Minimal qubit resources for the realization of measurement-based quantum computation

Monireh Houshmand, Mahboobeh Houshmand, and Joseph F. Fitzsimons

Phys. Rev. A **98**, 012318 — Published 17 July 2018

DOI: 10.1103/PhysRevA.98.012318

Minimal qubit resources for the realisation of measurement-based quantum computation

Monireh Houshmand, Mahboobeh Houshmand,* and Joseph F. Fitzsimons

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

In measurement-based quantum computation (MBQC), a special highly-entangled state (called a resource state) allows for universal quantum computation driven by single-qubit measurements and post-measurement corrections. The large number of qubits necessary to construct the resource state constitutes one of the main down sides to MBQC. However, in some instances it is possible to extend the resource state on the fly, meaning that not every qubit must be realised in the devices simultaneously. We consider the question of the minimal number of physical qubits that must be present in a system to directly implement a given measurement pattern. For measurement patterns which have quantum circuit representation as formalized by the notion of flow, with n inputs, n outputs and m total qubits, we show that only minimum of $n+1$ and m qubits are required; while the number of required qubits can be as high as $m-2$ for measurement patterns which implement a unitary, but do not have a quantum circuit representation, as formalized by the notion of generalized flow (gflow). We discuss the implications of removing the Clifford part of a measurement pattern, using well-established transformation rules for Pauli measurements, for the presence of flow versus gflow, and hence the effect on the minimum number of physical qubits required to directly realise the measurement pattern.

I. INTRODUCTION

The circuit model of quantum computation [1] provides a direct analogue to the common classical computational model based on networks of logic gates. On the other hand, measurement-based quantum computation (MBQC) [2], provides a conceptually and practically different model. This model harnesses unique features of quantum mechanics related to entanglement and measurement, and hence does not have a direct classical counterpart.

A measurement-based computation can be represented by a *measurement pattern*, where single-qubit measurements are made on a special resource state (known as graph state), consisting of qubits prepared in a specific entangled state. For a formal definition of a measurement pattern we refer the reader to [3]. Resource states can be formed by first preparing single-qubit states and then applying specific entangling operations. The entangling operations in a measurement pattern can be represented by a graph, where each vertex corresponds to a qubit and each edge corresponds to an entangling operation performed between the qubits indicated by the vertices it connects. This graph together with identified sets of input and output qubits is known as the *open graph* corresponding to the computation [4]. Since the measurements underlying such computations do not have predetermined outcomes, it is necessary to have some dependency structure in order to guarantee determinism. The existence of such a structure for arbitrary choices of measurement angles is determined fully by the open graph. For open graphs the presence of flow [5] is a sufficient condition, and generalized flow (gflow) [6] is a sufficient and necessary condition, for the existence of an appropriate dependency structure to ensure determinism [7]. The class of measurement patterns with flow is universal for quantum computing and the translation from quantum circuits to measurement patterns always leads to a pattern with flow [8]. The measurement patterns which implement a unitary but do not have a quantum circuit representation, are formalized by the notion of gflow.

Despite the advantages of the MBQC model [8–18], its realisation is often expensive in terms of physical qubits, as the number of qubits in a measurement pattern is usually much more than the number of logical qubits in the computation [15, 19–21]. This stems from the fact one qubit is required for each (non-Clifford) single-qubit gate in the computation. MBQC has been demonstrated experimentally using various discrete-variable (qubit) systems [22–28] and continuous variable systems [29–31]. However, experiments for qubit systems have generally been restricted to low numbers of qubits

* Corresponding author: mahboobehhoushmand@yahoo.com

and scaling them up is an important challenge [22, 31].

