

CLUSTER-STATE QUANTUM COMPUTATION

MICHAEL A. NIELSEN

School of Physical Sciences,
The University of Queensland, Brisbane 4072, Australia
(e-mail: nielsen@physics.uq.edu.au and www.qinfo.org/people/nielsen/)

(Received April 13, 2005 — Revised June 27, 2005)

This article is a short introduction to and review of the *cluster-state* model of quantum computation, in which coherent quantum information processing is accomplished via a sequence of single-qubit measurements applied to a fixed quantum state known as a *cluster state*. We also discuss a few novel properties of the model, including a proof that the cluster state cannot occur as the exact ground state of any naturally occurring physical system, and a proof that measurements on any quantum state which is linearly prepared in one dimension can be efficiently simulated on a classical computer, and thus are not candidates for use as a substrate for quantum computation.

Keywords: quantum computation, cluster states, one-way quantum computer.

1. Introduction

Every child who has played computer games understands intuitively that one physical system can simulate another. Despite the simplicity of this idea, it is only recently that researchers have begun to develop a deep understanding of simulation from the point of view of basic physics.

Perhaps the fundamental question to be answered about simulation is: “when can one physical system be used to efficiently simulate another?” Recent work on this question has been motivated by the blossoming of interest in quantum computers [1], as-yet hypothetical devices which, it is hoped, can be used to efficiently simulate any other physical system. Thus, by asking what physical resources are *universal* for quantum computation, i.e. can be used to build a quantum computer, we are asking a general question about what physical resources are sufficient to efficiently simulate any other physical system.

The purpose of the present paper is to review recent work on *measurement-based* quantum computation, i.e. models for quantum computation having the remarkable property that all the basic dynamical operations are non-unitary quantum measurements, yet they can still be used to simulate arbitrary quantum dynamics, including unitary dynamics. Such models of quantum computation thus challenge the conventional understanding of quantum measurement as a process that inherently destroys quantum coherence.

We focus on a class of measurement-based models of quantum computation proposed by Raussendorf and Briegel [2], the so-called *cluster-state* model, or *one-way quantum computer*. The cluster-state model has a remarkably rich structure that is not fully understood, but which differs substantially from the conventional unitary model of quantum computing. These differences have led to new insights into quantum computational complexity [3], and to dramatic simplifications in experimental proposals for quantum computation [4–6].

An alternate approach to measurement-based quantum computation has been proposed in [7], and developed in [8,9]. We will not explore this other approach here, but note that connections between the two approaches have been developed in [10–12]. More generally, the literature on measurement-based quantum computation has grown rapidly, and we cannot do a thorough survey of all developments here; see, for example, [3,13–23] and references therein for more information.

The structure of the paper is as follows. Section 2 presents a short review of the standard unitary quantum circuits model of quantum computation. Section 3 is an elementary introduction to and review of the basic cluster-state model, explaining the model and how it can be used to simulate the quantum circuit model of computation. In addition to this review function, the paper also contains in Section 4 a discussion of some novel results about two open problems, namely: (a) can the cluster state arise as the ground state of some reasonable physical system; and (b) what quantum states, when used as a substrate, can be efficiently simulated on a conventional classical computer? For neither problem do we obtain anything like a comprehensive solution, yet in both cases we obtain through elementary means results that hint at a beautiful structure yet to be fully understood. Section 5 concludes.

2. The quantum circuit model of quantum computation

A priori there are many ways one might construct a quantum-mechanical model of computation. To date, all the physically plausible models of quantum computation which have been proposed have turned out to be computationally equivalent. That is, each of these apparently different models of computation can efficiently simulate one another, and thus do not differ in the class of computational problems they can efficiently solve.

The most widely used model of quantum computation at the present time is the *quantum circuit* model [24], which is a generalization of the well-known classical circuit model based on Boolean logical operations such as AND and NOT. We provide a brief review of the quantum circuit model in this section, referring the reader to Chapter 4 of [1] for more details. Through the remainder of this paper we treat the quantum circuit model as the standard model of quantum computation.

The main elements of the quantum circuit model are illustrated by the following example of a quantum circuit:



The horizontal lines are *quantum wires*, representing *qubits*, abstract quantum mechanical systems with a two-dimensional state space spanned by the (orthogonal) *computational basis states* $|0\rangle$ and $|1\rangle$. The left-to-right progress of a wire does not represent movement of the qubit through space, but rather progress through time. The initial state of the qubits is usually taken to be some fiducial product state, such as the all $|0\rangle$ state, $|0\rangle^{\otimes n}$.

