Topological Quantum Computation

R. Walter Ogburn and John Preskill

California Institute of Technology, Pasadena, CA 91125, USA
reuben@cco.caltech.edu, preskill@theory.caltech.edu

Abstract. Following a suggestion of A. Kitaev, we explore the connection between fault-tolerant quantum computation and nonabelian quantum statistics in two spatial dimensions. A suitably designed spin system can support localized excitations (quasiparticles) that exhibit long-range nonabelian Aharonov-Bohm interactions. Quantum information encoded in the charges of the quasiparticles is highly resistant to decoherence, and can be reliably processed by carrying one quasiparticle around another. If information is encoded in pairs of quasiparticles, then the Aharonov-Bohm interactions can be adequate for universal fault-tolerant quantum computation. This paper was presented at the 1st Nasa International Conference on Quantum Computing and Quantum Communications, February 17-20, 1998, and published in Lecture Notes in Computer Science 1509: 341-356 (1999).

1 Fault-tolerant quantum computation

Quantum computers appear to be capable, at least in principle, of solving certain problems far faster than any conceivable classical computer[1]-[3]. In practice, though, quantum computing technology is still in its infancy. While a practical and useful quantum computer may eventually be constructed, we cannot clearly envision at present what the hardware of that machine will be like. Nevertheless, we can be quite confident that any practical quantum computer will incorporate some type of error correction into its operation. Quantum computers are far more susceptible to making errors than conventional digital computers [4]-[8], and some method of controlling and correcting those errors will be needed to prevent a quantum computer from crashing.

The future prospects for quantum computing received a tremendous boost from the discovery by Peter Shor[9] and Andrew Steane[10, 11] that quantum error correction is really possible in principle. But this discovery in itself is not sufficient to ensure that a noisy quantum computer can perform reliably. To carry out a quantum error-correction protocol, we must first encode the quantum information we want to protect, and then repeatedly perform recovery operations that reverse the errors that accumulate. Since encoding and recovery are themselves complex quantum computations, errors will inevitably occur while we perform these operations. Thus, we need to find methods for recovering from errors that are sufficiently robust to succeed with high reliability even when we make some errors during the recovery step. Such fault-tolerant recovery methods

were first developed by Shor[12] and Alexei Kitaev[13]; these methods were later generalized and improved by Shor and David DiVincenzo[14], and by Steane[15].

Furthermore, to operate a quantum computer, we must do more than just *store* quantum information; we must *process* the information. We need to be able to perform quantum gates, in which two or more encoded qubits come together and interact with one another. If an error occurs in one qubit, and then that qubit interacts with another through the operation of a quantum gate, the error is likely to spread to the second qubit. We must design our gates to minimize the propagation of error. The central challenge is to construct a universal set of quantum gates that can act on the encoded data blocks without introducing an excessive number of errors. Such a scheme for fault-tolerant quantum computation was first developed by Shor[12] and later generalized by Daniel Gottesman[16].

Once the elementary gates of our quantum computer are sufficiently reliable, we can perform fault-tolerant quantum gates on encoded information, along with fault-tolerant error recovery, to improve the reliability of the device. But for any fixed quantum code, or even for most infinite classes that contain codes of arbitrarily large block size, these procedures will eventually fail if we attempt a very long computation. However, there is a special class of codes (*concatenated codes*) which enable us to perform longer and longer quantum computations reliably, as we increase the block size at a modest rate[17]-[23]. Invoking concatenated codes we can establish an *accuracy threshold* for quantum computation; once our hardware meets a specified standard of accuracy, quantum error-correcting codes and fault-tolerant procedures enable us to perform arbitrarily long quantum computations with arbitrarily high reliability.

With the development of fault-tolerant methods, we now know that it is possible in principle for the operator of a quantum computer to actively intervene to stabilize the device against errors in a noisy (but not *too* noisy) environment. In the long term, though, fault tolerance might be achieved in practical quantum computers by a rather different route—with intrinsically fault-tolerant hardware. Such hardware, designed to be impervious to *localized* influences, could be operated relatively carelessly, yet could still store and process quantum information robustly.

In this paper, we explore a scheme for fault-tolerant hardware envisioned by Kitaev[24], in which the quantum gates exploit nonabelian Aharonov-Bohm interactions among distantly separated quasiparticles in a suitably constructed two-dimensional spin system. Though the laboratory implementation of Kitaev's idea may be far in the future, his work offers a new slant on quantum fault tolerance that shuns the analysis of abstract quantum circuits, in favor of new physics principles that might be exploited in the reliable processing of quantum information.

We explain in §2 that charges participating in long-range Aharonov-Bohm phenomena are impervious to local disturbances, so that quantum information encoded in such charges is robust. In §3 we argue that nonabelian Aharonov-Bohm interactions among quasiparticles arise in a class of two-dimensional spin

systems. These interactions are discussed in detail in §4; we see that the exchange of two quasiparticles can modify the charges carried by the particles; thus particles with *different* charges may actually be *indistinguishable*. In particular, a quasiparticle that carries a superposition of two different charges need not decohere, because the local environment is indifferent to the value of the charge. In §5 we sketch our main result: that nonabelian Aharonov-Bohm interactions are adequate for universal quantum computation, in a model with a sufficiently rich group-theoretic structure. We conclude in §6 with some tentative speculations regarding the implications of quantum fault tolerance for fundamental physics.

