

# Fermionic quantum computation

Sergey B. Bravyi

*L. D. Landau Institute for Theoretical Physics,  
Kosygina St. 2, Moscow, 117940, Russia,  
serg@itp.ac.ru*

and

Alexei Yu. Kitaev\*  
*Microsoft Research  
Microsoft, #113/2032, One Microsoft Way,  
Redmond, WA 98052, U.S.A.  
kitaev@microsoft.com*

March 31, 2000

## Abstract

We define a model of quantum computation with local fermionic modes (LFMs) — sites which can be either empty or occupied by a fermion. With the standard correspondence between the Fock space of  $m$  LFMs and the Hilbert space of  $m$  qubits, simulation of one fermionic gate takes  $O(m)$  qubit gates and vice versa. We show that using different encodings, the simulation cost can be reduced to  $O(\log m)$  and a constant, respectively. Nearest-neighbors fermionic gates on a graph of bounded degree can be simulated at a constant cost. A universal set of fermionic gates is found. We also study computation with Majorana fermions which are basically halves of LFMs. Some connection to qubit quantum codes is made.

## Introduction

The notion of *locality* plays the key role in the definition of computation process. The same basic principles apply to classical computers and the circuit model of quantum computation [1, 2]:

1. The computer consists of small pieces, or cells (bits, qubits, qutrits or something else).
2. It is allowed to operate on few cells at a time.
3. All cells are identical, so each operation has a model which can be applied to different sets of cells. We call such a model a *gate* (like the CNOT gate) while the operation itself is called a *gate application* (like CNOT applied to qubits 5 and 8).

---

\*On leave from L. D. Landau Institute for Theoretical Physics

In fact, the main difference between classical computation and quantum computation is the concrete interpretation of these postulates. The standard quantum interpretation is as follows.

- 1i. Each cell is described by a Hilbert space of small dimensionality. (Without loss of generality, these spaces are two-dimensional, in which case the cells are called qubits). The Hilbert space of the entire computer is the tensor product of the spaces associated to the individual cells.
- 2i. Each operation is described by a unitary operator which is the tensor product of some operator  $U$ , acting on the selected qubits, and the identity operator acting on the rest of the system.
- 3i. A  $p$ -qubit gate can be defined as  $U$  acting on some standard  $2^p$ -dimensional space (which is the same as a standard set of  $p$  qubits).

This interpretation might be perfect from the complexity-theoretic point of view, but it does not necessarily correspond to physics. At the fundamental level, Fermi systems do not satisfy the condition (2i). Hence using fermions as carriers of quantum information [3] should be considered as a different computation model, although it is equivalent to the standard one in a certain sense. At the macroscopic level, collective quantum degrees of freedom (or excitations, such as anyons [4, 5]) do not even satisfy the condition (1i). In all such cases, it makes sense to abstract the nontrivial locality properties from physical details. This will lead us to a definition of “fermionic gates”, “anyonic gates” and other quantum computation models which deserve careful study.

What can one expect from alternative models of quantum computation? It is very unlikely that any physical system would provide more computational power than the standard quantum computation model has. (This might be wrong for quantum gravity but here we can only guess). So, the alternative models should be polynomially equivalent to the standard one. There are indeed several results which support this statement. Firstly, D. Abrams and S. Lloyd [6] have shown that a system of  $m$  local fermionic modes (i.e. sites which can be empty or occupied) can be simulated on a quantum computer in such a way that one fermionic gate takes  $O(m)$  qubit operations. In some cases (one of the assumptions is that the number of particles is conserved) faster simulation is possible. We will extend this result by showing that in the general case (when the number of fermions is conserved only modulo 2) each fermionic gate can be simulated by  $O(\log m)$  qubit gates. Secondly, TQFT computation (which is more general than quantum computation with anyons) can be simulated in polynomial time on an ordinary quantum computer [7].

Thus alternative quantum computation models do not generate new computational classes. Rather, they provide new descriptions of the standard class BQP (the class of problems that are solvable on a quantum computer in polynomial time). These descriptions may be useful to find new quantum algorithms, error-correcting codes, fault-tolerant procedures, or to prove that BQP is contained in some other computational classes. They may also open the door to new physical implementations of a quantum computer.

## 1 A more general notion of locality

Why isn't the standard interpretation of locality good in all cases? The answer is in the way we describe quantum evolution. The Hilbert space and state vectors are very convenient tools

but they are not directly related to physically observable things. Operators are much more “real” as they allow one to describe interaction between the system and the rest of the world. In fact, the causality principle is usually stated in terms of operators: “operators in spatially separated points commute”. Our definition of locality will be in the same spirit.

A quantum system can be characterized by a finite-dimensional  $C^*$ -algebra<sup>1</sup>  $\mathcal{G}$  whose elements are called “physical operators”. As a matter of fact, they *are* operators on a suitable Hilbert space. Indeed, it is a theorem that  $\mathcal{G}$  can be represented as  $\bigoplus_j \mathbf{L}(\mathcal{H}_j)$ , where  $\mathbf{L}(\mathcal{L})$  stands for the algebra of operators on the space  $\mathcal{L}$ . Hence  $\mathcal{G}$  acts on  $\mathcal{H} = \bigoplus_j \mathcal{H}_j$ . (In the case of fermions,  $\mathcal{H} = \mathcal{H}_0 \oplus \mathcal{H}_1$  is the Fock space split into the subspaces corresponding to an even and odd number of particles;  $\mathcal{G}$  is the algebra of operators which preserve the parity).

To define locality, we will assume that the system is associated with some set of sites  $M$ . The following properties are postulated:

1. For each subset of sites  $S \subseteq M$ , there is a  $C^*$ -subalgebra  $\mathcal{G}(S) \subseteq \mathcal{G}$ . Elements of  $\mathcal{G}(S)$  are called *physical operators acting on  $S$* . We require that  $\mathcal{G}(M) = \mathcal{G}$ ,  $\mathcal{G}(\emptyset) = \mathbf{C} \cdot I$  (where  $\mathbf{C}$  is the algebra of complex numbers,  $I$  is the unit element of  $\mathcal{G}$ ), and  $\mathcal{G}(S) \subseteq \mathcal{G}(S')$  if  $S \subseteq S'$ .
2. If  $S_1 \cap S_2 = \emptyset$  then any two operators  $X_1 \in \mathcal{G}(S_1)$  and  $X_2 \in \mathcal{G}(S_2)$  commute.

The concept of unitarity is well defined in this setting: an element  $U \in \mathcal{G}(M)$  is called *unitary* if  $UU^\dagger = U^\dagger U = I$  (the operation  $\dagger$  is a part of the  $C^*$ -algebra structure). Note that nonunitary elements of  $\mathcal{G}(M)$  also have physical meaning because they can be used to construct a unitary operator on a larger space  $\mathcal{H} \otimes \mathcal{L}$ , where  $\mathcal{L}$  represents some external system (e.g. a measurement device). Such an operator generally has the form  $U = \sum_k A_k \otimes B_k$  ( $A_k \in \mathcal{G}(M)$ ), i.e.  $U \in \mathcal{G}(M) \otimes \mathbf{L}(\mathcal{L})$ .

Thus we have given a more general interpretation of the locality postulates 1 and 2 which were discussed in the introduction. (We put aside the postulate 3 here).

## 2 Local fermionic modes

Consider  $m$  sites (numbered 0 through  $m-1$ ) each of which can be either empty or occupied by a spinless fermionic particle. Such sites will be called *local fermionic modes (LFMs)*. The Hilbert space  $\mathcal{H}$  of this system, known as *Fock space*, is spanned by  $2^m$  basis vectors  $|n_0, \dots, n_{m-1}\rangle$ , where  $n_j = 0, 1$  is the occupation number of the  $j$ -th site. Everything related to fermions can be expressed in terms of annihilation and creation operators  $a_j, a_j^\dagger$ , ( $j = 0, \dots, m-1$ ). The operator  $a_j$  acts on basis vectors as follows:

$$\begin{aligned} a_j |n_0, \dots, n_{j-1}, 1, n_{j+1}, \dots, n_{m-1}\rangle &= (-1)^{\sum_{s=0}^{j-1} n_s} |n_0, \dots, n_{j-1}, 0, n_{j+1}, \dots, n_{m-1}\rangle, \\ a_j |n_0, \dots, n_{j-1}, 0, n_{j+1}, \dots, n_{m-1}\rangle &= 0; \end{aligned} \quad (1)$$

$a_j^\dagger$  is the Hermitian conjugate. Note that the definition depends on the order of LFMs! (One may rather say that the basis depends on the order while  $a_j, a_j^\dagger$  do not, since all relations

---

<sup>1</sup> $C^*$ -algebra is a generalization of the algebra of linear operators on a Hilbert space. The properties of operator addition, multiplication, Hermitian conjugation and the operator norm are axiomatized in a certain way. However, instead of using the axioms, we will rely on a characterization of finite-dimensional  $C^*$ -algebras given below.

between them are permutation-invariant). The annihilation and creation operators generate the algebra  $\bar{\mathcal{F}} = \mathbf{L}(\mathcal{H})$  and have the following commutation rules:

$$\begin{aligned} a_j a_k + a_k a_j &= 0, \\ a_j^\dagger a_k^\dagger + a_k^\dagger a_j^\dagger &= 0, \\ a_j a_k^\dagger + a_k^\dagger a_j &= \delta_{jk}. \end{aligned} \tag{2}$$

The Hilbert space of  $m$  LFMs splits into two parts:  $\mathcal{H} = \mathcal{H}_0 \oplus \mathcal{H}_1$ , where “0” and “1” refers to the total fermionic parity  $n = \sum_{j=0}^{m-1} n_j \pmod{2}$ . *Physical operators* are those which preserve the parity. Note that the Hamiltonian of a real Fermi system always satisfies this condition,<sup>2</sup> unlike the operators  $a_j, a_j^\dagger$  alone. The *algebra of physical operators*  $\mathcal{F} = \mathbf{L}(\mathcal{H}_0) \oplus \mathbf{L}(\mathcal{H}_1)$  is spanned by products of even number of  $a_j, a_j^\dagger$ . (The notation  $\mathcal{G}$  in the previous section referred to the general case whereas  $\mathcal{F}$  is reserved for LFMs).

