



ACADEMIC
PRESS

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Annals of Physics 303 (2003) 2–30

ANNALS
of
PHYSICS

www.elsevier.com/locate/aop

Fault-tolerant quantum computation by anyons

A.Yu. Kitaev*

L.D. Landau Institute for Theoretical Physics, 117940, Kosygina St. 2, Germany

Received 20 May 2002

Abstract

A two-dimensional quantum system with anyonic excitations can be considered as a quantum computer. Unitary transformations can be performed by moving the excitations around each other. Measurements can be performed by joining excitations in pairs and observing the result of fusion. Such computation is fault-tolerant by its physical nature.

© 2002 Elsevier Science (USA). All rights reserved.

1. Introduction

A quantum computer can provide fast solution for certain computational problems (e.g., factoring and discrete logarithm [1]) which require exponential time on an ordinary computer. Physical realization of a quantum computer is a big challenge for scientists. One important problem is decoherence and systematic errors in unitary transformations which occur in real quantum systems. From the purely theoretical point of view, this problem has been solved due to Shor's discovery of fault-tolerant quantum computation [2], with subsequent improvements [3–6]. An arbitrary quantum circuit can be simulated using imperfect gates, provided these gates are close to the ideal ones up to a constant precision δ . Unfortunately, the threshold value of δ is rather small;¹ it is very difficult to achieve this precision.

Needless to say, *classical* computation can be also performed fault-tolerantly. However, it is rarely done in practice because classical gates are reliable enough. Why is it possible? Let us try to understand the easiest thing—why classical

* Present address: Caltech 107-81, Pasadena, CA 91125, USA.

E-mail addresses: kitaev@itp.ac.ru, kitaev@cs.caltech.edu.

¹ Actually, the threshold is not known. Estimates vary from 1/300 [7] to 10^{-6} [4].

information can be stored reliably on a magnetic media. Magnetism arise from spins of individual atoms. Each spin is quite sensitive to thermal fluctuations. But the spins interact with each other and tend to be oriented in the same direction. If some spin flips to the opposite direction, the interaction forces it to flip back to the direction of other spins. This process is quite similar to the standard error correction procedure for the repetition code. We may say that errors are being corrected at the physical level. Can we propose something similar in the quantum case? Yes, but it is not so simple. First of all, we need a quantum code with local stabilizer operators.

I start with a class of stabilizer quantum codes associated with lattices on the torus and other two-dimensional surfaces [6,8]. Qubits live on the edges of the lattice whereas the stabilizer operators correspond to the vertices and the faces. These operators can be put together to make up a Hamiltonian with local interaction. (This is a kind of penalty function; violating each stabilizer condition costs energy.) The ground state of this Hamiltonian coincides with the protected space of the code. It is 4^g -fold degenerate, where g is the genus of the surface. The degeneracy is persistent to local perturbation. Under small enough perturbation, the splitting of the ground state is estimated as $\exp(-aL)$, where L is the smallest dimension of the lattice. This model may be considered as a quantum memory, where stability is attained at the physical level rather than by in explicit error correction procedure.

Excitations in this model are anyons, meaning that the global wavefunction acquires some phase factor when one excitation moves around the other. One can operate on the ground state space by creating an excitation pair, moving one of the excitations around the torus, and annihilating it with the other one. Unfortunately, such operations do not form a complete basis. It seems this problem can be removed in a more general model (or models) where the Hilbert space of a qubit have dimensionality >2 . This model is related to Hopf algebras.

In the new model, we do not need torus to have degeneracy. An n -particle excited state on the plane is already degenerate, unless the particles (excitations) come close to each other. These particles are non-abelian anyons, i.e., the degenerate state undergoes a non-trivial unitary transformation when one particle moves around the other. Such motion (“braiding”) can be considered as fault-tolerant quantum computation. A measurement of the final state can be performed by joining the particles in pairs and observing the result of fusion.

Anyons have been studied extensively in the field-theoretic context [9–13]. So, I hardly discover any new about their algebraic properties. However, my approach differs in several respects:

- The model Hamiltonians are different.
 - We allow a generic (but weak enough) perturbation which removes *any* symmetry of the Hamiltonian.²
 - The language of ribbon and local operators (see Section 6.2) provides unified description of anyonic excitations and long-range entanglement in the ground state.
- An attempt to use *one-dimensional* anyons for quantum computation was made by Castagnoli and Rasetti [14], but the question of fault-tolerance was not considered.

² Some local symmetry still can be established by adding unphysical degrees of freedom, see Section 4.

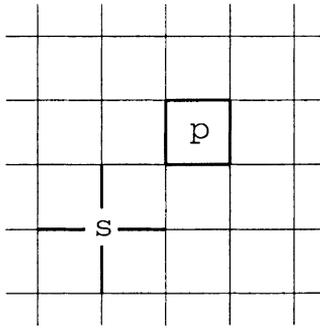


Fig. 1. Square lattice on the torus.

2. Toric codes and the corresponding Hamiltonians

Consider a $k \times k$ square lattice on the torus (see Fig. 1). Let us attach a spin, or qubit, to each edge of the lattice. (Thus, there are $n = 2k^2$ qubits). For each vertex s and each face p , consider operators of the following form:

$$A_s = \prod_{j \in \text{star}(s)} \sigma_j^x, \quad B_p = \prod_{j \in \text{boundary}(p)} \sigma_j^z. \tag{1}$$

These operators commute with each other because star (s) and boundary (p) have either 0 or 2 common edges. The operators A_s and B_p are Hermitian and have eigenvalues 1 and -1 .

Let \mathcal{N} be the Hilbert space of all $n = 2k^2$ qubits. Define a *protected subspace* $\mathcal{L} \subseteq \mathcal{N}$ as follows:³

$$\mathcal{L} = \{ |\xi\rangle \in \mathcal{N} : A_s |\xi\rangle = |\xi\rangle, B_p |\xi\rangle = |\xi\rangle \text{ for all } s, p \}. \tag{2}$$

This construction gives us a definition of a quantum code $\text{TOR}(k)$, called a *toric code* [6,8]. The operators A_s, B_p are the *stabilizer operators* of this code.

To find the dimensionality of the subspace \mathcal{L} , we can observe that there are two relations between the stabilizer operators, $\prod_s A_s = 1$ and $\prod_p B_p = 1$. So, there are $m = 2k^2 - 2$ independent stabilizer operators. It follows from the general theory of additive quantum codes [15,16] that $\dim \mathcal{L} = 2^{n-m} = 4$.

However, there is a more instructive way of computing $\dim \mathcal{L}$. Let us find the algebra $\mathbf{L}(\mathcal{L})$ of all linear operators on the space \mathcal{L} —this will give us full information about this space. Let $\mathcal{F} \subseteq \mathbf{L}(\mathcal{N})$ be the algebra of operators generate by A_s, B_p . Clearly, $\mathbf{L}(\mathcal{L}) \cong \mathcal{G}/\mathcal{I}$, where $\mathcal{G} \supseteq \mathcal{F}$ is the algebra of all operators which commute with A_s, B_p , and $\mathcal{I} \subset \mathcal{G}$ is the ideal generated by $A_s - 1, B_p - 1$. The algebra \mathcal{G} is generated by operators of the form

$$Z = \prod_{j \in c} \sigma_j^z, \quad X = \prod_{j \in c'} \sigma_j^x,$$

³ We will show that this subspace is really protected from certain errors. Vectors of this subspaces are supposed to represent “quantum information,” like codewords of a classical code represent classical information.

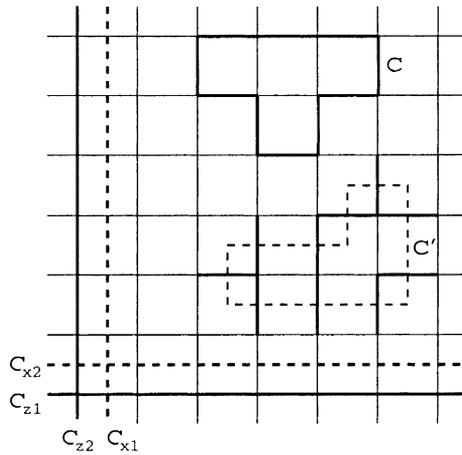


Fig. 2. Loops on the lattice and the dual lattice.

where c is a loop (closed path) on the lattice, whereas c' is a cut, i.e., a loop on the dual lattice (see Fig. 2). If a loop (or a cut) is contractible then the operator Z is a product of B_p , hence $Z \equiv 1 \pmod{\mathcal{I}}$. Thus, only non-contractible loops or cuts are interesting. It follows that the algebra $\mathbf{L}(\mathcal{L})$ is generated by 4 operators Z_1, Z_2, X_1, X_2 corresponding to the loops c_{z1}, c_{z2} and the cuts c_{x1}, c_{x2} (see Fig. 2). The operators Z_1, Z_2, X_1, X_2 have the same commutation relations as $\sigma_1^z, \sigma_2^z, \sigma_1^x, \sigma_2^x$. We see that each quantum state $|\xi\rangle \in \mathcal{L}$ corresponds to a state of 2 qubits. Hence, the protected subspace \mathcal{L} is four-dimensional.

In a more abstract language, the algebra \mathcal{F} corresponds to 2-boundaries and 0-coboundaries (with coefficients from \mathbb{Z}_2), \mathcal{G} corresponds to 1-cycles and 1-cocycles, and $\mathbf{L}(\mathcal{L})$ corresponds to 1-homologies and 1-cohomologies.

There is also an explicit description of the protected subspace which may be not so useful but is easier to grasp. Let us choose basis vectors in the Hilbert space \mathcal{N} by assigning a label $z_j = 0, 1$ to each edge j .⁴ The constraints $B_p|\xi\rangle = |\xi\rangle$ say that the sum of the labels at the boundary of a face should be zero (mod 2). More exactly, only such basis vectors contribute to a vector from the protected subspace. Such a basis vector is characterized by two topological numbers: the sums of z_j along the loops c_{z1} and c_{z2} . The constraints $A_p|\xi\rangle = |\xi\rangle$ say that all basis vectors with the same topological numbers enter $|\xi\rangle$ with equal coefficients. Thus, for each of the 4 possible combinations of the topological numbers v_1, v_2 , there is one vector from the protected subspace,

$$|\xi_{v_1, v_2}\rangle = 2^{-(k^2-1)/2} \sum_{z_1, \dots, z_n} |z_1, \dots, z_n\rangle : \sum_{j \in c_{z1}} z_j = v_1, \sum_{j \in c_{z2}} z_j = v_2. \tag{3}$$

Of course, one can also create linear combinations of these vectors.

⁴ 0 means “spin up,” 1 means “spin down.” The Pauli operators σ_z, σ_x have the standard form in this basis.

Now we are to show that the code $\text{TOR}(k)$ detects $k - 1$ errors⁵ (hence, it corrects $\lfloor \frac{k-1}{2} \rfloor$ errors). Consider a multiple error

$$E = \sigma(\alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_n) = \prod_j (\sigma_j^x)^{\alpha_j} \prod_j (\sigma_j^z)^{\beta_j} \quad (\alpha_j, \beta_j = 0, 1).$$

This error cannot be detected by syndrome measurement (i.e., by measuring the eigenvalues of all A_s, B_j) if and only if $E \in \mathcal{G}$. However, if $E \in \mathcal{F}$ then $E|\xi\rangle = |\xi\rangle$ for every $|\xi\rangle \in \mathcal{L}$. Such an error is not an error at all—it does not affect the protected subspace. The bad case is when $E \in \mathcal{G}$ but $E \notin \mathcal{F}$. Hence, the support of E should contain a non-contractible loop or cut. It is only possible if $|\text{Supp}(E)| \geq k$. (Here $\text{Supp}(E)$ is the set of j for which $\alpha_j \neq 0$ or $\beta_j \neq 0$.)

