Open access • Journal Article • DOI:10.1103/PHYSREVA.71.032318

Unified derivations of measurement-based schemes for quantum computation

Andrew M. Childs, Andrew M. Childs, Debbie Leung, Michael A. Nielsen ...+1 more authors

Institutions: Massachusetts Institute of Technology, California Institute of Technology, University of Queensland

Published on: 17 Mar 2005 - Physical Review A (American Physical Society)

Topics: Quantum computer and Qubit

Unified derivations of measurement-based schemes for quantum computation

Andrew M. Childs,[1,2,*] Debbie W. Leung,[1,†] and Michael A. Nielsen[1,3,‡]
[1]*Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125, USA*
[2]*Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[3]*School of Physical Sciences and School of Information Technology & Electrical Engineering, The University of Queensland, QLD 4072, Australia*
(Received 1 July 2004; published 17 March 2005)

We present unified, systematic derivations of schemes in the two known measurement-based models of quantum computation. The first model (introduced by Raussendorf and Briegel, [Phys. Rev. Lett. **86**, 5188 (2001)]) uses a fixed entangled state, adaptive measurements on single qubits, and feedforward of the measurement results. The second model (proposed by Nielsen, [Phys. Lett. A **308**, 96 (2003)] and further simplified by Leung, [Int. J. Quant. Inf. **2**, 33 (2004)]) uses adaptive two-qubit measurements that can be applied to arbitrary pairs of qubits, and feedforward of the measurement results. The underlying principle of our derivations is a variant of teleportation introduced by Zhou, Leung, and Chuang, [Phys. Rev. A **62**, 052316 (2000)]. Our derivations unify these two measurement-based models of quantum computation and provide significantly simpler schemes.

DOI: 10.1103/PhysRevA.71.032318 PACS number(s): 03.67.Lx, 03.65.Ta

I. INTRODUCTION

What physical resources are needed to simulate the evolution of an arbitrary physical system? In the context of information processing, the ability to perform *universal* computation is equivalent to the ability to simulate an arbitrary evolution—any computation is performed by evolving a computing machine, and conversely, a universal computing machine can be used to simulate the evolution of any system.

In the standard quantum circuit model of quantum computation [1–3], a quantum computation involves initializing quantum systems—typically *qubits* or two-level quantum systems—that are then acted on by a sequence of *quantum gates*, followed by some measurements. In this model, simple quantum gates (say, acting on one or two qubits at a time) can be used to build up an *arbitrary* unitary transformation. Nonunitary evolution such as dissipation can also be simulated in this model by introducing and later discarding ancilla qubits.

Since measurement is generally irreversible, until recently the conventional wisdom has held that the processing of quantum information should be kept coherent and measurements should be delayed until the final readout of computation results. A notable exception to this rule of thumb is quantum teleportation [4], in which a measurement by one party determines the correction that a remote party should apply to recover a quantum state. Another notable exception is the use of syndrome measurements in quantum error correction [5]. Syndrome measurements reveal the error that has occurred without measuring the encoded quantum state, thereby preserving its coherence. Indeed, there are many approaches to fault-tolerant quantum computation in which measurements and simple quantum gates are used to implement other quantum gates that are difficult to apply directly [6–12].

Raussendorf and Briegel [13] overturned this conventional wisdom, showing that it is possible to perform universal quantum computation using a *sequence of single-qubit measurements alone*, acting on some fixed entangled state called a *cluster state* [14]. Once the cluster state is prepared, no further interactions are required, and the only aspect of the computation that must remain coherent is the storage of quantum information. More precisely, *any* quantum circuit up to depth d and breadth b may be simulated using a single, fixed cluster state of $O(bd)$ qubits. Each simulation of a quantum gate is successful up to an additional known Pauli error. Since the act of measuring the cluster state is irreversible, this model is referred to as the *one-way quantum computer* (1WQC) model.

After the 1WQC was introduced, a very different measurement-based scheme for quantum computation was introduced by one of us [15], following the line of thought developed in [16,9,11]. We will refer to this model as a *teleportation-based model of quantum computation* (TQC), since it is conceptually derived from teleportation. The TQC uses similar physical resources to the 1WQC: (multiple-qubit) measurements, quantum memory, and feedforward. The initial TQC scheme proposed in [15] uses four-qubit measurements. It also requires a nondeterministic number of steps to perform each quantum gate. Simpler TQC schemes were later proposed [17–19], with the simplest using only two-qubit measurements and performing each gate deterministically (up to a known Pauli error).

The TQC is easy to understand since it is similar to the standard model of quantum computation. In comparison, the conceptual basis for the 1WQC is less clear. The prescriptions given in [13,20] for using a 1WQC can be easily verified, but there is no clear underlying principle. This makes it nontrivial to modify or optimize the existing 1WQC

*Email address: amchilds@cs.caltech.edu
†Email address: wcleung@cs.caltech.edu
‡Email address: nielsen@physics.uq.edu.au

schemes. It is also unclear what makes the cluster state a good substrate for quantum computation, and more generally, what makes a good or bad substrate. Finally, the 1WQC formalism is heavily based on the stabilizer language developed by Gottesman [21]. Although this language is powerful, it is also rather specialized, being limited primarily to the analysis of situations in which operations from a special set—the Clifford group—are being applied. Furthermore, the connection between the stabilizer language and the corresponding picture in terms of state vectors is not always straightforward.

On the other hand, the 1WQC has important advantages over the TQC. First, no quantum interactions are required after the initial preparation of the cluster state. Second, the cluster state is independent of the computation to be performed, except for its breadth and depth: arbitrary interactions can be extracted from the fixed cluster state. Third, there may be physical systems in which a cluster state offers experimental advantages over more conventional approaches [14,22].

Our initial goal in undertaking the research reported here was to identify simple underlying principles for the 1WQC and to systematically derive schemes similar to the proposed 1WQC. We eventually found such a systematic derivation using teleportation as an underlying principle [23], in accord with the conjecture that the 1WQC and the TQC are closely related. Our improved conceptual understanding of the 1WQC proved valuable, for we subsequently found much simpler 1WQC-like schemes [24] by choosing a simpler underlying principle, known as "one-bit teleportation" [10]. Such simplification is reminiscent of the work in [10], which simplifies the systematic fault-tolerant gate construction proposed in [9]. We then realized that one-bit teleportation also simplifies schemes in the TQC model [25].

We have therefore unified the 1WQC and the TQC models and obtained simplified measurement-based quantum computation schemes. The 1WQC schemes we derive combine the conceptual simplicity of the TQC with the practical advantages of the 1WQC. We have also identified one-bit teleportation as a single principle underlying both approaches to measurement-based quantum computation.

During the course of our investigation and preparation of the manuscript, several related results have been reported. A different explanation of the 1WQC model in terms of valence bond solids was reported by Verstraete and Cirac [26]. Whereas our 1WQC-like schemes differ from the original schemes of [13,20], an exact explanation of the latter in terms of teleportation was given by Aliferis and one of us [27]. A partial explanation of the 1WQC model in terms of one-bit teleportation was reported very recently by Jorrand and Perdrix [28], while schemes similar to our simplified TQC schemes were independently reported by Perdrix [29]. One of us has combined the 1WQC model with linear optics [22]. Several results announced after our initial posting may also be of interest. These include a model of measurement-based universal quantum Turing machines [30], a more efficient method to combine the 1WQC with linear optics [31], and a new fault-tolerance study in the 1WQC [32].

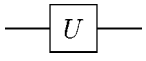
The structure of the paper is as follows. We begin in Sec. II by briefly reviewing the circuit model, introducing a notion of circuit simulation with Pauli errors, and describing the TQC and 1WQC models of quantum computation in more detail. We emphasize some conceptual ideas that may be useful elsewhere. Section III reviews one-bit teleportation and presents useful techniques obtained from it. The techniques are used to derive a simplified TQC scheme in Sec. IV A. Section IV C explains how one-bit teleportation can be used to derive a scheme that simulates arbitrary circuits using a circuit-dependent entangled initial state, single-qubit measurements, and feedforward. Section IV D explains several techniques to remove the dependence of the initial state on the circuit being simulated (except for its breadth and depth). We conclude the paper in Sec. V. Our initial systematic derivation of 1WQC-like schemes based on teleportation can be found in [23].

II. THE QUANTUM CIRCUIT MODEL, THE TQC, AND THE 1WQC

In this section, we summarize the circuit model of quantum computation as a way of introducing the notation used throughout the paper. We describe a notion of circuit simulation that is crucial to our discussion. Then, we outline the main features of the TQC and the 1WQC that motivate our derivation. Since we derive simplified TQC and 1WQC schemes, a full summary of the existing schemes will be omitted. Finally, we describe a diagrammatic representation of the 1WQC, which we call the *substrate representation*.

