Quantum Information and Computation, Vol. 7, No. 3 (2007) 184–208

CLUSTER STATE QUANTUM COMPUTATION FOR MANY-LEVEL SYSTEMS

WILLIAM HALL
Department of Mathematics, University of York
Heslington, York YO10 5DD, United Kingdom

Received January 6, 2006
Revised May 11, 2006

The cluster state model for quantum computation [Phys. Rev. Lett. **86**, 5188] outlines a scheme that allows one to use measurement on a large set of entangled quantum systems in what is known as a cluster state to undertake quantum computations. The model itself and many works dedicated to it involve using entangled qubits. In this paper we consider the issue of using entangled qudits instead. We present a complete framework for cluster state quantum computation using qudits, which not only contains the features of the original qubit model but also contains the new idea of adaptive computation: via a change in the classical computation that helps to correct the errors that are inherent in the model, the implemented quantum computation can be changed. This feature arises through the extra degrees of freedom that appear when using qudits. Finally, for prime dimensions, we give a very explicit description of the model, making use of mutually unbiased bases.

Keywords: Cluster state quantum computing, qudits, one-way quantum computer, measurement based quantum computation, mutually unbiased bases.
Communicated by: R Jozsa & B Terhal

1 Introduction

The problem of building a quantum computer that has computational power greater than that of classical computers is one that has concerned both theorists and experimentalists for a number of years. The recent development of the cluster state model for quantum computation [1, 2, 3], in which remarkably quantum computation is achieved essentially by tailored measurement of entangled states of a large number of qubits, has not only lead to significant implications in our understanding of quantum computation and quantum dynamics, but also to new experimental approaches to the possible realisation of large scale quantum computers [4, 22, 5].

Although much study has been devoted to this model [7, 8, 13, 16, 23] this work has almost exclusively been concerned with using qubits as the basic physical resource. However, many quantum systems cannot be treated as simple two-level systems, but rather as multi-level systems. Furthermore, recent work [6] has suggested that qutrit based quantum computation schemes yield in some sense the most efficient implementation of quantum computation.

In this paper we are going to present a generalisation of the cluster state model, by replacing the cluster state of qubits with more general cluster states of qudits. Such a generalisation

has already been presented in [10], but in this paper we will take a much more explicit approach, in which we try and present the cluster state model by presenting each constituent of the model in as simple a way possible. This allows us to see the critical ingredients that make cluster state QC possible.

The paper will be laid out as follows. In section 2 we will present a generalisaton of an idea used in [9] which we will call *one dit teleportation*. This forms the core to our approach to cluster state QC. One dit teleportation takes the form of a simple two-qudit circuit identity which can be thought of as implementing a certain quantum gate (namely the d-dimensional analogue of the Fourier transform gate) by measurement. We then proceed to show that this identity can be used to implement a much wider class of gates, and how this process can be turned into a quantum computational paradigm, which essentially involves a series of measurements on a entangled state of qudits to implement quantum computation. While this approach turns out to not be the best approach for some types of cluster states, it ties in our cluster state model for QC heavily with the circuit model, hence giving us an alternative and (in the eyes of the author) a simpler way of looking at the model.

In section 3 we will first discuss the issue of adapting measurements based on previous measurement results to allow us to implement any quantum operation we wish. Measurements on a quantum system by their very nature are statistical; and in the cluster state paradigm this randomness can be thought of as introducing errors into our computation which can be corrected for using *classical* computation. This notion is known as the issue of *adaptive measurement* and is crucial in the theory of cluster state QC. We will also introduce a new phenomena which we call *adaptive computation*, a feature that will be unique to cluster state QC on qudits, arising due to the extra degrees of freedom we are presented with. The basic idea is that by changing the method by which we correct the errors associated with a measurement outcome, we can implement different quantum gates. We will discuss this in further detail at the appropriate time. We conclude this section with an example of the simplicity of the one-dit teleportation approach which also makes use of adaptive computation.

In section 4, we briefly review the stabiliser method for cluster states, which is the most common approach in most of the existing literature. For details of the model we refer the reader to the appropriate paper, but we do give a comparison of the two approaches, highlighting the fact that both approaches are indeed useful.

In section 5 we will discuss the problem of generating a universal set of quantum gates for quantum computation, giving a general method by which quantum gates can be realised, and then discussing a connection of this method with the theory of *mutually unbiased bases*. While this connection is not a fundamental one, using the known theory for MUBs gives us a very elegant method of establishing measurement patterns for implementing a universal set of quantum gates. We will use the connection to give explicit calculations and details of the measurements required to generate certain quantum gates in prime dimensions. We conclude with a discussion in the final section.

2 One dit teleportation and cluster state quantum computation

2.1 Preliminaries: a basic measurement result

For clarity, we will start by giving a very basic result. We assume throughout this paper that all Hilbert space(s) involved here are of dimension d. Let $\{|k\rangle\}_{k=0}^{d-1}$ be a standard (compu-

tational) basis for our Hilbert space. We define *measuring in the basis defined by U* for a unitary $U \in U(d)$ to mean measurement in the orthonormal basis $\{U|k\rangle\}_{k=0}^{d-1}$ (i.e. the vectors defined by the columns of U when U is described in matrix form in the computational basis). Our result is as follows:

Lemma 1. *Given a bipartite state $|\Psi\rangle$, measuring one of the systems in the basis defined by U and discarding is equivalent to applying $U^\dagger$ to the first system, measuring it in the computational basis and then discarding it.*

Proof. Let $|\Psi\rangle = \sum_k U|k\rangle \otimes |\psi_k\rangle$. Measuring the first system in the basis defined by U leaves the second system in the state $|\psi_k\rangle / \sqrt{\langle\psi_k|\psi_k\rangle}$ with probability $\langle\psi_k|\psi_k\rangle$. Applying $U^\dagger$ to the first system and then measuring it in the computational basis can easily be seen to have the same effect. □.

This lemma gives us an alternative way to generate the appropriate statistics for measurement of one system of a bipartite system in a given basis.

2.2 One dit teleportation

The idea of one dit teleportation is a many-level generalisation of *one-bit teleportation* that was first presented in [11]. We will first simply present this relatively simple idea, and then show how it is integral to cluster state quantum compuation.

We first need some definitions. The Fourier transform basis is defined by

$$|+_j\rangle = \sum_{k=0}^{d-1} \omega^{jk} |k\rangle \tag{1}$$

where $\omega = e^{2\pi i/d}$, the primitive dth root of unity. We will often denote $|+_0\rangle$ by simply $|+\rangle$. We also need to introduce a set of operators known as the *generalised Pauli operators* [14]:

$$Z = \sum_{k=0}^{d-1} \omega^k |k\rangle\langle k|, \;\; X = \sum_{k=0}^{d-1} |k-1\rangle\langle k| \tag{2}$$

where we are using modulo d arithmetic within the bras and kets. Finally, we define the Fourier gate F by

$$F = \frac{1}{\sqrt{d}} \sum_{j,k=0}^{d-1} \omega^{jk} |j\rangle\langle k| = \sum_{k=0}^{d-1} |+_k\rangle\langle k|. \tag{3}$$

This gate is the d-dimensional Quantum Fourier Transform gate, and in $d = 2$ is equivalent to the Hadamard gate.

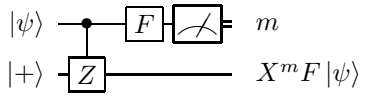

Fig. 1. The circuit diagram for one-dit teleportation.

The notion of one-dit teleportation is given by the circuit identity in Figure 1, where we

are using the d dimensional analog of controlled gates:

$$CZ = \sum_{k=0}^{d-1} |k\rangle\langle k| \otimes Z^k = \sum_{k,l=0}^{d-1} e^{2\pi i kl/d} |k\rangle\langle k| \otimes |l\rangle\langle l| \tag{4}$$

and the meter represents measurement in the computational basis, with outcome k corresponding to the state $|k\rangle$. Furthermore, each of the possible outcomes occurs with equal probability $1/d$.

Proof. First we note two important facts, both of which can be deduced by elementary means:

$$Z^j |+_k\rangle = |+_{j+k}\rangle \text{ (modulo } d \text{ addition in ket index);} \tag{5}$$

$$X^j |+_k\rangle = w^{jk} |+_k\rangle . \tag{6}$$

Let $|\psi\rangle = \sum_k a_k |k\rangle$. Then

$$\begin{aligned} |\psi\rangle |+\rangle &= \sum_k a_k |k\rangle |+\rangle \\ &\overset{CZ}{\rightarrow} \sum_k a_k |k\rangle |+_k\rangle \\ &\overset{F\otimes I}{\rightarrow} \sum_k a_k |+_k\rangle |+_k\rangle \equiv |\Psi\rangle \end{aligned}$$

where we calculate the effect of the CZ gate using equation (5). Now, we can write $|\Psi\rangle$ as

$$\begin{aligned} |\Psi\rangle &= \frac{1}{\sqrt{d}} \sum_{j,k} a_k \omega^{jk} |j\rangle |+_k\rangle \\ &= \frac{1}{\sqrt{d}} \sum_j |j\rangle \sum_k a_k \omega^{jk} |+_k\rangle \\ &= \frac{1}{\sqrt{d}} \sum_j |j\rangle \sum_k a_k X^j F |k\rangle \\ &= \frac{1}{\sqrt{d}} \sum_j |j\rangle X^j F |\psi\rangle \end{aligned}$$

where the penultimate line follows from equation (6) above; hence, when measuring the first qudit, an outcome j (occuring with probability $1/d$) yields a state $X^j F |\psi\rangle$ for the second qudit. □.