The processing of the qubits is done through a sequence of one- and two-qubit quantum gates. These quantum gates are unitary operations transforming the state of one or two qubits. For example, we have single-qubit gates like the Hadamard gate,

$$\text{---} \boxed{H} \text{---} \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (2)$$

where the matrix on the right is the unitary matrix representing the action of the Hadamard gate with respect to the $|0\rangle, |1\rangle$ basis. So, for example, the Hadamard gate takes the input $|0\rangle$ and transforms it to $(|0\rangle + |1\rangle)/\sqrt{2}$.

Other important single-qubit gates are the rotations about the X , Y and Z axes:

$$\text{---} \boxed{X(\theta)} \text{---} \equiv \exp(-i\theta X/2), \quad (3)$$

$$\text{---} \boxed{Y(\theta)} \text{---} \equiv \exp(-i\theta Y/2), \quad (4)$$

$$\text{---} \boxed{Z(\theta)} \text{---} \equiv \exp(-i\theta Z/2), \quad (5)$$

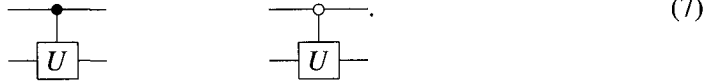
where X, Y and Z are abbreviated notations for the usual Pauli σ_x, σ_y and σ_z matrices.

Perhaps the most commonly-used two-qubit gate is the controlled-NOT gate,



The top qubit is the *control* qubit, while the bottom is the *target* qubit. These names are used because the action of the controlled-NOT in the computational basis is to take $|x, y\rangle$ to $|x, y \oplus x\rangle$, where \oplus is addition mod 2. That is, the control qubit remains unchanged, while the target is flipped if the control is set to 1, and is otherwise unchanged.

The controlled-NOT is a special case of more general controlled-unitary gates:



In both cases the first qubit is the control, while the second qubit is the target. In the first circuit, U is applied to the target qubit if the control qubit is set to 1, while in the second circuit U is applied to the target qubit if the control qubit is set to 0.

Beside the controlled-NOT, another specific controlled-unitary gate that is often useful is the controlled-PHASE gate,



The action of the controlled-PHASE in the computational basis is $|x, y\rangle \rightarrow (-1)^{xy}|x, y\rangle$.

Since the individual gates are unitary, the combined effect of the gates making up a circuit such as (1) is a joint unitary transformation on the n input qubits. Which unitary operations can be synthesized in this way? Provided the available gates include all single-qubit gates, and at least one entangling two-qubit gate, such as the controlled-NOT or controlled-PHASE, it turns out that the gate set is *universal*, meaning that it can be used to synthesize an arbitrary unitary operation on the qubits [25].

The challenge of quantum computation is to find small quantum circuits synthesizing desirable unitary operations. For a generic unitary U on n qubits, the number of gates required to synthesize U scales exponentially in n [26]. Such exponential scaling is prohibitively expensive, and it is far more desirable to find families of unitary operations which can be synthesized using a number of gates that scales polynomially in n .

The final step in a quantum circuit is to *read out* the state of the qubits, or some subset of the qubits. This is done by measuring the desired subset of the qubits in their respective computational bases. The resulting string of bits “0010110...” is the result of the computation. This idea is illustrated in (1), where the meter terminating the top wire indicates a measurement in the computational basis.

This concludes our basic overview of the quantum circuit model of computation. In practice, many straightforward variants of the quantum circuit model are often used. These include: (1) allowing the input state to be any tensor product of single-qubit states, $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$; (2) allowing measurements with respect to any orthonormal single-qubit basis, since this is equivalent to applying a single-qubit unitary operation followed by a computational basis measurement; and (3) allowing measurements and feedforward of the measurement results during the computation, so later actions (e.g. quantum gates) may depend on the results of earlier measurement outcomes. None of these modifications changes the computational power of the quantum circuit model, but it does make it more convenient to work with.

3. The cluster state model

In this section we explain the cluster-state model of quantum computation, and explain how cluster states can be used to efficiently simulate quantum circuits. Our discussion follows [17,27], which are based in turn on the original paper [2].

3.1. How a cluster-state computation works

A cluster-state computation begins with the preparation of a special entangled many-qubit quantum state, known as a *cluster state*, followed by an adaptive sequence of single-qubit measurements, which process the cluster, and finally read-out of the computation's result from the remaining qubits. We now discuss each of these steps in detail.

The term “cluster state” refers not to a single quantum state, but rather to a family of quantum states. The idea is that to any graph G on n vertices we can define an associated n -qubit cluster state, by first associating to each vertex a corresponding qubit, and then applying a graph-dependent preparation procedure to the qubits, as described below. As an example, the following graph represents a six-qubit cluster state,



The cluster state associated to the graph may be defined as the result of applying the following preparation procedure:

1. Prepare each of the n qubits in the state $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$.
2. Apply controlled-PHASE gates between qubits whose corresponding graph vertices are connected.

