $O(\mathcal{N})$ qubits to distill $\mathcal{N}$ $|a_4\rangle$ states. Since the number of qubits needed to make $|a_8\rangle$ states for a single $|a_4\rangle$ distillation (we will call these states $|a_8^{(4)}\rangle$) approaches $\mathcal{N}$ for $\mathcal{L} = 128$, our distillation scheme will be to dedicate approximately $\mathcal{N}$ qubits to making $|a_8^{(4)}\rangle$ states. We will then make as many $|a_8^{(4)}\rangle$ states as possible, do the $|a_4\rangle$ distillation, go back and reuse the qubits to make more $|a_8^{(4)}\rangle$ states, do another round of $|a_4\rangle$ distillation and repeat this process until the $|a_4\rangle$ states are fully distilled. $|a_4\rangle$ distillation is slow compared to $|a_8\rangle$ distillation, so when considering the total resources required, there will be a one to one trade-off between space and time that depends on the number of qubits dedicated to $|a_8^{(4)}\rangle$ production.

The results for how many qubits and how much time is required to perform modular exponentiation with Ising anyons are shown in Fig. 2. We define the time to perform one braid as a time step, and our calculations assume that a measurement can also be performed in a single time step. This assumption is probably unrealistic, but currently no model exists for estimating the time of a measurement. Measurements account for between 5% and 8% of the operations while running the distillation and executing the CNOT and CCNOT gates with the remainder being topological braids. If the time to perform a measurement is an order of magnitude longer than to perform a braid, then the total time will nearly double from that plotted

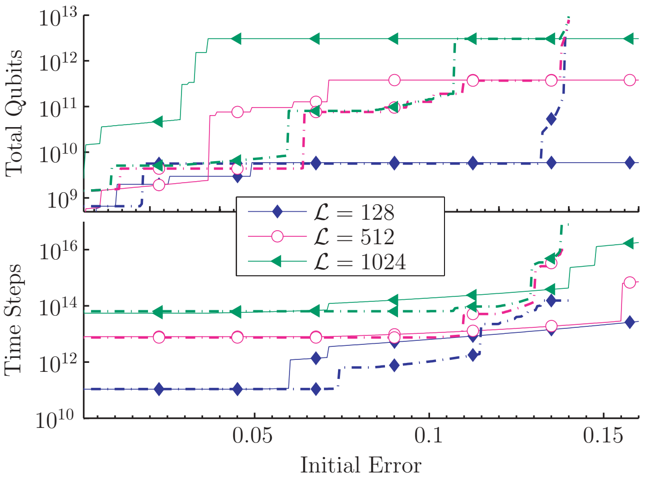

FIG. 2. (Color online) Total qubits and time steps necessary for modular exponentiation. The connected (dashed) lines are for changing the initial error of the $|a_8\rangle$ ($|a_4\rangle$) states while the $|a_4\rangle$ ($|a_8\rangle$) initial error is held constant at 0.01.

in Fig. 2 (this may be the case if repetitive measurement is required to obtain reliability).

Figure 2 can be considered in three regimes which are sketched in Fig. 3. When the initial error is small enough, t_{dist}, the time to distill all the required $|a_8\rangle$ and $|a_4\rangle$ states as outlined above, is short compared to the time to run the algorithm, t_{alg}. Rather than distilling the states all at once, we will minimize the number of qubits subject to the constraint that the total distillation time is comparable to t_{alg}. In this model, states are distilled, used to perform the algorithm, and then the qubits are reused to distill more states and continue the algorithm, and so on until the algorithm is completed. For any given $\mathcal{L}$, there always exists an initial error small enough such that the time to run the algorithm dominates, so state distillation does not need to change the scaling of the total time. In Figs. 2 and 3, this regime is seen where the time is nearly flat and the number of qubits is increasing.

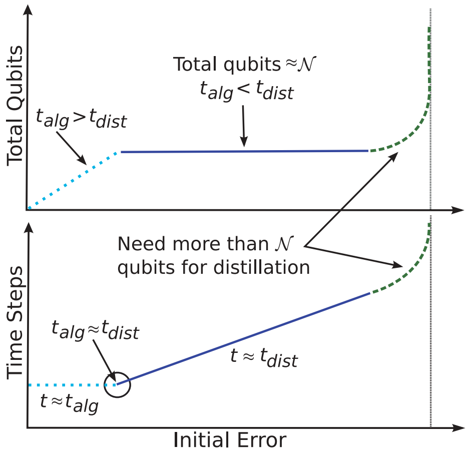

FIG. 3. (Color online) Cartoon sketch to help clarify Fig. 2. The three regimes which describe our results are when the time to run the algorithm, t_{alg}, is (a) greater than t_{dist}, (b) less than t_{dist}, and (c) when the number of qubits to distill a single state is comparable or large compared to $\mathcal{N}$. These three regimes are seen in Fig. 2 for $\mathcal{L} = 512$ while changing the initial error of $|a_8\rangle$ (solid line) for the approximate values (a) 0–0.07, (b) 0.07–0.35, and (c) 0.35–0.38 (not shown).