A. The quantum circuit model

Any unitary evolution can be built from simple quantum gates (say, acting on one or two qubits at a time). A circuit diagram represents a partially ordered set of unitary evolutions and measurements. The input states and measurement outcomes may be included. In a circuit diagram, time runs from left to right. Each horizontal line represents quantum information propagating forward in time, or equivalently, quantum storage. Often, each line represents one qubit of quantum information. A unitary gate is represented by a box on the line(s), and a symbol for the gate is written inside the box. Thus, the circuit symbol for a single-qubit gate U is given by



(1)

In the basis $\{|0\rangle,|1\rangle\}$, the matrix representations of some useful single-qubit gates are given by

$$X_\theta = e^{-i\theta X}, \quad Z_\theta = e^{-i\theta Z}, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{2}$$

where I, X, Y, Z are used to represent the Pauli operators

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3}$$

The action of the Pauli operators on each qubit generates a group, called the Pauli group. The Clifford group consists of those unitary operators that preserve the Pauli group by conjugation. For example,

$$HXH = Z, \quad HZH = X. \tag{4}$$

The only two-qubit gates we will use are within the Clifford group—for example, the *controlled-phase* and the *controlled*-NOT gates. They are denoted by $\Lambda(Z)$ and $\Lambda(X)$ respectively, and their circuit symbols are given by

$\Lambda(Z)$: $\Lambda(X)$: (5)

The target of $\Lambda(X)$ is taken to be the second qubit. The "upside down" controlled-NOT with the first qubit as the target is denoted by $V(X)$. In contrast, $\Lambda(Z)$ is symmetric between the two qubits, as is evident in the notation of Eq. (5). In the basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$, the matrix representations of $\Lambda(Z)$ and $\Lambda(X)$ are given by

$$\Lambda(Z) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \Lambda(X) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{6}$$

We will repeatedly use the following identities involving $\Lambda(X)$ and $\Lambda(Z)$:

$$(I \otimes H)\Lambda(Z)(I \otimes H) = \Lambda(X), \tag{7}$$

$$(H \otimes H)\Lambda(X)(H \otimes H) = V(X), \tag{8}$$

$$\Lambda(Z)(X \otimes I)\Lambda(Z) = X \otimes Z, \tag{9}$$

$$\Lambda(Z)(Z \otimes I)\Lambda(Z) = Z \otimes I, \tag{10}$$

$$\Lambda(X)(X \otimes I)\Lambda(X) = X \otimes X, \tag{11}$$

$$\Lambda(X)(I \otimes X)\Lambda(X) = I \otimes X, \tag{12}$$

$$\Lambda(X)(Z \otimes I)\Lambda(X) = Z \otimes I, \tag{13}$$

$$\Lambda(X)(I \otimes Z)\Lambda(X) = Z \otimes Z. \tag{14}$$

Equation (7) shows that $\Lambda(Z)$ and $\Lambda(X)$ differ only by the action of single-qubit unitary gates. Given the ability to perform single-qubit unitaries, either $\Lambda(Z)$ or $\Lambda(X)$ is universal for quantum computation.

We only consider *projective* measurements, since using generalized measurements trivializes the problem. A projective measurement can be specified by orthogonal subspaces of the measured Hilbert space: the measurement projects the state onto one subspace and outputs the subspace label. Common ways to specify a measurement include a partition of a basis or the eigenspaces of a Hermitian operator. Throughout the paper, a measurement of a Hermitian operator O is denoted by M_O.

A single-qubit measurement along the computational basis $\{|0\rangle,|1\rangle\}$ is equivalent to M_Z. It has the circuit symbol

j (15)

Throughout the paper, a double line coming out of a measurement box represents the classical measurement outcome, and a single line represents the postmeasurement quantum state. A single-qubit measurement along the basis $\{U^\dagger|0\rangle, U^\dagger|1\rangle\}$ (U unitary) is equivalent to $M_{U^\dagger ZU}$, which is equivalent to the sequence of operations U, M_Z, and finally $U^\dagger$ on the post-measurement quantum state. Whenever the post-measurement quantum state is irrelevant, the measurement is simply depicted as

U (16)

and conversely, we identify subcircuits of the form given by Eq. (16) as single-qubit measurements.

In addition to complete two-qubit measurements, we will also use *incomplete* two-qubit measurements. For example, $M_{Z\otimes Z}$ measures the parity defined in the computational basis. As another example, $M_{U^\dagger ZU\otimes Z}$ is equivalent to the sequence of operations $U\otimes I$, $M_{Z\otimes Z}$, and $U^\dagger \otimes I$.

We will often encounter a measurement of the form

U, V, H, $V^\dagger$, j (17)

where U,V are arbitrary single-qubit gates. The classical outcome j corresponds to the measurement of $(U^\dagger XU)\otimes(V^\dagger ZV)$, because $(H\otimes I)\Lambda(Z)(U\otimes V)$ maps the ±1 eigenspace of $(U^\dagger XU)\otimes(V^\dagger ZV)$ onto the ±1 eigenspace of $Z\otimes I$. However, $M_{(U^\dagger XU)\otimes(V^\dagger ZV)}$ does not give rise to the correct postmeasurement quantum state in Eq. (17). This requires an extra measurement $M_{U^\dagger ZU}$ on the first qubit and an extra gate $(V^\dagger ZV)^k$ on the second qubit if the outcome of $M_{U^\dagger ZU}$ is k. In other words, the following circuit is *equivalent* to Eq. (17):

$M_{(U^\dagger XU)\otimes(V^\dagger ZV)}$, j, $M_{U^\dagger ZU}$, k, $V^\dagger Z^k V$ (18)

where double-lined boxes are used to represent the measurements.

We emphasize that it is useful to view a circuit as an abstract representation of the evolution of quantum or classical information. A quantum circuit is often used to represent physical registers and transformations, but such association is not generally necessary, as is manifest in our discussion of circuit simulations in the next section.

B. Circuit simulation with Pauli errors

We now describe a notion of circuit simulation useful in the 1WQC and the TQC models. Most measurements in the TQC and 1WQC models output random outcomes and induce Pauli errors that are known functions of the measurement outcome. However, the presence of such known errors

is not a hindrance to the computation, provided subsequent measurements are adapted accordingly. Since our schemes share the same feature, it is useful to introduce some conventions that simplify later discussions of simulation.

A quantum circuit consists of ancilla preparations, gates, and measurements endowed with a partial time-ordering. We can group together operations that can be performed in parallel in a time step, although the grouping may not be unique. The minimal number of time steps is called the *logical depth* of the circuit. For each grouping of $\mathcal{C}$, an input state $|\psi_0\rangle$ specifies a sequence of quantum states $\{|\psi_i\rangle\}$ where $|\psi_i\rangle$ is the quantum state at the end of the ith time step of the computation. We say that a circuit $\mathcal{C}'$ *simulates* $\mathcal{C}$ *with Pauli errors* if there is a grouping of $\mathcal{C}$ so that, for any input state $|\psi_0\rangle$ and any given Pauli error P, applying $\mathcal{C}'$ on the input $P|\psi_0\rangle$ produces a sequence of states $P_i|\psi_i\rangle$ where P_i are known Pauli errors. These Pauli errors redefine the intermediate states and the final measurement outcomes, but do not affect the intended computation. From now on, we will simply say that $\mathcal{C}'$ *simulates* $\mathcal{C}$ to mean that $\mathcal{C}'$ simulates $\mathcal{C}$ with Pauli errors. As a simple example, a unitary gate simulates the identity if and only if it is in the Pauli group. As a second example, a unitary gate simulates itself if and only if it is in the Clifford group.

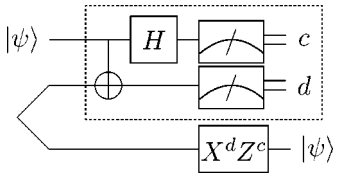
Our notion of simulation is defined to ensure an important property—circuit simulation is preserved under the composition of circuits. Therefore, to simulate a circuit, it suffices to compose simulations of individual circuit elements. Universality can then be proved by showing how to efficiently simulate all possible circuit elements required for universal quantum computation. Furthermore, even though a circuit element may act on part of an entangled state, it is sufficient to verify the simulation of a circuit element for all possible pure state inputs.

In the context of measurement-based quantum computation, initial (or ancilla) state preparation and read out of computation results can be simulated as follows. We will only need initial states that can be prepared by a simple measurement, up to known Pauli errors. For example, measuring a single qubit in the computational basis with outcome $d \in \{0,1\}$ results in the state $X^d|0\rangle$. Similarly, a measurement of two qubits in the Bell basis produces a singlet state up to a known Pauli error. Throughout the paper, we suppress the known Pauli errors in the ancillas whenever their effects are straightforward, so as to keep the discussion and the simulation circuits simple. We also omit physically irrelevant global phase factors that arise from the composition of Pauli errors. We restrict our attention to measurements that are deterministically affected by known Pauli errors, so that the actual outcomes and the knowledge of the Pauli errors can be used to determine the Pauli-error-free measurement outcomes. For example, the result of a measurement in the computational basis is simply flipped by an X error and unaffected by a Z error. Now, it suffices to focus on simulating a universal set of unitary gates in the measurement-based model of quantum computation.

C. The TQC model

In this section, we review some elements of the TQC. Our review follows the simplified approach of [19], which allows the computation to proceed with a deterministic number of steps. The universality of the TQC model follows from the ability to simulate any single-qubit gate U and a two-qubit gate such as $\Lambda(X)$.