Note that controlled-PHASE gates commute with one another, so we do not need to specify the order in which the gates are applied. Also, although we have described the preparation of the cluster in terms of applying quantum gates, later in the paper we briefly describe how to prepare clusters using measurements alone, and so the cluster-state model may be regarded as a truly measurement-only model of quantum computation.

Note that the states we have called cluster states are sometimes also known as *graph states*. Originally, the term “cluster state” was introduced by Raussendorf and Briegel [28] to refer to the case where the graph G is a two-dimensional square lattice. This was the class of states which they showed in [2] could be used as a substrate for quantum computation. The term “graph state” originally referred to the family of states associated with more general graphs G . This distinction was blurred by the introduction of schemes for quantum computing based on Raussendorf and Briegel’s ideas, but using different graphs.

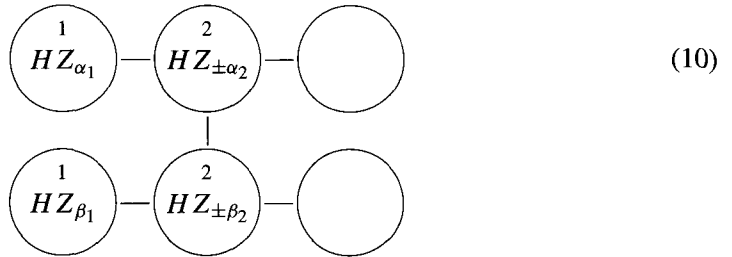
I believe it makes most sense to have a single terminology for the entire class of states, and then to specify in any instance what graph is being used (e.g. a

two-dimensional square lattice with boundary). I suggest using the term “cluster state” for this purpose, and will follow this terminology throughout this paper.

Once the cluster state is prepared, the next step in the computation is to perform a sequence of *processing measurements* on the state. These measurements satisfy: (1) they are single-qubit measurements; (2) the choice of measurement basis may depend on the outcomes of earlier measurements, i.e., feedforward of classical measurement results is allowed; and (3) measurement results may be processed by a classical computer to assist in the feedforward, so the choice of basis may be a complicated function of earlier measurement results. Note that for the cluster-state computation to be *efficient* we must constrain the classical computation to be of polynomial size.

The output of the cluster-state computation may be defined in two different ways, both useful. The first is to regard the computation as having a *quantum state* as output, namely, the quantum state of the qubits which remain when the sequence of processing measurements has terminated. The second definition is to add a set of *read-out measurements*, a sequence of single-qubit measurements applied to the qubits which remain when the processing measurements are complete. In this case the output of the computation is a classical bit string.

A concrete example of these ideas is the following cluster-state computation:

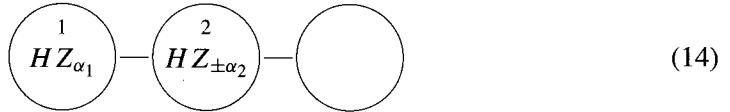


Labels indicate qubits on which processing measurements occur, while unlabelled qubits are those which remain as the output of the computation when the processing measurements are complete. Note that the qubits are labelled by a positive integer n and a single-qubit unitary, which we refer to generically as U ; here $U = HZ_{\pm\alpha_j}, HZ_{\pm\beta_j}$. The n label indicates the time-ordering of the processing measurements, with qubits having the same label capable of being measured in either order, or simultaneously. The time order is important, because it determines which measurement results can be feedforward to control later measurement bases. The U label indicates the basis in which the qubit is measured, denoting a rotation by the unitary U , followed by a computational basis measurement. Equivalently, a single-qubit measurement in the basis $\{U^\dagger|0\rangle, U^\dagger|1\rangle\}$ is performed. The \pm notation in $HZ_{\pm\alpha_2}$ and $HZ_{\pm\beta_2}$ indicates that the choice of sign depends on the outcomes of earlier measurements, in a manner to be specified separately. We'll give an example of how this works later.

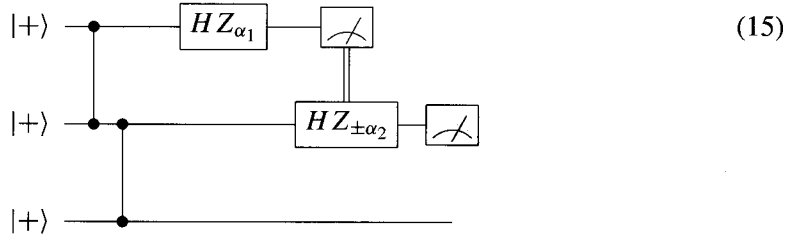
$$|+\rangle \text{---} \boxed{HZ_{\alpha_1}} \text{---} \boxed{HZ_{\alpha_2}} \text{---} \quad (13)$$

This apparently trivial case contains the most important ideas used in the general case. Note that we assume the qubit starts in the $|+\rangle$ state, and that single-qubit gates are of the form HZ_α . These assumptions are made for convenience, and do not cause any loss of generality, since it is clear that an arbitrary single-qubit circuit can be simulated using the ability to simulate these operations.