Here we examine the number of physical qubits required to realise a measurement pattern, when entanglement operations and measurements can be reordered. We consider the question of whether the whole resource state has to be constructed at the beginning, or whether it is possible to add qubits on an as needed basis. In the latter case, we consider the minimal number of necessary physical qubits at any time, which we denote min_{QR}. We show that min_{QR} is different for open graphs with flow versus those with only gflow, and in some instances this difference can be dramatic. The remainder of the paper is structured as follows. We begin by introducing needed definitions and background. We then derive the required physical qubit resources for measurement-based computations for the cases of flow and gflow. We also examine the effect of removing Pauli measurements, which implement Clifford group gates, in terms of its effect on the presence of flow.

II. DEFINITIONS AND BACKGROUND

For a graph $G = (V, E)$, V denotes the set of its vertices and E is the set of its edges. An open graph is a triplet (G, I, O), where $G = (V, E)$ is an undirected graph and $I, O \subseteq V$ are respectively the sets of input and output vertices. The *size* of G, m is its number of vertices. Non-input vertices are denoted by I^C and non-output vertices are denoted by O^C.

Flow and gflow on open graphs, as defined in the following, determine an ordering of measurements which guarantees that measurement angles can always be adapted based on previous results to implement a unitary transformation deterministically, for any choice of measurement angles.

Definition 1 (Danos & Kashefi [5])**.** *An open graph (G, I, O) has* flow *if and only if there exists a map $f : O^C \to I^C$ and a strict partial order $\prec_f$ over V such that all of the following conditions hold for all $i \in O^C$.*

- $i \prec_f f(i)$,
- *if $j \in N(f(i))$, then $j = i$ or $i \prec_f j$, where $N(v)$ contains adjacent vertices of v in G,*
- $i \in N(f(i))$.

In this case, $(f, \prec_f)$ is called a flow on (G, I, O).

To aid clarity, we will make use of the notation $u \to v$, if $f(u) = v$ and $u \Rightarrow v$, if $u \to v_1 \to v_2 \to \ldots \to v_{n-1} \to v_n$ where $v_n = v$.

Let (G, I, O) be an open graph with flow. Then, a collection P_f of directed paths in G is called a *path cover* of (G, I, O) [32] if (i) each $v \in V$ is included in exactly one path. In other words, paths are vertex-disjoint and they cover G, (ii) each path in P_f is either disjoint from I or intersects I only at its initial vertex, and (iii) each path in P_f intersects O only at its final vertex. In this paper, we assume that $|I| = |O| = n$ (corresponding to patterns performing unitary transformations). In this case, for (G, I, O), there are n paths, each starting from an input vertex, i_j, and ending at an output vertex, o_j (possibly overlapping), such that $i_j \to v_{1j} \to v_{2j} \to \ldots \to v_{n_{j}j} \to o_j \in P_f$. The path to which qubit w belongs is denoted by $\mathcal{P}(w)$.

Definition 2 (Browne et al. [6])**.** *An open graph (G, I, O) has* generalised flow (gflow) *if and only if there exists a map $g : O^C \to P^{I^C}$ (the set of all subsets of vertices in I^C) and a strict partial order $\prec_g$ over V such that all of the following conditions hold for all $i \in O^C$.*

- *if $j \in g(i)$ then $i \prec_g j$,*
- *if $j \in \mathrm{Odd}(g(i))$, then $j = i$ or $i \prec_g j$, where $\mathrm{Odd}(K) = \{k | \, |N(k) \cap K| = 1 \mod 2\}$, is the odd neighbourhood of K, i.e. the set of vertices which have an odd number of neighbours in K.*
- $i \in \mathrm{Odd}(g(i))$.

In this case, $(g, \prec_g)$ is called a gflow on (G, I, O).

There is a well-established method for translating from quantum circuits to measurement patterns through the use of gate teleportation [33]. The notion of flow captures the fact that $f(i)$ is the qubit that adaptively corrects the teleportation byproduct produced by measuring qubit i. The partial order guarantees that there is a chain of qubits which is teleported along disjoint paths in P_f in the open graph such that if they are measured in the partial order induced by flow, the corrections can be consistently applied. It should be noted that the class of patterns with flow is universal for quantum computing and the translation from circuits to the patterns always leads to a pattern with flow [34].