2.3 Application to cluster state quantum computation

One way we can think about the above circuit identity is that it gives us a very simple scheme for implementing the quantum Fourier gate F: Given a qudit pair in states $|\psi\rangle, |+\rangle$ entangled with a controlled-Z interaction, if we measure the first ($|\psi\rangle$) qudit in the $F^\dagger$ basis, and obtain the measurement outcome j, the second qudit ends up in the state $X^j F |\psi\rangle$. The X^j operator can be thought of as an *error operator*, and we will discuss this shortly.

Furthermore, from equation (4) we note that the controlled-Z gate is symmetric in the two qudits, and so any *phase* transformation in the computational basis (that is, a quantum gate of the form

$$Z(\mathbf{a}) = \sum_k e^{ia_k} |k\rangle\langle k|,$$

with $\mathbf{a} \in [0, 2\pi]^d$) that acts on the first (upper) qudit commutes through the controlled-Z gate. This means that measuring the first system in the basis defined by $(FZ(\mathbf{a}))^\dagger$, which (by lemma 1) is the same as applying $FZ(\mathbf{a})$ to the system before measurement in the computational basis, is equivalent to teleporting the initial state $Z(\mathbf{a})\,|\psi\rangle$. This leads to the more general circuit identity given in Figure 2, meaning we can implement the quantum gates $FZ(\mathbf{a})$ using this method.

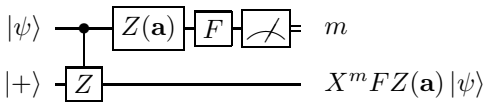

Fig. 2. The more general circuit diagram for one-dit teleportation.

If the transformation $|\psi\rangle \to FZ(\mathbf{a})\,|\psi\rangle$ forms our entire quantum computation, then since the powers of X merely permute the computational basis elements, and all known quantum algorithms conclude with a measurement in this basis, we can simply correct for the Pauli error X^j via a *classical* compuation.

This is the simplest possible example of cluster state computation: We take two qudits, one of which is our *initial* state $|\psi\rangle$, and an *output* qudit, which is initialised in the state $|+\rangle$. After entangling the pair using a controlled-Z interaction, and an appropriate measurement, we can map our input state $|\psi\rangle$ onto an output state $FZ(\mathbf{a})\,|\psi\rangle$, up to a Pauli error X^j.

If we wished to apply further quantum operations to our state, we could do so by using a *linear cluster* of qudits entangled in this way (Figure 3), and then measuring along the cluster appropriately to implement the appropriate product of gates. Since measurement on a qudit and an interaction between another pair of qudits commute, this is equivalent to several one-dit teleportations, with the output from one teleportation becoming the input to the next (see Figure 4). The measurements after the first however may have to be adapted due to the extra X factors brought in by previous measurements, so that the desired quantum operation is implemented. This issue of compensating for the randomness of previous measurement outcomes by a change of subsequent measurement bases is known as *adaptive measurement*, and will be discussed in section 3. For now however, we will assume that this issue is surmountable.

These ideas lead us to our definition of the cluster states we are going to use for computation:

Fig. 3. A linear cluster of 6 qudits. Each dot represents a physical qudit, and the lines an interaction between the two adjoined qudits.

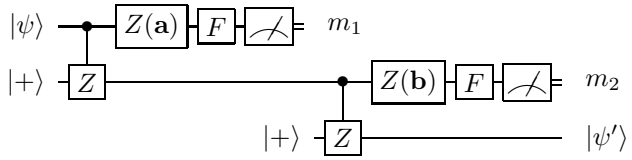

Fig. 4. A quantum circuit for two successive one-dit teleportations. The circuit diagram is arranged to illustrate that the teleportation between the upper two qudits is independent of any further structure in the cluster (in this case a third qudit entangled to the second). The final state will take the form $|\psi'\rangle = X^{a(m_1,m_2)}Z^{b(m_1,m_2)}FZ(\mathbf{c}(\mathbf{b},m_1))FZ(\mathbf{a})\,|\psi\rangle$, where $\mathbf{c}$ is a function of m_1 because of the generalised Pauli error introduced by the first measurement may require the second measurement to be adapted.

1. We prepare a set of qudits, each in the state $|+\rangle$ (except perhaps for an 'initial' set of qudits which are in an potentially entangled state $|\psi\rangle$; this represents the input to the algorithm);[a]

2. Finish creating the cluster by interacting 'neighbouring' pairs of qudits via a controlled-Z gate.

For qubits, this is identical to the original framework for cluster state QC [1, 2]. Cluster state computation then takes the form of a series of measurements on specified qudits, along with a scheme on how to adapt the measurements based on the previous measurement results. This definition also gives a possible method for generating these cluster states: suppose we have d-dimensional physical systems that we can prepare in the state $|\psi\rangle$, and we can allow them to interact with an appropriate interaction Hamiltonian between the systems e.g.

$$H_I = -g\sum_{k,l} kl|k\rangle\langle k| \otimes |l\rangle\langle l|$$

where g is some coupling constant. If we let this interaction run for a time $t = 2\pi/gd\hbar$, then the time evolution operator for the two qudits takes the form of a controlled-Z gate. Physical systems which could be used to implement this scheme are discussed in [10] and appropriate references therein. For the remainder of this paper, we are going to discuss the mathematical framework of this model.

Before we continue, we make one final remark about our cluster states: they satisfy a property known as *maximal connectedness*, which for our purposes we can state as follows: Given an arbitrary cluster state, if we measure any qudit of the cluster in the computational (Z) basis, the remaining states are left in a cluster state, up to some Pauli Z errors. For qubit clusters, this issue is first discussed in [12]. This fact can be used to design specific clusters from larger base clusters (e.g. a grid) as by the above, Z-measurements on a qudit effectively remove it from the cluster state. This is discussed in more detail in appendix 1.

Suppose we can use linear clusters to implement any single qudit operation. We can then use more general multi-dimensional clusters to allow the implementation of more complicated multi-qudit algorithms. One possible model is where rows of linear clusters, each representing a *logical* qudit (i.e. corresponding to a single 'qudit wire' in the circuit model) are used to

[a]Alternatively, some initial measurements on a cluster state where before any interactions are applied all qudits are initially in the state $|+\rangle$ could be used on a larger cluster to prepare this initial state.

implement single qudit operations, and entanglement (again in the form of a controlled-Z interaction) between the rows acts as an interaction between logical qudits. We will use this topology for cluster states a number of times throughout this paper; however, there are also a number of other ways of establishing this interaction between logical qudits.[b] It is a known fact that the set of one qudit gates along with any interacting two-qudit gate is sufficient to create any unitary gate on an arbitrary number of qudits (i.e. this set of gates is a *universal* set for multi-qudit quantum gates) [15]. Hence by establishing *single*-qudit universality, we obtain universality for an arbitrary number of qubits on an appropriate cluster. A diagram to illustrate this point is given in Figure 5.

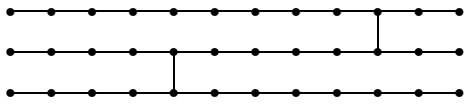

Fig. 5. An example of a topology for cluster states that can be used to establish universal quantum computation. The rows represent a logical qudit, with one-dit teleportation the mechanism for implementing single-qudit gates. The interactions between rows are used to implement two-qudit gates, and so we can implement any arbitrary multi-qudit unitary operation.

We note that although in this paper we study single-qudit universality on linear clusters, since ultimately these ideas are to be applied to larger multi-dimensional clusters, we are not contradicting the theorem of Nielsen [16] that says that quantum computation on linear clusters can be efficiently simulated on a classical computer (although the proof is for qubits, the same proof applies to qudits), as we ultimately want to use multi-dimensional clusters for multi-qudit QC.

For qubits, the set of gates given by $\mathcal{C}_2 = \{FZ(\mathbf{a}) \mid \mathbf{a} \in [0, 2\pi]^2\}$ (i.e. those that can be implemented via one-*bit* teleportation) is a *universal* set for single-qudit quantum gates.[c] In section 5 we will consider the same question for the set $\mathcal{C}_d = \{FZ(\mathbf{a}) \mid \mathbf{a} \in [0, 2\pi]^d\}$.

Finally, we note that our definition of qudit cluster states is the same as that used in [10]. In that paper the stabiliser formalism for cluster state computation (introduced in [2] and discussed later in section 4) is heavily used. We will use a much more direct approach to establish the theory.

3 Adaptive measurements and adaptive computation

In this section we outline how the unwanted X^m (generalised Pauli) operators that appear in our cluster state model can be corrected using classical computation, and by adapting, based on previous measurement results, the bases further measurements are taken in. This idea is known as *adaptive measurement*. We will also show that by changing our correction method for these errors, we can extend one-dit teleportation to a further class of quantum gates; we call this *adaptive computation*.