One may say that the toric codes have quite poor parameters. Well, they are not “good” codes in the sense of [17]. However, the code $\text{TOR}(k)$ corrects *almost any* multiple error of size $O(k^2)$. (The constant factor in $O(\dots)$ is related to the percolation problem.) So, these codes work if the error rate is constant but smaller than some threshold value. The nicest property of the codes $\text{TOR}(k)$ is that they are *local check codes*. Namely,

1. Each stabilizer operators involves bounded number of qubits (at most 4).
2. Each cubit is involved in a bounded number of stabilizer operators (at most 4).
3. There is no limit for the number of errors that can be corrected.

Also, at a constant error rate, the unrecoverable error probability goes to zero as $\exp(-ak)$.

It has been already mentioned that error detection involves syndrome measurement. To correct the error, one needs to find its characteristic vector $(\alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_n)$ out of the syndrome. This is the usual error correction scheme. A new suggestion is to perform error correction at the physical level. Consider the Hamiltonian

$$H_0 = - \sum_s A_s - \sum_p B_p. \quad (4)$$

Diagonalizing this Hamiltonian is an easy job because the operators A_s, B_p commute. In particular, the ground state coincides with the protected subspace of the code $\text{TOR}(k)$; it is 4-fold degenerate. All excited states are separated by an energy gap $\Delta E \geq 2$, because the difference between the eigenvalues of A_s or B_p equals 2. This Hamiltonian is more or less realistic because it involves only *local* interactions. We can expect that “errors,” i.e., noise-induced excitations will be removed automatically by some relaxation processes. Of course, this requires cooling, i.e., some coupling to a thermal bath with low temperature (in addition to the Hamiltonian (4)).

Now let us see whether this model is stable to perturbation. (If not, there is no practical use of it.) For example, consider a perturbation of the form

⁵ In the theory of quantum codes, the word “error” is used in a somewhat confusing manner. Here it means a single qubit error. In most other cases, like in the formula below, it means a multiple error, i.e., an arbitrary operator $E \in \mathbf{L}(\mathcal{N})$.

$$V = -\hbar \sum_j \vec{\sigma}_j - \sum_{j < p} J_{jp}(\vec{\sigma}_j, \vec{\sigma}_p).$$

It is important that the perturbation is local, i.e., each term of it contains a small number of σ (at most 2). Let us estimate the energy splitting between two orthogonal ground states of the original Hamiltonian, $|\xi\rangle \in \mathcal{L}$ and $|\eta\rangle \in \mathcal{L}$. We can use the usual perturbation theory because the energy spectrum has a gap. In the m th order of the perturbation theory, the splitting is proportional to $\langle \xi | V^m | \eta \rangle$ or $\langle \xi | V^m | \xi \rangle - \langle \eta | V^m | \eta \rangle$. However, both quantities are zero unless V^m contains a product of σ_j^z or σ_j^x along a non-contractible loop or cut. Hence, the splitting appears only in the $\lceil k/2 \rceil$ th or higher orders. As far as all things (like the number of the relevant terms in V^m) scale correctly to the thermodynamic limit, the splitting vanishes as $\exp(-ak)$. A simple physical interpretation of this result is given in the next section. (Of course, the perturbation should be small enough, or else a phase transition may occur).

Note that our construction is not restricted to square lattices. We can consider an arbitrary irregular lattice, like in Fig. 6. Moreover, such a lattice can be drawn on an arbitrary two-dimensional surface. On a compact orientable surface of genus g , the ground state is 4^g -fold degenerate. In this case, the splitting of the ground state is estimated as $\exp(-aL)$, where L is the smallest dimension of the lattice. We see that the ground state degeneracy depends on the surface topology, so we deal with *topological quantum order*. On the other hand, there is a finite energy gap between the ground state and excited states, so all spatial correlation functions decay exponentially. This looks like a paradox—how do parts of a macroscopic system know about the topology if all correlations are already lost at small scales? The answer is that there is long-range entanglement⁶ which cannot be expressed by simple correlation functions like $\langle \sigma_j^a \sigma_l^b \rangle$. This entanglement reveals itself in the excitation properties we are going to discuss.

3. Abelian anyons

Let us classify low-energy excitations of the Hamiltonian (4). An eigenvector of this Hamiltonian is an eigenvector of all the operators A_s, B_p . An *elementary excitation*, or *particle* occurs if only one of the constraints $A_s|\xi\rangle = |\xi\rangle, B_p|\xi\rangle = |\xi\rangle$ is violated. Because of the relations $\prod_s A_s = 1$ and $\prod_p B_p = 1$, it is impossible to create a single particle. However, it is possible to create a two-particle state of the form $|\psi^z(t)\rangle = S^z(t)|\xi\rangle$ or $|\psi^x(t')\rangle = S^x(t')|\xi\rangle$, where $|\xi\rangle$ is an arbitrary ground state, and

$$S^z(t) = \prod_{j \in t} \sigma_j^z, \quad S^x(t') = \prod_{j \in t'} \sigma_j^x \tag{5}$$

(see Fig. 3). In the first case, two particles are created at the endpoints of the “string” (non-closed path) t . Such particles live on the vertices of the lattice. We will call them

⁶ Entanglement is a special, purely quantum form of correlation.

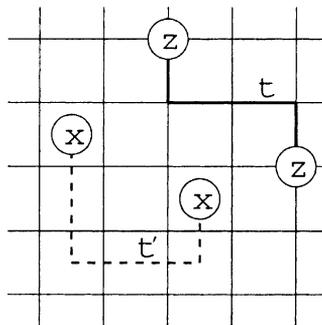


Fig. 3. Strings and particles.

z -type particles, or “electric charges.” Correspondingly, x -type particles, or “magnetic vortices” live on the faces. The operators $S^z(t)$, $S^x(t')$ are called *string operators*. Their characteristic property is as follows: they commute with every A_s and B_p , except for few ones (namely, 2) corresponding to the endpoints of the string. Note that the state $|\psi^z(t)\rangle = S^z(t)|\xi\rangle$ depends only on the homotopy class of the path t while the operator $S^z(t)$ depends on t itself.

Any configuration of an even number of z -type particles and an even number of x -type particles is allowed. We can connect them by strings in an arbitrary way. Each particle configuration defines a 4^g -dimensional subspace in the global Hilbert space \mathcal{N} . This subspace is independent of the strings but a particular vector $S^{a_1}(t_1) \cdots S^{a_m}(t_m)|\xi\rangle$ depends on t_1, \dots, t_m . If we draw these strings in a topologically different way, we get another vector in the same 4^g -dimensional subspace. Thus, the strings are unphysical but we cannot get rid of them in our formalism.

Let us see what happens if these particles move around the torus (or other surface). Moving a z -type particle along the path c_{z1} or c_{z2} (see Fig. 2) is equivalent to applying the operator Z_1 or Z_2 . Thus, we can operate on the ground state space by creating a particle pair, moving one of the particles around the torus, and annihilating it with the other one. Thus, we can realize some quantum gates. Unfortunately, too simple ones—we can only apply the operators σ_z and σ_x to each of the 2 (or $2g$) qubits encoded in the ground state.

Now we can give the promised physical interpretation of the ground state splitting. In the presence of perturbation, the two-particle state $|\psi^z(t)\rangle$ is not an eigenstate any more. More exactly, both particles will propagate rather than stay at the same positions. The propagation process is described by the Schrödinger equation with some effective mass m_z . (x -type particles have another mass m_x). In the non-perturbed model, $m_z = m_x = \infty$. There are no real particles in the ground state, but they can be created and annihilate virtually. A virtual particle can tunnel around the torus before annihilating with the other one. Such processes contribute terms $b_{z1}Z_1$, $b_{z2}Z_2$, $b_{x1}X_1$, $b_{x2}X_2$ to the ground state effective Hamiltonian. Here $b_{zi} \sim \exp(-a_z L_i)$ is the tunneling amplitude whereas $a_z \sim \sqrt{2m\Delta E}$ is the imaginary wavevector of the tunneling particle.

Next question: what happens if we move particles around each other? (For this, we do not need a torus; we can work on the plane). For example, let us move an x -type particle around a z -type particle (see Fig. 4). Then

$$|\Psi_{\text{initial}}\rangle = S^z(t)|\psi^x(q)\rangle, \quad |\Psi_{\text{final}}\rangle = S^x(c)S^z(t)|\psi^x(q)\rangle = -|\Psi_{\text{initial}}\rangle,$$

because $S^x(c)$ and $S^z(t)$ anti-commute, and $S^x(c)|\psi^x(q)\rangle = |\psi^x(q)\rangle$. We see that the global wavefunction (= the state of the entire system) acquires the phase factor -1 . It is quite unlike usual particles, bosons and fermions, which do not change their phase in such a process. Particles with this unusual property are called *abelian anyons*. More generally, abelian anyons are particles which realize non-trivial one-dimensional representations of (colored) braid groups. In our case, the phase change can be also interpreted as an Aharonov–Bohm effect. It does not occur if both particles are of the same type.

Note that abelian anyons exist *in real solid state systems*, namely, they are intrinsically related to the fractional quantum Hall effect [18]. However, these anyons have different braiding properties. In the fractional quantum Hall system with filling factor p/q , there is only one basic type of anyonic particles with (real) electric charge $1/q$. (Other particles are thought to be composed from these ones). When one particle moves around the other, the wavefunction acquires a phase factor $\exp(2\pi i/q)$.

Clearly, the existence of anyons and the ground state degeneracy have the same nature. They both are manifestations of a topological quantum order, a hidden long-range order that cannot be described by any local order parameter. (The existence of a local order parameter contradicts the nature of a quantum code—if the ground state is accessible to local measurements then it is not protected from local errors.) It seems that the anyons are more fundamental and can be used as a universal probe for this hidden order. Indeed, *the ground state degeneracy on the torus follows from the existence of anyons* [19]. Here is the original Einarsson’s proof applied to our two types of particles.

We derived the ground state degeneracy from the commutation relations between the operators Z_1, Z_2, X_1, X_2 . These operators can be realized by moving particles

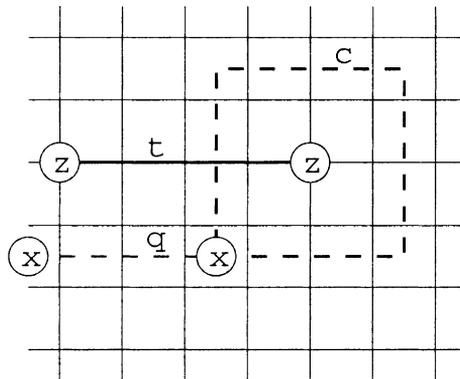


Fig. 4. An x -type particle moving around a z -type particle.

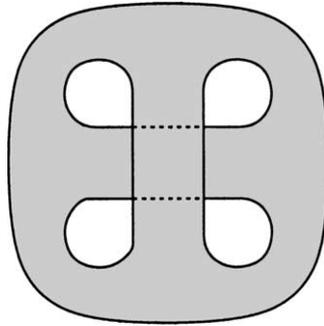


Fig. 5. A fly-over crossing geometry for a two-dimensional electron layer.

along the loops c_{z1} , c_{z2} , c_{x1} , c_{x2} . These loops only exist on the torus, not on the plane. Consider, however, the process in which an x -type particle and a z -type particle go around the torus and then trace their paths backward. This corresponds to the operator $W = X_1^{-1}Z_1^{-1}X_1Z_1$ which can be realized on the plane. Indeed, we can deform particles' trajectories so that one particle stays at rest while the other going around it. Due to the anyonic nature of the particles, $W = -1$. We see that X_1 and Z_1 anti-commute.

