Universality of quantum computation with cluster states and (X,Y)-plane measurements

Atul Mantri,[1] Tommaso F. Demarie,[1] and Joseph F. Fitzsimons[1, 2]

[1]*Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372*
[2]*Centre for Quantum Technologies, National University of Singapore,*
Block S15, 3 Science Drive 2, Singapore 117543

Measurement-based quantum computing (MBQC) is a model of quantum computation where quantum information is coherently processed by means of projective measurements on highly entangled states. Following the introduction of MBQC, cluster states have been studied extensively both from the theoretical and experimental point of view. Indeed, the study of MBQC was catalysed by the realisation that cluster states are universal for MBQC with (X,Y)-plane and Z measurements. Here we examine the question of whether the requirement for Z measurements can be dropped, while maintaining universality. We answer this question in the affirmative by showing that universality is possible in this scenario.

I. INTRODUCTION

Cluster states [1] are highly entangled quantum states that play the role of central resources in measurement-based quantum computing (MBQC). While the canonical understanding of quantum computation relies on the imagery and concepts of quantum circuits [2], MBQC recreates the full toolbox of wires and gates by means of local adaptive quantum measurements on said cluster states. This point of view is particularly appealing because it replaces the issue of coherently controlling quantum states with the less experimentally challenging action of creating an entangled resource at the initial stage of the computation. Indeed cluster states can be created efficiently in any system with a quantum Ising-type interaction (at very low temperatures) between two-state particles in a lattice configuration. In its original formulation [3], universality of MBQC was shown using a cluster state and single-qubit projective measurements: Precisely, this universality proof makes use of (X, Y)-plane measurements as well as Z-basis (computational) measurements used to remove redundant qubits from the cluster state. Such formulation of the MBQC universality proof is still considered today as *the benchmark proof*, particularly because of its simple intuitive power. Nonetheless it seems fair to ask whether universality can be achieved limiting the measurements to a single plane of the Bloch sphere.

Beyond more fundamental reasons, the motivation to reduce the angle set to a single plane follows from the prevalent formulation of delegated quantum computing (DQC) protocols. Critically, the adaptive nature of MBQC proved to be of great importance in the development of secure DQC: The first universal and unconditionally secure blind quantum computing protocol presented in [4] is entirely based on MBQC and exploits the interaction between a client and a server to protect the client's information. In this protocol, measurements are performed by the server and belong solely to the (X, Y)-plane. This succeeds because the resource state considered is a brickwork state, which can be prepared by performing an appropriate pattern of Z-measurements on a cluster state. More recently, there has been a plethora of work on blind DQC grounded on MBQC, see for example [5–9] and references therein (for a more general discussion about DQC we refer the readers to [10]).

The idea of secure DQC is motivated by very practical issues: One could safely anticipate that when quantum computers will be available they will be hosted by large institutions offering their services in a cloud fashion [11]. Blind protocols are there to allow for a client with limited quantum technologies to access the full-power of quantum computers while protecting the privacy of her information. In this letter we show that a 2-dimensional cluster state is universal for quantum computation with measurements restricted to the (X, Y)-plane. This result is general, novel to the best of our knowledge, and implies that every blind DQC protocol rooted on MBQC can use a cluster state as resource, with no fundamental necessity to introduce more particular states such as the brickwork state.

Here we try to keep the formalism needed for our proof at a minimum. All the relevant concepts are introduced, but a certain level of familiarity with the ideas of measurement-based quantum computing is assumed.

II. DEFINITIONS AND NOTATIONS

We start by defining the notation used throughout the text. The identity gate is $\hat{\mathbb{I}}$, we use the symbols $\hat{X}, \hat{Z}$ for the Pauli gates, $\hat{H}$ for the Hadamard gate and $\hat{R}_Z(\theta) = \exp(-i\frac{\theta}{2}\hat{Z})$ for a generic Z-rotation by an angle θ. The states $|0\rangle$ and $|1\rangle$ form the computational basis and they are eigenstates of $\hat{Z}$. The eigenstates of $\hat{X}$ are $|+\rangle$ and $|-\rangle$, with $|+\rangle = \hat{H}|0\rangle$ and $|-\rangle = \hat{H}|1\rangle$. One of the entangling gates for the $|\pm\rangle$ basis is the two-qubit controlled-$\hat{Z}$ operator, given by Ctrl-Z $= |0\rangle\langle 0| \otimes \hat{\mathbb{I}} + |1\rangle\langle 1| \otimes \hat{Z}$. We also define a two-qubit gate with weight α as $\hat{R}_{ZX}(\alpha) = \exp(-i\frac{\alpha}{2}\hat{Z} \otimes \hat{X})$. Note that if a Z-rotation (with angle θ) is applied to a