Recent claims about the potential for the fault-tolerant manipulation of complex quantum states may seem grandiose from the perspective of present-day technology. Surely, we have far to go before devices are constructed that can, say, exploit the accuracy threshold for quantum computation[25]. Nevertheless, we feel strongly that recent work relating to quantum error correction will have an enduring legacy. Theoretical quantum computation has developed at a spectacular pace over the past three years. If, as appears to be the case, the quantum classification of computational complexity differs from the classical classification, then no conceivable classical computer can accurately predict the behavior of even a modest number of qubits (of order 100). Perhaps, then, relatively small quantum systems will have far greater potential than we now suspect to surprise, baffle, and delight us. Yet this potential could never be realized were we unable to protect such systems from the destructive effects of noise and decoherence. Thus the discovery of fault-tolerant methods for quantum error recovery and quantum computation has exceptionally deep implications, both for the future of experimental physics and for the future of technology. The theoretical advances have illuminated the path toward a future in which intricate quantum systems may be persuaded to do our bidding.

2 Aharonov-Bohm Phenomena and Superselection Rules

Topological concepts have a natural place in the discussion of quantum error correction and fault-tolerant computation. Topology concerns the "global" properties of an object that remain unchanged when we deform the object locally. The central idea of quantum error correction is to store and manipulate quantum information in a "global" form that is resistant to local disturbances. A fault-tolerant gate should be designed to act on this global information, so that the action it performs on the encoded data remains unchanged even if we deform the gate slightly; that is, even if the implementation of the gate is not perfect.

In seeking physical implementations of fault-tolerant quantum computation, then, we ask whether there are known systems in which physical interactions have a topological character. Indeed, topology is at the essence of the *Aharonov-Bohm effect*. If an electron is transported around a perfectly shielded magnetic solenoid, its wave function acquires a phase $e^{ie\Phi}$, where e is the electron charge and Φ is the magnetic flux enclosed by the solenoid. This Aharonov-Bohm phase is a topological property of the path traversed by the electron — it depends only

on how many times the electron circumnavigates the solenoid, and is unchanged when the path is smoothly deformed. (See Fig. 1.) We are thus led to contemplate a realization of quantum computation in which information is encoded in a form that can be measured and manipulated through Aharonov-Bohm interactions — topological interactions that are immune to local disturbances.

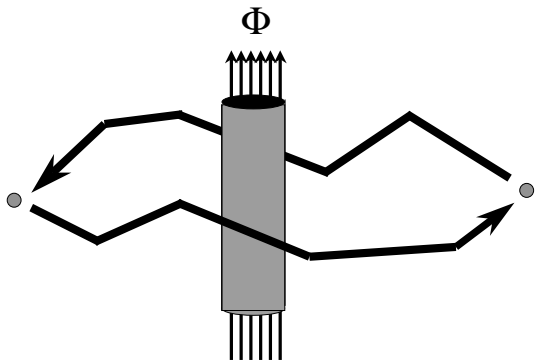

Fig. 1. A topological interaction. The Aharonov-Bohm phase acquired by an electron that encircles a flux tube remains unchanged if the electron's path is slightly deformed.

It is useful to reexpress this reasoning in the language of superselection rules. A superselection rule, as we are using the term here, arises (in a field theory or spin system defined in an infinite spatial volume) if Hilbert space decomposes into mutually orthogonal sectors, where each sector is preserved by any local operation. Perhaps the most familiar example is the charge superselection rule in quantum electrodynamics. An electric charge has an infinite range electric field. Therefore no local action can create or destroy a charge, for to destroy a charge we must also destroy the electric field lines extending to infinity, and no local procedure can accomplish this task.

The Aharonov-Bohm interaction is also an infinite range effect; the electron acquires an Aharonov-Bohm phase upon circling the solenoid no matter what its distance from the solenoid. So we may infer that no local operation can destroy a charge that participates in Aharonov-Bohm phenomena. If we consider two objects carrying such charges, widely separated and well isolated from other charged objects, then any process that changes the charge on either object would have to act coherently in the whole region containing the two charges. Thus, the charges are quite robust in the presence of localized disturbances; we can strike the particle with a hammer or otherwise abuse it without modifying the charges that it carries.

Following Kitaev[24], we may envision a *topological quantum computer*, a device in which quantum information is encoded in the quantum numbers carried by quasiparticles that reside on a two–dimensional surface and have long-range Aharonov-Bohm interactions with one another. At zero temperature, an accidental exchange of quantum numbers between quasiparticles (an error) arises only due to quantum tunneling phenomena involving the virtual exchange of charged objects. The amplitude for such processes is of the order of e^{-mL}, where m is the mass of the lightest charged object (in natural units), and L is the distance between the two quasiparticles. If the quasiparticles are kept far apart, the probability of an error afflicting the encoded information will be extremely low. At finite temperature T, there is an additional source of error, because an uncontrolled plasma of charged particles will inevitably be present, with a density proportional to the Boltzman factor $e^{-\Delta/T}$, where Δ is the mass gap (not necessarily equal to the "curvature mass" m). Sometimes one of the plasma particles will slip unnoticed between two of our data-carrying particles, resulting in an exchange of charge and hence an error. To achieve an acceptably low error rate, then, we would need to keep the temperature well below the gap Δ (or else we would have to monitor the thermal plasma very faithfully).