The above argument is also applicable to the fractional quantum Hall anyons [19]. The ground state on the torus is q -fold degenerate, up to the precision $\sim \exp(-L/l_0)$, where l_0 is the magnetic length. This result does not rely on the magnetic translational symmetry or any other symmetry. Rather, it relies on the existence of the energy gap in the spectrum (otherwise the degeneracy would be unstable to perturbation). Note that holes (= punctures) in the torus do not remove the degeneracy unless they break the non-trivial loops c_{x1} , c_{x2} , c_{z1} , c_{z2} . The fly-over crossing geometry (see Fig. 5) is topologically equivalent to a torus with 2 holes, but it is almost flat. In principle, such structure can be manufactured,⁷ cooled down and placed into a perpendicular magnetic field. This will be a sort of quantum memory—it will store a quantum state forever, provided all anyonic excitation are frozen out or localized. Unfortunately, I do not know any way this quantum information can get in or out. Too few things can be done by moving abelian anyons. All other imaginable ways of accessing the ground state are uncontrollable.

4. Materialized symmetry: is that a miracle?

Anyons have been studied extensively in the gauge field theory context [9–11,13]. However, we start with quite different assumptions about the Hamiltonian. A gauge theory implies a gauge symmetry which cannot be removed by external perturbation.

⁷ It is not easy. How will the two layers (the two crossing “roads,” one above the other) join in a single crystal layout?

To the contrary, our model is stable to *arbitrary* local perturbations. It is useful to give a field-theoretic interpretation of this model. The edge labels z_j (measurable by σ_j^z) correspond to a \mathbb{Z}_2 vector potential, whereas σ_j^x corresponds to the electric field. The operators A_s are local gauge transformations whereas B_p is the magnetic field on the face p . The constraints $A_s|\xi\rangle = |\xi\rangle$ mean that the state $|\xi\rangle$ is gauge-invariant. Violating the gauge invariance is energetically unfavorable but not forbidden. The Hamiltonian (which includes H_0 and some perturbation V) need not obey the gauge symmetry. The constraints $B_p|\xi\rangle = |\xi\rangle$ mean that the gauge field corresponds to a flat connection. These constraints are not strict either.

Despite the absence of symmetry in the Hamiltonian $H = H_0 + V$, our system exhibits two conservation laws: electric charge and magnetic charge (i.e., the number of vortices) are both conserved *modulo 2*. In the usual electrodynamics, conservation of electric charge is related to the local (= gauge) $U(1)$ symmetry. In our case, it should be a local \mathbb{Z}_2 symmetry for electric charges and another \mathbb{Z}_2 symmetry for magnetic vortices. So, our system exhibits a *dynamically created* $\mathbb{Z}_2 \times \mathbb{Z}_2$ symmetry which appears only at large distances where individual excitations are well-defined.

Probably, the reader is not satisfied with this interpretation. Really, it creates a new puzzle rather than solve an old one. What is this mysterious symmetry? How do symmetry operators look like at the microscopic level? The answer sounds as nonsense but it is true. This symmetry (as well as any other local symmetry) can be found in *any* Hamiltonian if we introduce some unphysical degrees of freedom. So, the symmetry is not actually being created. Rather, an artificial symmetry becomes a real one.

The new degrees of freedom are spin variables $v_s, w_p = 0, 1$ for each vertex s and each face p . The vertex spins will stay in the state $2^{-1/2}(|0\rangle + |1\rangle)$ whereas the face spins will stay in the state $|0\rangle$. So, all the extra spins together stay in a unique quantum state $|\zeta\rangle$. Obviously, $\sigma_s^x|\zeta\rangle = |\zeta\rangle$ and $\sigma_p^z|\zeta\rangle = |\zeta\rangle$, for every vertex s and every face p . From the mathematical point of view, we have simply defined an embedding of the space \mathcal{N} into a larger Hilbert space \mathcal{F} of all the spins, $|\psi\rangle \mapsto |\psi\rangle \otimes |\zeta\rangle$. So we may write $\mathcal{N} \subseteq \mathcal{F}$. We will call \mathcal{N} the *physical space* (or subspace), \mathcal{F} the *extended space*. Physical states (i.e., vectors $|\psi\rangle \in \mathcal{N}$) are characterized by the equations

$$\sigma_s^x|\psi\rangle = |\psi\rangle, \quad \sigma_p^z|\psi\rangle = |\psi\rangle$$

for every vertex s and face p .

Now let us apply a certain unitary transformation U on the extended space \mathcal{F} . This transformation is just a change of the spin variables, namely

$$v_s \mapsto v_s, \quad z_j \mapsto z_j + \sum_{s=\text{endpoint}(j)} v_s, \quad w_p \mapsto w_p + \sum_{j \in \text{boundary}(p)} z_j \tag{6}$$

(all sums are taken *modulo 2*). The physical subspace becomes $\mathcal{N}' = U\mathcal{N}$. Vectors $|\psi\rangle \in \mathcal{N}'$ are invariant under the following symmetry operators:

$$P_s = U\sigma_s^xU^\dagger = \sigma_s^x A_s, \quad Q_p = U\sigma_p^zU^\dagger = \sigma_p^z B_p. \tag{7}$$

The transformed Hamiltonian $H' = UHU^\dagger$ commutes with these operators. It is defined up to the equivalence $P_s \equiv 1, Q_p \equiv 1$. In particular,

$$H'_0 = UH_0U^\dagger = H'_0 \equiv -\sum_s \sigma_s^x - \sum_p \sigma_p^z. \quad (8)$$

In the field theory language, the vertex variables v_s (or the operators σ_s^z) are a Higgs field. The operators P_s are local gauge transformations. Thus, an arbitrary Hamiltonian can be written in a gauge-invariant form if we introduce additional Higgs fields. Of course, it is a very simple observation. The real problem is to understand how the artificial gauge symmetry “materialize,” i.e., give rise to a physical conservation law.

Electric charge at a vertex s is given by the operator σ_s^x . The total electric charge on a compact surface is zero⁸ because $\prod_s \sigma_s^x \equiv 1$. This is not a physically meaningful statement as it is. It is only meaningful if there are discrete charged particles. Then the charge is also conserved locally, in every scattering or fusion process. It is difficult to formulate this property in a mathematical language, but, hopefully, it is possible. (The problem is that particles are generally smeared and can propagate. Physically, particles are well-defined if they are stable and have finite energy gap.) Alternatively, one can use various local and non-local order parameters to distinguish between phases with an unbroken symmetry, broken symmetry, or confinement.

The artificial gauge symmetry materialize for the Hamiltonian (8) but this is not the case for every Hamiltonian. Let us try to describe possible symmetry breaking mechanisms in terms of local order parameters. If the gauge symmetry is broken then there is a non-vanishing vacuum average of the Higgs field, $\phi(s) = \langle \sigma_s^z \rangle \neq 0$. Electric charge is not conserved any more. In other words, there is a Bose condensate of charged particles. Although the second \mathbb{Z}_2 symmetry is formally unbroken, free magnetic vortices do not exist. More exactly, magnetic vortices are confined. (The duality between symmetry breaking and confinement is well known [25]). It is also possible that the second symmetry is broken, then electric charges are confined. From the physical point of view, these two possibilities are equivalent: there is no conservation law in the system.⁹

An interesting question is whether magnetic vortices can be confined without the gauge symmetry being broken. Apparently, the answer is “no.” The consequence is significant: electric charges and magnetic vortices cannot exist without each other. It seems that materialized symmetry needs better understanding; as presented here, it looks more like a miracle.

5. The model based on a group algebra

From now on, we are constructing and studying non-abelian anyons which will allow universal quantum computation.

⁸ Strictly speaking, the electric charge is not a numeric quantity; rather, it is an irreducible representation of the group \mathbb{Z}_2 . “Zero” refers to the identity representation.

⁹ The two possibilities only differ if an already materialized symmetry breaks down at much large distances (lower energies).

Let G be a finite (generally, non-abelian) group. Denote by $\mathcal{H} = \mathbb{C}[G]$ the corresponding group algebra, i.e., the space of formal linear combinations of group elements with complex coefficients. We can consider \mathcal{H} as a Hilbert space with a standard orthonormal basis $\{|g\rangle : g \in G\}$. The dimensionality of this space is $N = |G|$. We will work with “spins” (or “qubits”) taking values in this space.¹⁰ *Remark:* This model can be generalized. One can take for \mathcal{H} any finite-dimensional Hopf algebra equipped with a Hermitian scalar product with certain properties. However, I do not want to make things too complicated.

To describe the model, we need to define 4 types of linear operators, $L_+^g, L_-^g, T_+^h, T_-^h$ acting on the space \mathcal{H} . Within each type, they are indexed by group elements, $g \in G$ or $h \in G$. They act as follows:

$$\begin{aligned} L_+^g|z\rangle &= |gz\rangle, & T_+^h|z\rangle &= \delta_{h,z}|z\rangle, \\ L_-^g|z\rangle &= |zg^{-1}\rangle, & T_-^h|z\rangle &= \delta_{h^{-1},z}|z\rangle. \end{aligned} \tag{9}$$

(In the Hopf algebra context, the operators $L_+^g, L_-^g, T_+^h, T_-^h$ correspond to the left and right multiplications and left and right comultiplication, respectively.) These operators satisfy the following commutation relations:

$$\begin{aligned} L_+^g T_+^h &= T_+^{gh} L_+^g, & L_+^g T_-^h &= T_-^{hg^{-1}} L_+^g, \\ L_-^g T_+^h &= T_+^{hg^{-1}} L_-^g, & L_-^g T_-^h &= T_-^{gh} L_-^g. \end{aligned} \tag{10}$$

Now consider an arbitrary lattice on an arbitrary orientable two-dimensional surface, see Fig. 6. (We will mostly work with a plane or a sphere, not higher genus surfaces). Corresponding to each edge is a spin which takes values in the space \mathcal{H} . Arrows in Fig. 6 mean that we choose some orientation for each edge of the lattice. (Changing the direction of a particular arrow will be equivalent to the basis change $|z\rangle \mapsto |z^{-1}\rangle$ for the corresponding qubit). Let j be an edge of the lattice, s one of its endpoints. Define an operator $L^g(j, s) = L_{\pm}^g(j)$ as follows. If s is the origin of the arrow j then $L^g(j, s)$ is $L_-^g(j)$ (i.e., L_-^g acting on the j th spin), otherwise it is $L_+^g(j)$. This rule is represented by the diagram at the right side of Fig. 6. Similarly, if p is the left (the right) adjacent face of the edge j then $T^h(j, p)$ is T_-^h (resp. T_+^h) acting on the j th spin.

Using these notations, we can define local gauge transformations and magnetic charge operators corresponding to a vertex s and an adjacent face p (see Fig. 6). Put

$$\begin{aligned} A_g(s, p) &= A_g(s) = \prod_{j \in \text{star}(s)} L^g(j, s), \\ B_h(s, p) &= \sum_{h_1 \cdots h_k = h} \prod_{m=1}^k T^{h_m}(j_m, p), \end{aligned} \tag{11}$$

where j_1, \dots, j_k are the boundary edges of p listed in the counterclockwise order, starting from, and ending at, the vertex s . (The sum is taken over all combinations of $h_1, \dots, h_k \in G$, such that $h_1 \cdots h_k = h$. Order is important here!.) Although $A_g(s, p)$

¹⁰ In the field theory language, the value of a spin can be interpreted as a G gauge field. However, we do not perform symmetrization over gauge transformations.