Let  $S \subseteq \{0, \dots, m-1\}$  be a set of LFMs. *Physical operators on  $S$*  are linear combinations of even products of  $a_j, a_j^\dagger$ ,  $j \in S$ . The algebra of such operators is  $\mathcal{F}(S) = \bar{\mathcal{F}}(S) \cap \mathcal{F}$ , where  $\bar{\mathcal{F}}(S) \subseteq \bar{\mathcal{F}}$  is generated by  $a_j, a_j^\dagger$ ,  $j \in S$ . The conditions (1) and (2) from Sec. 1 are obviously satisfied. Moreover,  $\mathcal{F}(S_1)$  commutes with  $\bar{\mathcal{F}}(S_2)$  if  $S_1 \cap S_2 = \emptyset$ .

The occupation number  $n_j$  is an eigenvalue of the operator  $\hat{n}_j = a_j^\dagger a_j \in \mathcal{F}(\{j\})$ , which means it can be measured locally (by acting on the  $j$ -th LFM and some external device). The occupation number can not be changed locally, though.

Here are some examples of unitary operators acting on one or two LFMs:  $\exp(i\beta a_j^\dagger a_j)$  (action by an external potential),  $\exp(i\beta a_j^\dagger a_j a_k^\dagger a_k)$  (two-particle’s interaction),  $\exp(i(\gamma a_j^\dagger a_k + \gamma^* a_k^\dagger a_j))$  (tunneling) and  $\exp(i(\gamma a_k a_j + \gamma^* a_j^\dagger a_k^\dagger))$  (interaction with a superconductor). We will show that these operators (for all or for some particular values of  $\beta \in \mathbf{R}$  and  $\gamma \in \mathbf{C}$ ) form a universal set, i.e. any unitary operator can be represented as a composition of these ones to any given precision, using ancillas.

In our computation model we allow to use ancillas in the state  $|0\rangle$ . (To be more accurate, we should say that the input state is padded by some number of zeros to the right. Actually, the order does not matter in this case). If we speak about implementing a unitary operator, the ancillas must return to the state  $|0\rangle$  by the end of the procedure. As is usual, this restriction does not apply to computing a Boolean function which proceeds as follows. One starts from a basis vector  $|n_0, \dots, n_{m-1}\rangle$  representing the input data, adds some ancillas, applies some sequence of local unitary operators and reads the result by measuring some of the occupation numbers.

### 3 Relation between LFMs and qubits

The Hilbert space of  $m$  LFMs can be identified with the Hilbert space of  $m$  qubits  $\mathcal{B}^{\otimes m}$  (where  $\mathcal{B}$  stands for the two-dimensional space  $\mathbf{C}^2$  endowed with the standard basis  $\{|0\rangle, |1\rangle\}$ ):

$$|n_0, n_1, \dots, n_{m-1}\rangle \equiv |n_0\rangle \otimes |n_1\rangle \otimes \dots \otimes |n_{m-1}\rangle, \quad n_j = 0, 1. \tag{3}$$

---

<sup>2</sup>In electron systems, the Hamiltonian also preserves the electric charge, so terms with different numbers of  $a_j$  and  $a_j^\dagger$  are usually forbidden. Our model is mostly relevant to superconductors where the total charge of *excitations* is not conserved, so terms like  $a_j a_k$  appear in the effective Hamiltonian.

Measurement of  $n_j$  is the same as eigenvalue measurement of  $\sigma_j^z$ . A physical fermionic operator corresponds to a qubit operator which preserves the parity, i.e. commutes with  $\prod_{j=0}^{m-1} \sigma_j^z$ . However, “applying a gate to a set of LFMs” is very different from “applying a gate to a set of qubits”.

Let  $X$  be a parity-preserving  $p$ -qubit operator acting on qubits numbered 0 through  $p-1$ . Applying it to the qubits  $j_0, \dots, j_{p-1}$  is a straightforward procedure. The Hilbert space of  $m$  qubits  $\mathcal{B}^{\otimes m}$  can be identified with  $\mathcal{B}^{\otimes p} \otimes \mathcal{B}^{\otimes (m-p)}$  by the qubit permutation  $P : |n_0, \dots, n_{m-1}\rangle \mapsto |n_{j_0}, \dots, n_{j_{p-1}}\rangle \otimes |\text{the other } n_j\rangle$ . Then the action of  $X$  is defined as follows:

$$X[j_0, \dots, j_{p-1}] = P^{-1}(X \otimes I_{\mathcal{B}^{\otimes (m-p)}})P.$$

If we want to apply  $X$  to the LFMs  $j_0, \dots, j_{p-1}$ , the procedure is different. First, we should expand  $X$  into products of  $a_0, \dots, a_{p-1}, a_0^\dagger, \dots, a_{p-1}^\dagger$ . Then we replace each  $a_r$  by  $a_{j_r}$  and each  $a_r^\dagger$  by  $a_{j_r}^\dagger$ . The resulting operator will be denoted by  $X\{j_0, \dots, j_{p-1}\}$ . For example, if  $X = |1, 0\rangle\langle 0, 1| = a_0^\dagger a_1$  then  $X\{j, k\} = a_j^\dagger a_k$ . This operator acts as follows:

$$\begin{aligned} a_j^\dagger a_k |\dots, 0, n_{j+1}, \dots, n_{k-1}, 0, \dots\rangle &= 0, \\ a_j^\dagger a_k |\dots, 0, n_{j+1}, \dots, n_{k-1}, 1, \dots\rangle &= (-1)^{\sum_{s=j+1}^{k-1} n_s} |\dots, 1, n_{j+1}, \dots, n_{k-1}, 0, \dots\rangle, \\ a_j^\dagger a_k |\dots, 1, n_{j+1}, \dots, n_{k-1}, 0, \dots\rangle &= 0, \\ a_j^\dagger a_k |\dots, 1, n_{j+1}, \dots, n_{k-1}, 1, \dots\rangle &= 0. \end{aligned}$$

Not only  $X\{j, k\} \neq X[j, k]$  but also  $X\{j, k\}$  is non-local in terms of qubits: it involves all the qubits with numbers from  $j$  to  $k$ .

A unitary *qubit gate* (*LFM, or fermionic gate*) is a unitary operator  $U$  meant to be applied to a number of qubits (LFMs); a  $p$ -qubit or a  $p$ -LFM gate acts on the standard Hilbert space  $\mathcal{B}^{\otimes p}$ . Operators of the form  $U[j, k]$  or  $U\{j, k\}$  are called *gate applications*. We will usually consider unitary gates up to overall phase factors. A set of gates is also called a *basis*. A *circuit of size  $s$  in a basis  $\mathcal{A}$*  is a composition of  $s$  applications of gates from  $\mathcal{A}$ , i.e. an expression of the form  $U_s\{j_{s,0}, \dots, j_{s,p_s-1}\} \cdots U_1\{j_{1,0}, \dots, j_{1,p_1-1}\}$ , where  $U_k \in \mathcal{A}$ . Such an expression is evaluated by a unitary operator which is said to be *represented* by the circuit.

Note that  $X\{j\} = X[j]$ , so one-LFM gates are simply parity-preserving one-qubit gates. Up to an overall phase, such gates have the form  $\Lambda(e^{i\phi})$ , where  $\Lambda(U)$  denotes the controlled  $U$ . (If  $U$  acts on  $p$  qubits then  $\Lambda(U)$  acts on  $p+1$  qubits; in our case  $p=0$ ).

More generally,  $X\{j, j+1, \dots, j+p-1\} = X[j, j+1, \dots, j+p-1]$ . This allows one to represent fermionic gates in terms of qubit gates and vice versa. We will now show how to do that in the case  $p=2$ .

Suppose we want to execute a two-LFM operator  $X\{j, k\}$  (w.l.o.g.  $j < k$ ). First, we move the  $k$ -th qubit next to the  $j$ -th one by swapping it with its nearest neighbors. Then we apply  $X\{j, j+1\} = X[j, j+1]$  and move the  $k$ -th qubit back to its original position. However, what we actually need here is to interchange LFMs, not qubits. This is different even if the LFMs (qubits) are next to each other!