The crucial ingredient of the simulation is teleportation [4], which transmits a qubit $|\psi\rangle$ using the following circuit:



(19)

When two qubits are connected on the left side of a circuit diagram, as the bottom two qubits are in Eq. (19), they denote a two-qubit maximally entangled state $|\Phi_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. The dashed box performs a *Bell measurement* along the basis

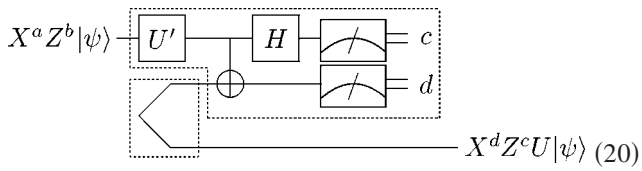
$$|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Phi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

The teleportation circuit can be verified by rewriting the initial state $|\psi\rangle|\Phi_{00}\rangle$ as $\frac{1}{2}\Sigma_{c,d}|\Phi_{cd}\rangle \otimes (Z^cX^d|\psi\rangle)$.

The teleportation circuit, Eq. (19), simulates the identity gate (in the sense described in Sec. II B). In fact, it does so even when the postmeasurement correction X^dZ^c is omitted: for any input state $X^aZ^b|\psi\rangle$, the output from the teleportation circuit without correction is simply $X^{a+d}Z^{b+c}|\psi\rangle$ (up to a global phase, as is our convention throughout the paper). From now on, Pauli corrections are always omitted in what we call teleportation.

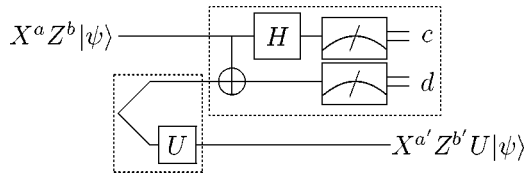
Suppose we want to simulate a single-qubit gate U. Consider a circuit in which we apply the gate $U' = UZ^bX^a$ to the input state $X^aZ^b|\psi\rangle$ and perform teleportation on the resulting state $U|\psi\rangle$. Following Eq. (19), the output quantum state of the circuit is $X^dZ^cU|\psi\rangle$. In other words, the following circuit simulates U:



(20)

The circuit in Eq. (20) can be divided into subcircuits, each of which can be simulated by a single two-qubit measurement. The first subcircuit (the dashed box in the lower left corner) is just the preparation of the state $|\Phi_{00}\rangle$. It can be simulated by a single Bell measurement, up to a Pauli error. The rest of the circuit, $(U' \otimes I)$ followed by a Bell measurement, is just a two-qubit measurement along a rotated Bell basis $\{(U'^{\dagger} \otimes I)|\Phi_{cd}\rangle\}$. Composing these two measurements provides a simulation of Eq. (20), and thus a simulation of U, in the TQC model.

An alternative simulation is applicable to gates in the Clifford group [9]:



(21)

The above is simply a simulation of the identity by teleportation followed by a simulation of U by itself. More specifically, the above circuit teleports the input state $X^a Z^b|\psi\rangle$ to produce the state $X^{a+d} Z^{b+c}|\psi\rangle$, and then applies the gate U. The output state is thus $UX^{a+d} Z^{b+c}|\psi\rangle$. Using the fact U is in the Clifford group, the output state can be rewritten as $X^{a'} Z^{b'} U|\psi\rangle$ for known a',b'.

The simulation of two-qubit gates is similar to that depicted in Eqs. (20) and (21). We omit the details of the existing simulation schemes, and we refer the interested reader to [19]. Instead, we will present a simplified simulation in Sec. IV A.

Comparing Eqs. (20) and (21), the latter simulation has a simpler teleportation measurement but a more complicated initial state $(I \otimes U)|\Phi_{00}\rangle$. This tradeoff is useful in the simulation of two-qubit gates in the Clifford group.

Note that in the TQC model we assume the ability to apply measurements to any subset of the qubits, without worrying about the respective locations of those qubits, just as in the circuit model. The TQC is simply a method for implementing each gate in the circuit model by a sequence of measurements.

D. The one-way quantum computer model

Since we will present a simple systematic derivation of 1WQC-like schemes, we omit the details of the existing 1WQC schemes, and refer interested readers to the ingenious schemes discussed in [13,20,33,34]. Instead, we focus on features of the 1WQC that differ from the TQC model.

The 1WQC is based on an input state known as the *cluster state* [14]. The cluster state consists of a two-dimensional square lattice of qubits. To simulate a computation of n qubits with logical depth m, the lattice is chosen to be of size $O(n) \times O(m)$. One way of defining the cluster state is as the result of a two-stage preparation procedure: (i) prepare all lattice sites in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and (ii) apply $\Lambda(Z)$ between each pair of qubits that are adjacent in the lattice. Since the $\Lambda(Z)$ operations all commute, it does not matter in what order they are applied. Note that this prescription is merely a convenient way of defining the cluster state, and there is no need to actually prepare it by following these steps.

The cluster states naturally generalize to *graph states*, for which an arbitrary graph defines the adjacency relation [34–36]. We will use a feature of any graph state called the *deletion principle*. When one of the qubits is measured in the computational basis, the unmeasured qubits will be left in a different graph state (up to known Pauli errors) corresponding to the graph obtained by deleting the measured qubit from the original graph.

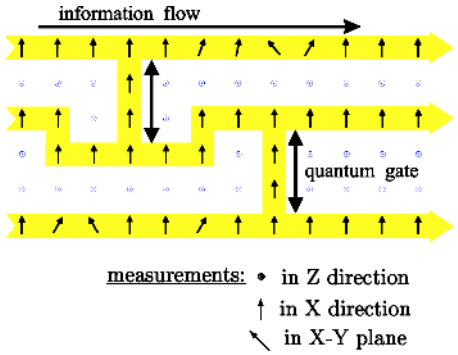


FIG. 1. A schematic diagram of a 1WQC computation. Figure courtesy H. J. Briegel and R. Raussendorf.

In the 1WQC model, once the cluster state is prepared, an *arbitrary* circuit $\mathcal{C}$ can be simulated using only single-qubit measurements. The first step is to "imprint" the circuit $\mathcal{C}$ onto the cluster state by deleting qubits from the lattice to obtain some graph state that depends on $\mathcal{C}$. Roughly speaking, this graph consists of horizontal lines of vertices, each line corresponding to a qubit in $\mathcal{C}$, and vertical edges connecting neighboring lines corresponding to interactions between the simulated qubits. The qubits in the graph are then measured from the left to the right. Each measurement propagates quantum information from the measured qubit to its unmeasured right neighbor. In general, the measurement basis will depend on previous measurement outcomes. Each region of the graph is used to simulate a circuit element. Qubits entering a region from the left boundary carry the input state of the circuit element, and qubits exiting at the right boundary carry the output. When composing element-wise simulation in the 1WQC model, the output registers of one region have to match the input registers of the next region. A schematic diagram for a computation in the 1WQC model is given in Fig. 1.

Simulation of a circuit using the 1WQC is discussed in detail in [20]. The precise protocols and their verification are beyond the scope of this paper. Interpretations in terms of valence bond solids [26] and teleportation [27,37] have been reported recently. In this paper, the derivation is based on a different underlying principle and the schemes are significantly simpler than those discussed in [20].

E. The substrate representation

Circuit representations of a computation in the 1WQC model turn out to be rather unwieldy. Instead, we prefer to use a more concise "substrate representation" in which we label each vertex in the graph representing the cluster with the measurement to be performed. The measurement bases may depend on previous measurement outcomes, and this dependency should be indicated in the labeling. Note that the interdependence of the measurement outcomes and measurement bases specifies a partial order in which the qubits must be measured. An example of the substrate representation is Eq. (44), in Sec. IV C 2, which simulates the circuit in Eq. (39).

The substrate representation for simulating a certain circuit often visually resembles the simulated circuit [cf. Eq. (39)]. One can identify the different physical qubits that carry the propagating quantum state at different times with propagation of quantum information in time, and the various regions of the graph state corresponding to different quantum gates with the action of those gates themselves.

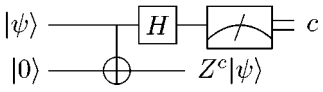
III. ONE-BIT TELEPORTATION AND SIMPLE SIMULATION CIRCUITS

All the measurement-based models of quantum computation share the common feature that measurements are not performed solely on the qubits storing the data. The reason is that doing so would destroy the coherence essential to quantum computation. Instead, ancilla qubits are prepared, and then measurements are used to interact the data with the ancilla. By choosing the measurements and initial states of the ancilla carefully, we can ensure that coherence is preserved. Even more remarkably, with suitable choices of ancilla and measurements, it is possible to effect a universal set of quantum gates.

In this section, we introduce two circuits that offer perhaps the simplest example of these principles in action, the one-bit teleportation circuits introduced in [10]. We will show how the one-bit teleportation circuits can be used to derive simulation circuits for a universal set of quantum gates. These simulation circuits are, again, based solely on measurements and interaction with an ancilla. In later sections, we will see that these simulation circuits can be used to derive both measurement-based models of quantum computation.