3 The Fractional Quantum Hall Effect and Beyond

If our device is to be capable of performing interesting computations, the Aharonov-Bohm phenomena that it employs must be *nonabelian*. Only then will we be able to build up complex unitary transformations by performing many particle exchanges in succession. Such nonabelian Aharonov-Bohm effects can arise in systems with nonabelian gauge fields. Nature has been kind enough to provide us with some fundamental nonabelian gauge fields, but unfortunately not very many, and none of these seem to be suited for practical quantum computation. To realize Kitaev's vision, then, we must hope that nonabelian Aharonov-Bohm effects can arise as complex collective phenomena in (two-dimensional electron or spin) systems that have only short-range fundamental interactions.

In fact, one of the most remarkable discoveries of recent decades has been that infinite range Aharonov-Bohm phenomena *can* arise in such systems, as revealed by the observation of the fractional quantum Hall effect. The electrons in quantum Hall systems are so highly frustrated that the ground state is an extremely entangled state with strong quantum correlations extending out over large distances. Hence, when one quasiparticle is transported around another, even when the quasiparticles are widely separated, the many electron wave function acquires a nontrivial Berry phase (such as $e^{2\pi i/3}$). This Berry phase is indistinguishable in all its observable effects from an Aharonov-Bohm phase arising from a fundamental gauge field, and its experimental consequences are spectacular[26].

The Berry phases observed in quantum Hall systems are abelian (although there are some strong indications that nonabelian Berry phases can occur under the right conditions[27,28]), and so are not very interesting from the viewpoint of quantum computation. But Kitaev[24] has described a family of simple spin

systems with local interactions in which the existence of quasiparticles with non-abelian Berry phases can be demonstrated. (The Hamiltonian of the system so frustrates the spins that the ground state is a highly entangled state with infinite range quantum correlations.) These models are sufficiently simple (although unfortunately they require four-body interactions), that one can imagine a designer material that can be reasonably well-described by one of Kitaev's models. The crucial topological properties of the model are relatively insensitive to the precise microscopic details, so the task of the fabricator who "trims" the material may not be overly demanding. If furthermore it were possible to control the transport of individual quasiparticles (perhaps with a suitable magnetic tweezers), then the system could be operated as a fault-tolerant quantum computer.

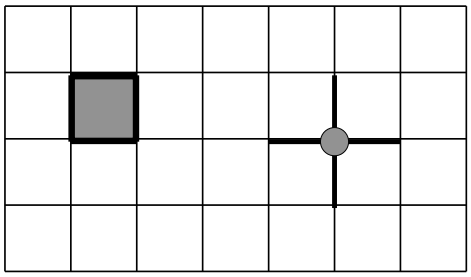

Fig. 2. A Kitaev spin model. Spins reside on the lattice links. The four spins that meet at a site or share a plaquette are coupled.

To construct his models, Kitaev considers a square lattice, with spins residing on each lattice link. The Hamiltonian is expressed as a sum of mutually commuting four-body operators, one for each site and one for each plaquette of the lattice. (See Fig. 2.) Because the terms are mutually commuting, it is simple to diagonalize the Hamiltonian by diagonalizing each term separately. The operators on sites resemble local gauge symmetries (acting independently at each site), and a state that minimizes these terms is invariant under the local symmetry, like the physical states that obey Gauss's law in a gauge theory. The operators on plaquettes are like "magnetic flux" operators in a gauge theory, and these terms are minimized when the magnetic flux vanishes everywhere. The excitation spectrum includes states in which Gauss's law is violated at isolated sites — these points are "electrically charged" quasiparticles — and states in which the magnetic flux is nonvanishing at isolated plaquettes — these are

magnetic fluxon quasiparticles. The quantum entanglement of the ground state is such that a nontrivial Berry phase is associated with the transport of a charge around a flux — this phase is identical to the Aharonov-Bohm phase in the analog gauge theory.

These Aharonov-Bohm phenomena are stable even as we deform the Hamiltonian of the theory. Indeed, if the deformation is sufficiently small, we can study its effects using perturbation theory. But as long as the perturbations are local in space, topological effects are robust, since perturbation theory is just a sum over localized influences. Whatever destroys the long-range topological interactions must be nonperturbative in the deformation of the theory.

Two types of nonperturbative effects can be anticipated[29]. The ground state of the theory might become a "flux condensate" with an indefinite number of magnetic excitations. In this event, there would be a long-range attractive interaction between charged particles and their antiparticles. It would be impossible to separate charges, and there would be no long-range effects. In a gauge theory, this phenomenon would be called *electric confinement*. Alternatively, a condensate of electric quasiparticles might appear in the ground state. Then the magnetic excitations would be confined, and again the long-range Aharonov-Bohm effects would be destroyed. In a gauge theory, we would call this the Higgs phenomenon (or magnetic confinement).