For larger values of the initial error, t_{dist} becomes large compared to t_{alg}, and we choose to use $O(\mathcal{N})$ qubits to distill all the states at once as described previously. In this case, the time does not depend directly on $\mathcal{L}$, but rather on the number of distillation rounds necessary to fully purify the $|a_4\rangle$ and $|a_8\rangle$ states. Hence, the time is nearly independent of $\mathcal{L}$ across a wide range of values and increases as the initial error increases. We choose the total number of qubits to scale as $\mathcal{N}$, but there is approximately a one to one trade-off between space and time. Conceivably, the number of qubits could be significantly reduced, but the total time would increase comparably. Additionally, for any initial error, there is always an $\mathcal{L}$ large enough to return us to the previous region where $t_{\mathrm{dist}} < t_{\mathrm{alg}}$.

Finally, as the initial error approaches its upper bound, the number of qubits to distill a single state becomes comparable and eventually exceeds $\mathcal{N}$. Once this happens, both the total number of qubits and total distillation time diverge. Note that the time does not exhibit a strong divergence in Fig. 2 as the initial error of the $|a_4\rangle$ states is increased because the initial $|a_8\rangle$ error remains small. The details of Fig. 2 depend on the exact distillation scheme, but the qualitative results sketched in Fig. 3 are more universal.

Using the results from Ref. [15] and the distillation scheme in Fig. 2, we can estimate the size of a $\nu = 5/2$ sample and the total time necessary to perform modular exponentiation when $\mathcal{L} = 128$. For approximately 10^9 gates, each gate must have error $\lesssim 10^{-9}$. Taking the initial $|a_4\rangle$ and $|a_8\rangle$ error to be 0.01, we need approximately 10^{11} time steps and 3×10^9 quasiparticles (qp's) to create all the states and perform the algorithm (see Fig. 2). To manipulate the qp's, we apply an electric field with magnitude much less than $\sim\Delta/(e^*\ell^*)$ to avoid particle-hole pair creation where Δ is the gap of the 5/2 state, $e^* = e/4$ is the qp charge and $\ell^* = 2\ell$ is the effective magnetic length. This results in a maximum $E \times B$ drift velocity of order $\Delta\ell/\hbar$. Using the decay length from Ref. [15], and assuming $\Delta = 1$ K, we find that the qp's need to be separated by at least 100ℓ and that the maximum step rate is 30 MHz. Modern single electron pumps can function at a rate of nearly 20 MHz with error rates as low as 15 per 10^9 [16], so achieving 30 MHz with comparably low error seems plausible. At this step rate, the calculation would take approximately 3×10^3 s on a sample that is at least 10×10 cm. While we can trade some amount of space for time, if one were to reduce the space by more than a few orders of magnitude, the runtime would become sufficiently long that classical computers could potentially compete. Parameters will differ and may be more favorable for other potential systems of Ising anyons [5–7].

III. FIBONACCI ANYONS

Computation with Fibonacci anyons is in many ways much simpler than using Ising anyons. Since braiding Fibonacci anyons is sufficient for UQC, we only need to find a braid to implement the desired gate. Additional entangled states to act on the target qubits are not necessary, so the space needed to perform modular exponentiation will be $O(\mathcal{L})$, the length

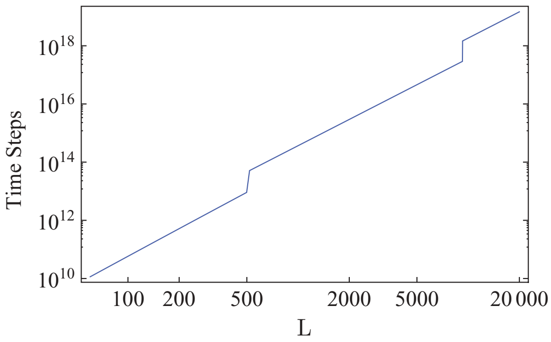

FIG. 4. (Color online) Number of time steps needed to complete modular exponentiation with Fibonacci anyons. Each jump is where an additional SK iteration is required, and for $\mathcal{L} \lesssim 500$, the braid is determined solely by the brute force search method.

of the number to factor. Further, only $O(\mathcal{L})$ measurements are required at the end of the calculation. However, Fibonacci anyons do not naturally implement NOT, CNOT, or CCNOT gates [17], so the challenge is to find a braid which approximates the desired gate to the necessary level of accuracy.

Brute force searches for braids have found that gate error becomes exponentially small as the braid length is increased linearly [18]; however, due to computational difficulty, the longest brute force braid available is about 80 steps with an error of about 10^{-10}. The accuracy of any braid can be improved using the Solovay-Kitaev (SK) algorithm [13]. With each iteration of SK, the error improves as $\epsilon_1 \sim c\epsilon_0^{3/2}$ and the braid length increases by a factor of 5. Therefore, we can again construct gates with arbitrarily small error, but at the expense of the braid length growing as 5^n, where n is the number of SK iterations. (Other schemes to obtain longer and more accurate braids may replace or be combined with SK beyond where brute force searches are feasible [19].)