3.1 Adaptive measurements for single qudit operations

In using linear clusters and successive one-dit teleportation defined in the previous section to implement one-qudit quantum gates, generalised Pauli errors of the form X^m are introduced

[b] The computational power of cluster states of many shapes are studied in [13].
[c] This is equivalent to the well known Euler decomposition for 2-dimensional unitaries.

to the overall state after each measurement. What we aim to show here is a remarkable feature of the original cluster state model that spreads to our generalisation, that we can compensate for these errors using solely *classical* computation.

Suppose we have a state $|\psi\rangle = X^x Z^z U |\phi\rangle$. The U represents the quantum gate applied so far, and the powers of X and Z are the generalised Pauli errors that we have due to previous measurements. Suppose now we apply one-dit teleportation to the pair $|\psi\rangle |+\rangle$ entangled by a controlled-Z operation as usual, and we obtain the new state $X^m FZ(\mathbf{a}) |\psi\rangle$. The final state can be written as $|\psi'\rangle = X^m FZ(\mathbf{a}) X^x Z^z U |\phi\rangle$.The problem that we appear to have is that we are implementing the gate $FZ(\mathbf{a})X^x Z^z U$ rather than the intended $FZ(\mathbf{a})U$. What we want is to move the powers of X and Z through the F and $Z(\mathbf{a})$ so that they appear on the left of the overall gate $FZ(\mathbf{a})U$, so we can treat the Pauli operator as an error operator. To do this, we can make use of the following identities:

$$Z(\mathbf{a})X = XZ(\mathbf{a}'); \qquad (a'_k = a_{k-1}) \tag{7}$$

$$Z(\mathbf{a})Z = ZZ(\mathbf{a}) \tag{8}$$

$$FZ = XF, \qquad FX = Z^{-1}F \tag{9}$$

and hence (ignoring any changes in the irrelevant overall phase),

$$\begin{aligned} |\phi'\rangle &= X^m F X^x Z^z Z(\mathbf{a}^{(x)}) U |\phi\rangle \\ &= X^m Z^{-x} X^z F Z(\mathbf{a}^{(x)}) U |\phi\rangle \\ &= \omega^{xz} X^{m+z} Z^{-x} F Z(\mathbf{a}^{(x)}) U |\phi\rangle \end{aligned} \tag{10}$$

where $\mathbf{a}^{(l)}$ is defined by $a^{(l)} = a_{k-l}$, and the final step is true because $XZ = \omega ZX$. Here we have succeeded in moving the generalised Pauli operators to where we want them; the only trouble now is that the overall gate that we are implementing is not identical to the one we want. We can get round this by using an *adaptive* measurement: Given x in advance, we can use one-dit teleportation to implement the gate $FZ(\mathbf{a}^{(-x)})$ instead of $FZ(\mathbf{a})$. With this adaptation, our new state is then given by (up to phase)

$$|\phi'\rangle = X^{x'} Z^{z'} FZ(\mathbf{a}) U |\phi\rangle$$

where

$$x' \equiv m + z \mod d; \quad z' = -x \mod d. \tag{11}$$

So, by keeping track of the exponents of the X and Z operators by classical computation, and adapting the measurement taken via the original exponent values, we can apply the gate $FZ(\mathbf{a})$ to our state, up to a generalised Pauli error. The final step of the algorithm, which is (at least in all quantum algorithms to date) a measurement on the computational basis, can simply be performed without any quantum corrections to the final state, because the Z errors have no effect on the probabilities of each outcome (they only change the computational basis vectors by a phase) and the X errors permute the computational basis elements, which can be compensated for by a final classical computation.

The above process would also work if we had a multi-qudit state $|\Psi\rangle$, with generalised Pauli errors acting on each qudit, and we entangled one of its qudits with a further $|+\rangle$ qudit via a controlled-Z interaction, and then performed one-dit teleportation. This would simply

implement a one-qudit operation on the given qudit, and change the generalised Pauli errors on that qudit also. This situation often arises when using more complicated multi-dimensional clusters, and is illustrated by Figure 6.

We also note that we can move generalised Pauli errors through controlled-Z gates, because of the identities

$$\begin{aligned} CZ(Z\otimes I) &= (Z\otimes I)CZ; \qquad & CZ(I\otimes Z) &= (I\otimes Z)CZ; \\ CZ(X\otimes I) &= (X\otimes Z^{-1})CZ; \qquad & CZ(I\otimes X) &= (Z^{-1}\otimes X)CZ \end{aligned} \tag{12}$$

which are easily established directly. These identities are necessary since we will sometimes need to treat a controlled-Z interaction as an actual two-qudit gate, rather than a means to allow the use of one-dit teleportation. An example of this (from Figure 5) is the vertical interaction between rows (logical qudits): we use these to create two-qudit interacting gates. The above relations mean that if two logical qudits are in a state $(X^{x_1}Z^{z_1}\otimes X^{x_2}Z^{z_2})\,|\Psi\rangle$, applying a controlled-$Z$ gate to this and commuting it past the error operators yields a state

$$(X^{x_1}Z^{z_1-x_2}\otimes X^{x_2}Z^{z_2-x_1})(CZ)\,|\Psi\rangle\,. \tag{13}$$

3.2 Adapative computation

Given that a quantum algorithm ends in a measurement in the computational basis, generalised Pauli X or Z errors are not the only error operators that can be compensated for by a *classical* compuation. Any overall operator that only permutes computational basis elements (and possibly modifies them by a phase) is also correctable by a final classical computation.

Let us develop this idea further. Suppose we wish to implement a single unitary gate U via a series of measurements on some cluster state, but end up with $Z^kP_\rho U$, where $\rho\in S_d$ and

$$P_\rho = \sum_{l=0}^{d-1} |\rho(l)\rangle\langle l|. \tag{14}$$

We can then compensate for this at the end of a quantum algorithm via classical computation also.

With this in mind, we can ask ourselves if we can somehow adapt our scheme for computation to include correction for more general permutation errors of the form above. We can express this more formally as follows: suppose we are given a state $|\phi\rangle = Z^nP_\rho U\,|\psi\rangle$, and we

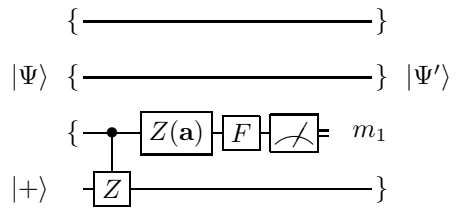

Fig. 6. One-dit teleportation applied to one qudit of a three-qudit state. It is easily seen (e.g. by writing $|\Psi\rangle = \Sigma_{ij}\,|i\rangle\,|j\rangle\,|\psi_{ij}\rangle$) that one-dit teleportation applied to one qudit of the multi-qudit state gives us the appropriate transformation on the transported qudit i.e. $|\Psi'\rangle = (I\otimes I\otimes X^mFZ(\mathbf{a}))\,|\Psi\rangle$.

wish to apply the gate $FZ(\mathbf{a})$ to the state via one-dit teleportation. We wish to establish whether we can peform a one-dit teleportation to obtain the state $|\phi'\rangle = X^m FZ(\tilde{\mathbf{a}})Z^n P_\rho U|\psi\rangle$, and then rewrite this in the form $|\phi'\rangle = Z^{m'} P_{\rho'} FZ(\mathbf{a})U|\psi\rangle$, with $\rho' \in S_d$.

A simple class of permutations for which this is possible can be defined as follows. Let c is a unit in the ring $\mathbb{Z}_d$.[d]It then follows that the operator

$$S_c = \sum_{k=0}^{d-1} |ck\rangle\langle k|$$

is a permutation operator. Furthermore, since

$$\begin{aligned} S_{c^{-1}}F &= \frac{1}{\sqrt{d}} \sum_k |c^{-1}k\rangle\langle k| \sum_l \omega^{ml}|m\rangle\langle l| \\ &= \frac{1}{\sqrt{d}} \sum_{l,m} \omega^{lm}|c^{-1}m\rangle\langle l| \\ &= \frac{1}{\sqrt{d}} \sum_{l,m} \omega^{clm}|m\rangle\langle l| \\ &= \frac{1}{\sqrt{d}} \sum_l |+_{cl}\rangle\langle l| \equiv F_c \end{aligned}$$

it may be possible to implement the gate F_c rather than F by using the identity $F = S_c S_{c^{-1}} F = S_c F_c$, and treating the remaining S_c permutation as an error operator (in the same way we treat powers of X and Z). We use the phrase *adaptive computation* to refer to this idea of implementing a different quantm gate by changing the leading error permutation that we correct for classically.