Thus, as we deform Kitaev's Hamiltonian, we can anticipate that a phase boundary will eventually be encountered, beyond which either electric confinement or the Higgs phenomenon will occur. The size of the region enclosed by this boundary will determine how precisely a material will need to be fabricated in order to behave as Kitaev specifies. A particularly urgent question for the material designer is whether cleverly chosen *two-body* interactions might so frustrate a spin system as to produce a highly entangled ground state and nonabelian Aharonov-Bohm interactions among the quasiparticle excitations.

The fractional quantum Hall effect, and Kitaev's models, speak a memorable lesson. We find gauge phenomena emerging as collective effects in systems with only short range interactions. It is intriguing to speculate that the gauge symmetries known in Nature could have a similar origin.

4 Topological Interactions

As we have noted, in Kitaev's spin models, there are two types of charges that can be carried by localized quasiparticles, which we may call "electric" and "magnetic" charges. In the simplest type of model, the "magnetic flux" carried by a particle can be labeled by an element of a finite group G, and "electric charges" are labeled by irreducible representations[1] of G. If a charged particle in the irreducible representation $D^{(\nu)}$, whose quantum numbers are encoded in an

[1] There can also be "dyons" that carry both types of charge, and the classification of the charge carried by a dyon is somewhat subtle, but we will not need to discuss explicitly the properties of the dyons.

internal wavefunction $|\psi^{(\nu)}\rangle$, is carried around a flux labeled by group element $u \in G$, then the wavefunction is modified according to

$$|\psi^{(\nu)}\rangle \to D^{(\nu)}(u)|\psi^{(\nu)}\rangle \ . \tag{1}$$

Exploiting this interaction, we can *measure* a magnetic flux by scattering a suitable charged particle off of the flux[30]. For example, we could construct a Mach-Zender flux interferometer as shown in Fig. 3 that is sensitive to the relative phase acquired by the charged particle paths that pass to the left or right of the flux. If we balance the interferometer properly, we can distinguish between, say, two flux values $u_1, u_2 \in G$; a u_1 flux will be detected emerging from one arm of the interferometer, and a u_2 flux from the other arm. Of course, the interferometer we build will not be flawless, but the flux measurement can nevertheless be fault-tolerant — if we have many charged projectiles and perform the measurement repeatedly, we can determine the flux with very high statistical confidence.

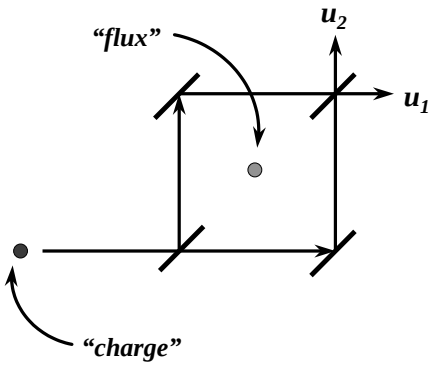

Fig. 3. A Mach-Zender interferometer for flux measurement, shown schematically. The flux to be measured is inserted inside. The test charge emerges from one arm if the flux has value u_1, the other arm if the flux has value u_2.

If the two fluxes u_1 and u_2 belong to the same conjugacy class in G, then there is a symmetry relating the two fluxons, so that all local physics is indifferent to the value of the flux (see below). Therefore, a coherent superposition of fluxes

$$a|u_1\rangle + b|u_2\rangle \tag{2}$$

will not readily decohere due to localized interactions with the environment. But the flux interferometer (operated repeatedly) will project the fluxon onto either of the flux eigenstates $|u_1\rangle$ (with probability $|a|^2$) or $|u_2\rangle$ (with probability $|b|^2$).

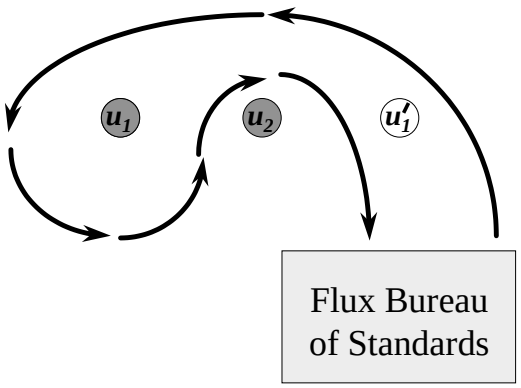

Fig. 4. The flux exchange interaction. The flux labeled u_1 is carried from its original position (shaded) to its new position (unshaded), and then remeasured. The charged particle path shown that encircles the original position of the flux is topologically equivalent to a path that encircles the new position; hence the value of the flux changes from u_1 to $u_1' = u_2^{-1} u_1 u_2$.