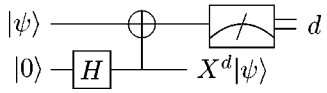
The one-bit teleportation circuits are as follows [10]:

Z-teleportation:



(22)

X-teleportation:

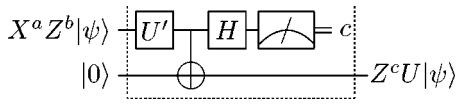


(23)

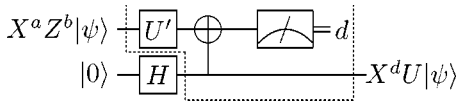
These circuits are analogous to teleportation in that they move a qubit from one register to another and simulate the identity operation. The circuits are named after the Pauli corrections required to fully recover the input state. The circuits are easily verified [10]. Note that the Z- and X-teleportation circuits can be interconverted by using the input state $H|\psi\rangle$ and applying Eqs. (4) and (8). Moreover, the teleportation circuit in Eq. (19) can be viewed as a composition of a Z-teleportation followed by an X-teleportation (by rewriting the state $|\Phi_{00}\rangle$ as $\Lambda(X)(H\otimes I)|00\rangle$). Thus, either one of Eqs. (22) or (23) alone can be viewed as a fundamental primitive from which all results due to Eqs. (19), (22), and (23) can be obtained.

We now derive from Eqs. (22) and (23) some useful simulation circuits for a universal set of gates. In subsequent sections, we will systematically derive schemes in the TQC and the 1WQC models using these simulation circuits.

Consider procedures analogous to the simulation circuits (20) and (21), but based on one-bit teleportation. To simulate a single-qubit gate U acting on an input state $|\psi\rangle$ with Pauli error X^aZ^b, a simulation circuit can consist of first applying $U'=UZ^bX^a$ before either form of one-bit teleportation:

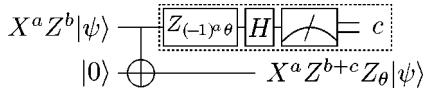


(24)



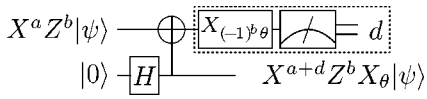
(25)

We will see that Eqs. (24) and (25) are most useful in the TQC model. In the 1WQC model, more specialized simulation circuits are required. To simulate the rotation Z_θ, our simulation circuit takes the input state $X^aZ^b|\psi\rangle$ and applies $Z_{(-1)^a\theta}$, followed by Z-teleportation. When the measurement outcome is c, the output state is $Z^cZ_{(-1)^a\theta}X^aZ^b|\psi\rangle$. Using the identity $X^aZ_{(-1)^a\theta}X^a=Z_\theta$, the output state is $X^aZ^{b+c}Z_\theta|\psi\rangle$. This is summarized in the circuit



(26)

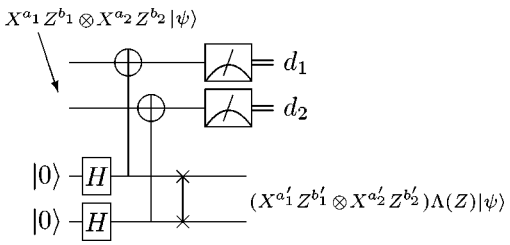
where we have commuted $\Lambda(X)$ and $Z_{(-1)^a\theta}$. Similarly, for the gate X_θ, consider a simulation circuit with an input state $X^aZ^b|\psi\rangle$, a gate $X_{(-1)^b\theta}$ applied to the input, followed by X-teleportation. When the measurement outcome is d, the output state is $X^dX_{(-1)^b\theta}X^aZ^b|\psi\rangle=X^{a+d}Z^bX_\theta|\psi\rangle$. This is summarized in the circuit



(27)

where we have commuted $\Lambda(X)$ and $X_{(-1)^b\theta}$.

Finally, we consider a simulation for $\Lambda(Z)$. One possible method is to simulate the identity on both inputs using X-teleportation followed by a self-simulation of $\Lambda(Z)$. More specifically, two X-teleportation circuits are applied to the two-qubit input $X^{a_1}Z^{b_1}\otimes X^{a_2}Z^{b_2}|\psi\rangle$, followed by applying $\Lambda(Z)$:

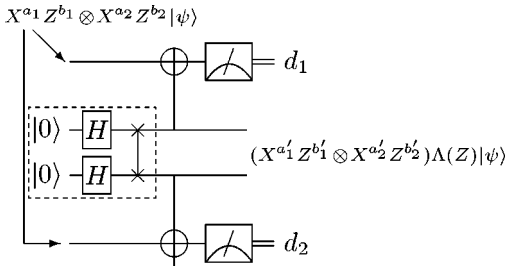


(28)

When the measurement outcomes of the two X-teleportation steps are d_1 and d_2, the output state of the circuit is $\Lambda(Z)(X^{a_1+d_1}Z^{b_1}\otimes X^{a_2+d_2}Z^{b_2})|\psi\rangle$. Using Eqs. (9) and (10), the output state is $(X^{a_1+d_1}Z^{b_1+a_2+d_2}\otimes X^{a_2+d_2}Z^{b_2+a_1+d_1})\Lambda(Z)|\psi\rangle$.

Thus in Eq. (28), $a_1'=a_1+d_1$, $b_1'=b_1+a_2+d_2$, $a_2'=a_2+d_2$, and $b_2'=b_2+a_1+d_1$.

We can derive useful simulation circuits from Eq. (28). Suppose we commute $\Lambda(Z)$ to the left of the controlled-NOTs, and reorder the qubits so that the second qubit from the top becomes the last:

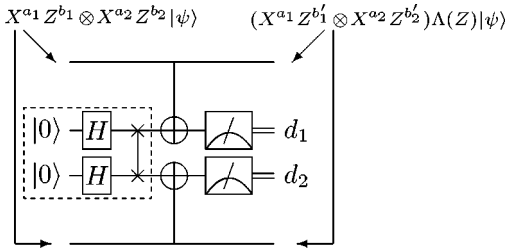


(29)

Furthermore, for the same input state, the following circuits produce the same outcomes and corresponding post-measurement states:

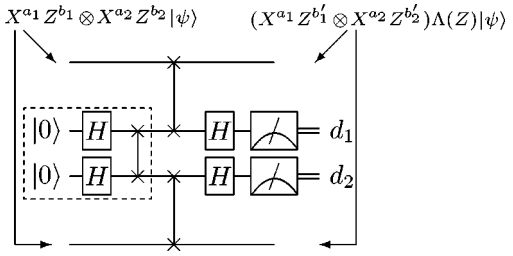
(30)

Thus Eq. (29) implies the following:



(31)

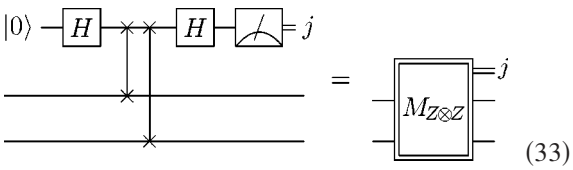
where, according to Eq. (30), the output X errors in Eq. (31) are obtained by adding d_1,d_2 to a_1',a_2' defined in Eq. (29). The results are simply a_1,a_2. Finally, rewrite both controlled-NOTs using Eq. (7), and note that the state in the dashed box in Eq. (31) is stabilized by $H\otimes H$, giving a "remote $\Lambda(Z)$" construction:



(32)

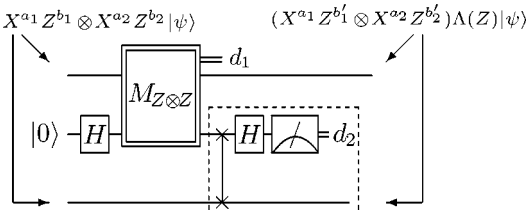
If we perform a remote controlled-NOT by performing H before and after the remote $\Lambda(Z)$ according to Eq. (7), we obtain the well-known remote $\Lambda(X)$ circuit due to Gottesman [38]. The current derivation is based only on composing the identity simulation (by one-bit teleportation) with self-simulation of the desired gate, and is different from the derivation in [10].

Our last simulation circuit for $\Lambda(Z)$ uses the standard (and easily-verified) result that the following circuit implements $M_{Z\otimes Z}$ on the two input qubits:



(33)

We can apply Eq. (33) to Eq. (32), and identify the operations involving the second qubit (from the top) in Eq. (32) as a two-qubit measurement on the first and third qubits. This gives a simulation circuit for $\Lambda(Z)$:



(34)

The operations in the dashed box can be implemented by $M_{X\otimes Z}$ followed by M_Z on the first qubit [see Eq. (18) in Sec. II A]. With this argument we have rederived Gottesman's remote controlled-NOT using a single-qubit ancilla and two two-qubit measurements [39], and shown that it is easily understood as a consequence of one-bit teleportation and the simple circuit identities (18) and (30).

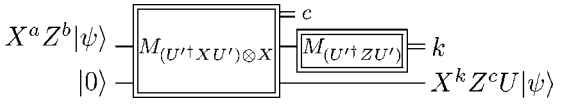
IV. MEASUREMENT-BASED UNIVERSAL QUANTUM COMPUTATION SCHEMES

In this section we derive simple variants of both the TQC and 1WQC models of computation using the principles described in earlier sections. Following the discussion in Sec. II B, it suffices to show how to perform a universal set of gates in each measurement-based model of quantum computation. We will first see that the simulation circuits derived in the previous section immediately give a universal scheme in the TQC model. This scheme is much simpler than those based on teleportation. (A similar simplified scheme was reported independently in [29].) Then we discuss a method to further reduce the required resources in the TQC model by identifying and simulating certain subunits of a circuit. We then turn to the 1WQC model and present a systematic derivation of universal quantum computation schemes using primitives discussed in the previous section.