Gflow is a generalization of flow and turns out to be a necessary condition where the state is not necessarily teleported into a single site, but across many sites during the computation. In these open graphs, the teleportation byproduct produced by measuring a qubit i can be consistently corrected by a correcting set denoted $g(i)$ instead of one single qubit.

III. MINIMAL QUBIT RESOURCES

In this section, we discuss the question of the minimal number of physical qubits that must be present in a system to directly implement a given measurement pattern. We consider the reordering of the entanglement and measurement operations such that the number of physical qubits necessary at any one time is minimised. The idea is based on postponing each entangling operation as long as possible. Suppose it is the turn of a qubit $w \in O^C$ to be measured with respect to an ordering of measurements induced by flow. We will denote the set of unmeasured qubits at this stage, excluding w, as $\mathcal{U}_w$ and the set of measured qubits as M_w. The measurement on a particular qubit w commutes with entangling operations between u and v when neither u nor v is equal to w, but does not commute with entanglement operations between w and its unmeasured neighbours [35]. Therefore, these operations have to be performed first before the measurement. The set of unmeasured neighbours of w is denoted by $\mathcal{N}_w$, which is equal to $N(w) \cap \mathcal{U}_w$. The measurement of the qubit w affects the state of qubits in $\mathcal{N}_w$. As no operation acts on a previously measured qubit [3], w is not required beyond this point during the realisation of a pattern.

Now, we investigate the minimal set of qubits which must simultaneously exist prior to the measurement of w, excluding w itself, which we label $\mathcal{Q}_w$. This set is the union of two subsets of vertices: (i) the subset that is required for performing the measurement on w, $\mathcal{N}_w$, and (ii) the subset of qubits which have been affected by previous operations and which have not been measured, and hence must be retained until measurement (if they do not belong to O) or until the end of computation. We now characterise this latter subset.

At the beginning of a measurement-based computation, the qubits in I are provided or prepared in some joint input state and must be retained until they are measured (if they do not belong to O), or until the end of computation. When it is the turn of a qubit w to be measured, the set of all unmeasured input qubits excluding w is denoted $\mathcal{I}_w$. During the computation, measurements cannot be commuted past entangling operations involving the same qubit, and hence the neighbours of any measured qubits must either be measured or retained. We will denote by $\mathcal{O}_w$ the subset of qubits in $\mathcal{U}_w$ with measured neighbours. More formally, $\mathcal{O}_w = \{v \in \mathcal{U}_w | N(w) \cap \mathcal{M}_w \neq \varnothing\}$, where $\varnothing$ is the empty set. Therefore, we have $\mathcal{Q}_w = \mathcal{N}_w \cup \mathcal{I}_w \cup \mathcal{O}_w$.

Suppose it is the turn of a qubit $w \in O^C$ to be measured with respect to an ordering of measurements induced by flow. The paths in P_f are like the teleportation paths of the qubits, and Lemma 3 indicates that there is exactly one qubit in each path that must exist prior to the measurement of w.

Lemma 3. *Let (G, I, O) be an open graph with flow. There exists exactly one member of $\mathcal{Q}_w$ in each path $\mathcal{P}$ of P_f.*

Proof. We first prove that in each $\mathcal{P}$ there exists at least one member of $\mathcal{Q}_w$, and then we prove that this lower bound must be saturated. We will use v to label this unique vertex for a particular path. Tackling the upper bound first, for a given $\mathcal{P}$, one of the following two cases will happen:

1. $w \in \mathcal{P}$: With respect to the flow definition, there is $v \in \mathcal{N}_w \cap \mathcal{U}_w$ given by $v = f(w)$ such that $\mathcal{P}(v) = \mathcal{P}(w)$.