$|+\rangle$ state (or to its orthogonal state $|-\rangle$) one gets,

$$\hat{R}_Z(\theta)|\pm\rangle = |\pm_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm \exp(i\theta)|1\rangle).$$

Analogously, a single-qubit projective (X,Y)-plane measurement with angle θ is equivalent to a measurement in the basis $\{|+_\theta\rangle, |-_\theta\rangle\}$. We now give two definitions for cluster states:

Definition 1. *(Cluster State) A cluster state $|CS_{n\times m}\rangle$, is an entangled state of $n \times m$ qubits constructed as follows:*

1. *Prepare all the qubits in the state $|+\rangle$ and assign to each qubit a unique index (i,j), i being a row ($i \in [n]$) and j being a column ($j \in [m]$).*

2. *For each row ($1 \leq i \leq n$), apply the operator Ctrl-Z on qubits (i,j) and (i,j+1) where $1 \leq j \leq m-1$.*

3. *For each column ($1 \leq j \leq m$), apply the operator Ctrl-Z on qubits (i,j) and (i+1,j) where $1 \leq i \leq n-1$.*

Definition 2. *(Open-ended Cluster State) A cluster state $|OCS_{n\times m}\rangle$, is an entangled state of $n \times m$ qubits constructed as follows :*

1. *Prepare all the qubits in the state $|+\rangle$ and assign to each qubit a unique index (i,j), i being a row ($i \in [n]$) and j being a column ($j \in [m]$).*

2. *For each row ($1 \leq i \leq n$), apply the operator Ctrl-Z on qubits (i,j) and (i,j+1) where $1 \leq j \leq m-1$.*

3. *For each column ($1 \leq j \leq m-1$), apply the operator Ctrl-Z on qubits (i,j) and (i+1,j) where $1 \leq i \leq n-1$.*

III. MBQC - PRELIMINARIES

The workhorse of MBQC is the well-known concept of one-bit teleportation [12–14], which is also particularly helpful to visualise our universality proof. We will present this idea using two qubits initialised in the following state: Ctrl-Z$(|\psi\rangle \otimes |+\rangle)$. Since Ctrl-Z is a symmetric operator any of the two qubits can be chosen as control (or target) qubit. This is conceptually equivalent to preparing a cluster state in MBQC where the first qubit has been replaced by a generic state $|\psi\rangle$. The teleportation happens when the first qubit ($|\psi\rangle$) is measured in the $\{|+\rangle, |-\rangle\}$ basis: Circuit-wise, this is represented by applying first an Hadamard gate and then measuring in the computational basis as shown in Figure 1. Importantly, after the measurement the state of the second qubit is equal to $\hat{X}^m\hat{H}|\psi\rangle$, where $\hat{X}^m$ is a Pauli correction induced by the measurement outcome m.

A generalised one-bit teleportation circuit corresponds to performing a measurement in the (X,Y)-plane instead of the $\{|+\rangle, |-\rangle\}$ basis measurement. This circuit
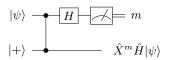

FIG. 1: The quantum circuit for the one-bit teleportation scheme.
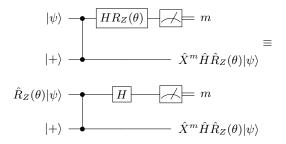

FIG. 2: Generalised one-bit teleportation circuit. LHS of the equivalence sign: measuring the first qubit with the θ angle in the (X,Y) plane, and RHS of the equivalence sign: applying a Z-rotation on the first qubit and measuring it in the X-basis. The two circuits are equivalent.

is shown in Figure 2. On the left hand side is shown the circuit corresponding to a measurement of angle θ in the (X,Y)-plane on the first qubit of the two-qubit state. Because any generic $\hat{R}_Z(\theta)$ rotation commutes with the Ctrl-Z gate, one can easily transform the circuit on the left to an instance of the one-bit teleportation circuit by simply updating the initial state. Note that the resulting state at the end of the circuit inherits the Z-rotation introduced by the measurement.