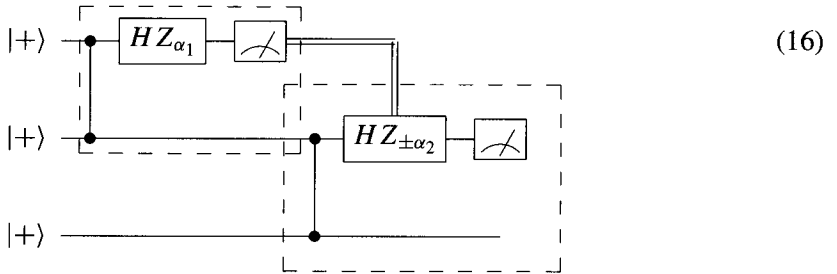
The cluster-state computation used to simulate circuit (13) is



By definition, this cluster-state computation has an output equal to the output of the following quantum circuit¹:



Equivalently, we can delay the operations on the second and third qubits until *after* the measurement on the first qubit is complete:



To determine the output, observe that the two highlighted boxes are both of the form of (12), and thus the output of the circuit is $X^{m_2} H Z_{\pm\alpha_2} X^{m_1} H Z_{\alpha_1} |+\rangle$, where m_1 and m_2 are the outputs of the measurements on the first and second qubits, respectively. Observe that feedforward can be used to choose the sign of $\pm\alpha_2$ so that $Z_{\pm\alpha_2} X^{m_1} = X^{m_1} Z_{\alpha_2}$. We also have $H X^{m_1} = Z^{m_1} H$, and thus the output may be rewritten as $X^{m_2} Z^{m_1} H Z_{\alpha_2} H Z_{\alpha_1} |+\rangle$, which, up to the known Pauli matrix $X^{m_2} Z^{m_1}$, is identical to the output of the conventional single-qubit quantum circuit (13).

¹Note that the double vertical lines emanating from the meter on the top qubit indicate classical feedforward and control of later operations. We use this and similar notations often later in the paper.

This example generalizes easily to larger single-qubit circuits containing gates of the form HZ_α . The general proof strategy is: (1) rewrite the cluster-state computation in terms of an equivalent quantum circuit; (2) reinterpret the quantum circuit as a sequence of circuits of the form (12); (3) in the resulting expression for the output state, commute operators of the form X^m all the way to the left, using feedforward to choose signs on the terms of the form $Z_{\pm\alpha}$ to ensure that after commutation they are of the form Z_α . The result is a state which, up to a known Pauli matrix, is equivalent to the output of the single-qubit quantum circuit.

These ideas generalize also to multi-qubit quantum circuits. For example, the circuit

$$\begin{array}{c}
 |+\rangle \text{ --- } \boxed{HZ_{\alpha_1}} \text{ --- } \bullet \text{ --- } \boxed{HZ_{\alpha_2}} \text{ ---} \\
 |+\rangle \text{ --- } \boxed{HZ_{\beta_1}} \text{ --- } \bullet \text{ --- } \boxed{HZ_{\beta_2}} \text{ ---}
 \end{array} \quad (17)$$

can be simulated using the cluster-state computation (10). The proof of this equivalence follows exactly the same lines as in the single-qubit case, and is only notationally more complicated. We omit the details, and suggest the interested reader fill them in.

Summing up, we have shown how the cluster-state model of computation can be used to efficiently simulate any quantum circuit whose inputs are all $|+\rangle$ states, and whose gates are either controlled-PHASE gates, or gates of the form HZ_α . This set of resources is universal for quantum computation, and thus the cluster-state model is capable of efficiently simulating any quantum circuit. Conversely, it is straightforward to see that any cluster-state computation may be efficiently simulated in the quantum circuit model, and thus the two models are computationally equivalent.

4. Properties of the cluster-state model

We've given a basic description of the cluster-state model of quantum computing. In this section we describe two simple but fundamental questions about cluster states, and present some progress on answering these questions. The results and methods presented are elementary, but hopefully instructive, and strongly suggestive of a rich and undiscovered structure in the theory of measurement-based quantum computation.

Subsection 4.1 asks when a cluster state can arise as the ground state of a quantum system, and shows that for typical graphs it is not possible for the cluster state to be the ground state of a realistic quantum system. Subsection 4.2 addresses the question of what general properties of a quantum state enable it to serve as a substrate for quantum computation, in a manner similar to the cluster state. We show that the two-dimensional geometry of the cluster is important, by demonstrating that a wide class of one-dimensional analogues of the cluster-state model can be simulated efficiently on a classical computer, and thus are unlikely to be useful for quantum information processing.