A swap between two qubits (with numbers 0 and 1) is defined in the obvious way:  $(\leftrightarrow) : |n_0, n_1\rangle \mapsto |n_1, n_0\rangle$ . A swap between two LFMs is a unitary operator  $(\Leftrightarrow)$  such that

$$(\Leftrightarrow) a_0 (\Leftrightarrow)^\dagger = a_1, \quad (\Leftrightarrow) a_1 (\Leftrightarrow)^\dagger = a_0. \quad (4)$$

These equations have a unique solution (up to an overall phase factor):

$$(\Leftrightarrow) = I - a_0^\dagger a_0 - a_1^\dagger a_1 + a_1^\dagger a_0 + a_0^\dagger a_1 = \exp\left(i\frac{\pi}{2}(a_0^\dagger - a_1^\dagger)(a_0 - a_1)\right) : \begin{cases} |0, 0\rangle \mapsto |0, 0\rangle \\ |0, 1\rangle \mapsto |1, 0\rangle \\ |1, 0\rangle \mapsto |0, 1\rangle \\ |1, 1\rangle \mapsto -|1, 1\rangle. \end{cases} \quad (5)$$

This differs from the qubit swap by the “-” sign. So,

$$(\Leftrightarrow) = (\leftrightarrow) D, \quad (6)$$

where  $D = \Lambda(\sigma^z) : |a, b\rangle \mapsto (-1)^{ab}|a, b\rangle$  is a “swap defect” operator.

To perform the procedure described above, we do not have to actually interchange LFMs or qubits. Instead, we can simply apply operators  $D\{l, r\} = D[l, r]$  to all pairs of qubits that otherwise would be interchanged. So, any two-LFM operator  $X\{j, k\}$  ( $j < k$ ) can be represented by a qubit circuit as follows:

$$X\{j, k\} = D[k-1, k] \cdots D[j+1, k] X\{j, k\} D[j+1, k] \cdots D[k-1, k]. \quad (7)$$

Conversely, any parity-preserving two-qubit operator is represented by a fermionic circuit:

$$X\{j, k\} = D\{k-1, k\} \cdots D\{j+1, k\} X\{j, k\} D\{j+1, k\} \cdots D\{k-1, k\}. \quad (8)$$

This method also works for operators which act on more than two LFMs (qubits).

## 4 A universal set of LFM gates.

We have shown that fermionic gates are equivalent to parity-preserving qubit gates modulo the swap defect operator  $D$ . So, to obtain a universal set of fermionic gates, we only need to find a universal set of parity-preserving qubit gates. It will be possible to represent the operator  $D$  by these gates too, exactly or approximately. (If only approximate representation is possible, one may have to pay extra cost when simulating a single fermionic gate because the more qubit gates are used, the more accurate they should be. We will avoid this problem, though).

We claim that the following gates are sufficient to represent any parity-preserving operator to any given precision (using ancillas):

$$\Lambda(e^{i\pi/4}), \quad \Lambda(\sigma^z), \quad \widetilde{H} : |a, b\rangle \mapsto \frac{1}{\sqrt{2}} \sum_c (-1)^{bc} |a+b+c, c\rangle. \quad (9)$$

(Here  $a, b, c \in \mathbf{F}_2 = \{0, 1\}$ , so the expression  $a + b + c$  is considered modulo 2). Note that  $D = \Lambda(\sigma^z)$  belongs to this set of gates.

Any parity-preserving operator  $U$  can be considered as a pair of operators  $(U_0, U_1)$ , where  $U_0$  acts on the even sector  $\mathcal{H}_0$  whereas  $U_1$  acts on the odd sector  $\mathcal{H}_1$ . We will first show how to get a given  $U_0$  while not caring about  $U_1$  — we will actually get  $U_1 = U_0$ . (The comparison between  $U_0$  and  $U_1$  is made through identifying  $\mathcal{H}_0$  and  $\mathcal{H}_1$  by the map  $\sigma^x[0]$ ). Then we will implement operators of the form  $(I, Y)$  which can be used to correct the first step.

Any operator  $X$  on  $m - 1$  qubits can be transformed to a parity-preserving operator  $\widetilde{X}$  on  $m$  qubits by using the extra qubit to maintain the parity:

$$\widetilde{X} = V^{-1} (I_B \otimes X) V, \quad V : |n_0, n_1, \dots, n_{m-1}\rangle \mapsto |n_0 + \dots + n_{m-1}, n_1, \dots, n_{m-1}\rangle. \quad (10)$$

Note that the gate  $\widetilde{H}$  (see eq. (9)) corresponds to the Hadamard gate  $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ . If  $\widetilde{X}$  already preserves the parity, as it is the case with the operators  $\Lambda(e^{i\pi/4})$  and  $\Lambda(\sigma^z)$ , then  $\widetilde{X} = I_{\mathcal{B}} \otimes X$ . (This equality is actually a characteristic property of parity-preserving operators).

The operator  $V$  is unitary. It maps the even sector  $\mathcal{H}_0$  onto the subspace  $\mathcal{L}_0$  which consists of vectors  $|0\rangle \otimes |\xi\rangle$  ( $|\xi\rangle \in \mathcal{B}^{\otimes(m-1)}$ ). Any operator on this subspace extends to an operator of the form  $I_{\mathcal{B}} \otimes X$ . Hence any  $U_0 \in \mathbf{L}(\mathcal{H}_0)$  extends to an operator of the form  $\widetilde{X}$ . Note that  $V$  and  $I_{\mathcal{B}} \otimes X$  commute with  $\sigma^x[0]$ , so  $\widetilde{X}$  also commutes with  $\sigma^x[0]$ . Therefore  $\widetilde{X} = (U_0, U_1)$ , where  $U_1 = \sigma^x[0] U_0 \sigma^x[0]$ , or simply  $U_1 = U_0$  if the identification between  $\mathcal{H}_0$  and  $\mathcal{H}_1$  is used.

If an operator  $X$  is represented by a quantum circuit  $A_L \cdots A_1$ , one can replace each gate application  $A_k$  by  $\widetilde{A}_k$  to get a quantum circuit for  $\widetilde{X}$ . Indeed, eq. (10) defines a  $*$ -algebra homomorphism, i.e.

$$X_1 \widetilde{X}_2 = \widetilde{X}_1 + \widetilde{X}_2, \quad c\widetilde{X} = \widetilde{cX}, \quad X_1 \widetilde{X}_2 = \widetilde{X}_1 \widetilde{X}_2, \quad \widetilde{X}^\dagger = \widetilde{X}^\dagger, \quad \widetilde{I} = I.$$

It follows that any universal gate set  $\mathcal{A}$  transforms to a set of parity-preserving gates  $\widetilde{\mathcal{A}}$  which are universal on the even sector. The following gate set is known to be universal [8]:  $\mathcal{A} = \{\Lambda(e^{i\pi/4}), \Lambda(\sigma^z), H\}$ . The corresponding gate set  $\widetilde{\mathcal{A}}$  is given by eq. (9). (The parity-preserving gates  $\Lambda(e^{i\pi/4})$  and  $\Lambda(\sigma^z)$  are copied from  $\mathcal{A}$  to  $\widetilde{\mathcal{A}}$  unchanged). Thus the basis (9) allows one to obtain at least unitary gates of the form  $(U_0, U_0)$ .

With parity-preserving operators, we can still use one of the standard techniques in quantum circuit design — gates with quantum control. Indeed, if  $U$  preserves the parity then  $\Lambda(U)$  also does. More generally,  $\Lambda(\widetilde{X}) = \Lambda(X)$  (up to a permutation of the control qubit and the parity qubit). So, if we can represent  $\Lambda(X)$  by a circuit,<sup>3</sup> we can also obtain a circuit for  $\Lambda(\widetilde{X})$  by the procedure described above. For example, the operator  $\Lambda(\sigma^x)[1, 2]$  can be represented as  $H[2] \Lambda(\sigma^z)[1, 2] H[2]$ , hence

$$\Lambda(\widetilde{\sigma^x})[1, 0, 2] = \widetilde{H}[0, 2] \Lambda(\sigma^z)[1, 2] \widetilde{H}[0, 2].$$

Here we use qubit 0 to maintain the parity whereas 1 is the control qubit. (The notation  $\Lambda(\widetilde{X})[\dots]$  suggests that the control qubit goes first).

Now we are in a position to implement operators of the form  $(I, Y)$  using the gates (9). We will also use one ancilla which will be assigned the number  $m$ . First, we execute the operator

$$\begin{aligned} W &: |n_0, n_1, \dots, n_{m-1}, n_m\rangle \mapsto |n_0 + \dots + n_{m-1}, n_1, \dots, n_{m-1}, n_1 + \dots + n_m\rangle, \\ W &= \Lambda(\widetilde{\sigma^x})[m-1, 0, m] \cdots \Lambda(\widetilde{\sigma^x})[1, 0, m], \end{aligned} \tag{11}$$

where  $\Lambda(\widetilde{\sigma^x}) : |a, b, c\rangle \mapsto |a, b+a, c+a\rangle$ . Now qubit 0 indicates the total parity.