2. $w \notin \mathcal{P}$: In this situation, there are only two possible cases:

   - None of the qubits in $\mathcal{P}$ have been measured previously. Therefore, there exists $v \in \mathcal{I}_w$ in this path.

   - At least one of the qubits in $\mathcal{P}$ has been measured previously. Let u be the last qubit which has been measured in this path. Therefore, we have $v = f(u) \in \mathcal{O}_w$.

This guarantees that at least one qubit in each path must be in $\mathcal{Q}_w$, when the input state is left unspecified.

We now show that if $u, v \in \mathcal{Q}_w$, and $u \neq v$, then $\mathcal{P}(u) \neq \mathcal{P}(v)$. The proof is done by contradiction. Suppose $\mathcal{P}(u) = \mathcal{P}(v)$ and without loss of generality, suppose $u \Rightarrow v$. In such a situation, it must be the case that $v \notin \mathcal{I}_w$. Therefore, one of the following two cases will occur:

1. $v \in \mathcal{N}_w$: Based on the flow definition, u has to be measured before w which belongs to $N(v)$. Therefore, $u \notin \mathcal{Q}_w$.

2. $v \in \mathcal{O}_w$: Based on the flow definition, u has to be measured before all of the neighbours of v, but since $v \in \mathcal{O}_w$, a neighbour of v has been previously measured. Therefore, $u \notin \mathcal{Q}_w$.

This leads directly to the conclusion that in each $\mathcal{P}$, v is the unique member of $\mathcal{Q}_w$. $\square$

In Theorem 4, min_{QR} is determined for open graphs with flow.

Theorem 4. *Let (G, I, O) be an open graph with flow, with the same number of inputs and outputs, n. To realise patterns with the underlying open graph, min_{QR} is $\min(n+1, m)$, where m is the whole number of qubits in the pattern.*

Proof. First, consider the case that $I = O\,(m = n)$, which implies that all qubits are inputs and outputs simultaneously. In this case, min_{QR} is trivially equal to $m = n$. Now, suppose that $I \neq O$, and in this case, according to Lemma 3, the size of $\mathcal{Q}_w$ is equal to the number of paths in the graph, trivially equal to n, and therefore by including the presence of w, we have $min_{QR} = n + 1$. $\square$

Although we have shown that min_{QR} for open graphs with flow on n inputs is $min(n+1, m)$, it is not the case for open graphs with gflow. This is demonstrated by constructing a family of open graphs which require large numbers of qubits to be present as a counter-example. We will consider open graphs (H_n, I, O) with $n > 1$ inputs, $\{i_1, i_2, ..., i_n\}$, n outputs, $\{v_1, v_2, ..., v_n\}$, and $(m-2n) \neq 0$ intermediate qubits, $\{v_{n+1}, v_{n+2}, ..., v_{m'}\}$, where $m' = m - n$. Rather than specifying the edges of H_n directly, we instead specify the edges of the graph H_n^C obtained by complementing the edges of H_n. This is for simplicity since H_n will be highly connected. The graph H_n^C, shown in Fig. 1, has the following edges: $\{i_j, v_j\}$ for $j \in \{1, 2, ..., n-2\}$, $\{v_{n+j}, v_{n+j+1}\}$ for $j \in \{0, 1, ..., m'-n-1\}$, and $\{i_{n-1}, v_{m'}\}$.

A gflow on H_n can be found by applying the algorithm proposed in Ref. [36], which yields the following: $g(i_j) = \{v_j, v_{n-1}\}$ for $j \in \{1, ..., n-2\}$, $g(v_j) = \{v_{j-2}, v_{j-1}\}$ for $j \in \{n+1, ..., m'\}$, $g(i_{n-1}) = \{v_{m'-1}, v_{m'}\}$ and $g(i_n) = v_{m'}$. Since from Fig. 1 the maximum degree of H_n^C can easily be seen to be 2, the minimal degree of H_n must be equal to $m-3$. Starting from a qubit w in a partial order induced by a gflow on this open graph, we have $|\mathcal{N}_w| \geq m-3$. Therefore $min_{QR} \geq m-2$.