Now imagine that two fluxons have been carefully calibrated, so that one is known to carry the flux u_1 and the other the flux u_2. And suppose that the two vortices are carefully "exchanged" by carrying the first around the second as shown in Fig. 4, and that we subsequently remeasure the fluxes. Carrying a charged particle around the fluxon on the right, after the exchange, is topologically equivalent to carrying the charged particle around first the right fluxon, then the left fluxon, and finally the right fluxon in the opposite direction, before the exchange. We infer that the exchange modifies the quantum numbers of the fluxons according to

$$|u_1\rangle|u_2\rangle \rightarrow |u_2\rangle|u_2^{-1} u_1 u_2\rangle \ , \tag{3}$$

a nontrivial interaction if the two fluxes fail to commute[31]. Thus, noncommuting fluxes have interesting Aharonov-Bohm interactions of their own, even in the absence of any electric charges. Because carrying one flux around another can *conjugate* the value of the flux, two fluxons carrying conjugate fluxes must be regarded as *indistinguishable* particles[32]. An exchange of two such objects can modify their internal quantum numbers; we will refer to them as *nonabelions*[33], indistinguishable particles in two dimensions that obey an exotic nonabelian variant of quantum statistics.

We will use the exchange interaction Eq. (3) as a fundamental logical operation in our Aharonov-Bohm quantum computer. However, it will actually be convenient to encode qubits in pairs of fluxons, where the total flux of the pair is trivial[24]. That is, we will consider fluxon-antifluxon pairs of the form $|u, u^{-1}\rangle$, but where the flux and antiflux are kept far enough apart from one another

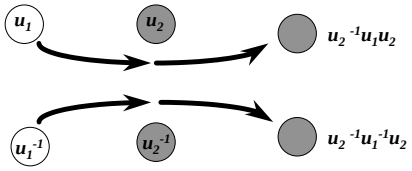

Fig. 5. The "pull-through" interaction. One flux pair is pulled through another. The outside flux is unmodified, but the inside flux is conjugated by the outside flux.

that an inadvertent exchange of quantum numbers between them is unlikely. To perform logic, we may pull one pair through another as shown in Fig. 5. Since the total flux that passes through the middle of the outside pair is trivial, this pair is not modified, but the inside fluxes are conjugated by the outside flux:

$$|u_1, u_1^{-1}\rangle|u_2, u_2^{-1}\rangle \rightarrow |u_2, u_2^{-1}\rangle|u_2^{-1}u_1u_2, u_2^{-1}u_1^{-1}u_2\rangle \ ; \tag{4}$$

an operation that is evidently isomorphic to the effect of the exchange of single fluxes described by Eq. (3). Using pairs instead of single fluxons has two advantages. First, since each pair has trivial total flux, the pairs do not interact unless one is pulled through another; therefore, we can easily shunt pairs around the device without inducing any unwanted interactions with distant pairs. Second, and more important, pairs can carry charges even if each member of the pair carries no charge[34, 35]. The charge of a pair can be measured, and this charge-measurement operation will be a crucial ingredient in the construction of a universal set of quantum gates. The operation Eq. (4) can be regarded as a *classical* logic gate; it takes flux eigenstates to flux eigenstates. To perform interesting quantum computations, we will need to be able to prepare coherent superpositions of flux eigenstates. This is what we can accomplish by measuring the charge of a pair.

Suppose that u_0 and $u_1 \in G$ are related by $u_1 = v^{-1}u_0v$ for some $v \in G$. Then if we think of the flux eigenstates $|u_0, u_0^{-1}\rangle$ and $|u_1, u_1^{-1}\rangle$ as computational basis states, the effect of pulling either pair through a $|v, v^{-1}\rangle$ pair can be interpreted as a NOT (or σ_x) gate:

$$|u_0, u_0^{-1}\rangle \leftrightarrow |u_1, u_1^{-1}\rangle \tag{5}$$

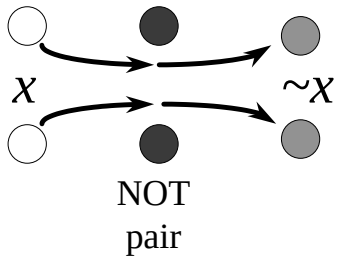

Fig. 6. The NOT gate. Pulling a computational flux pair through a NOT pair flips the value of the encoded bit.

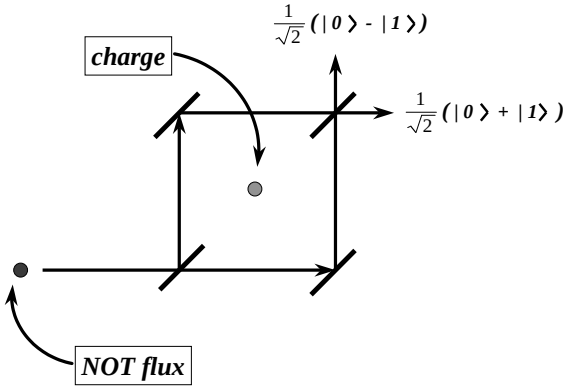

Fig. 7. A Mach-Zender interferometer for charge measurement, shown schematically. The flux pair whose charge is to be measured is inserted inside. If the test NOT flux emerges from one arm, the $|+\rangle$ charge state has been prepared; if it emerges from the other arm, $|-\rangle$ has been prepared.