Figure 4 shows the time to complete modular exponentiation using Fibonacci anyons as a function of $\mathcal{L}$. The total space scales as $\mathcal{L}$ and is $2\mathcal{L} + 3$ for this specific implementation of modular exponentiation [12]. For $\mathcal{L} = 128$, modular exponentiation requires 259 qubits (777 Fibonacci anyons). The time will be proportional to the braid length per gate times the number of gates, which is approximately 10^{11} time steps. Assuming a comparable minimum distance between qp's in the $\nu = 12/5$ state as the 5/2 state, the gap in the 12/5 state restricts the maximum step rate to about 3 MHz, so this computation would take on the order of 3×10^4 s.

To summarize, we explore the space and time requirements of Bravyi's distillation technique for Ising anyons. We find a good balance by producing $\mathcal{N}$ nontopological gates using $O(\mathcal{N})$ qubits. For this to succeed, the initial error in the $|a_4\rangle$ and $|a_8\rangle$ states must be small enough such that the number of qubits needed to distill a single $|a_8\rangle$ or $|a_4\rangle$ state is small compared to $\mathcal{N}$. When the time to run the algorithm is small compared to the time to distill states, we can reduce the space even further by distilling the states in batches while running the algorithm. We note that we have made certain assumptions concerning the trade-offs between space and time which we believe are appropriate and would give the best possible outcome in a realistic system. However, other choices can be made, and the results can be worked out from the details we provide.

Note added: Recently, we have learned of an unpublished method that allows for CNOT without $|a_8\rangle$ distillation [20]. Analysis of this new algorithm is beyond the scope of the current work, but rough estimates suggest that this new scheme could reduce t_{dist} by a factor of $\sim 10^5$ compared to the example presented here.

ACKNOWLEDGMENTS

The authors are grateful to M. Freedman and P. Bonderson for informing us of Ref. [20]. M.B. is supported by National Science Foundation Grant No. DMR-0603369, and N.E.B is supported by US Department of Energy Grant No. DE-FG02-97ER45639.

[1] P. Shor, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, 1994), pp. 124–134.

[2] C. Nayak *et al.*, Rev. Mod. Phys. **80**, 1083 (2008).

[3] A. Kitaev, Ann. Phys. **303**, 2 (2003).

[4] G. Moore and N. Read, Nucl. Phys. B **360**, 362 (1991).

[5] S. Das Sarma, C. Nayak, and S. Tewari, Phys. Rev. B **73**, 220502(R) (2006).

[6] V. Gurarie, L. Radzihovsky, and A. V. Andreev, Phys. Rev. Lett. **94**, 230403 (2005); S. Tewari, S. Das Sarma, C. Nayak, C. Zhang, and P. Zoller, *ibid.* **98**, 010506 (2007); N. R. Cooper and G. V. Shlyapnikov, *ibid.* **103**, 155302 (2009).

[7] L. Fu and C. L. Kane, Phys. Rev. Lett. **100**, 096407 (2008); J. D. Sau, R. M. Lutchyn, S. Tewari, and S. Das Sarma, *ibid.* **104**, 040502 (2010); P. A. Lee, e-print arXiv:0907.2681 (2009).

[8] S. Bravyi, Phys. Rev. A **73**, 042313 (2006).

[9] N. Read and E. H. Rezayi, Phys. Rev. B **59**, 8084 (1999); E. H. Rezayi and N. Read, *ibid.* **79**, 075306 (2009).

[10] M. A. Levin and X. G. Wen, Phys. Rev. B **71**, 045110 (2005); P. Fendley, Ann. Phys. **323**, 3113 (2008).

[11] This model assumes uncorrelated and phase coherent random errors. Additionally, for Fibonacci anyons the errors must add incoherently. If any of these conditions are not met, a worst case situation would require gates with accuracy of $\mathcal{O}(1/\mathcal{N}^2)$.

[12] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, Phys. Rev. A **54**, 1034 (1996).

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computing and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[14] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[15] M. Baraban, G. Zikos, N. Bonesteel, and S. H. Simon, Phys. Rev. Lett. **103**, 076801 (2009).

[16] M. W. Keller *et al.*, Science **285**, 1706 (1999).

[17] M. H. Freedman and Z. Wang, Phys. Rev. A **75**, 032322 (2007).

[18] L. Hormozi, G. Zikos, N. E. Bonesteel, and S. H. Simon, Phys. Rev. B **75**, 165310 (2007).

[19] M. Burrello, H. Xu, G. Mussardo, and X. Wan, Phys. Rev. Lett. **104**, 160502 (2010); R. Mosseri, J. Phys. A: Math. Theor. **41**, 175302 (2008).

[20] P. Bonderson *et al.* (unpublished).