Let  $\widetilde{X} = (Y, Y)$ . Since  $\widetilde{X}$  can be represented according to (10), and because

$$W = V^{-1}[m, 1, \dots, m-1] V, \quad \text{where } V = V[0, \dots, m-1],$$

---

<sup>3</sup>Implementing  $\Lambda(X)$  in the basis  $\mathcal{A}$  is only slightly harder than implementing  $X$ . Indeed, for each gate  $X$  from the basis  $\mathcal{A}$ , the operator  $\Lambda(X)$  can be represented by a circuit in the same basis *exactly*. Therefore, the circuit for  $\Lambda(X)$  will be larger than the circuit for  $X$  only by a constant factor. Note, however, that  $X$  may have been implemented up to a phase factor; this phase factor becomes important when we consider  $\Lambda(X)$ . The necessary correction can be achieved by an operator  $\Lambda(e^{i\phi})$  which should be implemented separately.

we conclude that

$$W^{-1} \Lambda(\widetilde{X})[0, m, 1, \dots, m-1] W = V^{-1} \Lambda(X)[0, 1, \dots, m-1] V = U \otimes I_{\mathcal{B}}, \quad U = (I, Y). \quad (12)$$

Note that in this case, the ancilla is not affected no matter what its initial state was; one can even use a data qubit as the ancilla.

We have proved that the gate set (9) is universal in the class of parity-preserving operators. It remains to represent these gates in terms of creation and annihilation operators. The first two are simple:

$$\Lambda(e^{i\pi/4}) = \exp\left(i\frac{\pi}{4}a_0^\dagger a_0\right), \quad \Lambda(\sigma^z) = \exp(i\pi a_0^\dagger a_0 a_1^\dagger a_1). \quad (13)$$

Unfortunately, the gate  $\widetilde{H}$  in the fermionic representation looks ugly, so we first represent it as follows:

$$\widetilde{H}[0, 1] = \Lambda(-i)[1] \widetilde{G}[0, 1] \Lambda(-i)[1], \quad G = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

So, the fermionic gates (13), together with

$$\widetilde{G} = \exp\left(-i\frac{\pi}{4}(a_0 - a_0^\dagger)(a_1 + a_1^\dagger)\right) = \exp\left(i\frac{\pi}{4}(a_0^\dagger a_1 + a_1^\dagger a_0)\right) \exp\left(i\frac{\pi}{4}(a_1 a_0 + a_0^\dagger a_1^\dagger)\right), \quad (14)$$

form a universal set. Obviously, this gate set is also universal:

$$\left\{ \begin{array}{l} \exp\left(i\frac{\pi}{4}a_0^\dagger a_0\right), \\ \exp\left(i\frac{\pi}{4}(a_0^\dagger a_1 + a_1^\dagger a_0)\right), \\ \exp\left(i\frac{\pi}{4}(a_1 a_0 + a_0^\dagger a_1^\dagger)\right), \\ \exp(i\pi a_0^\dagger a_0 a_1^\dagger a_1) \end{array} \right\}. \quad (15)$$

## 5 Fast simulation procedures

So far we have been using the standard identification (3) between the Fock space  $\mathcal{H}$  and the Hilbert space of  $m$  qubits  $\mathcal{B}^{\otimes m}$ . This identification has allowed us to consider qubit gate applications  $X[j, k] \in \mathbf{L}(\mathcal{B}^{\otimes m})$  and LFM gate applications  $X\{j, k\} \in \mathcal{F} \subseteq \mathbf{L}(\mathcal{H})$  as operators acting on the same space. Now we are going to discuss a more general way of simulating LFMs by qubits (or vice versa). Let  $J$  be an *encoding* of  $m$  LFMs by  $m'$  qubits, i.e.  $J : \mathcal{H} \rightarrow \mathcal{B}^{\otimes m'}$  is a unitary embedding. ( $J$  being a unitary embedding means that  $J^\dagger J = I_{\mathcal{H}}$ . Note that  $JJ^\dagger$  is the projector onto  $\mathcal{L} = \text{Im } J \subseteq \mathcal{B}^{\otimes m'}$ .) We say that an operator  $U' \in \mathbf{L}(\mathcal{B}^{\otimes m'})$  *represents* an operator  $U \in \mathbf{L}(\mathcal{H})$  if

$$\begin{array}{ccc} \mathcal{H} & \xleftarrow{U} & \mathcal{H} \\ \downarrow J & & \downarrow J \\ \mathcal{B}^{\otimes m'} & \xleftarrow{U'} & \mathcal{B}^{\otimes m'} \end{array} \text{ commutes,} \quad \text{i.e. } JU = U'J. \quad (16)$$

The operator  $U$ , as well as the LFMs or qubits equivalent to them, are called *logical*. The  $m'$  qubits the operator  $U'$  acts on are called *code qubits*.

In this section we will show that each LFM gate can be simulated by  $O(\log m)$  qubit gates. Surprisingly, this does not require quantum codes in the proper sense, i.e.  $J : \mathcal{H} \rightarrow \mathcal{B}^{\otimes m}$  is a

map onto. Moreover,  $J$  takes basis vectors to basis vectors. We will also show how to simulate qubit gates by LFM gates at a constant cost using a subspace of the Foch space.

Gate action on a set of qubits (LFMs) can be described as follows. First, we *extract* two (or some other number) qubits or LFMs from the *quantum memory* which is now considered as a “black box”. We place these qubits at positions  $-2$  and  $-1$ . Then we apply the gate and put the qubits (LFMs) back into the memory. In this description, it does not matter what gate we apply, a qubit one or a fermionic one (because  $X\{-2, -1\} = X[-2, -1]$ ). Once extracted, LFMs can be regarded as qubits — the difference is in the way we extract them. With qubits, we apply the operator

$$[\leftarrow j] : \mathcal{B}^{\otimes m} \rightarrow \mathcal{B} \otimes \mathcal{B}^{\otimes m} : |n_0\rangle \otimes \cdots \otimes |n_j\rangle \otimes \cdots \otimes |n_{m-1}\rangle \mapsto |n_j\rangle \otimes |n_0\rangle \otimes \cdots \otimes |0\rangle \otimes \cdots \otimes |n_{m-1}\rangle.$$

This is a unitary embedding into a larger Hilbert space; it can be represented as adding an ancilla in the state  $|0\rangle$  followed by a unitary operator. With fermions, we move the  $j$ -th LFM through all the LFMs left to it, so we should take swap defects into account. Thus we get another unitary embedding:

$$\begin{aligned} \{\leftarrow j\} &: \mathcal{H} \rightarrow \mathcal{B} \otimes \mathcal{H}, \\ \{\leftarrow j\} |n_0, \dots, n_j, \dots, n_{m-1}\rangle &= (-1)^{n_j \sum_{s=0}^{j-1} n_s} |n_j\rangle \otimes |n_0, \dots, 0, \dots, n_{m-1}\rangle. \end{aligned} \tag{17}$$

It is easy to verify that our recipe is correct, i.e. applying the operator  $X[-2, -1]$  after extracting two LFMs is equivalent to applying  $X\{j, k\}$  before the extraction:

$$X[-2, -1] \left( I_{\mathcal{B}} \otimes \{\leftarrow k\} \right) \{\leftarrow j\} = \left( I_{\mathcal{B}} \otimes \{\leftarrow k\} \right) \{\leftarrow j\} X\{j, k\}. \tag{18}$$

(Our notations are somewhat confusing so this comment could be helpful. When we extract the  $j$ -th LFM by applying  $\{\leftarrow j\}$ , we add one qubit at position  $-1$ . When we then extract the  $k$ -th LFM, this qubit moves to position  $-2$  while another one is being inserted; this can be described by the operator  $I_{\mathcal{B}} \otimes \{\leftarrow k\}$ .)

Suppose we want to simulate LFMs by qubits at low cost. The problem with the standard encoding (3) is that multiplication by the factor  $(-1)^{n_j \sum_{s=0}^{j-1} n_s}$  requires too many operations. The simplest solution would be to store  $y_j = \sum_{s=0}^{j-1} n_s$  instead of  $n_j$ . (Remember that we consider  $n_s$  as residues (mod 2), so the sum is also taken (mod 2)). This does solve the problem but also creates a new one: when  $n_j$  becomes 0 as a result of extraction, we have to modify all  $y_k$ ,  $k > j$ . So, we need to balance the complexity of computing  $\sum_{s=0}^{j-1} n_s$  and that of updating the encoded quantum memory when  $n_j$  changes. This kind of trade-off can be achieved by storing some partial sums  $\sum_{s=a}^b n_s$ .

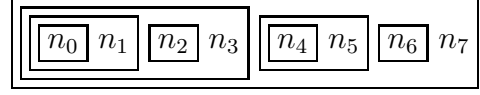
In general, we will use encodings of the form

$$\begin{aligned} J : \mathcal{H} \rightarrow \mathcal{B}^{\otimes m} &: |n_0, \dots, n_{m-1}\rangle \mapsto |x_0\rangle \otimes \cdots \otimes |x_{m-1}\rangle, \\ x_j &= \sum_{s \in S(j)} n_s, \quad S(j) \subseteq \{0, \dots, m-1\}. \end{aligned}$$

We start with an example of such an encoding for  $m = 8$  (the diagram next to the equation

illustrates grouping of  $n_s$  into  $x_j$ ):

$$\begin{aligned}
x_0 &= n_0 & x_2 &= n_2 & x_4 &= n_4 & x_6 &= n_6 \\
x_1 &= n_0 + n_1 & & & x_5 &= n_4 + n_5 & & \\
x_3 &= n_0 + n_1 + n_2 + n_3 & & & & & & \\
x_7 &= n_0 + n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 & & & & & & 
\end{aligned}$$



A binary tree structure is apparent here. To proceed, we will represent the qubit indices  $0, \dots, m-1$  by binary strings. The length of these strings is not fixed; we may add an arbitrary number of zeros to the beginning of a string, e.g.  $3 = 11 = 011 = 0011$ .