The customary understanding of MBQC is formulated in terms of a measurement *pattern*: One defines an input and output set on the resource state such that the measurements transform the corresponding input state into the desired outcome, identified by the qubits of the output set. Intuitively, the quantum information is transformed by the same process that governs the generalised one-bit teleportation scheme. For the cluster state (open-ended or not), if the cardinality of the input set is $|I|$, then the input state of the computation corresponds to $|+\rangle^{\otimes|I|}$. Note that this does not have to be the case in general, as shown for example in Figure 1 and Figure 2. Resource states can be concatenated, each representing the subroutine of a larger computation. Then, as dictated by the execution order, the output state of a previous resource state would correspond to the input state of the following one. Importantly, changing the input state of the MBQC resource state by replacing the $|+\rangle^{\otimes|I|}$ with a generic $|I|$-qubit state $|I\rangle$ does not affect the transformation induced by the measurements [15]. To define this concept properly, we give two modified definitions for cluster states:

Definition 3. *(Cluster State with generic input state) A quantum state $|inCS_{n\times m}\rangle$, is a cluster state of $n \times$*

m qubits with a well-defined input set of cardinality $|I|$. Additionally, the $|+\rangle^{\otimes|I|}$ qubits identified by the location of the input set are replaced by a generic $|I\rangle$ state before the entangling operations are performed.

Definition 4. *(Open-ended Cluster State with generic input state) A quantum state $|inOCS_{n\times m}\rangle$, is an open ended cluster state of $n \times m$ qubits with a well-defined input set of cardinality $|I|$. Additionally, the $|+\rangle^{\otimes|I|}$ qubits identified by the location of the input set are replaced by a generic $|I\rangle$ state before the entangling operations are performed.*

It is important to note that in MBQC measurements are in general adaptive in nature because of their inherent randomness, therefore future measurements might depend on previous outcomes. This is not problematic since suitable local corrections can be applied to move the computation back to the positive branch, i.e. where all the measurement outcomes are 0. We will therefore ignore the measurement dependencies in the rest of the manuscript and only deal with the unitary operations given by the positive branch of the measurement pattern [15, 16].

IV. UNIVERSALITY OF CLUSTER STATES WITH (X,Y)-PLANE MEASUREMENTS

In this section we present a proof of universality for a cluster state with measurements constrained to the (X, Y)-plane. We start by proving a number of lemmas that will make the exposition of the main theorem easier. We start by introducing the notion of a universal gate set [2, 17]. The aim of the later proof is to show that it is possible to reproduce such a gate set by appropriate (X, Y)-plane measurements.

Lemma 1. *Consider the gate set given by $\{\exp(-i\frac{\theta}{2}\hat{Z}_i), \exp(-i\frac{\theta}{2}\hat{X}_i), \exp(-i\frac{\theta}{2}\hat{Z}_i \otimes \hat{X}_{i+1})\}$, with i and $i+1$ adjacent qubits: It forms a universal set of quantum gates for quantum computing.*

Proof. The gates $\hat{R}_Z(\theta), \hat{R}_X(\theta)$ generate SU(2), and hence any single qubit operation can be implemented via a sequence of such gates. Together with the $\hat{R}_{ZX}(\theta)$ gate, these suffice to implement a CNOT gate between nearest neighbours. As a pair of qubits can be swapped through a sequence of three CNOT gates, the logical qubits can be permuted arbitrarily, allowing for CNOT gates to be implemented between arbitrary pairs of qubits. Thus the gate set considered here is equivalent to local unitaries together with CNOT gates, which has long been known to be universal [18]. □

In the rest of the paper, we consider a $n \times m$ open-ended cluster state with generic input state $|inOCS_{n\times m}\rangle$. There can be two cases either $m > n$ or $m \leq n$. We only consider the former case with measurements executed column-by-column from left to right. We fix the
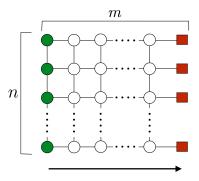

FIG. 3: A generic resource state $|inOCS_{n\times m}\rangle$. In green is shown the input set, in red the output set, while the arrow below indicates the sequential order of the measurements.

first column to be the input state $|I\rangle$ and the last (m-th) column to be the output state. All the $m - 1$ columns preceding the output set are measured, and their qubits called operational qubits. An example for clarity is shown in Figure 3.