4.1. Cluster states and the ground states of many-body quantum systems

Given the significance of cluster states for quantum computation, it is natural to ask whether or not cluster states may occur as nondegenerate ground states of some naturally occurring class of physical systems. If this were so then cooling and measuring such a system might offer a viable path to quantum computation. Unfortunately, we show in this subsection that this is typically not possible, provided we make a restriction that is usually physically reasonable, namely, that the system has only two-body interactions. The argument we give is based on [32], which studied the conditions under which quantum error-correcting code states can arise as ground states of Hamiltonian systems.

Our results are framed in terms of the stabilizer formalism introduced by Gottesman [33] (see Chapter 10 of [1] for a review). Using the two-stage preparation procedure for the cluster state associated to a graph G it is easy to verify that a set of generators for the stabilizer group of the cluster state is given by the operators

$$S_v \equiv X_v \bigotimes_{v'} Z_{v'}, \quad (18)$$

where there is one such stabilizer generator for each vertex, v , X_v and Z_v represent Pauli operators acting on the qubit associated to vertex v , and the tensor product is over all vertices v' neighbouring v . Up to an unimportant global phase factor the cluster is the unique quantum state such that $S_v|\psi\rangle = |\psi\rangle$ for all vertices v in the graph. As an aside, we note that this observation gives us a way of effectively preparing cluster states using measurements alone (cf. [23]): (1) measure all the stabilizer generators, obtaining a state which is a simultaneous eigenstate of the S_v , with eigenvalues ± 1 ; and then (2) make use of the result [1, 33] that such a state is equal, up to local unitary operations, to the state for which all the S_v have eigenvalue $+1$, i.e. the cluster state.

Suppose $|C\rangle$ is a cluster state associated to some fixed graph, G . Can $|C\rangle$ arise as the nondegenerate ground state of some two-body Hamiltonian, $H = \sum_{\sigma\tau} h_{\sigma\tau} \sigma \otimes \tau$, where the sum is over distinct pairs of Pauli (I, X, Y, Z) operators²? To answer this question, observe that the state $(\sigma \otimes \tau)|C\rangle$ has a stabilizer generated by the operators $(\sigma \otimes \tau)S_v(\sigma \otimes \tau) = n_v^{\sigma,\tau} S_v$, where $n_v^{\sigma,\tau} = \pm 1$. We call the vector $n^{\sigma,\tau}$ whose entries are the $n_v^{\sigma,\tau}$ the *syndrome vector* corresponding to $\sigma \otimes \tau$. Clearly, provided the syndrome vectors $n^{\sigma,\tau}$ are all distinct then the states $(\sigma \otimes \tau)|C\rangle$ are orthonormal. When this occurs, $H|C\rangle$ must contain terms orthonormal to $|C\rangle$, and thus $|C\rangle$ cannot be an eigenstate of H . Indeed, [32] generalizes this argument, showing that when this condition holds, the distance between $|C\rangle$ and the energy eigenstates may be bounded below by a *constant* independent of anything except the Hilbert space dimension. See [32] for details. When these properties hold we say the cluster satisfies the *unique syndrome condition*.

²We assume that interactions only occur between qubits whose corresponding vertices are connected; more general interaction topologies may be studied using similar techniques to those described here.

This argument can also be generalized in other ways. Observe that if H is to be nondegenerate, then no qubit can be isolated, i.e., every qubit must interact with at least one other qubit through H . Suppose the graph is such that we can find a qubit v with the following property: for all possible interaction terms $\sigma \otimes \tau$ between v and other qubits the syndrome vector $n^{\sigma,\tau}$ is unique among *all* the possible syndromes $n^{\sigma',\tau'}$. Once again, it is clear that under these conditions $H|C\rangle$ must contain nonzero terms orthogonal to $|C\rangle$, and thus $|C\rangle$ cannot be an eigenstate. We say that a vertex v with these properties satisfies the *unique syndrome condition*. To establish that a cluster can not arise as a ground state it therefore suffices to show that there is at least one vertex satisfying the unique syndrome condition.

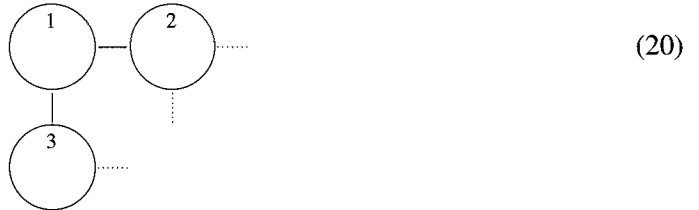
For which cluster geometries is there a vertex satisfying the unique syndrome condition? In a linear cluster it is not difficult to verify that the unique syndrome condition does not hold for any vertex v , and thus these techniques do not give any insight into whether or not such clusters can arise as the ground state. To see this, consider a segment of three cluster qubits:



Using the stabilizer arguments above we see that ZII and IXZ give rise to the same syndrome, and thus $ZII|C\rangle = IXZ|C\rangle$ (up to a global phase), and so neither the second nor the third vertex can satisfy the unique syndrome condition. A similar argument holds for other vertices in a linear cluster.