Let us define a partial order  $\preceq$  on the set of binary strings. We write  $\overline{\alpha_{t-1} \dots \alpha_0} \preceq \overline{\beta_{t-1} \dots \beta_0}$  if  $\alpha_l = \beta_l$  for  $l \geq l_0$  while  $\beta_{l_0-1} = \dots = \beta_0 = 1$  (for some  $l_0$ ). For example,

$$\left. \begin{array}{l} \overline{000} \prec \overline{001} \\ \overline{010} \end{array} \right\} \prec \overline{011} \\
\left. \begin{array}{l} \overline{100} \prec \overline{101} \\ \overline{110} \end{array} \right\} \prec \overline{111},$$

where  $j \prec k$  means that  $j \preceq k$  but  $j \neq k$ . Note that if  $j \prec k$  then  $j < k$ .

Now we can specify our encoding for arbitrary  $m$ :

$$|n_0, \dots, n_{m-1}\rangle \mapsto |x_0\rangle \otimes \dots \otimes |x_{m-1}\rangle, \quad x_j = \sum_{s \preceq j} n_s. \quad (19)$$

It is important that each  $n_s$  enters only  $O(\log m)$  of  $x_j$ . Hence applying  $\sigma^x[s]$  to one logical qubit amounts to logarithmically many  $\sigma^x$  gates being applied to the code qubits.

The inverse transformation (from  $x_j$  to  $n_s$ ) is also simple:

$$\begin{aligned}
n_j &= x_j - \sum_{s \in K(j)} x_s, \\
\overline{\alpha_{t-1} \dots \alpha_0} &\in K(\overline{\beta_{t-1} \dots \beta_0}) \quad \text{if and only if} \\
\beta_{l_0} &= \dots = \beta_0 = 1, \quad \alpha_l = \beta_l \text{ for } l \neq l_0, \quad \alpha_{l_0} = 0 \quad (\text{for some } l_0).
\end{aligned} \quad (20)$$

The sum in (20) contains only  $O(\log m)$  terms. Moreover,  $y_j = \sum_{s=0}^{j-1} n_s$  can be also expressed as a sum of  $O(\log m)$  numbers  $x_s$ :

$$\begin{aligned}
y_j &= \sum_{s \in L(j)} x_s, \\
\overline{\alpha_{t-1} \dots \alpha_0} &\in L(\overline{\beta_{t-1} \dots \beta_0}) \quad \text{if and only if} \\
\beta_{l_0} &= 1, \quad \alpha_l = \beta_l \text{ for } l > l_0, \quad \alpha_{l_0} = 0, \quad \alpha_{l_0-1} = \dots = \alpha_0 = 1 \quad (\text{for some } l_0).
\end{aligned} \quad (21)$$

It remains to actually represent the LFM extraction operator  $\{\leftarrow j\}$  by acting on the code qubits. Since  $\{\leftarrow j\}$  increases the number of qubits by 1, we should add this extra qubit first. We place it at position  $-1$  and initialize by  $|0\rangle$ . Then we make its value equal to  $n_j$  by applying

the operators  $\Lambda(\sigma^x)[s, -1]$ ,  $s \in K(j) \cup \{j\}$  (see eq. (20)). After that,  $n_j$  can be turned into 0 by executing the operators  $\Lambda(\sigma^x)[-1, k]$ ,  $k \succeq j$  (see eq. (19)). Finally, we multiply by  $(-1)^{n_j y_j}$  by applying  $\Lambda(\sigma^z)[-1, s]$ ,  $s \in L(j)$  (see eq. (21)). To summarize, we execute the operator

$$U' = \prod_{s \in L(j)} \Lambda(\sigma^z)[-1, s] \prod_{k \succeq j} \Lambda(\sigma^x)[-1, k] \prod_{s \in K(j) \cup \{j\}} \Lambda(\sigma^x)[s, -1] \quad (22)$$

which has the property  $(I_B \otimes J) \{ \leftarrow j \} |\xi\rangle = U'(|0\rangle \otimes J|\xi\rangle)$  for any  $|\xi\rangle \in \mathcal{H}$ . This requires  $O(\log m)$  operations.

Simulating qubits by LFMs is easier and faster. One can use this simple encoding:

$$|n_0\rangle \otimes |n_1\rangle \otimes \cdots \otimes |n_{m-1}\rangle \mapsto |n_0, n_0, n_1, n_1, \dots, n_{m-1}, n_{m-1}\rangle, \quad (23)$$

i.e. each qubit is represented by a pair of LFMs with an even number of fermions,  $|0\rangle \mapsto |00\rangle$ ,  $|1\rangle \mapsto |11\rangle$ . Each two-qubit operator  $X$  is represented by a four-qubit operator  $X'$ . The operators  $X'[2j, 2j+1, 2k, 2k+1]$  and  $X'\{2j, 2j+1, 2k, 2k+1\}$  act the same way on the code subspace. So, when we use the encoding (23), it does not matter whether the code elements are qubits or LFMs. The simulation cost is just a constant.

## 6 Majorana fermions

It is possible, at least mathematically, to split each local fermionic mode into two objects. These halves of LFMs are called Majorana fermions.<sup>4</sup>

Let us introduce a set of Hermitian operators  $c_j$  ( $j = 0, \dots, 2m-1$ ):

$$c_{2k} = a_k + a_k^\dagger = \sigma^x[k] \prod_{j=0}^{k-1} \sigma^z[j], \quad c_{2k+1} = \frac{a_k - a_k^\dagger}{i} = \sigma^y[k] \prod_{j=0}^{k-1} \sigma^z[j]. \quad (24)$$

These operators satisfy the commutation relations

$$c_j c_k + c_k c_j = 2\delta_{jk}. \quad (25)$$

We can define new locality rules on the algebra  $\mathcal{F} = \mathbf{L}(\mathcal{H}_0) \oplus \mathbf{L}(\mathcal{H}_1)$  which will be now denoted by  $\mathcal{M}$ . (Also  $\bar{\mathcal{F}} = \mathbf{L}(\mathcal{H})$  will be denoted by  $\bar{\mathcal{M}}$ ). We say that there are  $2m$  sites called *Majorana fermions*. For each set of sites  $S \subseteq \{0, \dots, 2m-1\}$ , let  $\bar{\mathcal{M}}(S) \subseteq \bar{\mathcal{M}}$  be the subalgebra generated by  $c_j$ ,  $j \in S$ . (Such an algebra is known as *complex Clifford algebra*). Then  $\mathcal{M}(S) = \bar{\mathcal{M}}(S) \cap \mathcal{M}$ , i.e. *physical operators* on  $S$  are linear combinations of even products of  $c_j$ ,  $j \in S$ .

According to this definition, Majorana fermions “exist” in any Fermi system. A nontrivial thing is that it is possible (at least theoretically) to pair them up by interaction, so that few Majorana fermions remain unpaired and *separated from each other* [9]. Such systems could be used as decoherence-free quantum memory. Indeed, a single Majorana fermion can not interact with the environment by itself (because the operator  $c_j$  is not physical), so the decoherence can only arise from environment-mediated interaction of two Majorana fermions. But if they are well separated in space, such interaction should be exponentially small (a finite correlation length in the environment is assumed). Roughly speaking, we keep two halves of a qubit apart, so the qubit is decoherence-free!

<sup>4</sup> In field theory, this term usually means something more specific, but it is sometimes used in this sense too.

An application of a *Majorana gate* is defined as in the case of LFMs. Let  $X$  be a physical operator acting on  $p$  Majorana fermions numbered 0 through  $p - 1$ . Then  $X$  can be expanded into (even) products of  $c_j$ ,  $j = 0, \dots, p - 1$ . If we substitute  $c_{j_r}$  for  $c_r$ , we will get an operator  $X \{\{j_0, \dots, j_{p-1}\}\} \in \mathcal{M}(\{j_0, \dots, j_{p-1}\})$ .

To find a universal set of Majorana gates, it suffice to rewrite the operators (13), (14) in terms of  $c_0 = a_0 + a_0^\dagger$ ,  $c_1 = -i(a_0 - a_0^\dagger)$ ,  $c_2 = a_1 + a_1^\dagger$ ,  $c_3 = -i(a_1 - a_1^\dagger)$ .

$$\begin{aligned} a_0^\dagger a_0 &= \frac{1}{2}(1 + ic_0 c_1), & a_1^\dagger a_1 &= \frac{1}{2}(1 + ic_2 c_3), \\ \exp\left(i\frac{\pi}{4}a_0^\dagger a_0\right) &= e^{i\pi/8} \exp\left(-\frac{\pi}{8}c_0 c_1\right), & \exp\left(-i\frac{\pi}{4}(a_0 - a_0^\dagger)(a_1 + a_1^\dagger)\right) &= \exp\left(\frac{\pi}{4}c_1 c_2\right), \\ \exp\left(i\pi a_0^\dagger a_0 a_1^\dagger a_1\right) &= e^{-i\pi/4} \exp\left(\frac{\pi}{4}c_0 c_1\right) \exp\left(\frac{\pi}{4}c_2 c_3\right) \exp\left(i\frac{\pi}{4}c_0 c_1 c_2 c_3\right). \end{aligned}$$

Hence the following gate set is universal (up to phase factors):

$$\left\{ \exp\left(\frac{\pi}{8}c_0 c_1\right), \exp\left(i\frac{\pi}{4}c_0 c_1 c_2 c_3\right) \right\}. \quad (26)$$

The second gate in the set (26) describes four-particle interaction. When it comes to physical implementation, this gate will be particularly difficult to realize. Unfortunately, it is not possible to do universal quantum computation by acting on three or fewer Majorana fermions at a time. This way one can only generate the group of unitary operators which act by conjugation as follows:

$$U c_j U^\dagger = \sum_k \beta_{jk} c_k, \quad (27)$$

where  $\beta \in SO(m)$ , i.e.  $(\beta_{jk})$  is a real orthogonal matrix with determinant +1.