(see Fig. 6). But suppose we wish to prepare one of the states

$$|\pm\rangle = \frac{1}{\sqrt{2}} \left(|u_0, u_0^{-1}\rangle \pm |u_1, u_1^{-1}\rangle \right) \ . \tag{6}$$

We can project a coherent superposition of $|u_0, u_0^{-1}\rangle$ and $|u_1, u_1^{-1}\rangle$ onto the $\{|\pm\rangle\}$ basis by scattering a $|v\rangle$ fluxon off the pair, or in other words by operating a *charge interferometer*, as in Fig. 7. When the $|v\rangle$ fluxon navigates around the pair, it acquires a trivial Aharonov-Bohm phase if the pair is in the state $|+\rangle$ and the nontrivial phase -1 if the pair is in the state $|-\rangle$. If the interferometer is properly balanced, then, the $|v\rangle$ projectile will be detected emerging from one arm of the interferometer if the pair is $|+\rangle$, and the other arm if the pair is $|-\rangle$. This is an example of charge measurement. Though the interferometer will not be perfect, charge measurement (like flux measurement) can be fault-tolerant, if we repeat the measurement enough times.

5 Universal Topological Computation

Working with fluxon pairs as computational basis states, we have seen how to perform the exchange (or "pull through") operation Eq. (4), how to measure flux (using previously calibrated charges), and how to measure charge (using previously calibrated fluxes). We will also suppose that we are able to produce a large supply of vortex pairs. Local processes produce pairs that carry no charge or flux; a charge-zero pair with trivial flux has the form (up to normalization)

$$|\text{charge zero}\rangle = \sum_u |u, u^{-1}\rangle \ , \tag{7}$$

where the sum ranges over a complete conjugacy class of G. Because this state is left invariant when conjugated by any element of G, it has trivial Aharonov-Bohm interactions with any flux, and so carries no detectable charge. After producing such a pair, we can perform flux measurement to project out one of the flux eigenstate pairs $|u, u^{-1}\rangle$. Performing many such measurements on many pairs, we can assemble a large reservoir of calibrated flux pairs that can be withdrawn as needed during the course of a computation.

But is our quantum computer universal — can we closely approximate any desired unitary transformation? To address this issue, we appeal to a theorem proved by Gottesman[16]. Suppose that we can perform any *classical* reversible operation; that is, any unitary transformation on n qubits that merely permutes the 2^n computational basis states. Then to achieve universal *quantum* computation, it is sufficient to be able to perform a few simple operations on individual qubits: the single-qubit gate σ_z, and measurement of the single-qubit observables σ_x, σ_y, and σ_z. In other words (if we envision the qubits as spin-$\frac{1}{2}$ objects), once we have a universal classical gate at our disposal, we can build a universal quan-

tum computer if we are able to rotate a spin by 180° about the z axis,[2] and can measure the spin along the x, y, and z axes.

In fact, there are groups G such that the operation Eq. (4) is sufficient for universal classical computation. The three-bit Toffoli gate, with action

$$\text{Toffoli} : |a, b, c\rangle \mapsto |a, b, c \oplus ab\rangle \tag{8}$$

on $a, b, c \in \{0, 1\}$, is a universal classical gate. We have found that a Toffoli gate can be constructed from Eq. (4) if $G = A_5$, the group of even permutations on five objects. We may, for example, choose computational basis states with

$$u_0 = (125) \ , \quad u_1 = (234) \ ; \tag{9}$$

that is, we choose our computational fluxes to be three-cycles with one object in common. Then a Toffoli gate can be constructed from a total of 16 elementary "pull-through" operations; six ancilla pairs are also used to catalyze this reaction. No Toffoli gate was found in any group smaller than A_5.[3] Since A_5 is also the smallest of the finite nonsolvable groups, it is tempting to conjecture that nonsolvablility is a necessary condition for universal classical computation generated by conjugation.[4]

We have already remarked that an σ_x gate can be realized by pulling a computational vortex pair through the pair with flux v such that $u_1 = v^{-1}u_0v$; here we choose $v = (14)(35)$. It turns out that the σ_z gate can be constructed with six pull-through steps and four ancilla pairs. Measuring σ_z is the same as measuring flux, and we have already seen that σ_x measurement can be achieved by measuring the charge of a pair, specifically, by using a v projectile in a charge interferometer. It only remains to verify that we can measure σ_y. Though σ_y measurement cannot be carried out exactly in this scheme, it turns out that a *controlled-σ_y* gate can be constructed from 31 pull-through steps, and using 7 ancilla pairs. Appealing to another trick invented by Kitaev[37], we can use the controlled-σ_y gate repeatedly to carry out σ_y-measurement to any desired accuracy.[5] Therefore, we have constructed a universal gate set using only the Aharonov-Bohm interactions of fluxes and charges; we have a fault-tolerant universal quantum computer.

Unfortunately, the spin model on which this construction is based is not so simple. Since the group A_5 has order 60, the Kitaev spin model that realizes this scenario has a 60-component spin residing at each lattice link (!) One hopes

[2] Since σ_x is a classical gate, and $i\sigma_y = \sigma_z\sigma_x$, it follows that we can perform 180° rotations about each of the x, y and z axes.