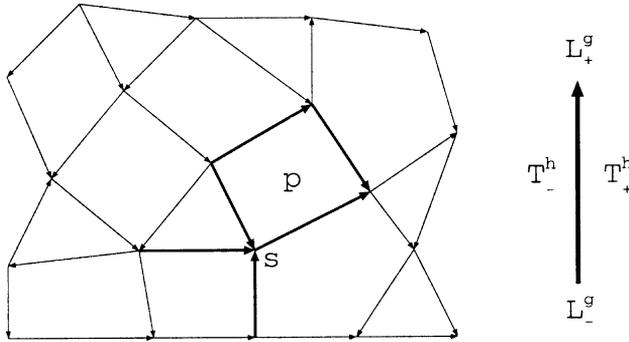


Fig. 6. Generic lattice and the orientation rules for the operators L_{\pm}^g and T_{\pm}^h .

does not depend on p , we retain this parameter to emphasize the duality between $A_g(s, p)$ and $B_h(s, p)$.¹¹ These operators generate an algebra $\mathcal{D} = \mathbf{D}(G)$, Drinfeld’s quantum double [20] of the group algebra $\mathbb{C}[G]$. It will play a very important role below. Now we only need two symmetric combinations of $A_g(s, p)$ and $B_h(s, p)$, namely

$$A(s) = N^{-1} \sum_{g \in G} A_g(s, p), \quad B(p) = B_1(s, p), \tag{12}$$

where $N = |G|$. Both $A(s)$ and $B(p)$ are projection operators. ($A(s)$ projects out the states which are gauge invariant at s , whereas $B(p)$ projects out the states with vanishing magnetic charge at p). The operators $A(s)$ and $B(p)$ commute with each other.¹² Also $A(s)$ commutes with $A(s')$, and $B(p)$ commutes with $B(p')$ for different vertices and faces. In the case $G = \mathbb{Z}_2$, these operators are almost the same as the operators (1), namely $A(s) = \frac{1}{2}(A_s + 1)$, $B(p) = \frac{1}{2}(B_p + 1)$.¹³

At this point, we have only defined the global Hilbert space \mathcal{N} (the tensor product of many copies of \mathcal{H}) and some operators on it. Now let us define the Hamiltonian.

$$H_0 = \sum_s (1 - A(s)) + \sum_p (1 - B(p)). \tag{13}$$

It is quite similar to the Hamiltonian (4). As in that case, the space of ground states is given by the formula

$$\mathcal{L} = \{|\xi\rangle \in \mathcal{N} : A(s)|\xi\rangle = |\xi\rangle, B(p)|\xi\rangle = |\xi\rangle \text{ for all } s, p\}. \tag{14}$$

The corresponding energy is 0; all excited states have energies ≥ 1 .

It is easy to work out an explicit representation of ground states similar to Eq. (3). The ground states correspond 1-to-1 to flat G -connections, defined up to conjugation, or super-positions of those. So, the ground state on a sphere is not degenerate. However, particles (excitations) have quite interesting properties even on the sphere or on the plane. (We treat the plane as an infinitely large sphere). The reader probably wants to know the answer first, and then follow formal calculations. So, I give a

¹¹ In the Hopf algebra setting, $A_g(s, p)$ does depend on p .

¹² This is not obvious. Use the commutation relations (10) to verify this statement.

¹³ Here A_s and B_p are the notations from Section 2; we will not use them any more.

brief abstract description of these particles. It is a mixture of general arguments and details which require verification.

The particles live on vertices or faces, or both; in general, one particle occupies a vertex and an adjacent face same time. A combination of a vertex and an adjacent face will be called a *site*. Sites are represented by dotted lines in Fig. 7. (The dashed lines are edges of the dual lattice.)

Consider n particles on the sphere pinned to particular sites x_1, \dots, x_n at large distances from each other. The space $\mathcal{L}[n] = \mathcal{L}(x_1, \dots, x_n)$ of n -particle states has dimensionality $N^{2(n-1)}$, including the ground state.¹⁴ Not all these states have the same energy. Even more splitting occurs under perturbation, but some degeneracy still survive. Of course, we assume that the perturbation is local, i.e., it can be represented by a sum of operators each of which acts only on few spins. To find the residual degeneracy, we will study the action of such *local operators* on the space $\mathcal{L}[n]$. Local operators generate a subalgebra $\mathcal{P}[n] \subseteq \mathbf{L}(\mathcal{L}[n])$. Elements of its center, $\mathcal{C}[n]$, are conserved classical quantities; they can be measured once and never change. (More exactly, they cannot be changed by local operators.) As these classical variables are locally measurable, we interpret them as particle’s types. It turns out that the types correspond 1-to-1 to irreducible representations of the algebra \mathcal{D} , the quantum double. Thus, each particle can belong to one of these types. The space $\mathcal{L}[n]$ and the algebra $\mathcal{P}[n]$ split accordingly:

$$\mathcal{L}[n] = \bigoplus_{d_1, \dots, d_n} \mathcal{L}_{d_1, \dots, d_n}, \quad \mathcal{P}[n] = \bigoplus_{d_1, \dots, d_n} \mathcal{P}_{d_1, \dots, d_n} \quad (\mathcal{P}_{d_1, \dots, d_n} \subseteq \mathbf{L}(\mathcal{L}_{d_1, \dots, d_n})), \quad (15)$$

where d_m is the type of the m th particle. The “classical” subalgebra $\mathcal{C}[n]$ is generated by the projectors onto $\mathcal{L}_{d_1, \dots, d_n}$.

But this is not the whole story. The subspace $\mathcal{L}_{d_1, \dots, d_n}$ splits under local perturbations from $\mathcal{P}_{d_1, \dots, d_n}$. By a general mathematical argument,¹⁵ this algebra can be characterized as follows:

$$\mathcal{L}_{d_1, \dots, d_n} = \mathcal{K}_{d_1, \dots, d_n} \otimes \mathcal{M}_{d_1, \dots, d_n}, \quad \mathcal{P}_{d_1, \dots, d_n} = \mathbf{L}(\mathcal{K}_{d_1, \dots, d_n}). \quad (16)$$

The space $\mathcal{K}_{d_1, \dots, d_n}$ corresponds to local degrees of freedom. They can be defined independently for each particle. So, $\mathcal{K}_{d_1, \dots, d_n} = \mathcal{K}_{d_1} \otimes \dots \otimes \mathcal{K}_{d_n}$, where \mathcal{K}_{d_m} is the space of “subtypes” (internal states) of the m th particle. Like the type, the subtype of a particle is accessible by local measurements. However, it can be changed, while the type cannot.

The most interesting thing is the *protected space* $\mathcal{M}_{d_1, \dots, d_n}$. It is not accessible by local measurements and is not sensitive to local perturbations, unless the particles come close to each other. This is an ideal place to store quantum information and operate with it. Unfortunately, the protected space does not have tensor product structure. However, it can be described as follows. Associated with each particle type a is an irreducible representation \mathcal{U}_a of the quantum double \mathcal{D} . Consider the product representation $\mathcal{U}_{d_1} \otimes \dots \otimes \mathcal{U}_{d_n}$ and split it into components corresponding to different irreducible representations. The protected space is the component corresponding to the identity representation.

¹⁴ The absence of particle at a given site is regarded as a particle of special type.

¹⁵ $\mathcal{P}_{d_1, \dots, d_n}$ is a subalgebra of $\mathbf{L}(\mathcal{L}_{d_1, \dots, d_n})$ with a trivial center, closed under Hermitian conjugation.

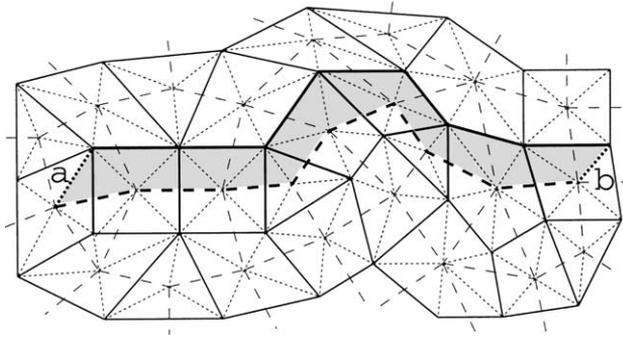


Fig. 7. A ribbon on the lattice.

If we swap two particles or move one around the other, the protected space undergoes some unitary transformation. Thus, the particles realize some multi-dimensional representation of the braid group. Such particles are called *non-abelian anyons*. Note that braiding does not affect the local degrees of freedom. If two particles fuse, they can annihilate or become another particle. The protected space becomes smaller but some classical information comes out, namely, the type of the new particle. So, we can do measurements on the protected space. Finally, if we create a new pair of particles of definite types, it always comes in a particular quantum state. So, we have a standard toolkit for quantum computation (new states, unitary transformations and measurements), except that the Hilbert space does not have tensor product structure. Universality of this toolkit is a separate problem, see Section 8.

Our model gives rise to the same braiding and fusion rules as gauge field theory models [10,11]. The existence of local degrees of freedom (subtypes) is a new feature. These degrees of freedom appear because there is no explicit gauge symmetry in our model.

6. Algebraic structure

6.1. Particles and local operators

This subsection is also rather abstract but the claims we do are concrete. They will be proven in Section 6.4.

As mentioned above, the ground state of the Hamiltonian (13) is not degenerate (on the sphere or on the plane regarded as an infinitely large sphere). Excited states are characterized by their energies. The energy of an eigenstate $|\psi\rangle$ is equal to the number of constraints $(A(s) - 1)|\psi\rangle = 0$ or $(B(p) - 1)|\psi\rangle = 0$ which are violated. Complete classification of excited states is a difficult problem. Instead of that, we will try to classify *elementary* excitations, or particles.

Let us formulate the problem more precisely. Consider a few excited “spots” separated by large distances. Each spot is a small region where some of the constraints are violated. The energy of a spot can be decreased by local operators but, generally, the spot cannot disappear. Rather, it shrinks to some minimal excitation (which need not

be unique). We will see (in Section 6.4) that any excited spot can be transformed into an excitation which violates at most 2 constraints, $A(s) - 1 \equiv 0$ and $B(p) - 1 \equiv 0$, where s is an arbitrary vertex, and p is an adjacent face. Such excitations are called *elementary excitations*, or *particles*. Note that definition of elementary excitations is a matter of choice. We could decide that an elementary excitation violates 3 constraints. Even with our definition, the “space of elementary excitations” is redundant.

By the way, the space of elementary excitations is not well-defined because such an excitation does not exist alone. More exactly, the only one-particle state on the sphere is the ground state. (This can be proven easily.) The right thing is the space of two-particle excitations, $\mathcal{L}(a, b)$. Here $a = (s, p)$ and $b = (s', p')$ are the sites occupied by the particles. (Recall that a site is a combination of a vertex and an adjacent face.) The projector onto $\mathcal{L}(a, b)$ can be written $\prod_{r \neq s, s'} A(r) \prod_{l \neq p, p'} B(l)$. Note that introducing a third particle (say, c) will not give more freedom for any of the two. Indeed, b and c can fuse without any effect on a .

Let us see how local operators act on the space $\mathcal{L}(a, b)$. In this context, a local operator is an operator which acts only on spins near a (or near b). Besides that, it should preserve the subspace $\mathcal{L}(a, b) \subseteq \mathcal{N}$ and its orthogonal complement. (\mathcal{N} is the space of all quantum states). Example: the operators $A_g(a)$ and $B_h(a)$, where $a = (s, p)$, commute with $A(r)$, $B(l)$ for all $r \neq s$ and $l \neq p$. Hence, they commute with the projector onto the subspace $\mathcal{L}(a, b)$. These operators generate an algebra $\mathcal{D}(a) \subset \mathbf{L}(\mathcal{N})$. It will be shown in Section 6.4 that $\mathcal{D}(a)$ includes *all* local operators acting on the space $\mathcal{L}(a, b)$, and the action of $\mathcal{D}(a)$ on $\mathcal{L}(a, b)$ is *exact* (i.e., different operators act differently).