## 7 An alternative to the four-particle Majorana gate

In this section we show that, for the purpose of universal computation with Majorana fermions, the gate  $\exp(i\frac{\pi}{4}c_0 c_1 c_2 c_3)$  can be replaced by a nondestructive eigenvalue measurement of the operator  $c_0 c_1 c_2 c_3$ . (A measurement being nondestructive means that vectors in each of the eigenspaces remain intact; in other words, no extra information is learned or leaks to the environment). Such measurements might be easier to implement, they are also useful in some theoretical application of fermionic computation [10].

Let us assume that the following operations are possible:

1. Applying the unitary gate  $R = \exp\left(\frac{\pi}{4}c_0 c_1\right)$ . (Note that  $R c_0 R^\dagger = -c_1$ ,  $R c_1 R^\dagger = c_0$ ).
2. Creation of an ancilla pair in a state which is the eigenstate of  $c_{2k} c_{2k+1} = i(1 - 2a_k^\dagger a_k)$  corresponding to the eigenvalue  $i$ .
3. Eigenvalue measurement of  $c_j c_k$ .
4. Nondestructive eigenvalue measurement of  $c_j c_k c_r c_s$ .

Moreover, we can base the choice of the next operation on the previous measurement outcomes. (One may call such quantum computation *adaptive*). Of course, the amount of classical computation involved in this choice should not be too large, so we should better include it into the overall size of the quantum circuit.

*Remark.* In the standard scheme of quantum computation, measurements in the middle of computation are redundant and can be simulated by unitary gates (e.g. see [11]). However, this is only true if one uses a universal set of unitary gates. Otherwise measurements and adaptiveness can indeed add extra power to unitary operators.

Suppose we want to apply the operator  $\exp(i\frac{\pi}{4}c_0c_1c_2c_3)$ . Let Majorana fermions 4 and 5 form an ancilla pair, so the input state of the system satisfies

$$(c_4 + ic_5)|\Psi_{\text{in}}\rangle = 0. \quad (28)$$

We measure the eigenvalue of  $c_0c_1c_3c_4$ . The outcome is either  $+1$  or  $-1$ , which means that  $|\Psi_{\text{in}}\rangle$  gets multiplied by the projector  $\Pi_{+1}^{(4)} = \frac{1}{2}(1 + c_0c_1c_3c_4)$  or  $\Pi_{-1}^{(4)} = \frac{1}{2}(1 - c_0c_1c_3c_4)$ , respectively. (More exactly,  $|\Psi_{\text{in}}\rangle \mapsto p_{\pm 1}^{-1/2}\Pi_{\pm 1}^{(4)}|\Psi_{\text{in}}\rangle$ , where  $p_z$  is the probability to get outcome  $z$ ). Then we measure the eigenvalue of  $c_2c_4$ . The possible eigenvalues  $+i$  and  $-i$  correspond to the projectors  $\Pi_{+i}^{(2)} = \frac{1}{2}(1 - ic_2c_4)$  and  $\Pi_{-i}^{(2)} = \frac{1}{2}(1 + ic_2c_4)$ . We claim that after some correction depending on the measurements outcomes, we will effectively execute the operator  $\exp(i\frac{\pi}{4}c_0c_1c_2c_3)$  while leaving the ancilla pair intact. Indeed,

$$\begin{aligned} \exp\left(i\frac{\pi}{4}c_0c_1c_2c_3\right)|\Psi_{\text{in}}\rangle &= \\ &= 2 \exp\left(\frac{\pi}{4}c_2c_5\right) \frac{1}{2}(1 - ic_2c_4) \frac{1}{2}(1 + c_0c_1c_3c_4) |\Psi_{\text{in}}\rangle = \\ &= 2i \exp\left(\frac{\pi}{2}c_0c_1\right) \exp\left(\frac{\pi}{2}c_2c_3\right) \exp\left(\frac{\pi}{4}c_2c_5\right) \frac{1}{2}(1 - ic_2c_4) \frac{1}{2}(1 - c_0c_1c_3c_4) |\Psi_{\text{in}}\rangle = \quad (29) \\ &= 2i \exp\left(\frac{\pi}{2}c_0c_1\right) \exp\left(\frac{\pi}{2}c_2c_3\right) \exp\left(-\frac{\pi}{4}c_2c_5\right) \frac{1}{2}(1 + ic_2c_4) \frac{1}{2}(1 + c_0c_1c_3c_4) |\Psi_{\text{in}}\rangle = \\ &= 2 \exp\left(-\frac{\pi}{4}c_2c_5\right) \frac{1}{2}(1 + ic_2c_4) \frac{1}{2}(1 - c_0c_1c_3c_4) |\Psi_{\text{in}}\rangle \end{aligned}$$

(we have used eq. (28)). Thus we can apply a suitable correction operator  $U_{yz}$  in each of the four cases ( $U_{+i,+1} = \exp(\frac{\pi}{4}c_2c_5)$  if the outcomes were  $+1$  and  $+i$ , etc.) so that

$$\exp\left(i\frac{\pi}{4}c_0c_1c_2c_3\right)|\Psi_{\text{in}}\rangle = 2U_{yz}\Pi_y^{(2)}\Pi_z^{(4)}|\Psi_{\text{in}}\rangle.$$

Each of the four outcome combinations occurs with probability  $2^{-2} = \frac{1}{4}$ . The final state is always the desired one,  $|\Psi_{\text{fin}}\rangle = \exp(i\frac{\pi}{4}c_0c_1c_2c_3)|\Psi_{\text{in}}\rangle$ .

## 8 Superfast simulation of fermions on a graph

The results of Sec. 5 suggest that fermions have slightly more computational power than qubits. The logarithmic slowdown in simulation of fermions seems to be inevitable in the general case. However, in the physical world fermions (e.g. electrons) interact locally not only in the sense that the interaction is pairwise, but also in the geometric sense: a particle can not instantly jump to another position far away. Such physical interactions might be easier to simulate. In this section we study an abstract model of geometrically local interactions. The result is that

geometrically local gates can indeed be simulated without any substantial slowdown, i.e. the simulation cost is constant. Therefore one can speculate that, in principle, electrons might not be fundamental particles but, rather, excitations in a (nonperturbative) system bosons. Of course, this is only a logical possibility which may or may not be true.

What follows is a definition of the model. Consider a *connected unoriented graph*  $\Gamma = (M, E)$ , where  $M = \{0, \dots, m-1\}$  is the set of vertices, and  $E \subset M \times M$  is the set of edges. (As the graph is unoriented,  $(j, k)$  and  $(k, j)$  either both belong to  $E$  or both do not belong to  $E$ ). We will assume that the degree of each vertex is bounded by some constant  $d$ . Let us put a *local fermionic mode* on each *vertex*. We will consider only the *even sector* of the system,  $\mathcal{H}_0$ , i.e. the total number of fermions is required to be even. The *allowed unitary operations* are one-LFM gates and two-LFM gates applied to any pair of vertices connected by an edge.

We are going to identify the Hilbert space  $\mathcal{H}_0$  with a codespace of a certain symplectic (stabilizer) code [12]<sup>5</sup> so that each elementary operator of the form  $a_k^\dagger a_k$ , as well as  $a_j^\dagger a_k$ ,  $a_k^\dagger a_j$ ,  $a_j a_k$  or  $a_k^\dagger a_j^\dagger$ , where  $(j, k) \in E$ , be represented by operators acting on  $O(d)$  qubits. Then each one-LFM gate and each two-LFM gate applied to neighboring vertices will be also represented by an operator acting on  $O(d)$  qubits. As  $d = \text{const}$ , this means one can simulate each of the allowed fermionic operations by a constant number of one-qubit and two-qubit gates.

It will be convenient to use the Majorana fermions operators  $c_{2k}, c_{2k+1}$  (see eq. (24)) instead of  $a_k, a_k^\dagger$ . The list of elementary operators to be represented can be reduced to these ones:

$$\begin{aligned} B_k &= -ic_{2k}c_{2k+1} & \text{for each vertex } k, \\ A_{jk} &= -ic_{2j}c_{2k} & \text{for each edge } (j, k) \in E. \end{aligned} \quad (30)$$

These operators satisfy the following relations:

$$B_k^\dagger = B_k, \quad A_{jk}^\dagger = A_{jk}, \quad B_k^2 = 1, \quad A_{jk}^2 = 1, \quad A_{kj} = -A_{jk}, \quad (31)$$

$$B_k B_l = B_l B_k, \quad A_{jk} B_l = (-1)^{\delta_{jl} + \delta_{kl}} B_l A_{jk}, \quad A_{jk} A_{ls} = (-1)^{\delta_{jl} + \delta_{js} + \delta_{kl} + \delta_{ks}} A_{ls} A_{jk}, \quad (32)$$

$$i^p A_{j_0, j_1} A_{j_1, j_2} \cdots A_{j_{p-2}, j_{p-1}} A_{j_{p-1}, j_0} = 1 \quad \text{for any closed path on the graph.} \quad (33)$$

It is easy to prove that  $B_k, A_{jk}$  modulo these relations generate the algebra of physical operators  $\mathcal{F} = \mathbf{L}(\mathcal{H}_0) \oplus \mathbf{L}(\mathcal{H}_1)$ . However, we are considering only the even sector now. Having been restricted to  $\mathcal{H}_0$ , the operators  $B_k$  satisfy an additional relation (which was false in  $\mathcal{F}$ ):

$$\prod_k B_k = 1. \quad (34)$$

Hence the algebra  $\mathbf{L}(\mathcal{H}_0)$  is generated by  $B_k, A_{jk}$  modulo the relations (31)–(34).