Let us suppose we are given a state $|\psi\rangle = X^x Z^z U|\phi\rangle$, which is in a linear cluster, and we measure it to induce a one dit teleportation, so the state becomes (by equation (10)) $|\psi'\rangle = X^{m+z} Z^{-x} FZ(\mathbf{a}^{(x)})U|\phi\rangle$ (if the measurement outcome is m). Note that the powers of the X and Z operators have already been updated. By applying the identity $F = S_c F_c$ here, we obtain the state

$$|\psi'\rangle = X^{m+z} Z^{-x} S_c F_c Z(\mathbf{a}^{(x)})U|\phi\rangle\,. \tag{15}$$

From this form we can see that by considering the S_c operator as an error, our computational state is equal to $F_c Z(\mathbf{a}^{(x)})U|\phi\rangle$, modulo a permutation error operator of the form $X^x Z^z S_c$. To be able to maintain this form after later one-dit teleportations and further uses of the identity $F = S_{c'} F_{c'}$ (c' any other unit in $\mathbb{Z}_d$), we need appropriate relations between S_c and the operators F, $Z(\mathbf{a})$ that appear through the measurement process; however, it can easily be verified that

$$FS_c = S_{c^{-1}}F; \quad Z(\mathbf{a})S_c = S_c Z(\mathbf{a}')\ (a'_k = a_{ck}). \tag{16}$$

which allow us to move the S_c operator to the left of the intended unitary gate (the change in $\mathbf{a}$ above will mean adaptive measurement is needed here), and furthermore since $S_c S_d = S_{cd}$,

[d]A unit in a ring is an element that has a multiplicative inverse within the ring. $\mathbb{Z}_d$ is equal to the quotient $\mathbb{Z}/(d\mathbb{Z})$, and can be thought of as the ring of modulo d arithmetic. In $\mathbb{Z}_d$, the units are the integers coprime to d (i.e. have no common factor with d). Hence, when d is prime, all non-zero elements are units; for non-prime dimensions not all elements are units e.g. 2 in $\mathbb{Z}_4$. If c is a unit, then $cj = ck$ if and only if $j = k$. This property establishes S_c as a permutation operator.

it follows that we are always able to obtain an error operator of the form $X^x Z^z S_c$, where $c = 1, \ldots, d-1$ and a unit in $\mathbb{Z}_d$.

Note that we are still using the *same* quantum process (one-dit teleportation), but a *different* classical correction procedure. This means that we can implement the gates $F^\dagger Z(\mathbf{a})$ by choosing the measurement bases appropriately.

We note that for qubits, since the only unit in $\mathbb{Z}_2$ is $1 = -1$, this means that $S_{-1} = I$, and since $F^\dagger = F$, this effect does not exist for cluster computation using qubits.

With this success for single-qudit operations, however, comes a word of warning for multi-qudit operations, through the identities

$$CZ(S_c \otimes I) = (S_c \otimes I)C[Z^c]; \quad CZ(I \otimes S_c) = (I \otimes S_c)C[Z^c] \tag{17}$$

and since in our model the interactions between qudits are fixed, these changes in the effective interaction between e.g. neighbouring linear clusters are an artefact of this framework. However, since these extra permutation operators are *not* introduced by a measurement process but instead through our choice in the classical computation, we can in theory design quantum algorithms to get round this problem or even utilise it to allow us to implement different interactions between neighbouring logical qudits. For example, since $S_{-1}^2 = I$, applying $F^\dagger$ rather than F twice in a linear cluster produces two cancelling S_{-1} factors which we no longer need worry about.

The group of permutations generated by the shifts X^j and the multiplication maps S_c is of order $\leq d(d-1)$, which is in general less than $d!$, the order of the symmetric group S_d. This means that the above does not deal with the most general permutation error. One issue with trying to correct for general permutation errors is that we would have to find a commutation relation between P_ρ and F for general ρ, which seems hard to ascertain.

We could have chosen to place the S_c operator in front of the Pauli operators; in this case, we would need the following commutation relations:

$$S_c X = X^c S_c; \quad S_c Z = Z^{c^{-1}} S_c. \tag{18}$$

These relations mean that S_c (where c is a unit in $\mathbb{Z}_d$) is a member of the *generalised local Clifford group* C_d, which we define by the normaliser of the generalised Pauli group $\mathcal{P}_d = \{\omega^a X^b Z^c \mid a, b, c \in \mathbb{Z}_d\}$ i.e.

$$C_d = \{U \in U(d) \mid UPU^\dagger \in \mathcal{P}_d \; \forall \; P \in \mathcal{P}_d\}.$$

In this case, S_c corresponds to U, and products of powers of X and Z correspond to P. By looking in this group, we may find more permutations that we can correct for. However, it can be shown that in *prime dimensions* the operators Z, X, F, S_c and P defined by $P : |j\rangle \rightarrow \omega^{j(j+1)/2} |j\rangle$ are sufficient to generate C_d (see appendix C). Since our permutations are already built out of products of X and S_c, we cannot obtain any more *single qudit* permutations from the Clifford group. This strongly suggests (but does not prove) that we cannot correct for any of the other single qudit permutation operators within cluster computation. It is harder to specify the Clifford group more generally, and so it may be the case that in non-prime dimensions one can implement further quantum gates by introducing other types of single qudit permutation error operators.

3.2.1 Adaptive computation using multi-level permutations

When working with multi-qudit quantum algorithms, we can similarly introduce *multi-qudit* permutation operators. Given an n qudit state $EU|\Psi\rangle$, where E represents an error operator on the n qudits, and $U \in U(d^n)$ the desired quantum evolution acting on an initial state $|\Psi\rangle$, we can write

$$EU|\Psi\rangle = EP.P^{-1}U|\Psi\rangle$$

i.e. we let P^{-1} become part of the quantum evolution, and P part of the error operator E. To allow us to maintain this form of error operator we need P to have appropriate relations with F and tensor products of $Z(\mathbf{a})$. For example, consider a two qudit permutation P. After moving P left through $(Z(\mathbf{a})\otimes Z(\mathbf{b}))$, the operator to the right of P must be in tensor product form, so the transformations can be implemented using single qudit measurements. Up to permutations on individual systems, the only non-trivial permutation that does this is the swap operator V, since $V(A\otimes B) = (B\otimes A)V$. This gives us a swap of two qudits for free at any time, and the above relation for V can be used to both update leading error operators and to calculate how measurement patterns need to be changed due to the introduction of the swap operator. However, we again have an issue with interacting gates between logical qudits changing form (for example, through the identity $CZ_{1,2}V_{23} = V_{23}CZ_{1,3}$; the indices represent the two systems each of these unitaries operates on). As before however, it could be that this is a help rather than a hinderance if utilised correctly. The swap can be introduced even in the qubit model, and, more generally, we can introduce any system swapping operator in this manner for an arbitrary number of qudits.[e]

3.3 Example - a variation on Deutsch-Josza

Here we give an example of using one-dit teleportations to calculate the effect of a cluster state computation, and how adaptive computation can be useful in implementing quantum algorithms on qudit cluster states.

Suppose we have a function $f : \mathbb{Z}_d^2 \to \mathbb{Z}_d; (x, y) \mapsto (x - a)(y - b)$, and we are interested in finding a and b. Classically, this will require at least two evaluations of f. In this section we will show that the quantum algorithm presented in Figure 7 can find (a, b) with one use of the function f, and that it can be implemented on a cluster state of few qudits.

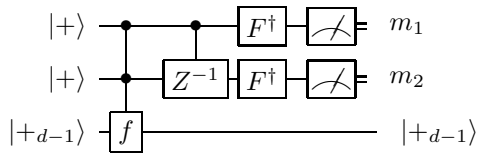

Fig. 7. The quantum circuit for finding a, b.

Let U_f be the unitary gate corresponding to the controlled evaluation of f (the first gate

[e]However, at the end of a computation before the final computational basis measurement, any permutation can be introduced in the above manner and corrected for classically, since there is no need to propogate the intoduced operators through other operators.

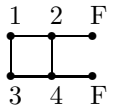

Fig. 8. The cluster state used to implement our quantum algorithm, complete with numbering for qudits (see text). The qudits labelled F represent the final two qudits at the end of the computation.

in Figure 7). It can easily be verified that

$$\begin{aligned} U_f \left|x_1\right\rangle \left|x_2\right\rangle \left|+_{d-1}\right\rangle &= \omega^{f(x_1,x_2)} \left|x_1\right\rangle \left|x_2\right\rangle \left|+_{d-1}\right\rangle \\ &= \omega^{ab} (Z^{-a} \otimes Z^{-b}) CZ \left|x_1\right\rangle \left|x_2\right\rangle \left|+_{d-1}\right\rangle \end{aligned}$$

and using this result it is easy to verify that this quantum algorithm maps the first two qudits to $\left|-a\right\rangle \left|-b\right\rangle$ (up to a phase), and so the final measurements yield the values of (a, b).