[3] Kitaev had reported earlier that universal classical computation is possible for $G = S_5$.

[4] A finite group is *nonsolvable* if it has a nontrivial subgroup whose commutator subgroup is itself. Barrington[36] also found evidence for a separation in the computational complexity of group multiplication for solvable vs. nonsolvable groups.

[5] Actually, what we really construct is a controlled-ω ($i\sigma_y$) gate where $\omega = e^{2\pi i/3}$, which is also adequate for measurement of σ_y.

that a simpler implementation of universal Aharonov-Bohm computation will be found.

The fabrication of materials that emulate Kitaev's spin systems may lie far in the future. And even when such materials are available, there will be further challenges to the machine designer, such as finding a reliable way to shepherd individual quasiparticles along prescribed trajectories. In the nearer term, it is interesting to consider whether nontrivial quantum information processing might be feasible in existing quantum Hall systems. Furthermore, even if we are unable to operate an actual spin system as a quantum computer, a quantum cellular automaton that simulates the spin system may provide a promising paradigm for fault-tolerant quantum computation.

6 Is Nature Fault Tolerant?

The discovery of quantum error correction and fault tolerance has so altered our thinking about quantum information that it is appropriate to wonder about the potential implications for fundamental physics. And in fact, a fundamental issue pertaining to loss of quantum information has puzzled the physics community for over twenty years.

In 1975, Stephen Hawking[38] argued that quantum information is unavoidably lost when a black hole forms and then subsequently evaporates completely. The essence of the argument is very simple: because of the highly distorted causal structure of the black hole spacetime, the emitted radiation is actually on the *same* time slice as the collapsing body that disappeared behind the event horizon. If the quantum information that is initially encoded in the collapsing body is eventually to re-emerge encoded in the microstate of the emitted information, then that information must be in two places at once. In other words, the quantum information must be *cloned*, a known impossibility under the usual assumptions of quantum theory[39, 40]. Hawking concludes that not all physical processes can be governed by unitary time evolution; the laws of quantum theory need revision.

This argument is persuasive, but many physicists are very distrustful of the conclusion. Perhaps one reason for the skepticism is that it seems odd for Nature to tolerate just a little bit of information loss[41]. If processes involving black holes can destroy information, then one expects that information loss is unsuppressed at the Planck length scale $(G\hbar/c^3)^{1/2} \sim 10^{-33}$ cm, a scale where virtual black holes continually arise as quantum fluctuations. It becomes hard to understand why quantum information can be so readily destroyed at the Planck scale, yet is so well preserved at the much longer distance scales that we have been able to explore experimentally — violations of quantum mechanics, after all, have never been observed.

Our newly acquired understanding of fault–tolerant quantum computation provides us with a fresh and potentially fruitful way to think about this problem. In Kitaev's spin models, we might imagine that localized processes that destroy quantum information are quite common. Yet were we to follow the evolution of

the system with coarser resolution, tracking only the information encoded in the charges of distantly separated quasiparticles, we would observe unitary evolution to remarkable accuracy; we would detect no glimmer of the turmoil beneath the surface.[6]

Likewise, it is tempting to speculate that Nature has woven fault tolerance into her design, shielding the quantum noise at the Planck scale from our view. The discovery that quantum systems can be stabilized through suitable coding methods prompts us to ask the question: Is Nature fault tolerant? If so, then quantum mechanics may reign (to excellent accuracy) at intermediate length scales, but falter both at the Planck scale (where "errors" are common) and at macroscopic scales (where decoherence is rapid).

Acknowledgments

This work has been supported in part by DARPA under Grant No. DAAH04-96-1-0386 administered by the Army Research Office, by the Department of Energy under Grant No. DE-FG03-92-ER40701, and by Caltech's Summer Undergraduate Research Fellowship program. We are grateful for helpful conversations with David DiVincenzo, Daniel Gottesman, Michael Nielsen, and especially Alesha Kitaev.

References

1. R. P. Feynman, Simulating physics with computers, *Int. J. Theor. Phys.* **21**, 467 (1982).
2. D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, *Proc. Roy. Soc. Lond.* A **400**, 96 (1985).
3. P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposiumoon Fundamentals of Computer Science* (Los Alamitos, CA, IEEE Press, 1994), pp. 124-134.
4. R. Landauer, Is quantum mechanics useful? *Phil. Tran. R. Soc. Lond.* **353**, 367 (1995).
5. R. Landauer, The physical nature of information, *Phys. Lett.* A **217**, 188 (1996).
6. R. Landauer, Is quantum mechanically coherent computation useful? In *Proc. Drexel-4 Symposium on Quantum Nonintegrability-Quantum-Classical Correspondence*, Philadelphia, PA, 8 September 1994, ed. D. H. Feng and B.-L. Hu (Boston, International Press, 1997).
7. W. G. Unruh, Maintaining coherence in quantum computers, *Phys. Rev.* A **51**, 992 (1995).
8. S. Haroche and J. M. Raimond, Quantum computing: dream or nightmare? *Phys. Today* **49** (8), 51 (1996).