Lemma 2. *A resource state $|inOCS_{n\times m}\rangle$ together with (X, Y)-plane measurements $\{|+_\theta\rangle\langle+_\theta|\}$ along the X-axis, i.e. $\theta = 0$, can be used to perform the unitary $\hat{U}$ on any input state $|I\rangle$, where U is given by:*

$$\hat{U} = \prod_{j=1}^{m-1} \left(\otimes_{i=1}^{n}\hat{H}_i\right)_j \left(\otimes_{i=1}^{n-1} Ctrl\text{-}Z_{i,i+1}\right)_j . \quad (1)$$

Proof. From the one-bit teleportation scheme we can see that by measuring in the $\{|+\rangle, |-\rangle\}$ basis all the operational qubits, the output of the computation is equal to $\hat{U}$, where $\hat{U}$ corresponds to the unitary implemented by the positive branch of the MBQC pattern. □

Let us now define:

$$\hat{C}_n := \left(\otimes_{i=1}^{n}\hat{H}_i\right) \left(\otimes_{i=1}^{n-1}\text{Ctrl-}Z_{i,i+1}\right) . \quad (2)$$

Note that for a cluster state $|inOCS_{n\times m}\rangle$ the unitary operation $\hat{U}$ consists of $(m-1)$ repetitions of $\hat{C}_n$ applied on the input state $|I\rangle$. A simple example of such MBQC pattern is shown in Figure 4 for the 2×4 cluster state $|OCS_{2\times4}\rangle$ with standard input state $|I\rangle = |++\rangle$.

To show that it is possible to reproduce the universal gate set from Lemma 1, we study the effects of performing (X,Y)-plane measurements with generic angle θ in different positions of the $|inOCS\rangle_{n\times(n+2)}$, for $m = n+2$. This choice of m is justified by reasons of symmetry and does not affect the generality of the proof, which can be rewritten for generic values of m at the cost of a less clear interpretation of the findings.

Lemma 3. *Consider a $n \times (n + 2)$ open-ended cluster state $|inOCS_{n\times(n+2)}\rangle$, then the following statements are true:*

1. *When the i-th qubit of the first column is measured with a generic angle θ on the (X, Y)-plane, and all the other operational qubits are measured along the X-basis, the MBQC pattern implements a Z-rotation, $\hat{R}_Z(\theta)$, on the $(n+1-i)$-th qubit of the input state $|I\rangle$.*

2. *When the i-th qubit of the $(n+1)$-th column is measured with a generic angle θ on the (X, Y)-plane, and all the other operational qubits are measured along the X-basis, the MBQC pattern implements a X-rotation, $\hat{R}_X(\theta)$, on the $(n+1-i)$-th qubit of the input state $|I\rangle$.*

3. *When the i-th qubit of the p-th column with $i = 1$ and $1 < p < n+1$ is measured with a generic angle θ on the (X, Y)-plane, and all the other operational qubits are measured along the X-basis, the MBQC pattern implements an entangling gate, $\hat{R}_{ZX}(\theta)$, on the $n-p+1$ and $n-p+2$ qubits of the input state $|I\rangle$ for $i = 1$. Analogously, for $i = n$ the same MBQC pattern implements the entangling gate $\hat{R}_{ZX}(\theta)$ on the p and $p-1$ input qubits.*

Proof. To prove the lemma we look at how the corresponding quantum circuits change with the position on the state $|\text{inOCS}_{n \times (n+2)}\rangle$ of a single (i, j)-th qubit measured with an angle θ. As stated above, all the other operational qubits are measured along the X-basis. This change of measurement basis can be equivalently written as a Z-rotation with angle θ, i.e. $\hat{R}_Z(\theta) = \exp(-i\frac{\theta}{2}\hat{Z})$ on the (i, j)-qubit before the measurement.