The situation changes if we move to two-dimensional clusters. For example, if we consider a toric cluster, then computation of all the possible cases shows that for any vertex v and for any interaction terms $\sigma \otimes \tau$ between v and other qubits the syndrome vector $n^{\sigma,\tau}$ is unique among *all* the possible syndromes $n^{\sigma',\tau'}$. It follows that the distance between the cluster state and the nondegenerate ground state of a two-body Hamiltonian whose couplings respect the cluster topology is bounded below by a constant.

For rectangular lattices the situation changes because of the boundary. Consider the cluster



A computation shows $X_1Z_2I_3$ has the same syndrome as $I_1I_2Z_3$, and so our conditions cannot hold for all vertices. However, if we consider a vertex v in the interior, then case enumeration shows that for any interaction $\sigma \otimes \tau$ between v and other qubits the syndrome $n^{\sigma,\tau}$ is unique among *all* possible syndromes $n^{\sigma',\tau'}$. Thus the unique syndrome condition holds for this vertex, and so this cluster cannot

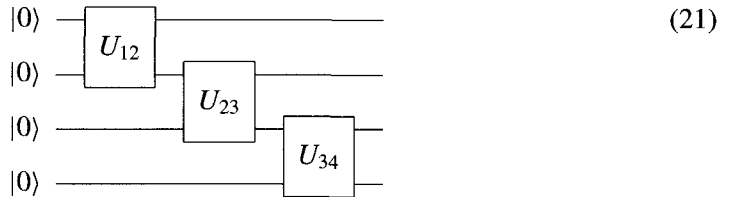
arise as the nondegenerate ground state of a two-body Hamiltonian whose couplings respect the cluster topology.

Similar computations may be carried out for a wide variety of clusters. Consideration of some examples shows that, generically, the clusters arising in simulations of non-trivial multi-qubit quantum circuits cannot be nondegenerate ground states. However, the question of obtaining a general classification of which clusters satisfy these conditions is still open. More generally, it would be of great interest to develop a general understanding of which clusters can and cannot arise as ground states of physically reasonable Hamiltonians. Note that when the use of ancilla qubits is allowed, the techniques of [34] may be used to obtain any cluster state as an approximate nondegenerate ground state of a reasonable Hamiltonian. However, these techniques have the disadvantage that the resulting gap to the first excited state may be very small, and so the cluster state may not be stable to thermal fluctuations.

4.2. Linearly assembled quantum states can be efficiently simulated on a classical computer

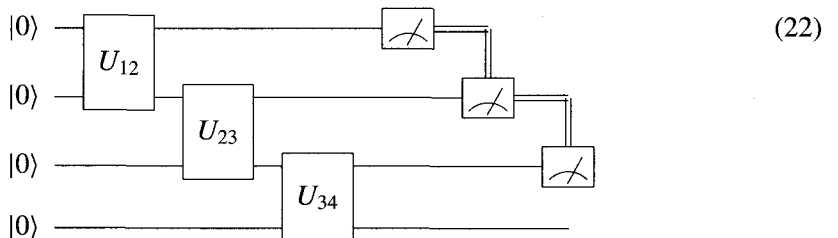
In this subsection we investigate what makes cluster states useful substrates for quantum computation. We show that spatial dimension plays a role, proving that quantum states which can be linearly prepared in one dimension can always be simulated efficiently on a classical computer, and thus are not useful for quantum computation.

By a *linearly preparable* quantum state we mean a state $|\psi\rangle$ that can be prepared using a circuit of the form

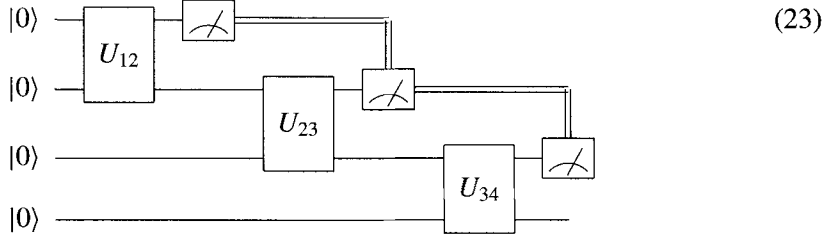


i.e. a cascaded sequence of two-qubit quantum gates applied to some product starting state. It is easy to show that the two-dimensional cluster states we have been using are not linearly preparable.