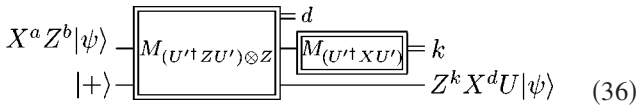
A. Derivation of simplified TQC schemes

1. Universality

Consider the universal set consisting of the single-qubit gates and $\Lambda(Z)$. A single-qubit gate can be performed in the TQC model using either Eq. (24) or Eq. (25)—the operations in the dashed boxes are of the form of Eq. (17), with V in the Clifford group and $V^\dagger ZV$ in the Pauli group. Thus Eq. (18) without the Pauli correction $V^\dagger ZV$ can be used to implement the dashed boxes in the TQC model. More concretely, Eqs. (24) and (25) imply the following simulation circuits:

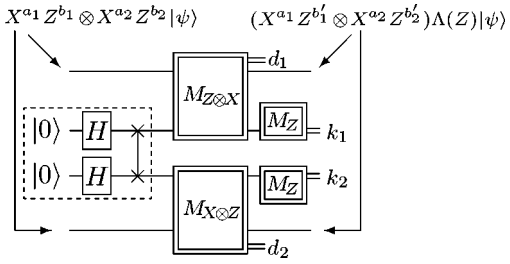


(35)

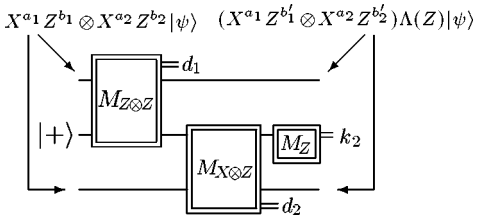


(36)

In Eqs. (35) and (36) the ancillas can be prepared up to known Pauli errors that *commute* with the subsequent two-qubit measurements. Simulation circuits for $\Lambda(Z)$ can be obtained from Eqs. (32) and (34):



(37)



(38)

In the above, k_1 should be added to the value of b_1' from Eq. (32), and k_2 should be added to b_2'. The state $\Lambda(Z)|+\rangle|+\rangle$ in Eq. (37) can be prepared by a two-qubit measurement. In both Eqs. (37) and (38), the ancillas can be prepared up to known Z errors, which have no effect other than flipping the measurement outcomes of subsequent $M_{X\otimes Z}$ and $M_{Z\otimes X}$. The simulation (37) uses two ancillary qubits, three two-qubit measurements, and two single-qubit measurements, and its logical depth is 3. The simulation (38) uses one ancillary qubit, two two-qubit measurements, and two single-qubit measurements, but its logical depth is 4.

2. Reduced-cost combined pseudosimulations

In the TQC model, how many single- and two-qubit measurements are required to simulate a circuit $\mathcal{C}$ consisting of single-qubit gates, m $\Lambda(Z)$ gates, and n final single-qubit measurements on the n computation qubits? We can do better than the method described above by combining some of the gates in the circuit into larger subunits, and simulating the subunits directly in the TQC model. In particular, without loss of generality, there are single-qubit gates U_i, V_i for $i = 1, \ldots, m$, such that $\mathcal{C}$ only consists of m "composite" gates $(U_i^\dagger \otimes V_i^\dagger)\Lambda(Z)(U_i \otimes V_i)$ applied in order, followed by single-qubit measurements.

Starting from Eqs. (32) and (34) and using Eq. (18), analogues of Eqs. (37) and (38) can be used to attempt the simulation of $W=(U^\dagger \otimes V^\dagger)\Lambda(Z)(U \otimes V)$ for any single-qubit gates U and V. These analogues of Eqs. (37) and (38) simply have $M_{U'^\dagger ZU' \otimes X}$, $M_{X \otimes V'^\dagger ZV'}$, and $M_{U'^\dagger ZU' \otimes Z}$ in place of $M_{Z\otimes X}$, $M_{X\otimes Z}$, and $M_{Z\otimes Z}$ respectively. We call these analogues "pseudosimulations," because W is simulated up to possible left multiplications of $U^\dagger ZU$ and $V^\dagger ZV$, which can easily be compensated for in the next pseudosimulation involving the same qubit.

The reduced-cost combined pseudosimulations use measurements of complexity comparable to those required in Eqs. (35) and (36). Altogether, a computation using m $\Lambda(Z)$ gates and n computation qubits can be pseudosimulated in TQC using m ancillary qubits, $2m$ two-qubit measurements, and $2m+n$ single-qubit measurements. In comparison, a full simulation [say, using Eqs. (35) and (38)] requires $3m$ ancillary qubits, $4m$ two-qubit measurements, and $6m+n$ single-qubit measurements.

B. Derivation of schemes similar to the 1WQC starting from the TQC

In this and subsequent subsections, we present our derivation of 1WQC-like schemes using one-bit teleportation as the underlying principle, preserving the conceptual simplicity of the TQC. The derivation is motivated by the differences between the TQC and 1WQC models. The TQC and 1WQC models differ in three main respects.

(a) The TQC model is similar to the circuit model in that no action is required on a qubit unless a nonidentity gate is applied. In contrast, in the 1WQC model, it is necessary to keep measuring qubits simply to propagate quantum information forward on the lattice.

(b) In the TQC model, interactions are effected by multi-qubit measurements. In contrast, no interactions are used in the 1WQC model after the initial preparation of the cluster state. In some sense, all interactions are built into the initial state before the computation begins.

(c) In the 1WQC model, a circuit $\mathcal{C}$ can be simulated using a $\mathcal{C}$-dependent graph state, which can in turn be produced from a $\mathcal{C}$-independent cluster state. Thus, the built-in interactions in the 1WQC model can be made independent of $\mathcal{C}$. In contrast, a TQC simulation has a one-to-one correspondence with $\mathcal{C}$.

These differences suggest a strategy to derive 1WQC-like schemes using the principles of the TQC model: every gate is performed by simulation circuits based on teleportation or one-bit teleportation [such as Eqs. (20), (21), (26), (27), and (32)]. Suppose the goal is to simulate a circuit $\mathcal{C}$ with n qubits and m time steps.

(a) Each gate in $\mathcal{C}$ will be simulated by circuits like Eqs. (26), (27), and (32). Furthermore, in each time step, identity gates will be explicitly simulated on qubits that are not being acted on. Thus, each qubit will be "teleported" in each step. Matching the output of one gate simulation to the input of the next, we obtain a circuit $\mathcal{C}'$ that "teleports" each of the n qubits m times, with the desired gates performed along the way. $\mathcal{C}'$ contains initial $|0\rangle$ states, one- or two-qubit gates, and single-qubit measurements. Note that in this circuit we do not interpret a two-qubit gate followed by a single-qubit measurement as an incomplete two-qubit measurement, as we did in the TQC. The reason is that in the next step we will build the two-qubit gates into the initial state, leading to an equivalent circuit containing only single-qubit measurements.

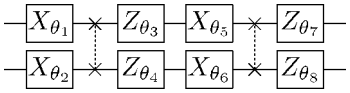
(b) To build interactions into the initial state, we apply standard circuit identities to rewrite $\mathcal{C}'$ so that all two-qubit gates occur before the $\mathcal{C}$-dependent single-qubit gates, followed by single-qubit measurements. The circuits used to simulate each gate are chosen to facilitate this step. The resulting circuit $\mathcal{C}''$ consists of (i) two-qubit gates acting on circuit-independent product states and (ii) circuit-dependent single-qubit gates followed by single-qubit measurements. We regard the state $|\psi_{\mathcal{C}}\rangle$ after step (i) as a new initial state, and the remaining single-qubit gates and measurement in step (ii) as single-qubit measurements in redefined bases. We can thus interpret $\mathcal{C}''$ as starting from a $\mathcal{C}$-dependent initial state $|\psi_{\mathcal{C}}\rangle$, followed by single-qubit measurements. We will see that $|\psi_{\mathcal{C}}\rangle$ is like the circuit-dependent graph state in the original 1WQC scheme. Schemes derived in this way will be called 1WQC_{TG} schemes, with T standing for the underlying principle of teleportation, and G for an initial graph state. Besides being an intermediate step to our final model, the 1WQC_{TG} model is also useful in its own right if the simulated circuit is known at the time of the initial state preparation and the interactions can be selectively implemented (for example, in [22,31]).

(c) We want to modify the 1WQC_{TG} schemes to start with a fixed, universal initial state analogous to the cluster state. The idea is to find a circuit that simulates a two-qubit gate or the identity gate depending on the choices of the subsequent single-qubit measurements. In other words, the interactions built into the initial state are "optional," in the sense they may or may not be implemented. The desired universal initial state simply has an optional interaction built in wherever the interaction may occur. We call the resulting model 1WQC_{T}.