Using Lemma 2, we know that a measurement of all the qubits of one layer of $|\text{inOCS}_{n \times (n+2)}\rangle$ in the X-basis implements the $\hat{C}_n$ operator. Most importantly, since the $\hat{C}_n$ operator belongs to the Clifford group [2] it is easy to study how a single Z-rotation propagates through the circuit by using the canonical commutation relations of the Pauli matrices.

We define some helpful properties of the $\hat{C}_n$ operator. Inspired by models of quantum computation that exhibit particular mirror symmetries [19, 20], we note that a repetition of $(n+1)$ $\hat{C}_n$ operators acts as a global mirror operation on the initial n-qubit state. Precisely, the following relations hold : $\hat{C}_n^{n+1}\hat{Z}_i|I\rangle = \hat{Z}_{\bar{i}}|I\rangle$ where the mirror qubit $\bar{i} = n+1-i$. Similarly, $\hat{C}_n^{n+1}\hat{X}_i|I\rangle = \hat{X}_{\bar{i}}|I\rangle$. More generally, the repetition of the $\hat{C}_n$ gate is used as a generalised swap gate as shown in [19, 20].

As always, examples are helpful to support the mathematical intuition: In Figure 4, we show the effects of a repetition of $\hat{C}_2$ gates on the familiar $|\text{OCS}_{2 \times 4}\rangle$ state.

Using the mirror symmetry relations shown above, it is easy to see that a cluster state $|\text{inOCS}_{n \times (n+2)}\rangle$ whose $(i, 1)$-th qubit is measured in the (X, Y)-plane with some angle θ, while the remaining qubits are measured along the X-axis, implements a $\hat{R}_{Z_{n+1-i}}(\theta)|I\rangle$. Equally, measuring the $(i, n+1)$-th qubit in the (X, Y)-plane with some angle θ implements a $\hat{R}_{X_{n+1-i}}(\theta)|I\rangle$. This proves the first two statements of the lemma.

To prove the final statement, we analyse the situation when a rotation $\hat{Z}_i$ (or generally a $\hat{R}_{Z_i}$) is applied in the middle of a sequence of $\hat{C}_n$ operators. Explicitly, interposing an (X, Y)-measurement by an angle θ on the (i, p)-th qubit of a state $|\text{inOCS}_{n \times (n+2)}\rangle$ entirely measured along the X-basis implements $\hat{C}_n^{n-p+2}\hat{R}_{Z_i}(\theta)\hat{C}_n^{p-1}|I\rangle$. For a 2-qubit entangling gate it suffices to consider $i = 1, n$. We have already considered the case when $p = 1$ and $p = n+1$, and to derive a relation for any other p, we will use the following commutation relations and circuit identities (to simplify the notation we are not writing the identity gates):

1. $\text{Ctrl-Z}_{(i,j)}\hat{Z}_i = \hat{Z}_i\text{Ctrl-Z}_{(i,j)}$

2. $\text{Ctrl-Z}_{(i,j)}\hat{X}_i = \hat{X}_i\hat{Z}_j\text{Ctrl-Z}_{(i,j)}$

3. $\text{Ctrl-Z}_{(i,j)}\hat{R}_{Z_i}(\theta) = \hat{R}_{Z_i}(\theta)\text{Ctrl-Z}_{(i,j)}$

4. $\hat{H}\hat{Z}\hat{H} = \hat{X}$

Using the above circuit identities it is easy to see that:

$$\hat{C}_n(\hat{Z}_1 \otimes_{i=2}^n \hat{\mathbb{1}}_i) = (\hat{X}_1 \otimes \hat{Z}_2 \otimes_{i=3}^n \hat{\mathbb{1}}_i)\hat{C}_n,$$
$$\hat{C}_n(\otimes_{i=1}^{n-1}\hat{\mathbb{1}}_i \otimes \hat{Z}_n) = (\otimes_{i=1}^{n-2}\hat{\mathbb{1}}_i \otimes \hat{Z}_{n-1} \otimes \hat{X}_n)\hat{C}_n. \quad (3)$$