Suppose we perform a sequence of quantum measurements on a linearly assembled quantum state, e.g.

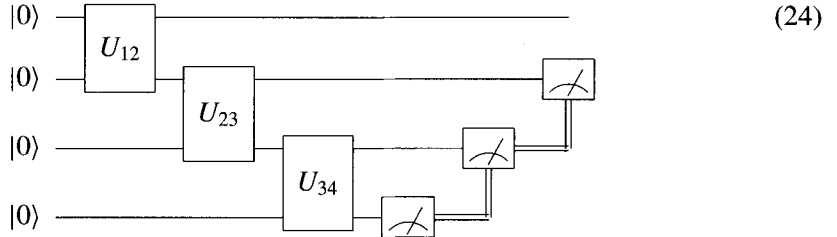


where earlier measurement results may be used to control later measurement bases. Note that the measurement gates above may be in any single-qubit basis, not just the computational basis. This is equivalent to the following circuit:



It is easy to use a classical computer to simulate such a circuit. First, we consider the result of applying U_{12} to $|00\rangle$, and compute the probabilities for the measurement on qubit 1. We then sample from this distribution to produce a posterior state for qubit 2, which is used as an input for U_{23} . We then repeat this cycle of computing probabilities, sampling, and computing posterior states. In order that the overall result be accurate, it suffices to carry out computations to $O(\log(1/n))$ bits of precision, and thus the entire computation can be carried out using $O(n \log^c(1/n))$ operations, where c is some constant arising from the need to multiply floating point numbers. Thus, efficient classical simulation of such a computation can be performed.

What happens if we measure the qubits in some other order, e.g.,



An elaboration of our earlier argument takes care of this case, too. Define ρ_j to be the state of the j th qubit after $U_{j-1,j}$ has been applied, but before $U_{j,j+1}$ has been applied. Using an argument similar to that earlier, it is not difficult to determine ρ_j for all j .

Suppose there are n qubits involved; in our example, $n = 4$. When we measure the n th qubit we induce trace-decreasing operations $\mathcal{E}_{n,0}$ and $\mathcal{E}_{n,1}$ on qubit $n - 1$, corresponding to the two possible measurement outcomes. These operations can be computed in a compact form using standard methods (see, e.g., [1]). By computing the trace of these operations applied to ρ_{n-1} we can simulate the measurement statistics on the n th qubit.

To simulate the measurement on the $(n - 1)$ th qubit, we first compute the two possible trace-decreasing operations $\mathcal{E}_{n-1,0}$ and $\mathcal{E}_{n-1,1}$ describing the change in state of qubit $n - 2$, conditional on the two possible measurement outcomes on qubit $n - 1$. We now simulate the measurement statistics on the $(n - 1)$ th qubit by computing the

trace of these operations applied to ρ_{n-2} , renormalizing according to the probability of the measurement outcome obtained on the n th qubit. Iterating this procedure, we can simulate all the different measurement outcomes using a classical computer. In order to be accurate, computations are carried out to $O(n)$ bits of accuracy, and so this procedure introduces a time overhead which is polynomial in n , and so is efficient.

This efficient classical simulation procedure can easily be generalized to a sequence of measurements performed in any order on the qubits, including adaptive orderings. Furthermore, it is straightforward to extend these results to some simple variants on the linear topology, including rings, and a small (e.g. constant) number of interlinking rings.

It remains an interesting open problem to determine what class of states can be used as a substrate for quantum computation. The examples in this subsection indicate that the geometry underlying the preparation procedure plays a key role. It would be interesting to develop a better understanding of what that role is, and what, if anything, that tells us about the physical properties responsible for the power of quantum computing.

5. Conclusion

We have described the basic ideas behind the quantum circuit and cluster-state models of quantum computation, including the proof of the remarkable fact that measurements on a cluster state can be used to simulate the unitary operations at the heart of the quantum circuit model. We have also illustrated the cluster state model with some simple observations about two questions of fundamental interest: (a) can the cluster state arise as the ground state of a naturally occurring Hamiltonian; and (b) what properties make the cluster state a useful substrate for quantum computation? Our results illustrate the rich structure of the cluster-state model, and emphasize the importance of further investigations of this structure.

Acknowledgements

It is a pleasure to dedicate this paper to Tony Bracken. As a student, I had the good fortune to receive Tony's supervision for an Honours project on quasi-distribution functions in quantum mechanics. That project combined in a pleasing way fundamental physical questions with simple yet beautiful and sometimes surprising mathematics. I hope the present subject offers something of the same character to readers.