The form of the transformation induced by U_f on the first two qudits is ideal for implementation on a cluster state depicted in figure 8. The two rows will form the upper two (logical) qudits, and the vertical interactions will form interacting gates. In place of the unitary evaluation of f will be a measurement on qudits 1 and 3, since we can write $Z^k = Z(\mathbf{z}^k)$ with $(z^k)_l = 2\pi kl/d$. We will hence measure these qudits in the basis defined by $(FZ(\mathbf{z}^k))^\dagger$. To implement the $F^\dagger$ gates, we then measure in the $F^\dagger$ basis on qudits $2, 4$, and use adaptive computation in the form $F = S_{-1}F_{-1} = S_{-1}F^\dagger$. Let m_k be the result of the measurement on qudit k. We can then calculate the evolution of the cluster state algorithm (ignoring any overall phases), updating the error operators as we proceed using the relations established in the previous section:

$$\begin{aligned} \left|+\right\rangle \left|+\right\rangle &\overset{CZ}{\rightarrow} CZ \left|+\right\rangle \left|+\right\rangle = \frac{1}{\sqrt{d}} \sum_k \left|+\right\rangle \left|+_k\right\rangle \\ &\overset{\text{measure 1,3}}{\rightarrow} (X^{m_1} \otimes X^{m_3})(FZ(\mathbf{z}^{-a}) \otimes FZ(\mathbf{z}^{-b}))CZ \left|+\right\rangle \left|+\right\rangle \\ &= (X^{-a+m_1} \otimes X^{-b+m_3} S_{-1})(F \otimes F^\dagger) \frac{1}{\sqrt{d}} \sum_k \left|+\right\rangle \left|+_k\right\rangle \\ &= (X^{-a+m_1} \otimes X^{-b+m_3} S_{-1}) CZ \left|+\right\rangle \left|+\right\rangle \\ &\overset{CZ}{\rightarrow} CZ(X^{-a+m_1} \otimes X^{-b+m_3} S_{-1}) CZ \left|+\right\rangle \left|+\right\rangle \\ &= (X^{-a+m_1} Z^{b-m_3} \otimes X^{-b+m_3} Z^{a-m_1} S_{-1}) C[Z^{-1}] CZ \left|+\right\rangle \left|+\right\rangle \\ &\overset{\text{measure 2,4}}{\rightarrow} (X^{m_2} F \otimes X^{m_4} F)(X^{-a+m_1} Z^{b-m_3} \otimes X^{-b+m_3} Z^{a-m_1} S_{-1}) \left|+\right\rangle \left|+\right\rangle \\ &= (X^{b+m_2-m_3} Z^{a-m_1} S_{-1} \otimes X^{a+m_4-m_1} Z^{b-m_3})(F^\dagger \otimes F^\dagger) \left|+\right\rangle \left|+\right\rangle \\ &= \left|-b - m_2 + m_3 \mod d\right\rangle \left|-a - m_4 + m_1 \mod d\right\rangle \end{aligned}$$

The values of a and b can then be read off from the final qudits. We note two things about the above computation:

1. The measurement of qudits 1 and 3 introduce extra F gates on both logical qudits not present in the original algorithm. However, because $(F \otimes F^\dagger)CZ \left|+\right\rangle \left|+\right\rangle = CZ \left|+\right\rangle \left|+\right\rangle$, by using the identity $F = S_{-1}F^\dagger$ on one qudit, these extra gates do not affect the rest

of the computation, except for the fact that the first qudit corresponds to the value of b rather than a as in the circuit of Figure 7 (and vice versa).

2. The original algorithm requires the use of a controlled-Z^{-1} gate, where as our cluster state only has controlled-Z gate between the logical qudits. However, pulling through the S_{-1} error operator (introduced in the previous step) to the left through the CZ gate between qudits 2 and 4, the CZ gate changes into a $C[Z^{-1}]$ gate.

While this example thought of purely as a quantum algorithm is a bit of a toy example, it does illustrates not only how adaptive computation can be helpful in the implementation of algorithms on cluster states, but also how the non-trivial commutation relation between S_c and CZ can actually prove to be of help rather than a hinderance.

4 The stabiliser formalism for cluster state QC

Up to this point, we have presented a completely self-contained approach to cluster state computation. Most of the current papers [1, 2, 10] take a much more algebraic approach using the *stabiliser formalism*, developed by Gottesman [17] in the context of error-correcting quantum codes. The stabiliser formalism allows us to describe cluster states through sets of eigenvalue equations, and manipulation of these eigenvalue equations leads to a theorem that can be used to establish how a particular set of measurements can implement a quantum gate on a particular cluster state. In this section we will briefly summarise this approach, and compare the merits of the two.

4.1 Representation of cluster states using stabilisers

Before we describe how stabilisers can be used to represent cluster states, let us give a more formal definition of cluster states. Let $G = (V, E)$ be a graph; the set V are the vertices (this corresponds to a labelling of our physical qudits) and $E \subseteq V \times V$ are the edges of G (corresponding to which pairs of vertices have a controlled-Z interaction between them). For $a \in V$, let $|.\rangle_a$ represent the state of qudit a. Then our cluster state $|\phi\rangle_{C(G)}$ can be written as

$$|\phi\rangle_{C(G)} = \left(\prod_{(a,b)\in E} CZ_{(a,b)} \right) \left(\bigotimes_{a\in V} |+\rangle_a \right)$$

where $CZ_{(a,b)}$ represents the controlled-Z gate between qudits a and b.

It can be shown [2, 10] that $|\phi\rangle_{C(G)}$ is uniquely determined (up to phase) by the eigenvalue equations

$$X_a^\dagger \otimes \left(\bigotimes_{b\in N(a)} Z_b \right) |\psi\rangle = |\psi\rangle$$

where U_a is the application of the unitary U to qudit a, and $N(a) = \{b \in V \mid (a, b) \in E\}$ represents the neighbours of qudit a i.e. the qudits b connected to a by an interaction (edge in G). The operators $S(a) = X_a^\dagger \otimes \left(\bigotimes_{b\in N(a)} Z_b \right)$ are the *stabilisers* of the state $|\phi\rangle_{C(G)}$, and totally determine up to an irrelevant phase the cluster state.

4.2 Measurement patterns in the stabiliser formalism

Before we can state the main result that shows how stabilisers can be used to help find measurement patterns that implement useful quantum algorithms, we need to establish a few definitions. Given a cluster state $|\phi\rangle_{C(G)}$, let us break its graph up into three parts: an input cluster $C_I(G)$ and output cluster $C_O(G)$, and the remaining body of the cluster, which we will denote $C_M(G)$. We will number the n qudits in $C_I(G)$ and $C_O(G)$ from 1 to n, where qudit i in the output cluster can be thought of as qudit i from the input cluster after the quantum computation has concluded. We suppose further that the n qudits in $C_I(G)$ can, before any interactions between qudits is applied, be initialised in the more general entangled state $|\psi(\text{in})\rangle$.

We define a *measurement pattern* on a cluster $C(G)$ to be a set of the form of a function $M_{C(G)} : V \to U(d)$, such that the columns of the unitary matrix $M_{C(G)}(a)$ form the measurement basis on qudit a in the cluster.[f] If the measurement outcomes form a vector $\mathbf{m}$, let $P(M_{C(G)}, \mathbf{m})$ represent the projector onto the states corresponding to the particular measurement outcomes.

We are now ready to state the main theorem for cluster state QC and stabilisers:

Theorem 1 ([2, 10])**.** *Suppose the state* $|\psi\rangle_{C(G)} = (I_{C_I(G)} \otimes P(\mathcal{M}_{C(G)}, \mathbf{m}) \otimes I_{C_O(G)}) |\phi\rangle_{C(G)}$ *obeys the* $2n$ *eigenvalue equations*

$$X_{i,C_I(G)}(UX_iU^\dagger)_{C_O(G)} |\psi\rangle_{C(G)} = \omega^{\lambda_{x,i}} |\psi\rangle_{C(G)} \tag{19}$$

$$Z^\dagger_{i,C_I(G)}(UZ_iU^\dagger)_{C_O(G)} |\psi\rangle_{C(G)} = \omega^{\lambda_{z,i}} |\psi\rangle_{C(G)} . \tag{20}$$

Then, if $\mathcal{M}_{C_I(G)} = \{(i, F_i) \mid i \in C_I(G)\}$*, and the measurement outcomes on* $C_I(G)$ *are given by* s_i*, then after all measurements on* $C_I(G)$ *and* $C_M(G)$ *of* $|\phi\rangle_{C(G)}$*, the final state* $|\psi(out)\rangle_{C_O(G)}$ *is given by* $|\psi(out)\rangle_{C_O(G)} = UU_e |\psi(in)\rangle$*, where*

$$U_e = \bigotimes_{i=1}^{n} (Z_i)^{\lambda_{x,i} - s_i} (X_i)^{\lambda_{z,i}}.$$

The unitary gate U and the numbers $\lambda_{x,i}, \lambda_{z,i}$ can all depend on the outcomes of the measurements on the input and body parts of the cluster state. Many examples of the use of this formalism can be found in [2, 10].

4.3 A comparison of the two approaches to cluster state QC

The two approaches to cluster state QC that we have mentioned are very different. The stabiliser formalism is a powerful tool in establishing cluster states and measurements on them to implement particular quantum gates, but as examples in [2] show, using it is an involved and difficult process. The one-dit teleportation approach described here is a much more elementary description of the model, and it has two important advantages over the stabiliser approach. Since this approach is very closely linked to the circuit model for quantum computation, it means that it is possible to use some of the intuition and results from this line of thought in designing quantum algorithms using cluster states. This approach is also

[f] This definition differs slighlty from that used in other papers but is completely equivalent.

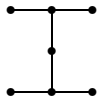

Fig. 9. An example of a cluster that we cannot evaluate using one-dit teleportations alone.

the easiest to understand as it uses no more than some basic linear algebra to establish the theory behind the model.