This relation can be extended to the case of a generic value of $p : 1 < p < n+1$ via a recursive application of the gate $\hat{C}_n$. Therefore, for $p' = n-p+2$ we have that

$$\hat{C}_n^{p'}(\hat{Z}_1 \otimes_{i=2}^n \hat{\mathbb{1}}_i) = (\otimes_{i=1}^{n-p}\hat{\mathbb{1}}_i \otimes \hat{Z}_{n-p+1} \otimes \hat{X}_{n-p+2} \otimes_{i=n-p+3}^n \hat{\mathbb{1}}_i)\hat{C}_n^{p'},$$
$$\hat{C}_n^{p'}(\otimes_{i=1}^{n-1}\hat{\mathbb{1}}_i \otimes \hat{Z}_n) = (\otimes_{i=1}^{p-2}\hat{\mathbb{1}}_i \otimes \hat{X}_{p-1} \otimes \hat{Z}_p \otimes_{i=p+1}^n \hat{\mathbb{1}}_i)\hat{C}_n^{p'}. \quad (4)$$

Note that for $i \neq 1, n$ the resulting gate on the output state will still be an entangling gate, but it will have a more complicated form than the simple two-qubit gate one presented above. Since we are only interested in the universality proof we need not to discuss the most general case.

Using the procedure above one can steer a $\hat{Z}_k \otimes \hat{X}_{k+1}$ or $\hat{X}_k \otimes \hat{Z}_{k+1}$, for any $1 \leq k < n$, to an arbitrary position of the output state depending on the number p of $\hat{C}_n$ operations in the circuit. The above results can be generalised by replacing the Pauli-Z with any Z-rotation, $\hat{R}_Z(\theta)$, and hence one can obtain arbitrary rotations and nearest neighbour entangling gates. We show a particular example of implementing a nearest neighbour entangling gate with cluster state $|\text{OCS}_{2 \times 4}\rangle$ in Figure 4. This completes the proof of Lemma 3. $\square$

By using the lemmas proved above we can state the first universality theorem.

Theorem 1. *The family of open-ended cluster states $|\text{inOCS}_{n \times m}\rangle$ is universal for quantum computation when used as a resource in MBQC with measurements limited to the (X, Y)-plane of the Bloch sphere.*
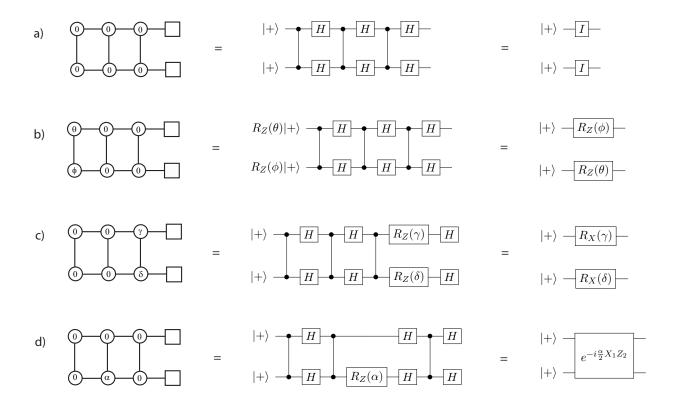
FIG. 4: Implementation of a) Identity gate, b) single-qubit Z rotation, c) single-qubit X rotation, and d) nearest neighbour entangling gate using $|\mathrm{OCS}_{2\times4}\rangle$ and (X,Y)-plane measurements. In these figures we use the convention that circles represent operational qubits, i.e. qubits that are measured during the computation, and squares represent output qubits, i.e. qubits left unmeasured at the end of the computation.

Proof. Using Lemma 1 and Lemma 3 we conclude that any gate constructed using the gates from the universal set $\{\hat{R}_Z(\theta), \hat{R}_X(\theta), \hat{R}_{ZX}(\theta)\}$ can be implemented using $|\mathrm{inOCS}\rangle$ as a resource state and (X,Y)-plane measurements. $\square$

Corollary 1. *The family of cluster states $|CS_{n\times m}\rangle$ is universal for quantum computation with the additional constraint that the measurement angles are chosen solely from the (X,Y)-plane.*

Proof. In this section we will prove that universality of $|\mathrm{inOCS}\rangle$ implies universality of $|CS\rangle$. To show this, we note that a $|\mathrm{inOCS}_{n\times m}\rangle$ and a $|CS_{n\times m}\rangle$ differ only by (possibly) the input state, and the $(n-1)$ Ctrl-Z operators on the last column of the graph.