Actually, the algebra $\mathcal{D}(a) = \mathcal{D}$ does not depend on a , only the embedding $\mathcal{D} \rightarrow \mathbf{L}(\mathcal{N})$ does. This algebra is called the *quantum double* of the group G and denoted by $\mathbf{D}(G)$. Its structure is determined by the following relations between the operators $A_g = A_g(a)$ and $B_h = B_h(a)$:

$$A_f A_g = A_{fg}, \quad B_h B_i = \delta_{h,i} B_h, \quad A_g B_h = B_{ghg^{-1}} A_g. \tag{17}$$

The operators $D_{(h,g)} = B_h A_g$ form a linear basis of \mathcal{D} . (In [10,11] these operators were denoted by $h \lfloor_g$.) The following multiplication rules hold

$$D_{(h_1, g_1)} D_{(h_2, g_2)} = \delta_{h_1, g_1 h_2, g_1^{-1}} D_{(h_1, g_1 g_2)}.$$

This identity can be also written in a symbolic tensor form, with h and g being combined into one index:

$$D_m D_n = \Omega_{mn}^k D_k \quad \Omega_{(h_1, g_1)(h_2, g_2)}^{(h, g)} = \delta_{h_1, g_1 h_2, g_1^{-1}} \delta_{h, h_1} \delta_{g, g_1 g_2} \tag{18}$$

(summation over k is implied). Actually, \mathcal{D} is not only an algebra, it is a quasi-triangular Hopf algebra, see Sections 6.2 and 6.3.

Note that $\mathcal{D} = \mathcal{D}(a)$ is closed under Hermitian conjugation (in $\mathbf{L}(\mathcal{N})$) which acts as follows:

$$A_g^\dagger = A_{g^{-1}}, \quad B_h^\dagger = B_h, \quad D_{(h,g)}^\dagger = D_{(g^{-1} h g, g^{-1})}. \tag{19}$$

Thus, $\mathcal{D} = \mathcal{D}(a)$ is a finite-dimensional C^* -algebra. Hence it has the following structure:

$$\mathcal{D} = \bigoplus_d \mathbf{L}(\mathcal{K}_d), \quad (20)$$

where d runs over all irreducible representations of \mathcal{D} . We can interpret d as particle's type.¹⁶ The absence of particle corresponds to a certain one-dimensional representation called the *identity representation*. More exactly, the operators $D_{(h,g)}$ act on the ground state $|\xi\rangle$ as follows:

$$D_k|\xi\rangle = \varepsilon_k|\xi\rangle, \quad \text{where} \quad \varepsilon_{(h,g)} = \delta_{h,1}. \quad (21)$$

The “space of subtypes,” \mathcal{K}_d actually characterize the redundancy of our definition of elementary excitations. However, this redundancy is necessary to have a nice theory of ribbon operators (see Section 6.2).

Irreducible representations of \mathcal{D} can be described as follows [10]. Let $u \in G$ be an arbitrary element, $C = \{gug^{-1} : g \in G\}$ its conjugacy class, $E = \{g \in G : gu = ug\}$ its centralizer. There is one irreducible representation $d = (C, \chi)$ for each conjugacy class C and each irreducible representation χ of the group E (see below). It does not matter which element $u \in C$ is used to define E . The conjugacy class C can be interpreted as magnetic charge whereas χ corresponds to electric charge. For example, consider the group S_3 (the permutation group of order 3). It has 3 conjugacy classes of order 1, 2, and 3, respectively. So, the algebra $\mathbf{D}(S_3)$ has irreducible representations of dimensionalities 1, 1, 2; 2, 2, 2; 3, 3.

The simplest case is when χ is the identity representation, i.e., the particle carries only magnetic charge but no electric charge. Then the subtypes can be identified with the elements of C , i.e., the corresponding space (denoted by \mathcal{B}_C) has a basis $\{|v\rangle : v \in C\}$. The local operators act on this space as follows:

$$D_{(h,g)}|v\rangle = \delta_{h,gv g^{-1}}|gv g^{-1}\rangle. \quad (22)$$

Now consider the general case. Denote by $W_f = W_f^{(\chi)}$ the irreducible action of $f \in E$ on an appropriate space \mathcal{A}_χ . Choose arbitrary elements $q_v \in G$ such that $q_v u q_v^{-1} = v$ for each $v \in C$. Then any element $g \in G$ can be uniquely represented in the form $g = q_v f$, where $v \in C$ and $f \in E$. We can define a unique action of \mathcal{D} on $\mathcal{B}_C \otimes \mathcal{A}_\chi$, such that

$$\begin{aligned} B_h(|v\rangle \otimes |\eta\rangle) &= \delta_{h,v}|v\rangle \otimes |\eta\rangle, \\ A_{q_v f}(|u\rangle \otimes |\eta\rangle) &= |v\rangle \otimes W_f|\eta\rangle \quad (v \in C, f \in E). \end{aligned} \quad (23)$$

More generally, $D_{(h,g)}(|v\rangle \otimes |\eta\rangle) = \delta_{h,gv g^{-1}}|gv g^{-1}\rangle \otimes W_f|\eta\rangle$, where $f = q_v(q_{vg^{-1}})^{-1}g$. This action is irreducible.

6.2. Ribbon operators

The next task is to construct a set of operators which can create an arbitrary two-particle state from the ground state. I do not know how to deduce an expression

¹⁶ *Caution.* The local operators should not be interpreted as symmetry transformations. The true symmetry transformations, so-called *topological operators*, will be defined in Section 7. Mathematically, they are described by the same algebra \mathcal{D} , but their action on physical states is different.

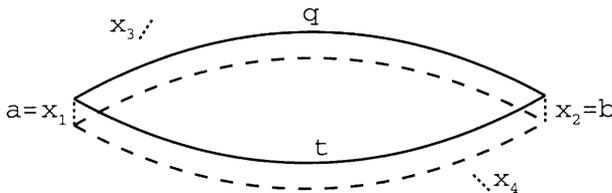
for such operators; I will just give an answer and explain why it is correct. In the abelian case (see Section 3) there were two types of such operators which corresponded to paths on the lattice and the dual lattice, respectively. In the non-abelian case, we have to consider both types of paths together. Thus, the operators creating a particle pair are associated with a *ribbon* (see Fig. 7). The ribbon connects two sites at which the particles will appear (say, $a = (s, p)$ and $b = (s', p')$). The corresponding operators act on the edges which constitute one side of the ribbon (solid line), as well as the edges intersected by the other side (dashed line).

For a given ribbon t , there are N^2 ribbon operators $F^{(h,g)}(t)$ indexed by $g, h \in G$. They act as follows:¹⁷

$$\begin{array}{c}
 \begin{array}{c}
 \xleftarrow{x_1} \quad \xleftarrow{x_2} \quad \xleftarrow{x_3} \\
 \begin{array}{|c|} \hline y_1 \\ \hline \end{array} \quad \begin{array}{|c|} \hline y_2 \\ \hline \end{array} \quad \begin{array}{|c|} \hline y_3 \\ \hline \end{array} \\
 \end{array} \\
 \\
 \begin{array}{c}
 \xleftarrow{x_1} \quad \xleftarrow{x_2} \quad \xleftarrow{x_3} \\
 \begin{array}{|c|} \hline h y_1 \\ \hline \end{array} \quad \begin{array}{|c|} \hline x_1^{-1} h x_1 y_2 \\ \hline \end{array} \quad \begin{array}{|c|} \hline (x_1 x_2)^{-1} h (x_1 x_2) y_3 \\ \hline \end{array} \\
 \end{array}
 \end{array} \tag{24}$$

These operators commute with every projector $A(r), B(l)$, except for $r = s, s'$ and $l = p, p'$. This is the first important property of ribbon operators.

The operators $F^{(h,g)}(t)$ depend on the ribbon t . However, their action on the space $\mathcal{L}(a, b)$ depends only on the *topological class* of the ribbon. This is also true for a multi-particle excitation space $\mathcal{L}(x_1, \dots, x_n)$. More exactly, consider two ribbons, t and q , connecting the sites $x_1 = a$ and $x_2 = b$. The actions of $F^{(h,g)}(t)$ and $F^{(h,g)}(q)$ on $\mathcal{L}(x_1, \dots, x_n)$ coincide provided none of the



¹⁷ Horizontal and vertical arrows are the two types of edges. Each of the two diagrams (6 arrows with labels) stand for a particular basis vector.

sites, x_3, \dots, x_n lie on or between the ribbons. This is the second important property of ribbon operators. We will write $F^{(h,g)}(t) \equiv F^{(h,g)}(q)$, or, more exactly,

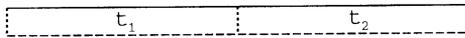
$$F^{(h,g)}(t) \equiv M^{(h,g)}(q), \text{ where } M = \{x_1, \dots, x_n\}.$$

Linear combination of the operators $F^{(h,g)}(t)$ are also called ribbon operators. They form an algebra $\mathcal{F}(t) \cong \mathcal{F}$. The multiplication rules are as follows:

$$F^m(t)F^n(t) = A_k^{mn}F^k(t), \quad A_{(h,g)}^{(h_1,g_1)(h_2,g_2)} = \delta_{h_1h_2,h} \delta_{g_1,g} \delta_{g_2,g} \tag{25}$$

(summation over m and n is implied).

Any ribbon operator on a long ribbon $t = t_1t_2$ (see figure below) can be represented in terms of ribbon operators corresponding to its parts, t_1 and t_2



$$F^k(t_1t_2) = \Omega_{mn}^k F^m(t_1)F^n(t_2), \quad \Omega_{(h_1,g_1)(h_2,g_2)}^{(h,g)} = \delta_{g,g_1g_2} \delta_{h_1,h} \delta_{h_2,g_1^{-1}hg_1} \tag{26}$$

(Note that $F^m(t_1)$ and $F^n(t_2)$ commute because the ribbons t_1 and t_2 do not overlap.) By some miracle, the tensor Ω_{**}^* is the same as in e.g., (18). From the mathematical point of view, (26) defines a linear mapping $\Delta(t_1, t_2) : \mathcal{F}(t_1, t_2) \rightarrow \mathcal{F}(t_1) \otimes \mathcal{F}(t_2)$, or just $\Delta : \mathcal{F} \rightarrow \mathcal{F}$. Such a mapping is called a *comultiplication*.

The comultiplication rules (26) allow to give another definition of ribbon operators which is nicer than Eq. (24). Note that a ribbon consists of triangles of two types (see Fig. 7). Each triangle corresponds to one edge. More exactly, a triangle with two dotted sides and one dashed side corresponds to a combination of an edge and its endpoint, say, i and r . Similarly, a triangle with a solid side corresponds to a combination of an edge and one of the adjacent faces, say, j and l . Each triangle can be considered as a short ribbon. The corresponding ribbon operators are

$$F^{(h,g)}(i, r) = \delta_{g,1} L^h(i, r), \quad F^{(h,g)}(j, l) = T^{g^{-1}}(j, l).$$

The ribbon operators on a long ribbon can be constructed from these ones.

It has been already mentioned that the multiplication in \mathcal{D} and the comultiplication in \mathcal{F} are defined by the same tensor Ω_{**}^* . Actually, \mathcal{D} and \mathcal{F} are Hopf algebras dual to each other.