To construct the code, we put a qubit on each edge of the graph. Thus  $\sigma_{jk}^\alpha = \sigma_{kj}^\alpha$  denotes the Pauli operator  $\sigma^\alpha$  ( $\alpha = x, y, z$ ) acting on the edge  $(j, k)$ . The operators  $B_k, A_{jk}$  defined above will be identified with some operators  $\tilde{B}_k, \tilde{A}_{jk}$  acting on the code subspace  $\mathcal{L}$  (which will be defined later). We start with defining the action of  $\tilde{B}_k$  and  $\tilde{A}_{jk}$  on the entire Hilbert space of the qubits. Our construction depends on two arbitrary choices. Firstly, we choose orientation for each edge of the graph. This can be described by a matrix  $(\epsilon_{jk})$  such that  $\epsilon_{kj} = -\epsilon_{jk}$ ,

---

<sup>5</sup>The term ‘‘stabilizer code’’ has become traditional but it is somewhat confusing because any code can be defined in terms of stabilizer operators. (It is actually practical to do so for nonbinary codes related to anyons [5]). We prefer to use the more specific terms ‘‘symplectic code’’ [13].

$\epsilon_{jk} = \pm 1$  for each edge  $(j, k) \in E$ . Secondly, for each vertex  $k$ , we order all incident edges  $(j, k)$ . This order will be denoted by  $\prec_k$ . Now we put

$$\begin{aligned}\tilde{B}_k &= \prod_{j: (j,k) \in E} \sigma_{jk}^z, \\ \tilde{A}_{jk} &= \epsilon_{jk} \sigma_{jk}^x \prod_{l: (l,j) \prec_j (k,j)} \sigma_{lj}^z \prod_{s: (s,k) \prec_k (j,k)} \sigma_{sk}^z.\end{aligned}\tag{35}$$

These operators satisfy the relations analogous to (31), (32) and (34), but not (33).

Finally, we define the code subspace  $\mathcal{L} \subseteq \mathcal{B}^{\otimes u}$  (where  $u$  is the number of qubits) by imposing stabilizer conditions:

$$\begin{aligned}|\psi\rangle \in \mathcal{L} \quad \text{if and only if} \quad & \tilde{C}_{j_0, \dots, j_{p-1}} |\psi\rangle = |\psi\rangle \text{ for any closed path } (j_0, \dots, j_{p-1}, j_0), \\ & \tilde{C}_{j_0, \dots, j_{p-1}} = i^p \tilde{A}_{j_0, j_1} \tilde{A}_{j_1, j_2} \cdots \tilde{A}_{j_{p-2}, j_{p-1}} \tilde{A}_{j_{p-1}, j_0}.\end{aligned}\tag{36}$$

The stabilizer operators  $\tilde{C}_{j_0, \dots, j_{p-1}}$  are Hermitian and can be represented in the form  $\pm \prod_{(j,k)} \sigma_{jk}^{\alpha_{jk}}$ , where  $(j, k)$  runs over a set of different qubits. The set of stabilizer operators is obviously redundant but it is consistent, meaning that (i) they commute with each other, and (ii) whenever the product of several stabilizer operators is a constant, this constant is 1. The number of independent stabilizer operators equals the number of linearly (mod 2) independent cycles which in turn equals  $u - m + 1$ . Hence

$$\dim \mathcal{L} = 2^{u-(u-m+1)} = 2^{m-1} = \dim \mathcal{H}_0.\tag{37}$$

The operators  $\tilde{B}_k, \tilde{A}_{jk}$  commute with  $\tilde{C}_{j_0, \dots, j_{p-1}}$ , so they leave the code subspace invariant. The restrictions of these operators,  $\tilde{B}_k|_{\mathcal{L}}$  and  $\tilde{A}_{jk}|_{\mathcal{L}}$ , satisfy the relations analogous to (31)–(34). Thus the correspondence  $B_k \mapsto \tilde{B}_k|_{\mathcal{L}}, A_{jk} \mapsto \tilde{A}_{jk}|_{\mathcal{L}}$  extends to a  $*$ -algebra homomorphism  $\mu: \mathbf{L}(\mathcal{H}_0) \rightarrow \mathbf{L}(\mathcal{L})$ . But  $\dim \mathcal{L} = \dim \mathcal{H}_0$ , hence  $\mu$  is an isomorphism. It can be represented as  $\mu(X) = JXJ^\dagger$ , where  $J: \mathcal{H}_0 \rightarrow \mathcal{L}$  is a unitary map which is unique up to an overall phase.

Now that the main construction is complete, we can give exact rules for converting the allowed (geometrically local) operations on LFMs into qubit gates. These rules are almost obvious but still worth putting them into a rigorous form. For most generality, consider a two-LFM gate application  $U\{j, k\}$ , where  $(j, k) \in E$ . Here  $U$  is a physical operator acting on 2 LFMs (= 4 Majorana fermions = 2 qubits), so it can be expressed in terms of  $A = -ic_0c_2 = -\sigma^y[0]\sigma^x[1]$ ,  $B' = -ic_0c_1 = \sigma^z[0]$  and  $B'' = -ic_2c_3 = \sigma^z[1]$ . Applying  $U$  to LFMs  $j$  and  $k$  means substituting  $A_{jk}, B_j, B_k$  for  $A, B', B''$ . Instead of that, we actually do another substitution:

$$\nu_{jk}: \quad A \mapsto \tilde{A}_{jk}, \quad B' \mapsto \tilde{B}_j, \quad B'' \mapsto \tilde{B}_k.\tag{38}$$

It extends to a  $*$ -algebra homomorphism  $\mathcal{G} \rightarrow \mathbf{L}(\mathcal{B}^{\otimes S_{jk}})$ , where  $\mathcal{G}$  is the algebra generated by  $A, B'$  and  $B''$  (= the algebra of parity-preserving operators on two qubits), and  $S_{jk}$  is the set of qubits consisting of all edges incident to  $j$  and  $k$ . (Note that we do not have to restrict  $\tilde{A}_{jk}, \tilde{B}_j, \tilde{B}_k$  to the subspace  $\mathcal{L}$  because the cycle relation (33) is irrelevant in this context). So,  $U\{j, k\}$  is simulated by  $\nu_{jk}(U)$ .

It turns out that this simulation is pretty efficient even if  $d$  (= the largest degree of a vertex in the graph) is not a constant. W.l.o.g.  $m > 2$ , so  $S_{jk}$  contains at least one edge besides

$(j, k)$ , say,  $(j, l)$ . Then  $\tilde{B}_j$ ,  $\tilde{B}_k$  and  $\tilde{A}_{jk}$  have no nontrivial relations (like  $\tilde{B}_j\tilde{B}_k = 1$ ). More exactly, the map  $\nu_{jk}$  is injective, so  $\tilde{B}_j$ ,  $\tilde{B}_k$  and  $\tilde{A}_{jk}$  satisfy exactly the same relations as  $\sigma^z[0]$ ,  $\sigma^z[1]$  and  $-\sigma^y[0]\sigma^x[1]$ . It follows that there is a ‘‘symplectic transformation’’ [13] of the form  $X \mapsto WXW^\dagger$  which takes  $\tilde{B}_j$ ,  $\tilde{B}_k$  and  $\tilde{A}_{jk}$  to  $\sigma_{jl}^z$ ,  $\sigma_{jk}^z$  and  $-\sigma_{jl}^y\sigma_{jk}^x$ . The unitary operator  $W$  acts on the qubits from  $S_{jk}$  and can be represented as a product of elementary ‘‘symplectic gates’’:  $H$ ,  $\Lambda(\sigma^x)$  and  $\Lambda(i)$ . It is easy to show that  $O(d)$  applications of these gates are sufficient. Hence executing the operator

$$\nu_{jk}(U) = W^\dagger U[(j, l), (j, k)] W \quad (39)$$

takes  $O(d)$  one-qubit and two-qubit gate applications.

In the above analysis, we did not take into account the number of operations required to prepare an initial state  $|\psi\rangle \in \mathcal{L}$ , which is necessary to begin simulation. For definiteness, we will consider the unique quantum state  $|\xi\rangle \in \mathcal{L}$  which satisfies additional constraints:

$$\tilde{B}_k|\xi\rangle = |\xi\rangle \text{ for each } k. \quad (40)$$

Note that  $B_k = -ic_{2k}c_{2k+1} = 1 - 2a_k^\dagger a_k$ , so  $|\xi\rangle$  represents the fermionic state  $|0, \dots, 0\rangle$ . By a general argument, the qubit state  $|0\rangle \otimes \dots \otimes |0\rangle$  can be transformed into  $|\xi\rangle$  by applying  $O(u^2)$  symplectic gates.