Firstly, we see that universality of $|\mathrm{inOCS}\rangle$ implies it can implement a circuit with $(n-1)$ Ctrl-Z on a n-qubit state such that all the neighbouring qubits have Ctrl-Z applied between them. Let us call such state $|\mathrm{CZ}_{\mathrm{inOCS}}\rangle$, which is given by $\prod_{i=1}^{n-1} \text{Ctrl-Z}_{i,i+1}|+\rangle^{\otimes n}$ and it is constructed using specific measurement angles on an open-

ended cluster state $|\mathrm{inOCS}_{n\times m}\rangle$. Then, any arbitrary unitary that can be constructed using the cluster state $|\mathrm{inCS}_{n\times m}\rangle$ can be also constructed by concatenating the output of a cluster state $|\mathrm{inOCS}_{n\times m}\rangle$ with the $|\mathrm{CZ}_{\mathrm{inOCS}}\rangle$ state.

Hence, using such construction, universality of $|\mathrm{inOCS}\rangle$ (given by Theorem 1) implies universality of $|\mathrm{inCS}\rangle$. However, one can think of any $|CS\rangle$ as the concatenation of two $|\mathrm{inCS}\rangle$ states, the first with input state $|I\rangle = |+\rangle^{\otimes n}$ and the second with input state given by the output of the first. Then, universality of $|\mathrm{inCS}\rangle$ immediately implies that the cluster state $|CS\rangle$ is universal with (X,Y)-plane measurements. $\square$

[1] Michael A. Nielsen. Cluster-State Quantum Computation. *Rep. Math. Phys.*, 57(1):147–161, February 2006.

[2] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[3] R Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188, 2001.

[4] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2009.

[5] S. Barz, E. Kashefi, A. Broadbent, J.F. Fitzsimons, A. Zeilinger, and P. Walther. Demonstration of blind quantum computing. *Science*, 335(6066):303–308, 2012.

[6] S. Barz, J.F. Fitzsimons, E. Kashefi, and P. Walther. Experimental verification of quantum computation. *Nat. Phys.*, 9:727–731, 2013.

[7] J.F. Fitzsimons and E. Kashefi. Unconditionally verifiable blind computation. *arXiv:1203.5217*, 2013.

[8] T. Morimae and K. Fujii. Blind quantum computation protocol in which alice only makes measurements. *Phys. Rev. A*, 87:050301(R), 2013.

[9] A. Mantri, T.F. Demarie, N.C. Menicucci, and J. Fitzsimons. Flow ambiguity: A path towards classically driven blind quantum computation. *arXiv:1608.04633*, 2016.

[10] V. Dunjko, J.F. Fitzsimons, C. Portmann, and R. Renner. *Advances in Cryptology - ASIACRYPT 2014*. Springer Berlin Heidelberg, 2014.

[11] http://www.research.ibm.com/quantum/, 2016.

[12] Daniel Gottesman and Isaac L Chuang. Quantum teleportation is a universal computational primitive. *arXiv preprint quant-ph/9908010*, 1999.

[13] Daniel Gottesman and Isaac L Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature (London)*, 402:390, 1999.

[14] Xinlan Zhou, Debbie W Leung, and Isaac L Chuang. Methodology for quantum logic gate constructions. *Phys. Rev. A*, 62:052316, 2000.

[15] V. Danos, E. Kashefi, and P. Panangaden. The measurement calculus. *Journal of ACM*, 54(8), 2007.

[16] V. Danos and E. Kashefi. Determinism in the one-way model. *Phys. Rev. A*, 74:052310, 2006.

[17] P Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. A new universal and fault-tolerant quantum basis. *Information Processing Letters*, 75(3):101–107, 2000.

[18] Adriano Barenco, Charles H Bennett, Richard Cleve, David P DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457, 1995.

[19] Robert Raussendorf. Quantum computation via translation-invariant operations on a chain of qubits. *Physical Review A*, 72(5):052301, 2005.

[20] Joseph Fitzsimons and Jason Twamley. Globally controlled quantum wires for perfect qubit transport, mirroring, and computing. *Physical review letters*, 97(9):090502, 2006.