C. Derivation of a scheme using circuit-dependent graph states (1WQC_{TG})

1. A universal circuit decomposition

The most general quantum circuit $\mathcal{C}$ can be viewed as consisting of alternating steps of (i) arbitrary single-qubit gates and (ii) optional *nearest-neighbor* $\Lambda(Z)$ gates [because H and $\Lambda(Z)$ can be composed to make swap gates]. We want gate-simulation circuits in which the interactions can be performed before the $\mathcal{C}$-dependent single-qubit gates. Thus, simulation circuits like Eqs. (26) and (27) are preferred to ones like Eqs. (24) and (25). Such choices preserve universality since any single-qubit gate has an Euler angle decomposition $U=Z_{\theta_3}X_{\theta_2}Z_{\theta_1}$. The circuit $\mathcal{C}$ now contains cycles of (i) arbitrary Z rotations, (ii) arbitrary X rotations, (iii) arbitrary Z rotations, and (iv) optional nearest-neighbor $\Lambda(Z)$ gates, represented mathematically as $\Lambda(Z)^k$ where k can be freely chosen from $\{0,1\}$. Since a $\Lambda(Z)$ commutes with the Z rotations before and after, the Z rotations can be merged. For example, two cycles on two qubits can be represented by

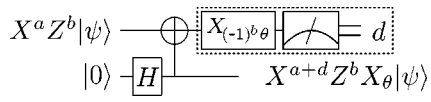


(39)

where θ_i are arbitrary angles of rotation, and the dotted line for $\Lambda(Z)$ denotes an optional gate. We will see that it is more efficient to simulate $\Lambda(Z)$ and Z rotations together. Thus, a circuit should be decomposed into cycles, each with two steps: (i) arbitrary X rotations, and (ii) arbitrary Z rotations and optional nearest-neighbor $\Lambda(Z)$ gates.

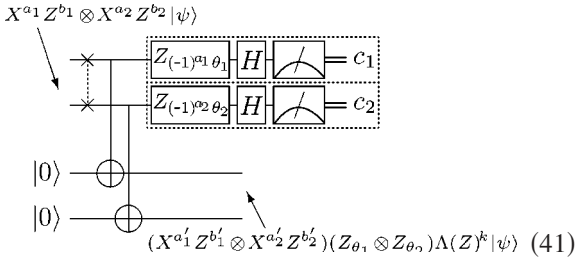
2. Simulation using one-bit teleportation

We first describe the simulation circuits for the elementary steps just described. We use Eq. (27) to simulate X_θ, restated here:



(40)

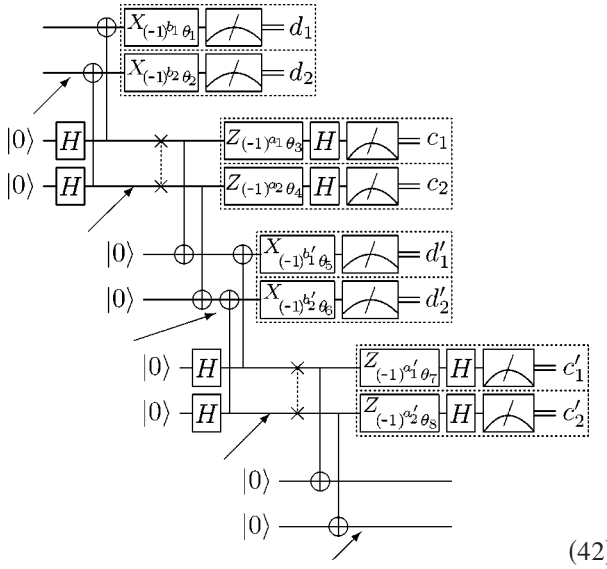
We will identify $H|0\rangle=|+\rangle$ as part of the initial state preparation. We simulate an optional $\Lambda(Z)$ gate and Z rotations in a single step, by composing a self-simulation of an optional $\Lambda(Z)$ with simulations of Z rotations as follows:



(41)

In the above, $\Lambda(Z)$ is performed if $k=1$, and not if $k=0$. The state after $\Lambda(Z)^k$ is $(X^{a_1}Z^{b_1+a_2k}\otimes X^{a_2}Z^{b_2+a_1k})\Lambda(Z)^k|\psi\rangle$. After the Z rotations and teleportation, the final output is $(X^{a_1}Z^{b_1+a_2k+c_1}\otimes X^{a_2}Z^{b_2+a_1k+c_2})\ (Z_{\theta_1}\otimes Z_{\theta_2})\Lambda(Z)^k|\psi\rangle$. Therefore, $a_1'=a_1$, $a_2'=a_2$, $b_1'=b_1+a_2k+c_1$, and $b_2'=b_2+a_1k+c_2$ in Eq. (41).

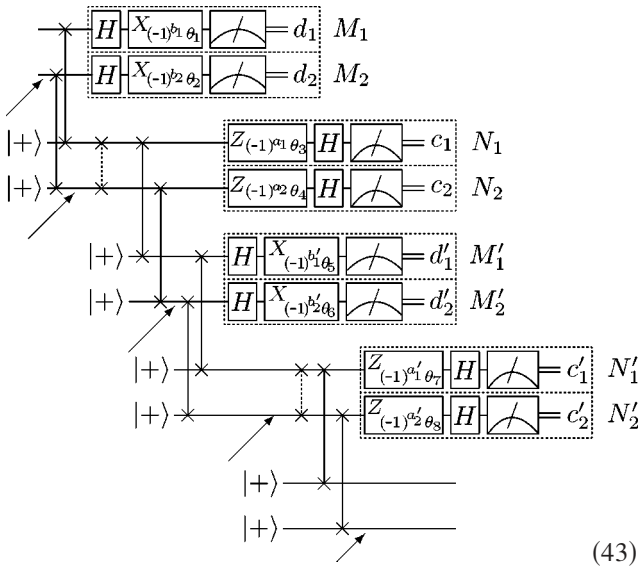
Finally, we chain together the simulation circuits for the repeating cycles of (i) arbitrary X rotations and (ii) arbitrary Z rotations and optional nearest-neighbor $\Lambda(Z)$ gates. The resulting circuit to simulate Eq. (39), with two cycles for two qubits, is



(42)

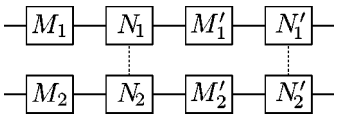
Each arrow in Eq. (42) indicates where the output of a certain teleportation step matches the input of the subsequent teleportation. The values of a_i' and b_i' can be read from Eqs. (40) and (41). The circuit of Eq. (42) generalizes easily to n qubits with multiple optional $\Lambda(Z)$ gates.

The simulation (42) can be simplified by (i) rewriting $\Lambda(X)$ as $(I\otimes H)\Lambda(Z)(I\otimes H)$, (ii) canceling out consecutive Hadamard gates (since $H^2=I$), (iii) rewriting $H|0\rangle$ as $|+\rangle$, and (iv) absorbing H before a single-qubit measurement as part of the measurement. We thus obtain a simpler simulation scheme for Eq. (39):



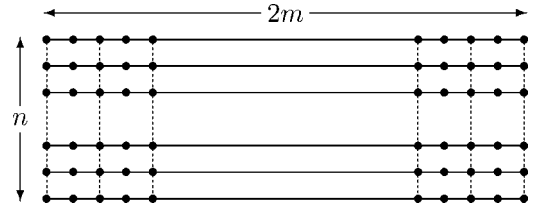
(43)

We can view the operations in the dashed boxes as single-qubit measurements, and the rest of the circuit as an initial state $|\psi_{\mathcal{C}}\rangle$. Note that $|\psi_{\mathcal{C}}\rangle$ is a graph state, as defined in Sec. II D. The circuit $\mathcal{C}$ determines whether each $\Lambda(Z)^k=I$ or $\Lambda(Z)$ in $|\psi_{\mathcal{C}}\rangle$. The substrate representation of Eq. (43) is



(44)

where the measurements are as specified in Eq. (43). The initial graph state for an n-qubit circuit $\mathcal{C}$ with m time steps can be chosen to be



(45)

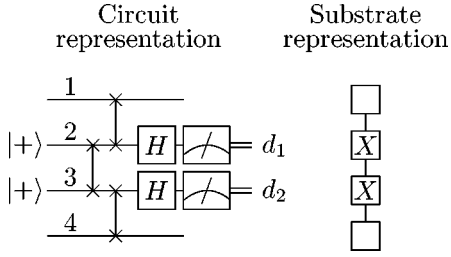
Equations (44) [with measurements specified in Eq. (43)] and (45) form a complete recipe for the simulation of a known quantum circuit by the $1WQC_{TG}$ scheme. This approach is generally more efficient than the circuit-independent ($1WQC_T$) schemes described in the following section. Indeed, the $1WQC_{TG}$ approach is useful in its own right when the simulated circuit is known at the time of initial state preparation.

D. Derivation of schemes using a universal family of initial states ($1WQC_T$)

We now present methods for performing an optional $\Lambda(Z)$. Composing the optional $\Lambda(Z)$ simulation with the $1WQC_{TG}$ scheme described in the previous section, we obtain various $1WQC_T$ schemes.