The fact however that the one-dit teleportation approach is so closely linked to the ciruit model means that this approach is not suitable for considering all possible cluster states. Up to this point, we have always implicitly considered clusters that are in a grid (two-dimensional), such that each row of entangled qudits corresponds to a logical qudit, to which we apply successive one-dit teleportations, and any vertical interactions (columns) form two-qudit gates between logical qudits (as in Figure 4). However, clusters where a row does not form a logical qubit of the computation, but forms part of an interaction between logical qudits, cannot have one-dit teleportation ideas applied to it. The cluster in Figure 9 is an example of this. The central qudit causes the problem: its presence means that there are not two disjoint paths from left to right through the cluster such that every qudit is in one path, so we cannot treat the cluster by implementing one-dit teleportations along the paths (to give single qudit operations) and considering links between the paths as interacting gates.

Another issue with the one-dit teleportation approach is that of the timings of the measurements. In all of our clusters so far, all measurements in a row of entangled qudits must be taken 'from left to right' i.e. we must apply each teleportation in turn. While we could make joint measurements of qudits where no adaptive measurements take place, we cannot measure the qudits out of turn in the teleportation approach. Examples in [2] using the stabiliser method however distinctly allow measurements to be taken in an arbitrary order (up to the issue where some measurements may depend on other measurement results).

Importantly though, the tool of adaptive computation does not naturally arise within the stabiliser formalism. It seems difficult to incorporate the extra operator errors that arise from adaptive computation into the major theorem above (particularly as their deterministic origin differs from the randomness of the origin of the Pauli operators), and it remains to be seen if there is an elegant or natural way that these two methods could be combined. The fact that the same quantum process is taking place but a different correction procedure is implemented would somehow have to be reflected in any such grander theorem.

5 Universal gates

In this section we are going to discuss how we can implement any unitary evolution on a single qudit using linear clusters of qudits. Universality for many qudits using multi-dimensional clusters follows from the comments in section 2.

5.1 An approach to generating unitary gates

In this section we are going to present a couple of basic results that present a possible method of generating unitary transformations on any QC system.

We start by quoting the following result:

Lemma 2 (p48, [19]). *Let H_k be a basis over the reals for the space of $d \times d$ Hermitian matrices. Then any $U \in U(d)$ can be formed by products of the matrices $\exp(i\beta_k H_k)$ for real β_k.*

Now, given a matrix U, with eigenvectors $|U_j\rangle$, we will define

$$U(\mathbf{a}) = \sum_k e^{ia_k} |U_k\rangle\langle U_k|. \tag{21}$$

Suppose we can find a (minimal) set of matrices $U_1, \ldots, U_m$ such that the projectors onto the eigenvectors of these matrices form (over the reals) a spanning set for the space of $d \times d$ hermitian matrices. It follows from lemma (2) that products of the unitaries from the set

$$\mathcal{C} = \{U_j(\mathbf{a}) | j \in \{1, \ldots, d\},\ \mathbf{a} \in [0, 2\pi]^d\}$$

is enough to generate any unitary in $U(d)$.[g]

This result in itself does not specifically apply to our model of QC yet; we need to add more constraints to the kinds of bases that we can use.

5.2 Mutually unbiased bases and Hermitian matrices

To motivate this discussion, we will state here (and prove later) that, using a linear cluster of three qudits and two measurements, with the first (left-most) qudit in a given state $|\psi\rangle$, we can implement the gates $Z(\mathbf{a})$ and $X(\mathbf{a}) = \sum_k e^{ia_k}|+_k\rangle\langle+_k|$ for any dimension d. The two bases $\{|k\rangle\}_{k=0}^{d-1}$ and $\{|+_k\rangle\}_{k=0}^{d-1}$ are what we call *mutually unbiased*, a property defined as such:

Definition 1. *Two bases $\{|a_k\rangle\}_{k=0}^{d-1}$ and $\{|b_k\rangle\}_{k=0}^{d-1}$ are **mutually unbiased** if $|\langle a_i|b_j\rangle| = 1/\sqrt{d}$ for all i, j.*

Indeed, if we accept one-dit teleportation as the basis of the cluster state model, the only bases that we can measure are those that are mutually unbiased with respect to the standard basis. We can take this connection further with the following observation:

Lemma 3. *Let $\{|\psi_j^k\rangle\}_{j=1}^d$ be $d+1$ bases of $\mathbb{C}^d$ (with $k = 1, \ldots, d+1$), such that they are mutually unbiased. Then real combinations of projectors of all these vectors span the space of $d \times d$ Hermitian matrices.*

This arises from the fact that mutually unbiased bases arise in the problem of quantum state determination. In the limit of many measurements, measurements in each of a full set of $d+1$ mutually unbiased bases are enough to specify any Hermitian matrix [20]. So mutually unbiased bases are potentially a route into finding a basis of projectors for the set of Hermitian matrices that are appropriate to our model.

We will list briefly some known facts about mutually unbiased bases. It is known [20, 21] that the maximum number of possible mutally unbiased bases in dimension d is $d+1$. In dimensions that are prime powers, a construction is known that gives this maximal possible number of such bases [20, 21]. However, more generally no construction is known to find such a maximal set in arbitrary dimension. For the first non-prime power case, $d = 6$, there are 3 known MUBs, but it is not known if any larger set exists.

[g] Note that we not using operators of the form e.g. $exp(i\alpha Z)$ for some real α, as is used for qubits. This is because for $d \geq 3$, Z, X are not hermitian, and so $exp(i\alpha Z), exp(i\alpha X)$ are not unitary matrices.

5.3 An explicit construction for prime dimensions

For dimension d a prime, it can be shown via a result of [21] that a set of $d+1$ mutually unbiased bases can be obtained via the eigenvectors of the $d+1$ matrices

$$Z, X, ZX, ZX^2, \ldots, ZX^{d-1}.$$

The bases $\{|k\rangle\}_{k=0}^{d-1}$ and $\{|+_k\rangle\}_{k=0}^{d-1}$ are the eigenvectors of Z and X respectively.

What we will show in this section is that we can generate the gates $Z(\mathbf{a})$, $X(\mathbf{a})$ and $ZX^k(\mathbf{a})$ for prime dimensions on linear clusters. Then, by the results of the previous two sections, this will establish single-qudit universality on linear clusters as required.

It is easy to implement $Z(\mathbf{a})$ and $X(\mathbf{a})$ in any dimension using two measurements on a linear cluster of size three, because we may write

$$Z(\mathbf{a}) = F^\dagger.FZ(\mathbf{a}); \quad X(\mathbf{a}) = FZ(\mathbf{a}).F^\dagger.$$

and hence by appropriate one-dit teleportations and use of adaptive computation we can implement these gates.[h] We note that this scheme uses fewer measurements to implement these gates than the one given in [10]. These two gates will be the building blocks for implementing the gates $ZX^k(\mathbf{a})$. The following lemma is crucial in allowing us to do this:

Lemma 4. *Let $\{|\psi_j^k\rangle\}_{j=1}^d$ be the eigenvectors of ZX^k for $k = 1, \ldots, p-1$, with eigenvalues ω^j. There exists a phase transformation $Z(\mathbf{b}_k)$ such that*

$$Z(\mathbf{b}_k)\,|+_j\rangle = |\psi_{jk}^k\rangle\,.$$

The index jk in the ket determines which eigenstate of ZX^k the phase transformation $Z(\mathbf{b}_k)$ maps $|+_j\rangle$ onto; importantly, the index is *not* solely j, and depends on k. The proof of the lemma is a little technical and hence we postpone it to appendix B. The result of this is that we may write

$$ZX^k(\mathbf{a}) = Z(\mathbf{b}_k)X(\mathbf{a}^{(\times,k)})Z(\mathbf{b_k})^\dagger$$

where $\mathbf{a}^{(\times,k)}$ is a permutation of the elements of $\mathbf{a}$ defined by $a_l^{(\times,k)} = a_{k^{-1}l}$. Hence we can decompose $ZX^k(\mathbf{a})$ as

$$ZX^k(\mathbf{a}) = F^\dagger.FZ(\mathbf{b}_k).FZ(\mathbf{a}^{(\times,k)}).F^\dagger Z(-\mathbf{b_k})$$

and so we can implement these gates using four measurements and use of adaptive computation.

5.4 The $d = 3$ case

In this section we will give the above results in dimension 3 in more detail, to show explicitly which measurements are needed to implement each gate.