(For general account on Hopf algebras, see [21–23].) The multiplication in \mathcal{F} corresponds to a comultiplication in \mathcal{D} defined as follows:

$$\Delta(D_k) = A_k^{mn} D_m \otimes D_n. \tag{27}$$

(More explicitly, $\Delta(D_{(h,g)}) = \sum_{h_1h_2=h} D_{(h_1,g)} \otimes D_{(h_2,g)}$.) The unit element of \mathcal{F} is $1_{\mathcal{F}} = \varepsilon_k F^k$, where ε_k are given by (21); the tensor ε_* also defines a counit of \mathcal{D} (i.e., the mapping $\varepsilon : \mathcal{D} \rightarrow \mathbb{C} : \varepsilon(D_k) = \varepsilon_k$). The unit of \mathcal{D} and the counit of \mathcal{F} are given by

$$e^{(h,g)} = \delta_{g,1}. \tag{28}$$

The Hopf algebra structure also includes an antipode, i.e., a mapping $S : \mathcal{D} \rightarrow \mathcal{D} : S(D_k) = S_k^m D_m$, or $S : \mathcal{F} \rightarrow \mathcal{F} : S(F^m) = S_k^m F^k$. The tensor S_{**}^* is given by the equation

$$S_{(h_2, g_2)}^{(h_1, g_1)} = \delta_{g_1^{-1} h_1 g_1, h_2^{-1} \delta_{g_1, g_2^{-1}}}. \tag{29}$$

Here is the complete list of Hopf algebra axioms.

$$A_i^{lm} A_k^{in} = A_k^{lj} A_j^{mn}, \quad \varepsilon_i A_k^{im} = A_k^{mj} \varepsilon_j = \delta_k^m, \tag{30}$$

$$\Omega_{lm}^i \Omega_{in}^k = \Omega_{lj}^k \Omega_{mn}^j, \quad e^i \Omega_{im}^k = \Omega_{mj}^k e^j = \delta_m^k, \tag{31}$$

$$A_q^{lm} \Omega_{kn}^q = \Omega_{ij}^l \Omega_{rs}^m A_k^{ir} A_n^{js}, \quad \varepsilon_q \Omega_{kn}^q = \varepsilon_k \varepsilon_n, \quad A_q^{lm} e^q = e^l e^m, \tag{32}$$

$$S_l^k A_p^{lm} \Omega_{kn}^q \delta_m^n = \delta_l^k A_p^{lm} \Omega_{kn}^q S_m^n = \varepsilon_p e^q. \tag{33}$$

Most of these identities correspond to physically obvious properties of ribbon operators. Eq. (30) is a statement of the usual multiplication axioms in the algebra \mathcal{F} , namely, $(F^l F^m) F^n = F^l (F^m F^n)$ and $1 F^m = F^m 1 = F^m$. The first equation in (31) (coassociativity of the comultiplication in \mathcal{F}) can be proven by expanding $F^k(t_1 t_2 t_3)$ as $\Omega_{in}^k F^i(t_1 t_2) F^n(t_3)$ or $\Omega_{lj}^k F^l(t_1) F^j(t_2 t_3)$ —the result must be the same.¹⁸ Equation (32) mean that the multiplication and comultiplication are consistent with each other. To prove the first equation in (32), expand $F^l(t_1 t_2) F^m(t_1 t_2)$ in two different ways. The second equation follows from the fact that $\varepsilon_q F^q(t_1 t_2)$ is the identity operator.

The antipode axiom (33) does not have explicit physical meaning. Mathematically, it is a *definition* of the tensor S_*^* : the element $\gamma = S_k^l F^k \otimes D_l \in \mathcal{F} \otimes \mathcal{D}$ is the inverse to the canonical element $\delta = F^i \times D_i$. The antipode have the following properties which can be derived from (30)–(33):

$$S_l^i S_m^j A_p^{lm} = A_q^{ji} S_p^q, \quad S_q^p \Omega_{ij}^q = \Omega_{ml}^p S_j^m S_l^l. \tag{34}$$

Finally, we can define a so-called *skew antipode* \tilde{S}_*^* as follows:

$$\tilde{S}_i^m S_n^i = S_j^m \tilde{S}_n^j = \delta_n^m. \tag{35}$$

In our case, $\tilde{S}_i^m = S_i^m$, but this is not true for a generic Hopf algebra. The skew antipode have the following properties similar to (33) and (34):

$$\tilde{S}_l^n A_p^{lm} \Omega_{kn}^q \delta_m^k = \delta_l^n A_p^{lm} \Omega_{kn}^q \tilde{S}_m^k = \varepsilon_p e^q, \tag{36}$$

$$\tilde{S}_l^i \tilde{S}_m^j A_p^{lm} = A_l^{ji} \tilde{S}_p^q, \quad \tilde{S}_q^p \Omega_{ij}^q = \Omega_{ml}^p \tilde{S}_j^m \tilde{S}_i^l \tag{37}$$

(Note the distinction between (33) and (36), however.)

The reader may be overwhelmed by a number of formal things, so let us summarize what we know by now. We have denned two algebras, \mathcal{D} and \mathcal{F} , and their actions on the Hilbert space \mathcal{N} . In this context, we denote them by $\mathcal{D}(a)$ and $\mathcal{F}(t)$ because the actions depend on the site a or on the ribbon t , respectively. Operators from $\mathcal{D}(a)$ affect one particle whereas operators from $\mathcal{F}(t)$ affect two particles. The

¹⁸ The coassociativity is necessary and sufficient for that. The sufficiency is rather obvious; the necessity follows from the fact that the mapping $\mathcal{F} \rightarrow \mathcal{F}(t)$ is injective, i.e., the operators $F^k(t)$ with different k are linearly independent.

action of $\mathcal{F}(t)$ on the space of n -particle states $\mathcal{L}(x_1, \dots, x_n)$ depends only on the topological class of the ribbon t . This space have not been found yet, even for $n = 2$. (It will be found after we learn more about local and ribbon operators.) The algebra \mathcal{F} is a Hopf algebra. The comultiplication allows to make up a long ribbon from parts. There is a formal duality between \mathcal{F} and \mathcal{D} . The comultiplication in \mathcal{F} is dual to the multiplication in \mathcal{D} . The multiplication in \mathcal{F} is dual to a comultiplication in \mathcal{D} . (The meaning of the latter is not clear yet.)

6.3. Further properties of local and ribbon operators

Let us study commutation relations between ribbon operators. Consider two ribbons attached to the same site, as shown in Fig. 8a or b. Then

$$\begin{aligned} F^{(h,g)}(t_1)F^{(v,u)}(q_1) &= F^{(v,u)}(q_1)F^{(v^{-1}hv, v^{-1}g)}(t_1), \\ F^{(h,g)}(t_2)F^{(v,u)}(q_2) &= F^{(v,u)}(q_2)F^{(h, gu^{-1}vu)}(t_2). \end{aligned}$$

In a tensor form, these equations read as follows:

$$\begin{aligned} F^m(t_1)F^n(q_1) &= R^{ik}\Omega_{ij}^n\Omega_{kl}^mF^j(q_1)F^l(t_1), \\ F^m(t_2)F^n(q_2) &= F^i(q_2)F^k(t_2)\Omega_{ij}^n\Omega_{kl}^m\bar{R}^{il}, \end{aligned} \quad (38)$$

where

$$R^{(h,g)(v,u)} = \delta_{h,u}\delta_{g,1}, \quad \bar{R}^{(h,g)(v,u)} = \delta_{h^{-1},u}\delta_{g,1}. \quad (39)$$

Note that

$$\bar{R}^{ik}\Omega_{ij}^n\Omega_{kl}^mR^{jl} = R^{ik}\Omega_{ij}^n\Omega_{kl}^m\bar{R}^{jl} = e^n e^m. \quad (40)$$

To prove¹⁹ (and to see the physical meaning of) this equation, consider the configuration shown in Fig. 9b. Clearly, $F^r(t_2t_1)$ and $F^s(q')$ commute. On the other hand, $F^s(q') \equiv F^s(q_2q_1)$, so $F^r(t_2t_1)$ and $F^s(q_2q_1)$ commute. It follows that $\bar{R}^{ik}\Omega_{ij}^n\Omega_{kl}^m = e^n e^m$. This identity can be easily written in an invariant form, namely, $\bar{R}R = I_{\mathcal{D} \otimes \mathcal{D}}$, where $R = R^{jl}D_j \otimes D_l$ and $\bar{R} = \bar{R}^{ik}D_i \otimes D_k$. It also implies that $R\bar{R} = I_{\mathcal{D} \otimes \mathcal{D}}$ because the algebra $\mathcal{D} \otimes \mathcal{D}$ is finite dimensional. Thus, $\bar{R} = R^{-1}$.

The tensor R_* (or the element $R \in \mathcal{D} \otimes \mathcal{D}$) is called the *R-matrix*. It satisfies the following axioms:

$$A_k^{ij}R^{km} = R^{il}R^{jn}\Omega_{ln}^m, \quad R^{mk}A_k^{ji} = \Omega_{ln}^mR^{li}R^{nj}, \quad (41)$$

$$A_k^{ji} = \Omega_{lmr}^i\Omega_{pns}^jR^{lp}A_k^{mn}\bar{R}^{rs}, \quad (42)$$

where $\Omega_{lmr}^i = \Omega_{lu}^i\Omega_{mr}^u = \Omega_{lm}^u\Omega_{ur}^i$. Eq. (41) follow from (38). Conversely, these equations ensure that the commutation relation are consistent. To prove the first equation in (41), commute $F^m(t_1)F^i(q_1)F^j(q_1)$ in two different ways. You will get $W_{ab}^{ijm}F^a(q_1)F^b(t_1)$, with two different expressions for W_{ab}^{ijm} . Then calculate $W_{ab}^{ijm}e^ae^b$

¹⁹ This proof is not rigorous, but an interested reader can easily fix it. Anyway, you can just substitute (39) into (40) and check it directly.

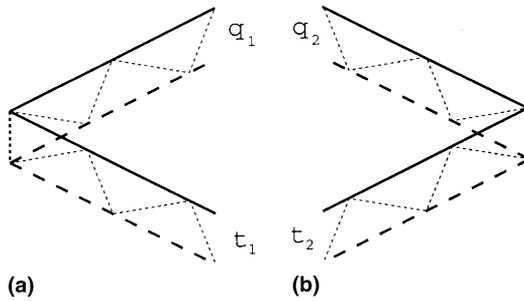


Fig. 8. Two ribbons attached to the same site.

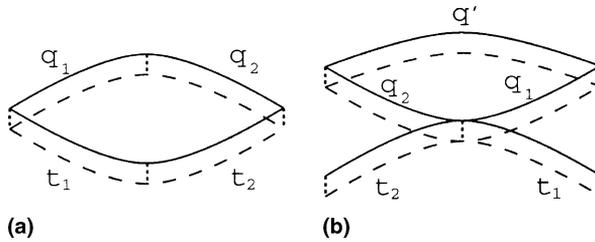


Fig. 9. Checking consistency of the commutation relations.

using the axioms (30)–(32). The second equation in (41) can be proven in a similar way.

To prove Eq. (42), consider the configuration shown in Fig. 9a. Clearly, $F^i(q_1q_2) \equiv F^i(t_1t_2)$, so $F^j(t_1t_2)F^i \equiv A_k^{ji}F^k(t_1t_2)$. On the other hand, we can first expand $F^j(t_1, t_2)$ and $F^i(q_1q_2)$ using the comultiplication rules, and then apply the commutation relations (38). The result must be the same.

Let t be a ribbon connecting sites a and b . The local and ribbon operators commute as follows:

$$a \overbrace{\hspace{10em}}^t b$$

$$F^m(t)D_i(a) = A_i^{ik}\Omega_{kl}^m D_j(a)F^l(t), \quad D_i(b)F^m(t) = \Omega_{lk}^m A_i^{kj}F^l(t)D_j(b). \tag{43}$$

These commutation relations can be also written in the form

$$\begin{aligned} D_j(a)F^l(t) &= A_j^{ik}\tilde{S}_k^n \Omega_{nm}^l F^m(t)D_i(a), \\ F^l(t)D_j(b) &= \Omega_{mn}^l \tilde{S}_k^n A_j^{ki} D_i(b)F^m(t), \end{aligned} \tag{44}$$

where \tilde{S}_*^* is the skew antipode (see (35) and (36)).