[6] Similar language could be used to characterize the performance of a concatenated code—errors are rare when we inspect the encoded information with poor resolution, but are seen to be much more common if we probe the code block at lower levels of concatenation.

9. P. Shor, Scheme for reducing decoherence in quantum memory, *Phys. Rev. A* **52**, 2493 (1995).
10. A. M. Steane, Error correcting codes in quantum theory, *Phys. Rev. Lett.* **77**, 793 (1996).
11. A. M. Steane, Multiple particle interference and quantum error correction, *Proc. Roy. Soc. Lond.* A **452**, 2551 (1996).
12. P. Shor, Fault-tolerant quantum computation, in *Proceedings of the Symposium on the Foundations of Computer Science* (Los Alamitos, CA: IEEE Press, online preprint quant-ph/9605011, 1996).
13. A. Yu. Kitaev, Quantum error correction with imperfect gates, in *Quantum Communication, Computing and Measurement* ed. O. Hirota, A. S. Holevo, and C. M. Caves (New York, Plenum, 1997).
14. D. DiVincenzo and P. Shor, Fault-tolerant error correction with efficient quantum codes. *Phys. Rev. Lett.* **77**, 3260 (1996).
15. A. M. Steane, Active stabilization, quantum computation and quantum state synthesis, *Phys. Rev. Lett.* **78**, 2252 (1997).
16. D. Gottesman, A theory of fault-tolerant quantum computation, *Phys. Rev. A* (online preprint quant-ph/9702029, 1997).
17. E. Knill and R. Laflamme, Concatenated quantum codes (online preprint quant-ph/9608012, 1996).
18. E. Knill, R. Laflamme, and W, Zurek, Accuracy threshold for quantum computation, (online preprint quant-ph/9610011, 1996).
19. E. Knill, R. Laflamme, and W. Zurek, Resilient quantum computation: error models and thresholds *Science* **279**, 342 (1998).
20. D. Aharonov and M. Ben-Or, Fault tolerant quantum computation with constant error (online preprint quant-ph/9611025, 1996).
21. A. Yu. Kitaev, Quantum computing: algorithms and error correction, *Russian Math. Surveys* **6** (1997)..
22. J. Preskill, Reliable quantum computers, *Proc. R. Soc. Lond. A* **454**, 385 (1998).
23. C. Zalka, Threshold estimate for fault tolerant quantum computing (online preprint quant-ph/9612028, 1996).
24. A. Yu. Kitaev, Fault-tolerant quantum computation by anyons (online preprint quant-ph/9707021, 1997).
25. J. Preskill, Quantum computing: pro and con, *Proc. Roy. Soc. Lond. A* **454**, 469 (1998).
26. R. Prange and S. Girvin, eds., *The Quantum Hall Effect* (New York, Springer-Verlag, 1987).
27. N. Read and E. Rezayi, Quasiholes and fermionic zero modes of paired fraction quantum Hall states: the mechanism for nonabelian statistics (online preprint cond-mat/9609079, 1996).
28. C. Nayak and F. Wilczek, $2n$ quasihole states realize 2^{n-1}-dimensional spinor braiding statistics in paired quantum Hall states (online preprint cond-mat/9605145, 1996).
29. G, 't Hooft, On the phase transition toward permanent quark confinement, *Nucl. Phys.* B **138**, 1 (1978).
30. M. Alford, S. Coleman, and J. March-Russell, Disentangling nonabelian discrete quantum hair, *Nucl. Phys.* B **351**, 735 (1991).
31. F. A. Bais, Flux metamorphosis, *Nucl. Phys.* B **170**, 32 (1980).
32. H.-K. Lo and J. Preskill, Nonabelian vortices and nonabelian statistics, *Phys. Rev.* D **48**, 4821 (1993)

33. G. Moore and N. Read, Nonabelions in the fractional quantum Hall effect, *Nucl. Phys.* B **360**, 362 (1991).
34. M. G. Alford, K. Benson, S. Coleman, J. March-Russell, and F. Wilczek, Interactions and excitations of nonabelian vortices, *Phys. Rev. Lett.* **64**, 1632 (1990).
35. J. Preskill and L. M. Krauss, Local discrete symmetry and quantum mechanical hair, *Nucl. Phys.* B **341**, 50 (1990).
36. D. A. Barrington, Bounded width polynomial size branching programs recognize exactly those languages in NC^1, J. Comp. Sys. Sci. **38**, 150-164 (1989).
37. A. Yu. Kitaev, Quantum measurements and the abelian stabilizer problem (online preprint quant-ph/9511026, 1995).
38. S. W. Hawking, Breakdown of predictability in gravitational collapse, *Phys. Rev.* D **14**, 2460 (1976).
39. D. Dieks, Communication by electron-paramagnetic-resonance devices. *Phys. Lett.* A **92**, 271 (1982).
40. W. K. Wootters, and W. H. Zurek, A single quantum cannot be cloned, *Nature* **299**, 802 (1982).
41. T. Banks, M. E. Peskin, and L. Susskind, Difficulties for the evolution of pure states into mixed states, *Nucl. Phys.* B **244**, 125 (1984).