In dimension 3, we have four primitive gates in our construction: $Z(\mathbf{a}), X(\mathbf{a}), ZX(\mathbf{a})$ and $ZX^2(\mathbf{a})$. We need the eigenvectors of each of the matrices Z, X, ZX and ZX^2. The

[h] Note that the gate $F^\dagger$ can be implemented without the use of adaptive computation with three one-dit teleportations, since $F^\dagger = F^3$, but this takes up more resources.

computational basis elements are the eigenvectors of Z. The eigenvectors of X are the columns of F i.e.

$$\begin{aligned} |+_0\rangle &= \tfrac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + |2\rangle\right) \\ |+_1\rangle &= \tfrac{1}{\sqrt{3}}\left(|0\rangle + \omega\,|1\rangle + \omega^2\,|2\rangle\right) \\ |+_2\rangle &= \tfrac{1}{\sqrt{3}}\left(|0\rangle + \omega^2\,|1\rangle + \omega\,|2\rangle\right); \end{aligned}$$

the eigenvectors of ZX are

$$\begin{aligned} |ZX_0\rangle &= \tfrac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + \omega^2\,|2\rangle\right) \\ |ZX_1\rangle &= \tfrac{1}{\sqrt{3}}\left(\omega^2\,|0\rangle + |1\rangle + |2\rangle\right) \\ |ZX_2\rangle &= \tfrac{1}{\sqrt{3}}\left(|0\rangle + \omega^2\,|1\rangle + |2\rangle\right); \end{aligned}$$

and the eigenvectors of ZX^2 are

$$\begin{aligned} \left|ZX_0^2\right\rangle &= \tfrac{1}{\sqrt{3}}\left(|0\rangle + \omega\,|1\rangle + |2\rangle\right) \\ \left|ZX_1^2\right\rangle &= \tfrac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + \omega\,|2\rangle\right) \\ \left|ZX_2^2\right\rangle &= \tfrac{1}{\sqrt{3}}\left(\omega\,|0\rangle + |1\rangle + |2\rangle\right). \end{aligned}$$

By utilising the proof of lemma 4 in appendix B (or indeed by direct verification) defining $\mathbf{b}_1 = (0, 0, 4\pi/3)^T$ and $\mathbf{b}_2 = (0, 2\pi/3, 0)^T$, so that

$$Z(\mathbf{b}_1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \quad Z(\mathbf{b}_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we have that

$$\begin{aligned} Z(\mathbf{b}_1)\,|+_0\rangle &= |ZX_0\rangle \\ Z(\mathbf{b}_1)\,|+_1\rangle &= \omega\,|ZX_1\rangle \\ Z(\mathbf{b}_1)\,|+_2\rangle &= |ZX_2\rangle \end{aligned}$$

and

$$\begin{aligned} Z(\mathbf{b}_2)\,|+_0\rangle &= \left|ZX_0^2\right\rangle \\ Z(\mathbf{b}_2)\,|+_1\rangle &= \omega^2\left|ZX_2^2\right\rangle \\ Z(\mathbf{b}_2)\,|+_2\rangle &= \left|ZX_1^2\right\rangle. \end{aligned}$$

From these relations we can deduce that

$$ZX(\mathbf{a}) = Z(\mathbf{b}_1)X(\mathbf{a})Z(\mathbf{b_1})^\dagger$$

and

$$ZX^2(\mathbf{a}) = Z(\mathbf{b}_2)X(\mathbf{a}')Z(\mathbf{b_2})^\dagger$$

where $\mathbf{a}'$ is defined by

$$a_1' = a_1; \quad a_2' = a_3; \quad a_3' = a_2$$

and using the measurement patterns in the previous subsection we can implement these gates on linear clusters.

The issue of adaptive computation in this dimension is simple, because only when $c = -1$ is S_c unitary and not equal to the identity. So we can implement the gates $FZ(\mathbf{a})$ and $F^\dagger Z(\mathbf{a})$ in this dimension, and by doing so we only introduce one new kind of error, namely that introduced by S_{-1}.

Furthermore, it is easy to show that the shift permutation (312) and the transposition (23) generate the whole of the permutation group S_3; these permutations correspond to X and S_{-1} and so when $d = 3$ we can in fact correct for all possible permutation errors.

5.5 Other cases

As noted above, constructions for full sets of mutually unbiased bases exist in all prime power dimensions, but their constructions are not as simple as the one listed above. In [21], an explicit description for a set of mutually unbiased bases in $d = 4$ is given, and can be seen by inspection that a relationship similar to that for prime dimensions given by lemma (4) can be given. It remains to be seen whether this relationship exists more generally.

Furthermore, these mutually unbiased bases should be compatible with our scheme for generating universal gates in the cluster state model. Ideally one of the bases should coincide with the Fourier basis (1), to fit in with the F transformation from one-dit teleportation. This is not the case in the example in [21], which makes the task of generalising the ideas in this paper to non-prime dimensions more difficult.

It is clearly not the case however that non-existence of a full set of MUBs implies that our cluster state model is not universal. It is established in [10] that our given model is universal for all dimensions. They also prescribe a method which is equivalent to finding a set of projectors that is not only a basis for the set of Hermitian matrices, but also suitable for the cluster state model. It remains to be seen whether the model can be described more directly as in this paper.

6 Conclusion

In this paper we have developed a framework for quantum computation using cluster states with qudits as our basic physical resource, and while we have recovered all of the features of the qubit model, we have found that the extra degrees of freedom in using qudits allows us to control the quantum computation using adaptive computation in a way that is not possible (for single qudit operations) when using qubits. The cases of prime dimension lend themselves particularly well to a simple description, and as a result it is hopeful that these ideas could be taken further and used to design quantum algorithms on qudits.

One important issue we have not covered in this paper is that of fault tolerance. There are a number of works on this issue specifically pertaining to the qubit cluster state model [8, 23, 25], and given the similarities between this and the qudit model, it seems likely that a number of the results may well jump across to the qudit model. How the issue of adaptive computation will fit into the picture could however be a sticking point for generalising these results.

The most technologically advanced physical implementation of cluster state QC is an optical solution as proposed by Nielsen [4] and refined by Browne and Rudolph [22]. A photon can be thought of as a qubit by treating the polarisation of the photon as the relevant degrees of freedom, and in [24] Knill, Laflamme and Milburn presented a scheme for entangling

photons using measurement. This idea is at the center of Nielsen's proposal; Browne and Rudolph present another optical scheme that is more efficient in its use of resources (linear optical elements).[i] However, by using other degrees of freedom present for photons, they could be potentially thought of as qudits. It would most definitely be interesting if one could find a scheme that is similar to any of the above proposals, but within which photons are treated as qudits, and furthermore, whether this idea lends itself to a scheme for qudit cluster state quantum computation.

A number of other interesting questions arise from this model. One immediate question is whether the computational paradigm that arises from adaptive computation lends itself to solving a particular class of problems. Furthermore, we have not explored the potential for designing clusters with controlled-Z^k interactions, as was mentioned in section 3. Finally, we have not made any attempt here to consider fundamentally the role of entanglement within the cluster state model. This encompasses a large number of potential questions, and further investigation could lead to some insight into the relationship between computation and entanglement.

Acknowledgements

The author would like to thank Tony Sudbery for reading this manuscript and his continual support throughout the research, Terry Rudolph whose presentation on cluster states encouraged the author to tackle this subject, Simone Severeni for a useful discussion, Sam Braunstein for the use of his library, Paul Butterley and Calvin Smith for pointing out a number of mistakes in the final draft, and the Engineering and Physical Science Research Council (U.K.) for financial support. The circuit diagrams were created using Qcircuit, available at `http://info.phys.unm.edu/Qcircuit`.

References

1. R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001)
2. R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003)
3. R. Raussendorf and H. J. Briegel, J. Mod Opt. **49**, 1299 (2002).
4. M. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004)
5. P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Nature **454**, 169 (2005)
6. A. D. Greentree, S. G. Schirmer, F. Green, L. C. L. Hollenberg, A. R. Hamilton, and R. G. Clark , Phys. Rev. Lett. **92**, 097901 (2004)
7. F. Verstraete and J. I. Cirac, Phys. Rev. A **70** 060302 (R) (2004)
8. P. Aliferis and D. W. Leung, quant-ph/0503130
9. M. Nielsen, Journal club notes on cluster state quantum computation, `http://www.qinfo.org/qc-by-measurement/cluster-state.pdf`
10. D. L. Zhou, B. Zeng, Z. Xu, and C. P. Sun, Phys. Rev. A **68**, 062303 (2003)
11. P. Aliferis and D. W. Leung, Phys. Rev. A **70**, 062314 (2004)
12. H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001)
13. A. M. Childs, D. W. Leung, and M. A. Nielsen, Phys. Rev. A **71**, 032318 (2005)
14. E. Knill, quant-ph/9608048
15. J.-L. Brylinski and R. Brylinski, quant-ph/0108062

[i] Expermiental work using photonic cluster states has been reported in [5].

16. M. Nielsen, Rev. Math. Phys. (to be published); quant-ph/0504097
17. D. Gottesman, Ph.D. Thesis (Caltech); quant-ph/9705052
18. D. Gottesman, `http://www.perimeterinstitute.ca/personal/dgottesman/CO639-2004/Sols5.pdf`
19. R. R. Puri, *Mathematical Methods of Quantum Optics* (Springer, Berlin, 2001)
20. W. K. Wootters and B. D. Fields, Annals of Physics **191**, 363 (1989)
21. S. Bandyopadhyay, P.O. Boykin, V.P. Roychowdhury, F. Vatan, Algorithmica **34**, 512 (2002)
22. D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005)
23. M. Varnava, D. E. Browne, and T. Rudolph, quant-ph/0507036
24. E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001)
25. R. Raussendorf, Ph.D. Thesis (Munich); `http://edoc.ub.uni-muenchen.de/archive/00001367/01/Raussendorf_Robert.pdf`

Appendix A Maximal connectedness of cluster states

This appendix establishes the result that if any one qudit in a cluster is measured, the remaining qudits form a cluster state up to some Pauli Z errors. As mentioned in the body of the text, for cluster of qubits this issue was first discussed in [12]; here we give a different but elementary proof of the same fact.