Finally, we introduce some special elements $C \in \mathcal{D}$ and $\tau \in \mathcal{F}$. The first one has a clear physical meaning: the corresponding operator $C(a) = A(a)B(a)$ projects out states with no particle at the site a . The element C can be represented in the form

$$C = c^i D_i, \quad \text{where } c^{(h,g)} = N^{-1} \delta_{h,1}. \quad (45)$$

It has the following properties:

$$CX = XC = \varepsilon(X)C \text{ for any } X \in \mathcal{D} \quad \varepsilon(C) = 1,$$

or, in tensor notations,

$$\Omega_{ij}^k c^i = \Omega_{ji}^k c^j = \varepsilon_j c^k \quad \varepsilon_k c^k = 1. \quad (46)$$

The element $\tau \in \mathcal{F}$ is dual to C ; it is defined as follows:

$$\tau = \tau_i F^i, \quad \text{where } \tau_{(h,g)} = N^{-1} \delta_{1,g}. \quad (47)$$

Its properties are as follows:

$$A_k^{ij} \tau_i = A_k^{ji} \tau_j = e^j \tau_k, \quad e^k \tau_k = 1. \quad (48)$$

Note that $\tau_k c^k = N^{-2}$. Using these properties, we can derive an important consequence from the commutation relations (43)

$$\tau_s \Omega_{mp}^s S_p^q F^m(t) C(a) F^q(t) = \tau_s \Omega_{pm}^s S_p^q F^q(t) C(b) F^m(t) = N^{-2}. \quad (49)$$

6.4. The space $\mathcal{L}(a, b)$

Now we are in a position to find the space $\mathcal{L}(a, b)$ and to prove the assertions from Section 6.1. The first assertion was that any excited spot can be transformed into one particle. It is simple if we can transform two particles into one by ribbon operators. Let us choose an arbitrary site b the excited spot to be compressed to. Let some constraint, $A(s) - 1 \equiv 0$ or $B(p) - 1 \equiv 0$, be violated. Choose any site a containing the vertex s or the face p . Connect a and b by a ribbon. By the assumption, we can clean up the site a while changing the state of b , but without violating any more constraint. We can repeat this procedure again and again to clean up the whole spot.

So, we only need to show that two particles can be transformed into one. What does it mean exactly? Physically, any transformation must be unitary, but it can involve also some external system. (Otherwise, it is impossible to “decrease entropy,” i.e., to convert many states into fewer.) On the other hand, it is clear that unitarity is not relevant to this problem. However, we should exclude degenerate transformations, such as multiplication by the zero operator. So, it is better to reformulate the assertion as follows: any two-particle state (plus some other excitations far away) can be obtained from one-particle states (plus the same excitations far away). Let $|\psi\rangle \in \mathcal{L}(a, b, \dots)$ be such a two-particle state. We are going to use the formula (49). Let

$$G_q = N^2 \tau_s \Omega_{mp}^s S_p^q F^m(t), \quad |\eta^q\rangle = C(a) F^q(t) |\psi\rangle. \quad (50)$$

Then $|\psi\rangle = G_q |\eta^q\rangle$. The states $|\eta^q\rangle$ belong to $\mathcal{L}(b, \dots)$, i.e., do not contain excitation at a . This is exactly what we need.

The other two assertions were about the action of local operators on the space $\mathcal{L}(a, b)$, so we need to find this space first. We can consider this space as a

representation of the algebra $\mathcal{E} \cong \mathcal{E}(t)$ generated by the operators $D_j = D_j(a)$, $F^l = F^l(t)$, and $D'_j = D_j(b)$. As a linear space, $\mathcal{E} = \mathcal{D} \otimes \mathcal{F} \otimes \mathcal{D}$. (Thus, \mathcal{E} has dimensionality N^6 .) Multiplication in \mathcal{E} is defined by the commutation relations (43). We will call $\mathcal{E} \cong \mathcal{E}(t)$ the algebra of *extended ribbon operators*. It is just an algebra, not a Hopf algebra. More exactly, it is a finite-dimensional C^* -algebra. The involution (= Hermitian conjugation) is given by the formulas (cf. (19))

$$(D_{(h,g)})^\dagger = D_{(g^{-1}hg, g^{-1})}, \quad (F^{(h,g)})^\dagger = F^{(h^{-1}, g)}, \quad (D'_{(h,g)})^\dagger = D'_{(g^{-1}hg, g^{-1})}. \quad (51)$$

Remark. Apparently, the algebra \mathcal{E} will play the central role in a general theory of topological quantum order. Indeed, we were lucky to define ribbon operators separately from local operators. In the general case, ribbon operators should be mixed with local operators.

So, we are looking for a particular representation \mathcal{L} of the algebra \mathcal{E} . This representation must contain a special vector $|\xi\rangle$ (the ground state) such that

$$D_k|\xi\rangle = \varepsilon_k|\xi\rangle, \quad D'_k|\xi\rangle = \varepsilon_k|\xi\rangle. \quad (52)$$

We start with constructing a representation $\tilde{\mathcal{L}}$ spanned by the vectors $|\psi^k\rangle = F^k|\xi\rangle$. (It will be proven after that $\tilde{\mathcal{L}} = \mathcal{L}$.) We assume that the vectors $|\psi^k\rangle$ are linearly independent. This need not be the case in the representation \mathcal{L} but we can postulate $|\psi^k\rangle$ being linearly independent in $\tilde{\mathcal{L}}$. Thus, \mathcal{L} contains a factor-representation of $\tilde{\mathcal{L}}$.

The representation $\tilde{\mathcal{L}}$ is given by the formulas

$$D_j|\psi^k\rangle = \tilde{S}_j^n \Omega_{nm}^k |\psi^m\rangle, \quad F^j|\psi^k\rangle = A_m^k |\psi^m\rangle, \quad D'_j|\psi^k\rangle = \Omega_{mj}^k |\psi^m\rangle. \quad (53)$$

It is easy to show that this representation is irreducible. Hence, \mathcal{L} contains $\tilde{\mathcal{L}}$, i.e., the vectors $|\psi^k\rangle$ are linearly independent in \mathcal{L} . The scalar products between the vectors $|\psi^k\rangle$ can be found from (53) and (51),

$$\langle \psi^{(v,u)} | \psi^{(h,g)} \rangle = N^{-1} \delta_{v,h} \delta_{u,g}. \quad (54)$$

To prove that $\tilde{\mathcal{L}} = \mathcal{L}$, we use the Eq. (49) again. For an arbitrary two-particle state $|\psi\rangle \in \mathcal{L}$, define the vectors $|\eta^q\rangle$ and operators G_q as in Eq. (50). Then $|\psi\rangle = G_q|\eta^q\rangle$. One could say that $|\eta^q\rangle \in \mathcal{L}(b)$ but, actually, the space $\mathcal{L}(b)$ is spanned by the sole vector $|\xi\rangle$. It follows that $|\psi\rangle \in \tilde{\mathcal{L}}$ —the assertion has been proven. Thus, the action of local and ribbon operators on the space $\mathcal{L} = \mathcal{L}(a, b)$ is given by Eq. (53).

It is easy to see that the action of $\mathcal{D}(a)$ on $\mathcal{L}(a, b)$ is exact (though it is reducible). Besides that, $\mathcal{D}(a)$ is the commutant of $\mathcal{D}(b)$ in $\mathbf{L}(\mathcal{L}(a, b))$ and vice versa. (That is, $\mathcal{D}(a)$ consists of all operators $X \in \mathbf{L}(\mathcal{L}(a, b))$ which commute with every $Y \in \mathcal{D}(b)$.) Hence, $\mathcal{D}(a)$ includes *all* local operators acting on the space $\mathcal{L}(a, b)$. Indeed, a local operator, which involves only spins near the site a , must commute with any operator acting on distant spins. Of course, there are many such operators, but their action on the two-particle space $\mathcal{L}(a, b)$ coincides with the action of the operators from $\mathcal{D}(a)$. This is also true for a multi-particle excitation space $\mathcal{L}(x_1, \dots, x_n)$.

The space $\mathcal{L}(x_1, \dots, x_n)$ can be described as follows. Let us connect the sites x_1, \dots, x_n by $n - 1$ ribbons t_1, \dots, t_{n-1} in an arbitrary way so that the ribbons form a tree. Then the vectors $|\psi^{k_1, \dots, k_{n-1}}\rangle = F^{k_1}(t_1) \dots F^{k_{n-1}}(t_{n-1})|\xi\rangle$ form a basis of $\mathcal{L}(x_1, \dots, x_n)$. Choosing different ribbons means choosing a different basis. In the next section we will give another description of multi-particle excitation spaces.

7. Topological operators, braiding, and fusion

Let us consider again the n -particle excitation space $\mathcal{L} = \mathcal{L}(x_1, \dots, x_n)$. The algebra $\mathbf{L}(\mathcal{L})$ includes the local operator algebras $\mathcal{D}(x_1), \dots, \mathcal{D}(x_n)$. An operator $Y \in \mathbf{L}(\mathcal{L})$ which commutes with every $X \in \mathcal{D}(x_j)$ ($j = 1, \dots, n$) is called a *topological operator*. Physically, topological operators correspond to non-local degrees of freedom. For $n = 2$, the algebra of topological operators coincides with the center of $\mathcal{D}(x_1)$ or $\mathcal{D}(x_2)$. (The two centers coincide). Hence, the only non-local degree of freedom is the type of either particle. (The two particles correspond to dual representations of \mathcal{D} ; in other words, these are a particle and an anti-particle.) So, there is no hidden (i.e., quantum non-local) degree of freedom in this case. Such hidden degrees of freedom appear for $n \geq 3$.

To describe the space \mathcal{L} and operators acting on it, let us choose an arbitrary site x_0 (distinct from x_1, \dots, x_n) and connect it with x_1, \dots, x_n by non-intersecting ribbons t_1, \dots, t_n , see Fig. 10a. As stated above, the space $\mathcal{L}(x_0, x_1, \dots, x_n)$ is spanned by the vectors

$$|\psi^{k_1, \dots, k_n}\rangle = F^{k_1}(t_1) \dots F^{k_n}(t_n)|\xi\rangle. \tag{55}$$

The space in question, $\mathcal{L} = \mathcal{L}(x_1, \dots, x_n)$ is contained in $\mathcal{L}(x_0, x_1, \dots, x_n)$. It consists of all vectors $|\psi\rangle \in \mathcal{L}(x_0, x_1, \dots, x_n)$ which are invariant under the action of $\mathcal{D}(x_0)$ on the latter space.

The advantage of this description is that we can easily find all operators on the space $\mathcal{L}(x_0, x_1, \dots, x_n)$ which commute with $\mathcal{D}(x_1) \otimes \dots \otimes \mathcal{D}(x_n)$. These are simply operators which act on the ends of the ribbons t_1, \dots, t_n attached to the site x_0 . More

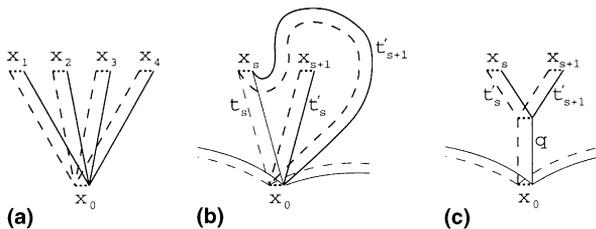


Fig. 10. Braiding and fusion in terms of ribbon transformations.

exactly, an operator $D_j^{(r)}$ ($r = 1, \dots, n$) acts on the r th ribbon as $D'_j = D_j(x_0)$ (see Eq. (53)), but does not affect the other ribbons,

$$\left(D_{j_1}^{(1)} \otimes \dots \otimes D_{j_n}^{(n)} \right) |\psi^{k_1, \dots, k_n}\rangle = \Omega_{m_1 j_1}^{k_1} \dots \Omega_{m_n j_n}^{k_n} |\psi^{m_1, \dots, m_n}\rangle. \tag{56}$$

Thus, we arrive to an interesting physical conclusion. Let us consider only one particle attached to an end of a semi-infinite ribbon (an analog of Dirac’s string). Then *the topological operators act on the far end of the ribbon*.