1. The remote $\Lambda(Z)$ approach (I)

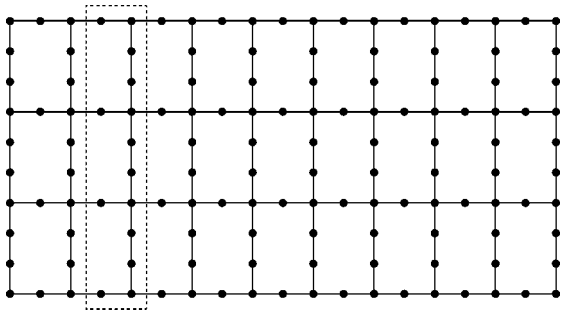
Consider the circuit (32) that simulates $\Lambda(Z)$:



(46)

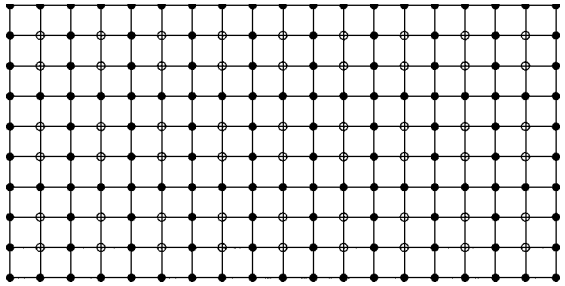
Note that we have explicitly labeled all the qubits. The circuit in Eq. (46) starts with a graph state, and applies the gate $Z^{d_2}\otimes Z^{d_1}\Lambda(Z)$ to qubits 1 and 4. On the other hand, the deletion principle from [13] (see Sec. II D) shows that, if the H gates on qubits 2 and 3 are simply omitted, and those qubits are measured along $\{|0\rangle,|1\rangle\}$, then qubits 1 and 4 are disentangled, and an identity gate is simulated instead.

Substituting the initial graph state of Eq. (46) for the optional $\Lambda(Z)$ in Eq. (45), the initial graph state for our first $1WQC_T$ scheme is given by



(47)

This graph state can be used to simulate a 4-qubit circuit for 9 cycles of (i) arbitrary X rotations and (ii) arbitrary Z rotations and optional nearest-neighbor $\Lambda(Z)$. The region corresponding to the simulation of one cycle is marked by a dashed box. The above state can in turn be obtained by "deleting" qubits denoted by empty circles (by measuring them in the computational basis) in the following cluster state:

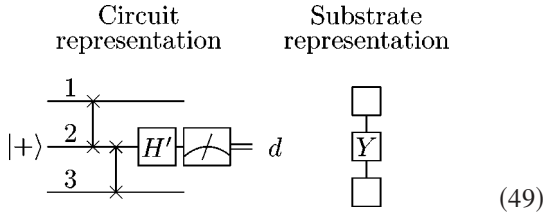


(48)

This cluster state-based simulation requires six physical qubits per logical qubit per cycle.

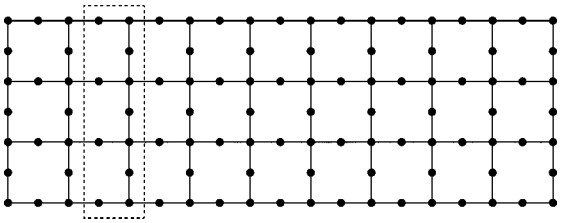
2. The remote $\Lambda(Z)$ approach (II)

The remote $\Lambda(Z)$ described in the previous section requires two ancilla qubits per $\Lambda(Z)$. We can save resources by relaxing the exact simulation condition, and use the following circuit:



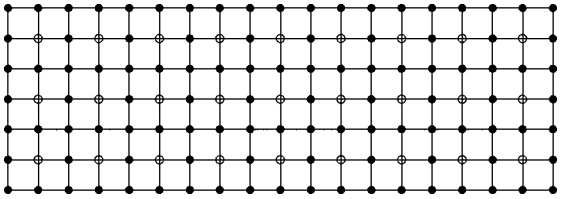
(49)

where $H'=(Z+Y)/\sqrt{2}$ and H' followed by M_Z is simply M_Y. Let R_d be the Z-rotation $Z_{(-1)^{d+1}\pi/2}$. The above circuit implements the gate $(R_d\otimes R_d)\Lambda(Z)$, and yields a $1\mathrm{WQC_T}$ scheme from the $1\mathrm{WQC_{TG}}$ model in Sec. IV C 2, because arbitrary Z rotations are always simulated with the optional $\Lambda(Z)$. Substituting Eq. (49) into Eq. (45) gives another universal initial graph state



(50)

which can again be obtained from the cluster state by deleting the cites marked by empty circles:



(51)

This scheme requires only four physical qubits per logical qubit per cycle.

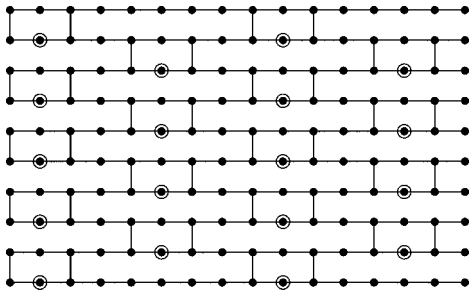
The above schemes are quite efficient in terms of the number of physical qubits per logical operation. Moreover, such efficiency is achieved with remarkably little manipulation; rather, it arises from following simple guidelines in a systematic derivation.

3. The cancellation approach

The cancellation approach uses the fact that in $1\mathrm{WQC_{TG}}$, the angle of single-qubit rotations can be entirely determined by the measurement basis, and can be chosen online. The idea is to intersperse two consecutive $\Lambda(Z)$ gates with a single-qubit rotation so that proper choices of the angle of rotation allow the two interactions to add up or cancel out. In particular,

$$\Lambda(Z)(I\otimes X_\theta)\Lambda(Z)=\begin{cases} I & \text{if } \theta=0,\\ (I\otimes X_{\pi/2})\Lambda(X) & \text{if } \theta=-\dfrac{\pi}{2}.\end{cases}$$

The gate $\Lambda=(I\otimes X_{\pi/2})\Lambda(X)$ is locally equivalent to $\Lambda(X)$, and is universal given the ability to perform all single-qubit gates. Thus, we can perform optional nearest-neighbor Λ gates by introducing pairs of $\Lambda(Z)$ with a variable X rotation interspersed between each pair. This observation can be used to extend $1\mathrm{WQC_{TG}}$ to a scheme with a fixed initial state. The idea is to represent a quantum computation as a set of repeating subunits. A subunit consists of the following: (i) arbitrary X rotations, (ii) arbitrary Z rotations and $\otimes_{i\ \mathrm{odd}}\Lambda(Z)_{i,i+1}$, (iii) interspersed X rotations, (iv) arbitrary Z rotations and $\otimes_{i\ \mathrm{odd}}\Lambda(Z)_{i,i+1}$, (v) arbitrary X rotations, (vi) arbitrary Z rotations and $\otimes_{i\ \mathrm{even}}\Lambda(Z)_{i,i+1}$, (vii) interspersed X rotations, and (viii) arbitrary Z rotations and $\otimes_{i\ \mathrm{even}}\Lambda(Z)_{i,i+1}$, where subscripts on $\Lambda(Z)$ denote the qubits being acted on. Following the discussion in Sec. IV C 2, the initial graph state is given by



(52)

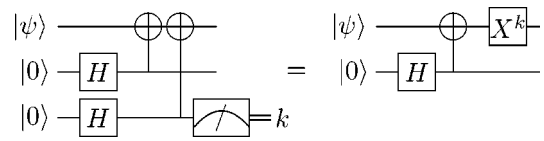
In this diagram, qubits corresponding to the interspersed X rotations are marked by extra circles. The above state can be used to simulate a five-qubit circuit for two cycles.

The above graph state can also be produced from a cluster state, though the resulting scheme is not as efficient as the first approach.

4. The routing approach

In the routing approach, a qubit can be teleported to an interaction or a non-interaction site. The interaction is always applied at the interaction site, but it may be applied to the quantum data or to some dummy state.

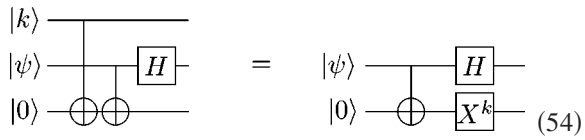
Using X teleportation, it is possible to teleport a given input state to one of several possible destinations. To see how this works, we consider the case of two destinations:



(53)

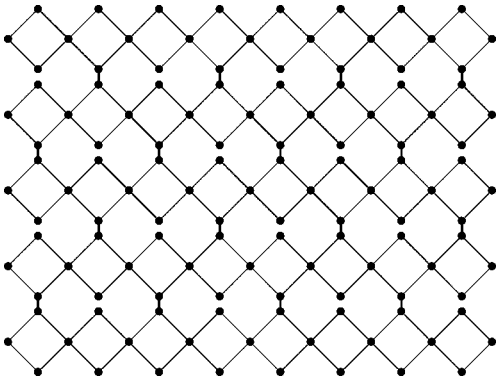
Examining this circuit identity and comparing with the circuit for X-teleportation, we see that by measuring the third qubit we can effect an X-teleportation of the first qubit to the second. Alternately, if we had decided instead to measure the second qubit, we would have been able to effect an X-teleportation of the first qubit to the third. Thus, we are able to choose to route the state $|\psi\rangle$ to one of two destina-

tions. The other qubit will be in a known state $|k\rangle=|0\rangle$ or $|1\rangle$. After this X-teleportation, the next simulation step is a Z-teleportation that will perform $\Lambda(Z)$ on the path meant for interaction and I on the other path. Z rotations are also performed at the same time. In the previous step, the qubit state was teleported to the desired destination, and the unwanted destination is in some known random state $|k\rangle$. The Z-teleportation can also be constructed to take its input from either location, using the identity



(54)

We can combine the teleportation steps as in Eq. (42), and we obtain a simplified circuit analogous to Eq. (43). The following graph state is the initial state for this routing approach:


(55)

The processing of information in this graph state is easy to understand. Consider the top three lines of qubits in the graph, i.e., the eight adjacent "diamonds" at the top of the graph. This line of diamonds represents the processing of a single logical qubit. Information starts out in the leftmost vertex of the diamond, and is then routed either to the top vertex of the diamond, or to the bottom vertex. If it is routed to the bottom vertex, then it may be interacted with the second row of diamonds, representing the second logical qubit, effecting a $\Lambda(Z)$ gate between logical qubits. If it is routed through the top vertex, then no interaction takes place. Finally, Z teleportation is used to reroute the information from either the top or the bottom vertex into the rightmost vertex of the diamond. Thus, we see that this state can be used to simulate a five-qubit circuit for four cycles.