However, if we continue the speculations about fermions being possibly mimicked by bosons, the vacuum state of the bosonic system must absorb new degrees of freedom as the Universe expands. Certainly, this process should be reversible, i. e. it should also work when the space shrinks. In our model, shrinking the space corresponds to contracting some edges. More specifically, contracting an edge  $(j, k)$  means removing it while identifying the vertices  $j$  and  $k$ . If both  $j$  and  $k$  are connected to the same vertex  $l$ , a double edge between  $j \equiv k$  and  $l$  appears; it must be then reduced to a single one. We should be able to update our ‘‘vacuum state’’  $|\xi\rangle$  through these transformations. (The qubit being removed should come out in the state  $|0\rangle$ ). One can show that a single contraction or reduction step requires  $O(d)$  symplectic gates. This does not involve any nonlocality and can be done simultaneously in different places, which is quite consistent with the idea of adiabatic vacuum transformation in the expanding Universe.

## 9 Quantum codes by Majorana fermions

Some symplectic codes *on qubits* can be conveniently described in terms of Majorana fermions. We will show how it works for the Shor code [14]. Whether this approach can help to find new codes still remains to be seen.

By inverting the formula (24), we can represent the operators  $a_k, a_k^\dagger$  in terms of the Majorana operators:  $a_k = \frac{1}{2}(c_{2k} + ic_{2k+1})$ ,  $a_k^\dagger = \frac{1}{2}(c_{2k} - ic_{2k+1})$ . However, one can also introduce another set of annihilation and creation operators which will satisfy the same commutation relations:

$$b_k = \frac{1}{2}(c_{\tau(2k)} + ic_{\tau(2k+1)}), \quad b_k^\dagger = \frac{1}{2}(c_{\tau(2k)} - ic_{\tau(2k+1)}), \quad (41)$$

where  $\tau : \{0, \dots, 2m-1\} \rightarrow \{0, \dots, 2m-1\}$  is arbitrary permutation on  $2m$  elements. One can define a quantum code by fixing the occupation numbers of some of the new LFMs, e. g. by requiring that each codevector  $|\psi\rangle$  satisfies  $b_k^\dagger b_k |\psi\rangle = 0$  for  $k = 1 \dots m-1$ . In other words, the set of stabilizer operators is

$$X_k = -i c_{\tau(2k)} c_{\tau(2k+1)}, \quad k = 1, \dots, m-1. \quad (42)$$

The number of encoded qubits is  $m - (m - 1) = 1$ . The logical operators for this code are generated by  $c_{\tau(0)}$  (the encoded  $\sigma^x$ ) and  $c_{\tau(1)}$  (the encoded  $\sigma^y$ ).

Thus each permutation  $\tau : \{0, \dots, 2m-1\} \rightarrow \{0, \dots, 2m-1\}$  defines a quantum code which encodes 1 qubit into  $m$  qubits. It turns out that these codes can have arbitrary large code distances. We are to define a family of such codes which can be considered as slightly modified Shor codes. Let  $l \geq 2$  be an integer (the index of a code in the family),  $m = l^2$ . There will be two types of stabilizer operators:

$$\begin{aligned} Z_k &= -i c_{2kl+1} c_{2(k+2)l-2}, & k &= 0 \dots l-2, \\ Y_{k,j} &= -i c_{2kl+2j+3} c_{2kl+2j}, & k &= 0, \dots, l-1, \quad j = 0, \dots, l-2. \end{aligned} \quad (43)$$

They can be expressed in terms of the Pauli operators as follows :

$$Z_k = \sigma^x[kl] \sigma^x[(k+2)l-1] \prod_{s=kl+1}^{(k+2)l-2} \sigma^z[s], \quad Y_{k,j} = \sigma^y[kl+j] \sigma^y[kl+j+1] \quad (44)$$

For example, let us consider the  $l = 3$  code. Its 9 qubits can be arranged into a  $3 \times 3$  array as follows

$$\begin{array}{ccc} 0, & 1, & 2, \\ 3, & 4, & 5, \\ 6, & 7, & 8. \end{array}$$

Then the stabilizer operators of the first type become:

$$Z_0 = \left( \begin{array}{ccc} \sigma^x, & \sigma^z, & \sigma^z, \\ \sigma^z, & \sigma^z, & \sigma^x, \\ I, & I, & I \end{array} \right), \quad Z_1 = \left( \begin{array}{ccc} I, & I, & I, \\ \sigma^x, & \sigma^z, & \sigma^z, \\ \sigma^z, & \sigma^z, & \sigma^x \end{array} \right).$$

(These are not matrices. We just mean that, for example,  $Z_0 = \sigma^x \otimes \sigma^z \otimes \sigma^z \otimes \sigma^z \otimes \sigma^z \otimes \sigma^x \otimes I \otimes I \otimes I$ ). The stabilizer operators of the second type are

$$\begin{aligned} Y_{0,0} &= \left( \begin{array}{ccc} \sigma^y, & \sigma^y, & I, \\ I, & I, & I, \\ I, & I, & I \end{array} \right), & Y_{0,1} &= \left( \begin{array}{ccc} I, & \sigma^y, & \sigma^y, \\ I, & I, & I, \\ I, & I, & I \end{array} \right), & Y_{1,0} &= \left( \begin{array}{ccc} I, & I, & I, \\ \sigma^y, & \sigma^y, & I, \\ I, & I, & I \end{array} \right), \\ Y_{1,1} &= \left( \begin{array}{ccc} I, & I, & I, \\ I, & \sigma^y, & \sigma^y, \\ I, & I, & I \end{array} \right), & Y_{2,0} &= \left( \begin{array}{ccc} I, & I, & I, \\ I, & I, & I, \\ \sigma^y, & \sigma^y, & I \end{array} \right), & Y_{2,1} &= \left( \begin{array}{ccc} I, & I, & I, \\ I, & I, & I, \\ I, & \sigma^y, & \sigma^y \end{array} \right). \end{aligned}$$

If one performs the cyclic permutation  $\sigma^x \mapsto \sigma^y \mapsto \sigma^z \mapsto \sigma^x$ , the operators  $Y_{k,j}$  turn into certain stabilizer operators of the Shor code. The operators  $Z_k$  will not become exactly the same as in the Shor code. Each of them will contain two  $\sigma^y$  instead of  $\sigma^x$ . However, the code distance of this code is the same, namely, 3.

For arbitrary  $l$ , the code distance is  $d_l = l$ . (The proof is essentially the same as for the Shor code).

## References

- [1] R. P. Feynman, "Quantum mechanical computers", *Optics News* **11**, 11 (1985).

- [2] D. Deutsch, “Quantum computational networks”, *Proc. Roy. Soc. Lond.*, Ser. A, **425**, 73–90 (1989).
- [3] S. Lloyd, “Unconventional Quantum Computing Devices,” in *Unconventional Models of Computation*, C.S. Calude, J. Casti, M.J. Dinneen, eds., Springer, Singapore, 1998.
- [4] G. Moore, N. Read, “Nonabelians in the fractional quantum Hall effect”, *Nucl. Phys B* **360**, 362–396 (1991);  
C. Nayak, F. Wilczek, “ $2n$ -quasihole states realize  $2^{n-1}$ -dimensional spinor braiding statistics in paired quantum Hall states”, *Nucl. Phys B* **479**, 529–553 (1996).
- [5] A. Yu. Kitaev, “Fault-tolerant quantum computation by anyons”, ArXiv: quant-ph/9707021.
- [6] D. S. Abrams and S. Lloyd, “Simulation of many-body fermi systems on a universal quantum computer”, *Phys. Rev. Lett.* **79**, 2586–2589 (1997) (ArXiv: quant-ph/9703054).
- [7] M. H. Freedman, A. Kitaev, Z. Wang, “Simulation of topological field theories by quantum computers”, ArXiv: quant-ph/0001071.
- [8] E. Knill, R. Laflamme, W. H. Zurek, “Resilient quantum computation: error models and thresholds”, *Proc. Roy. Soc. Lond.*, Ser. A, **454**, 365–384 (1998) (ArXiv: quant-ph/9702058);  
P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, F. Vatan, “On universal and fault-tolerant quantum computing”, ArXiv: quant-ph/9906054.
- [9] A. Kitaev, “Unpaired Majorana fermions and protected quantum memory”, In preparation.
- [10] A. Kitaev, S. Bravyi, In preparation.
- [11] D. Aharonov, A. Kitaev, N. Nisan, “Quantum Circuits with Mixed States”, *Proc. 30th Annual ACM Symposium on Theory of Computation (STOC)*, 20–30 (1997) (ArXiv: quant-ph/9806029).
- [12] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, “Quantum error correction and orthogonal geometry”, *Phys. Rev. Lett.* **78**, 405–408 (1997) (ArXiv: quant-ph/9605005).
- [13] A. Yu. Kitaev, “Quantum computations: algorithms and error correction”, *Russian Math. Surveys* **52:6**, 1191–1249 (1997) (original Russian version: *Uspekhi Mat. Nauk* **52:6**, 53–112).
- [14] P. W. Shor, “Schemes for reducing decoherence in quantum computer memory”, *Phys. Rev. A* **52**, 2493–2496 (1995).