Thanks to Sean Barrett, Hans Briegel, Andrew Doherty, Jens Eisert, Daniel Gottesman, Henry Haselgrove, Charles Hill, David Mermin, and Tim Ralph for helpful comments, and to Steve Flammia and Bryan Eastin for adding cluster state support to their \LaTeX "Qcircuit" package, which was used to produce the figures in this paper. The results on efficient classical simulation of linearly prepared states were obtained jointly with Andrew Doherty, and I thank Andrew for permission to include them here.

REFERENCES

- [1] M. A. Nielsen and I. L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge 2000.
- [2] R. Raussendorf and H. J. Briegel: *Phys. Rev. Lett.* **86** (2001), 5188.
- [3] R. Raussendorf, D. E. Browne and H. J. Briegel: *J. Mod. Opt.* **49** (2002), 1299.
- [4] M. A. Nielsen: *Phys. Rev. Lett.* **93** (2004), 040503.
- [5] D. E. Browne and T. Rudolph: *Resource-efficient linear optical quantum computation*, quant-ph/0405157.
- [6] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger: *Nature* **434** (2005), 169.
- [7] M. A. Nielsen: *Phys. Lett. A* **308** (2003), 96.
- [8] D. W. Leung: *Two qubit projective measurements are universal for quantum computation*, quant-ph/0111122.
- [9] D. W. Leung: *Quantum computation by measurements*, quant-ph/0310189.
- [10] P. Aliferis and D. W. Leung: *Computation by measurements: a unifying picture*, quant-ph/0404082.
- [11] A. M. Childs, D. W. Leung and M. A. Nielsen: *Unified derivation of measurement-based schemes for quantum computation*, quant-ph/0404132.
- [12] P. Jorrand and S. Perdrix: *Unifying quantum computation with projective measurements only and one-way quantum computation*, quant-ph/0404125.
- [13] T. Rudolph and S. S. Virmani: *A relational quantum computer using only two-qubit total spin measurement and an initial supply of highly mixed single qubit states*, quant-ph/0503151.
- [14] P. Aliferis and D. W. Leung: *Fault-tolerant quantum computation with graph states*, quant-ph/0503130.
- [15] V. Danos, E. Kashefi and P. Panangaden: *The measurement calculus*, quant-ph/0412135.
- [16] M. Mhalla and S. Perdrix: *Complexity of graph state preparation*, quant-ph/0412071.
- [17] M. A. Nielsen and C. M. Dawson: *Fault-tolerant quantum computation with cluster states*, quant-ph/0405134.
- [18] S. Perdrix and P. Jorrand: *Measurement-based quantum Turing machines and their universality*, quant-ph/0404146.
- [19] F. Verstraete and J. I. Cirac: *Phys. Rev. A* **70** (2004), 060302(R).
- [20] S. D. Barrett and P. Kok: *Efficient high-fidelity quantum computation using matter qubits and linear optics*, quant-ph/0408040.
- [21] G. D. Hutchinson and G. J. Milburn: *J. Mod. Opt.* **51** (2004), 1211.
- [22] R. Raussendorf and H. J. Briegel: *J. Mod. Opt.* **49** (2002), 1299.
- [23] R. Raussendorf, D. E. Browne and H. J. Briegel: *Phys. Rev. A* **68** (2003), 022312.
- [24] D. Deutsch: *Proc. R. Soc. Lond. A* **425** (1989), 73.
- [25] J. L. Brylinski and R. Brylinski: *Universal quantum gates*, chapter II in [35], Chapman & Hall, CRC Press, 2002.
- [26] E. Knill: *Approximating quantum circuits*, quant-ph/9508006.
- [27] M. A. Nielsen: Journal club notes on cluster-state quantum computation, <http://www.qinfo.org/qc-by-measurement>.
- [28] R. Raussendorf and H. J. Briegel: *Phys. Rev. Lett.* **85** (2001), 910.
- [29] X. Zhou, D. W. Leung and I. L. Chuang: *Phys. Rev. A* **62** (2000), 052316.
- [30] A. Einstein, B. Podolsky and N. Rosen: *Phys. Rev.* **47** (1935), 777.
- [31] E. Knill: *Thresholds for linear optics quantum computation*, quant-ph/0006120.
- [32] H. L. Haselgrove, M. A. Nielsen and T. J. Osborne: *Phys. Rev. Lett.* **91** (2003), 052311.
- [33] D. Gottesman: *Stabilizer codes and quantum error correction*, Ph.D. thesis, California Institute of Technology, Pasadena 1997.
- [34] J. Kempe, A. Kitaev and O. Regev: *The complexity of the local Hamiltonian problem*, in Proc. 24th FSTTCS, page 373, 2004.
- [35] R. K. Brylinski and G. Chen (eds.): *Mathematics of Quantum Computation*, Computational Mathematics, Chapman & Hall, CRC Press, 2002.