Example. Let us see how the topological operators act on magnetic vortices. As shown in Section 6.1, a vortex type is characterized by a conjugacy class C of the group G . Individual topological states of the particle are characterized by particular elements $v \in C$. In terms of the notation (55), such a state can be represented as follows:

$$|u, v\rangle = |C|^{1/2} \sum_{x: x^{-1}ux=v} |\psi^{(u,x)}\rangle,$$

where $u \in C$ characterize the local state of the particle. One can easily check that $D'_{(h,g)}|u, v\rangle = \delta_{h,gv} |u, h\rangle$. This is consistent with Eq. (22). Note that the local degree of freedom, u , is not affected.

How can we physically apply topological operators to particles? We can just move the particles around each other; this process is called *braiding*. Let us see what happens if we interchange two particles, x_s and x_{s+1} , counterclockwise, as shown in Fig. 10b. The state $|\psi^{\dots; k; l; \dots}\rangle$ becomes a new state

$$|\psi^{\dots; k; l; \dots}\rangle_{\text{new}} = \mathcal{R}_x |\psi^{\dots; k; l; \dots}\rangle = \dots F^k(t'_s) F^l(t'_{s+1}) \dots |\xi\rangle.$$

To represent this state in the old basis, we should represent the operator $F^k(t'_s) F^l(t'_{s+1})$ in terms of $F^m(t_s)$ and $F^n(t_{s+1})$. Obviously, $F^k(t'_s) = F^k(t_{s+1})$; also $F^l(t'_{s+1}) \equiv F^l(t_s)$ as long as there is no particle at x_{s+1} , i.e., the operator $F^k(t_{s+1})$ is not applied yet. Hence,

$$F^k(t'_s) F^l(t'_{s+1}) \equiv F^k(t_{s+1}) F^l(t_s).$$

Now we can apply the second commutation relation from (38). (Actually, we should reverse it.) It follows that:

$$F^k(t_{s+1}) F^l(t_s) = R^i \Omega_{m_i}^l \Omega_{n_j}^k F^m(t_s) F^n(t_{s+1}),$$

$$\mathcal{R}_x |\psi^{\dots; k; l; \dots}\rangle = R^i \left(D_i^{(s)} \otimes D_j^{(s+1)} \right) |\psi^{\dots; l; k; \dots}\rangle.$$

(see Eq. (56)). Consequently, the counterclockwise interchange operator has the form

$$\mathcal{R}_x = R^i \left(D'_i \otimes D'_j \right) \sigma = \sigma R^{ij} \left(D'_i \otimes D'_j \right), \tag{57}$$

where σ is the permutation operator, and D'_i, D'_j are understood as topological operators. (Note that the operator σ permutes both topological and local degrees of freedom.)

Example. Consider two magnetic vortices characterized by topological parameters $v_1, v_2 \in G$. The operator $\mathcal{R}_x \curvearrowright$ acts on the state $|v_1, v_2\rangle$ as follows:

$$\mathcal{R}_x |v_1 v_2\rangle = |v_1 v_2 v_1^{-1}, v_1\rangle. \quad (58)$$

(The local parameters, u_1 and u_2 , are suppressed in this formula.)

Finally, let us see what happens if two particles, x_s and x_{s+1} , fuse into one. The resulting particle can be characterized by the action of topological operators on it. From this point of view, we can just glue parts of the corresponding ribbons (see Fig. 10c) instead of fusing the particles themselves. Then

$$\begin{aligned} F^k(t_s) F^l(t_{s+1}) &\equiv \Omega_{m_i}^k \Omega_{n_j}^l A_p^{ij} F^m(t'_s) F^n(t'_{s+1}) F^p(q), \\ |\psi^{\dots k, l, \dots}\rangle &\equiv \Omega_{m_i}^k \Omega_{n_j}^l A_p^{ij} F^m(t'_s) F^n(t'_{s+1}) |\psi^{\dots p, \dots}\rangle, \\ A_r^{uv} D_u^{(s)} \otimes D_v^{(s+1)} &\equiv D'_r, \end{aligned}$$

where D'_r acts on the end of the ribbon q . Thus, fusion is described by the comultiplication in the algebra \mathcal{D} , see Eq. (27). (To avoid confusion, one should replace D_* with D'_* in that equation.) The topological operator $\Delta(D'_k)$ acts on a particle pair as the topological operator D'_k on the particle resulting from fusion.

Example. Consider a pair of opposite magnetic vortices $|v, v^{-1}\rangle$. The operators $\Delta(D'_k)$ act on this state as follows:

$$\Delta(D'_{(h,g)}) |v, v^{-1}\rangle = \delta_{h,1} |g v g^{-1}, g v^{-1} g^{-1}\rangle. \quad (59)$$

In terms of the representation classification (see Section 6.1), this action corresponds to the pair (C, χ) , where $C = \{1\}$, and χ is the adjoint representation of G . Thus, when opposite magnetic vortices fuse, the resulting particle has no magnetic charge but may have some electric charge.

8. Universal computation by anyons

(This section should be considered as an abstract of results to be presented elsewhere.)

Universal quantum computation is possible in the model based on the permutation group S_5 . (Unsolvability of the group seems to be important.) Vortex pairs $|v, v^{-1}\rangle$, where v is a transposition, are used as qubits. It is possible to perform the following operations:

1. To produce pairs with zero charge. If a pair is created from the ground state, it has no charge automatically.

2. To measure the electric charge of a vortex pair destructively. For this, we should simply fuse the pair into one particle.
3. To perform the following unitary transformation on two pairs

$$|u, u^{-1}\rangle \otimes |v, v^{-1}\rangle \mapsto |vuv^{-1}, vu^{-1}v^{-1}\rangle \otimes |v, v^{-1}\rangle. \quad (60)$$

For this, we pull the first pair (as a whole) between the particles of the second pair.

4. To measure the value of v and produce an unlimited number of pure states $|v, v^{-1}\rangle$ for any given transposition v (say, $(1, 2)$ or $(2, 3)$). [At first sight, it is impossible because we can only measure the conjugacy class of a v . However, we can agree on a given state to correspond to $v = (1, 2)$. Then we use it as a reference to produce an unlimited number of copies.]

The operations 3 and 4 are sufficient to perform universal classical computation. It is relatively simple to run quantum algorithms based on measurements [24]. Simulating a universal gate set is more subtle and requires *composite qubits*. That is, a usual qubit (with two distinct states) is represented by several vortex pairs.

9. Concluding remarks

It has been shown that anyons can arise from a Hamiltonian with local interactions but without any symmetry. These anyons can be used to perform universal quantum computation. There are still many things to do and questions to answer. First of all, it is desirable to find other models with anyons which allow universal quantum computation. (The group S_5 is quite unrealistic for physical implementation). Such models must be based on a more general algebraic structure rather than the quantum double of a group algebra. A general theory of anyons and topological quantum order is lacking. [In a sense, a general theory of anyons already exists [10]; it is based on quasi-triangular quasi-Hopf algebras. However, this theory either merely postulates the properties of anyons or connects them to certain field theories. This is quite unlike the theory of local and ribbon operators which describes both the properties of excitations and the underlying spin entanglement.] It is also desirable to formulate and prove some theorem about existence and the number of local degrees of freedom. (It seems that the local degrees of freedom are a sign that anyons arise from a system with no symmetry in the Hamiltonian.) Finally, general understanding of dynamically created, or “materialized” symmetry is lacking. There one may find some insights for high-energy physics. If we adopt a conjecture that the fundamental Hamiltonian or Lagrangian is not symmetric, we can probably infer some consequences about the particle spectrum.

Acknowledgments

I am grateful to J. Preskill, D.P. DiVincenzo and C.H. Bennett for interesting discussions and questions which helped me to clarify some points in my constructions. This work was supported, in part, by the Russian Foundation for Fundamental

Research, Grant No. 96-01-01113. Part of this work was completed during the 1997 Elsas-Bailey—I.S.I. Foundation research meeting on quantum computation.

References

- [1] P. Shor, in: *Proceedings of the 35th Annual Symposium on Fundamentals of Computer Science*, IEEE Press, Los Alamitos, CA, 1994, pp. 124–134.
- [2] P. Shor, in: *Proceedings of the Symposium on the Foundations of Computer Science*, IEEE Press, Los Alamitos, CA, 1996, e-print quant-ph/9605011.
- [3] E. Knill, R. Laflamme, Concatenated quantum codes, 1996 (e-print quant-ph/9608012).
- [4] E. Knill, R. Laflamme, W. Zurek, Accuracy threshold for quantum computation, 1996 (e-print quant-ph/9610011).
- [5] D. Aharonov, M. Ben-Or, Fault-tolerant quantum computation with constant error, 1996 (e-print quant-ph/9611025).
- [6] A.Yu. Kitaev, Quantum computation: algorithms and error correction, *Russian Math. Surveys*, 52 (6) (1997) 1191.
- [7] C. Zalka, Threshold estimate for fault-tolerant quantum computing, 1996 (e-print quant-ph/9612028).
- [8] A.Yu. Kitaev, in: O. Hirota, A.S. Holevo, C.M. Caves (Eds.), *Quantum Communication, Computing and Measurement*, Plenum, New York, 1997.
- [9] F. Wilczek, *Fractional Statistics and Anyon Superconductivity*, World Scientific, Singapore, 1990.
- [10] R. Dijkgraaf, V. Pasquier, P. Roche, *Nucl. Phys. B (Proc. Suppl.)* 18B (1990).
- [11] F.A. Bais, P. van Driel, M. de Wild Propitius, *Phys. Lett. B* 280 (1992) 63.
- [12] F.A. Bais, M. de Wild Propitius, Discrete gauge theories, 1995 (e-print hep-th/9511201).
- [13] H.K. Lo, J. Preskill, *Phys. Rev. D* 48 (1993) 4821.
- [14] G. Castagnoli, M. Rasetti, *Int. J. Mod. Phys.* 32 (1993) 2335.
- [15] D. Gottesman, *Phys. Rev. A* 54 (1996) 1862.
- [16] A.R. Calderbank, E.M. Rains, P.M. Shor, N.J.A. Sloane, *Phys. Rev. Lett.* 78 (1997) 405.
- [17] A.R. Calderbank, P.W. Shor, Good quantum error-correcting codes exist, 1995 (e-print quant-ph/9512032).
- [18] D. Arovas, J.R. Schrieffer, F. Wilczek, *Phys. Rev. Lett.* 53 (1984) 722–723.
- [19] T. Einarsson, *Phys. Rev. Lett.* 64 (1984) 1995–1998.
- [20] V.G. Drinfeld, in: *Proc. Int. Cong. Math. (Berkeley, 1986)*, 1987, pp. 798–820.
- [21] M. Sweedler, *Hopf Algebras*, W.A. Benjamin, New York, 1969.
- [22] S. Majid, *Int. J. Mod. Phys. A* 5 (1990) 1–91.
- [23] C. Kassel, *Quantum Groups*, Springer-Verlag, New York, 1995.
- [24] A.Yu. Kitaev, Quantum measurements and Abelian stabilizer problem, 1995 (e-print quant-ph/9511026).
- [25] G. 'tHooft, *Nucl. Phys. B* 138 (1978) 1.