V. CONCLUSION

In this paper we have explained how one-bit teleportation can be used as a simple underlying principle to systematically derive measurement-based schemes for universal quantum computation. These derivations provide a single unified approach that encompasses schemes similar to both the 1WQC (one-way quantum computer) model introduced in [13], and the TQC (teleportation-based model of quantum computation) introduced in [15]. However, our schemes have the added advantage of being significantly simpler than previously known schemes in either approach. Most importantly, our derivation has elicited a simple underlying principle for the 1WQC.

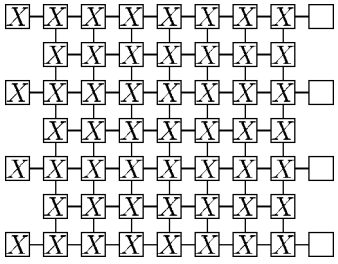
We have also outlined a variety of tools and techniques for designing schemes for measurement-based quantum computation. Our schemes have many variants, indicating the flexibility of our constructions. We hope that the library of tools we have described will be of use both in developing further insight into the power and limitations of measurement-based quantum computation, and in designing 1WQC schemes suited to a particular information processing task or physical implementation. To illustrate how our systematic method and tools can be applied, we derive a 1WQC scheme for the bit-reversal operation in the Appendix. This scheme was presented in [33], but no network explanation had previously been given.

ACKNOWLEDGMENTS

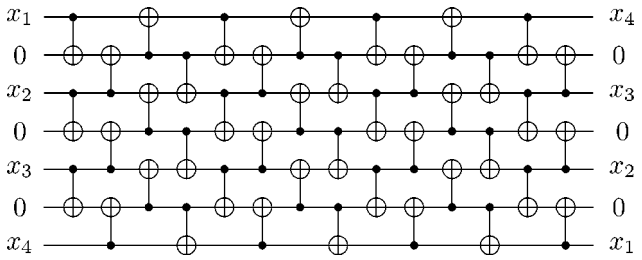
We thank Panos Aliferis for sharing many thoughts and unpublished results. We thank Michael Ben-Or, Hans Briegel, Daniel Browne, Isaac Chuang, Chris Dawson, Steven van Enk, Christopher Fuchs, Daniel Gottesman, Ashwin Nayak, Robert Raussendorf, and Frank Verstraete for stimulating discussions. We thank Hans Briegel and Robert Raussendorf for their permission to use Fig. 1. We also thank Jozef Gruska for drawing our attention to the independent result by Perdrix [29]. A.M.C. and M.A.N. acknowledge the hospitality of the Caltech IQI, where this work was initiated. Part of this work was done while A.M.C. and D.W.L. were visiting the Perimeter Institute and while D.W.L. was visiting the University of Toronto. Their hospitality is also much appreciated. A.M.C. received support from the Fannie and John Hertz Foundation, and was also supported in part by the Cambridge-MIT Institute, by the U.S. Department of Energy under cooperative research agreement DE-FC02-94ER40818, and by the National Security Agency and Advanced Research and Development Activity under Army Research Office Contract No. DAAD19-01-1-0656. D.W.L. received support from the Richard C. Tolman Endowment Fund, the Croucher Foundation, and the National Science Foundation under Grant No. EIA-0086038. M.A.N. received support from the Australian Research Council.

APPENDIX: THE BIT-REVERSAL OPERATION

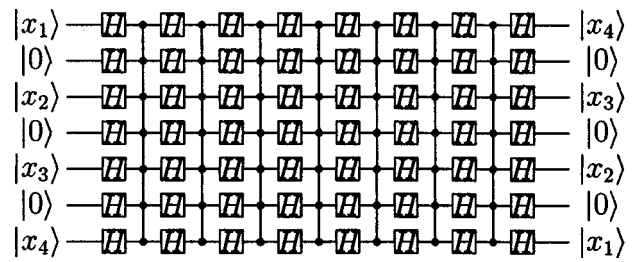
The bit-reversal operation on n qubits is defined on the computational basis as $|x_1\rangle|x_2\rangle\cdots|x_n\rangle\rightarrow|x_n\rangle\cdots|x_2\rangle|x_1\rangle$. A simple 1WQC scheme was presented in [31]. Following [31], we illustrate the idea for $n=4$, while similar results hold for arbitrary n. The substrate representation of the scheme in [31] is given by


(A1)

where the $n=4$ leftmost (rightmost) qubits carry the input (output). Every qubit in the input or the $(2n-1)\times(2n-1)$ middle block is measured in the X basis. To derive Eq. (A1), we first depict a classical circuit for the bit-reversal operation:



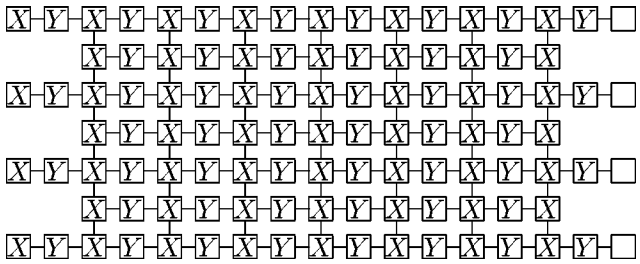
Note that the above is a valid quantum circuit for bit-reversal as well. Adding H to each of the input and output qubits in bit-reversal preserves the operation. Furthermore, rewriting $\Lambda(X)$ using Eq. (7), we obtain the following quantum circuit decomposition for bit-reversal:



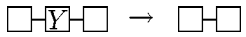
Using the Euler angle decomposition

$$H = ie^{-iZ\pi/4}e^{-iX\pi/4}e^{-iZ\pi/4} \tag{A2}$$

and following our procedure in Sec. IV C, we obtain a $1\mathrm{WQC}_{\mathrm{TG}}$ scheme with substrate representation:



Finally, we can simplify the above to become Eq. (A1) by making the replacement:



due to Eq. (49). (The extra Z rotations on the two qubits always occur together, and compose to become a Pauli operation.)

[1] D. P. DiVincenzo, Science **270**, 255 (1995).
[2] J. Preskill, *Physics 229, Advanced Mathematical Methods of Physics: Quantum Computation and Information* (Caltech, Pasadena, CA, 1998), URL http://www.theory.caltech.edu/people/preskill/ph229.
[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[5] P. Shor, Phys. Rev. A **52**, R2493 (1995).
[6] P. Shor, in *Proceedings of the 37th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1996); p. 56, e-print quant-ph/9605011.
[7] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1999), e-print quant-ph/9906054.
[8] E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998).
[9] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
[10] X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000).
[11] E. Knill, R. Laflamme, and G. Milburn, Nature (London) **409**, 46 (2001).
[12] L.-A. Wu and D. A. Lidar, Phys. Rev. A **67**, 050303 (2003).
[13] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[14] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
[15] M. A. Nielsen, Phys. Lett. A **308**, 96 (2003).
[16] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
[17] S. A. Fenner and Y. Zhang, e-print quant-ph/0111077.
[18] D. W. Leung, e-print quant-ph/0111122.
[19] D. W. Leung, Int. J. Quantum Inf. **2**, 33 (2004).
[20] R. Raussendorf and H. J. Briegel, Quantum Inf. Comput. **2**, 443 (2002).
[21] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[22] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).
[23] A. M. Childs, seminar at the Perimeter Institute, 2003, URL http://www.qinfo.org/qc-by-measurement.
[24] D. W. Leung, group meeting talk at the Institute for Quantum Information, Caltech, February 2004, URL http://www.qinfo.org/qc-by-measurement.
[25] D. W. Leung, seminar at ERATO Tokyo office, March 2004, URL http://www. qinfo.org/qc-by-measurement.
[26] F. Verstraete and J. I. Cirac, e-print quant-ph/0311130.
[27] P. Aliferis and D. W. Leung, e-print quant-ph/0404082.
[28] P. Jorrand and S. Perdrix, e-print quant-ph/0404125.

[29] S. Perdrix, e-print quant-ph/0402204.
[30] S. Perdrix and P. Jorrand, e-print quant-ph/0404146.
[31] D. E. Browne and T. Rudolph, e-print quant-ph/0405157.
[32] M. A. Nielsen and C. M. Dawson, e-print quant-ph/0405134.
[33] R. Raussendorf, D. E. Browne, and H. J. Briegel, J. Mod. Opt. **49**, 1299 (2002).
[34] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[35] D. Schlingemann and R. F. Werner, Phys. Rev. A **65**, 012308 (2001).
[36] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).
[37] M. A. Nielsen, journal club notes on the cluster-state model of quantum computation, 2003, URL http://www.qinfo.org/qc-by-measurement.
[38] D. Gottesman, in *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, MA, 1999), pp. 32 and 33, e-print quant-ph/9807006.
[39] D. Gottesman, Lect. Notes Comput. Sci. **1509**, 302 (1999).