Let $|\psi\rangle$ be a cluster state. Since all the controlled-Z interactions between pairs of qudits commute, we can write this as

$$|\psi\rangle = S\,|+\rangle\,|\psi'\rangle$$

where $|\psi'\rangle$ is the cluster state of all but one of the qudits, and S represents the controlled-Z interactions with the remaining $|+\rangle$ qudit. We can write the above as

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{d}} S \sum_{k=0}^{d-1} |k\rangle\,|\psi'\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle\,(Z^k \otimes \ldots \otimes Z^k \otimes I \otimes \ldots \otimes I)\,|\psi'\rangle \end{aligned}$$

where the Z^k operators act only on the qudits that are immediately connected to the final qudit (that is, those that have been made to interact with the final qudit by a controlled-Z operation). It is clear from this form that measuring this qudit in the computational basis and obtaining result j will project the rest of the state onto a cluster state with Pauli Z^j errors on all qudits that were adjoined to the measured qudit in the original cluster.

Since the cluster state of two qudits is equivalent (up to unitaries on the individual qudits) to a Bell state, our notion of maximal connectedness is identical to that discussed for linear clusters in [12].

Appendix B Proof of lemma 4

To prove the lemma, we first need to compute the eigenvectors of ZX^k in prime dimensions $d \geq 3$.

Lemma 5. *Define* $\left|\underline{\alpha}^{(k)}\right\rangle$ *by*

$$\left|\underline{\alpha}^{(k)}\right\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\alpha_l}\,|l\rangle$$

where $\underline{\alpha}$ *satisfies* $\alpha_{l+k} + l \equiv \alpha_l \mod d$ *(with mod* d *arithmetic in indices also). Then* $\left|\underline{\alpha}^{(k)}\right\rangle$ *is an eigenvector of* ZX^k *with eigenvalue 1.*

Proof. Rewrite $\left|\underline{\alpha}^{(k)}\right\rangle$ as

$$\left|\underline{\alpha}^{(k)}\right\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\alpha_{l+k}} |l+k\rangle$$

(with modulo d addition as appropriate). Then

$$\begin{aligned} ZX^k \left|\underline{\alpha}^{(k)}\right\rangle &= \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\alpha_{l+k}+l} |l\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\alpha_l} |l\rangle \\ &= \left|\underline{\alpha}^{(k)}\right\rangle. \end{aligned}$$

□.

The other eigenvectors of ZX^k are then given by $X^{-m}\left|\underline{\alpha}^{(k)}\right\rangle$, since

$$\begin{aligned} ZX^k.X^{-m}\left|\underline{\alpha}^{(k)}\right\rangle &= \omega^m X^{-m}.ZX^k \left|\underline{\alpha}^{(k)}\right\rangle \\ &= \omega^m X^{-m} \left|\underline{\alpha}^{(k)}\right\rangle \end{aligned}$$

For definiteness, we define the phases of the eigenvectors by letting $\left|\psi_0^k\right\rangle = \left|\underline{\alpha}^{(k)}\right\rangle$, with $\alpha_0^{(k)} = 0$, and $\left|\psi_j^k\right\rangle = X^{-j}\left|\underline{\alpha}^{(k)}\right\rangle$. The following lemma is equivalent to lemma 4:

Lemma 6. *Let* $\{\left|\psi_j^k\right\rangle\}_{j=0}^{d-1}$ *be the eigenvectors of* ZX^k *for* $k = 1, \ldots, p-1$ *as defined above. Then there exists a phase transformation* $Z(\mathbf{b}_k)$ *such that*

$$Z(\mathbf{b}_k)\,|+_j\rangle = \omega^{\frac{1}{2}j(j+1)k}\left|\psi_{jk}^k\right\rangle.$$

Proof. By the above lemma,

$$\left|\psi_m^k\right\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\alpha_l} |l+m\rangle$$

where $\alpha_{l+k} + l \equiv \alpha_l \mod d$. Define $\mathbf{b}_k$ by $(b_k)_l = \alpha_l$. Then

$$Z(\mathbf{b}_k)\,|+_{-j}\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\alpha_l - jl} |l\rangle.$$

However, it is easily seen (e.g. by induction) that, for any r, s,

$$\alpha_l \equiv \alpha_{l+jk} + jl + \frac{1}{2}j(j-1)k \tag{B.1}$$

and hence

$$\begin{aligned} Z(\mathbf{b}_k)\,|+_{-j}\rangle &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{\alpha_{l+jk}+\frac{1}{2}j(j-1)k}\,|l\rangle \\ &= \omega^{\frac{1}{2}j(j-1)k}\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{\alpha_{l+jk}}\,|l\rangle \\ &= \omega^{\frac{1}{2}j(j-1)k}\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{\alpha_l}\,|l-jk\rangle \\ &= \omega^{\frac{1}{2}j(j-1)k}\left|\psi^k_{-jk}\right\rangle \end{aligned}$$

So we have that

$$Z(\mathbf{b}_k)\,|+_j\rangle = \omega^{\frac{1}{2}j(j+1)k}\left|\psi^k_{jk}\right\rangle$$

and since the dimension here is prime, as j runs over all values $0,\ldots,k-1$, so does jk. □. We can recover lemma 4 from this by the phase transformation $\left|\psi^k_j\right\rangle \mapsto \omega^{\frac{1}{2}j(jk^{-1}+1)}\left|\psi^k_j\right\rangle$,

hence removing the phase that appears in the above lemma.

The eigenvectors of ZX for $d=2$ are given by $|\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)$. The above proof fails because (B.1) is only self-consistent when d is odd: By substituting j for d, then modulo d, we obtain that $\alpha_l \equiv \alpha_{l+dk} + dl + \frac{1}{2}d(d-1)k \equiv \alpha_l + \frac{1}{2}d(d-1)k \mod d$ i.e. we require $\frac{1}{2}d(d-1)k \equiv 0 \mod d$, which is true if and only if d is odd. However, lemma 4 still holds: let $\mathbf{b} = (0,\pi)$. Then $Z(\mathbf{b}) = |0\rangle\langle 0| + i|1\rangle\langle 1|$, and it is easy to verify that

$$Z(\mathbf{b})\,|+_0\rangle = |\psi_+\rangle\,; \quad Z(\mathbf{b})\,|+_1\rangle = |\psi_-\rangle\,.$$

Appendix C The Clifford group in prime dimension

The sole result of this appendix is a result of Gottesman [18]:

Lemma 7. *The Clifford group C_d (normaliser of the generalised Pauli group $\mathcal{P}_d$) is, when d is a prime, generated by the operators Z, X, F, S_c and P defined by $P : |j\rangle \to \omega^{j(j+1)/2}\,|j\rangle$.*

Proof. The one-qudit Pauli group consists of elements of the form $\omega^a X^b Z^c$. Let us (for now) ignore the preceding powers of ω. Then, under conjugation by a Clifford group operation (i.e. for $U \in C_d$, the transformation is the conjugation $P \mapsto UPU^\dagger$), we must have that (up to phases) $X \mapsto X^i Z^j$ and $Z \mapsto X^k Z^l$. For $A, B \in \mathcal{P}_d$, define $\alpha(A,B)$ by $AB = \omega^{\alpha(A,B)}BA$. Under conjugation by a Clifford operation, this commutation relation is preserved and so we must have that $\alpha(X^iZ^j, X^kZ^l) = \alpha(X,Z) = 1$. Furthemore,

$$\begin{aligned} \alpha(X^iZ^j, X^kZ^l) &= \alpha(Z^j, X^k) + \alpha(X^i, Z^l) \\ &= jk\alpha(Z,X) + il\alpha(X,Z) = il - jk \end{aligned}$$

and so a general Clifford operation is an element of $\mathcal{P}_d$ (to choose the phases for the images of X and Z) times some operation from some class of operations labelled by (i,j,k,l), with $il - jk = 1$. We know that the Pauli operators are in the Clifford group, and so we can ignore

any phases as the Pauli operators can correct for these. We split up considering the full set of operations into two groups. First let us assume that $i \neq 0$. It can be shown via elementary methods that if we define $C(i,m,n) = S_i P^m Q^n$ (where $Q = FPF^\dagger$), then, under conjugation by $C(i,m,n)$,

$$X \mapsto X^i Z^{-i^{-1}m}; \quad Z \mapsto X^{in} Z^{i^{-1}(1-mn)}$$

(note that since $i \neq 0$, i always has an inverse). By choosing $m = -ij$ and $n = i^{-1}k$, we find that $X \mapsto X^i Z^j$ and $Z \mapsto X^k Z^l$, with $l = i^{-1}(1+jk)$ as required. This gives us all Clifford operations for $i \neq 0$. For $i = 0$, we must then have $jk = 1$, and so $j \neq 0$. We wish to implement the operation $X \mapsto Z^j$ and $Z \mapsto X^k Z^l$. We can do this by first performing $X \mapsto X^{-j}$ and $Z \mapsto Z^k X^{-l}$ (which can be done from the calculations above) and then conjugating by F to implement the required transformation. This gives us all Cifford group operations. □.

The above proof does not work for non-prime dimensions because of the need for inverses of all non-zero elements in $\mathbb{Z}_d$, which only exist if d is prime.