We conclude by examining the effect of measurement of Pauli operators on graphs with flow and those with gflow, since this can alter the presence of flow. Unitary operators which map Pauli group operators to the Pauli group under conjugation are known as Clifford group operations. Any of these operators can be implemented by patterns with Pauli

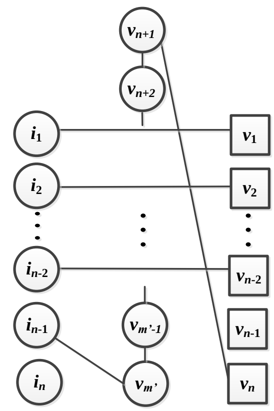

FIG. 1. Representation of (H_n^C, I, O). Input qubits are shown by $i_1, i_2, ..., i_n$ and squared vertices represent output qubits.

measurements X and Y only [37]. Due to the nature of corrections made during an MBQC, measurements of Pauli operators are unaffected and can be shifted to the start of the computation. In Ref. [19], general transformation rules for graphs are described when Pauli measurements are performed on qubits. This allows for Pauli measurements to be eliminated by modifying the graph state to be prepared and updating the other measurement bases. For example, in the case of a Y measurement on qubit w, the graph corresponding to the resulting state is obtained by replacing the subgraph consisting of neighbours of w by its complement, and removing w and any incident edges. Measurement bases of qubits neighbouring w also need to be updated.

Consider an open graph (H'_n, I, O) where H'_n is a graph consisting of H_n^C (shown in Fig. 1) and another vertex, y which is connected to all of the vertices of H_n^C. (H'_n, I, O) has a flow as follows: $f(i_j) = v_j$ for $j \in \{1, ..., n-2\}$, $f(i_{n-1}) = v_{m'}$, $f(i_n) = y$, $f(v_j) = v_{j-1}$ for $j \in \{n+1, ..., m'\}$, and $f(y) = v_{n-1}$. Thus, $min_{QR} = n+2$. It can be readily verified that when y is measured in the Y-basis, H'_n will be transformed to H_n, which has been previously shown that has gflow, with $min_{QR} \geq m-2$. On the other hand, when any vertex in H_n is measured in the Y-basis, (H_n, I, O) will lead to an open graph which has gflow but not flow. In Fig. 2, further examples are given where measurement maintains flow and where Pauli measurement introduces flow to an open graph that previously had only gflow. This highlights the fact that when certain measurements are fixed to a Pauli basis in measurement pattern, their removal can have either a positive or neg-

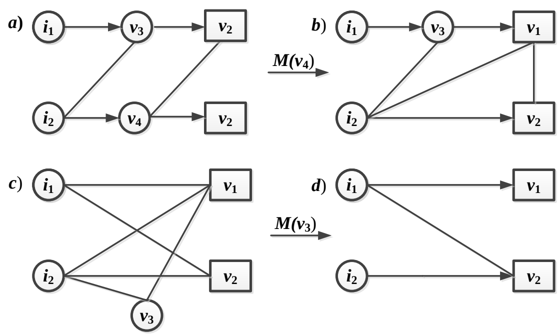

FIG. 2. Examples of removing or introducing flow in open graphs after measuring a single qubit in the Y basis. Input qubits are shown by i_1, i_2 and squared vertices represent output qubits. a) A sample open graph, (G_a, I, O) with flow. b) The resulting open graph after measuring v_4 in (G_a, I, O), which has flow. c) A sample open graph (G_c, I, O) with gflow. d) The resulting open graph with flow after measuring v_3 in (G_c, I, O).

ative effect on the minimal physical qubit resources necessary to implement the pattern.

IV. SUMMARY OF RESULTS AND CONCLUSION

In this paper, we considered the question of the minimal number of physical qubits that must be present in a system to directly implement a given measurement pattern. We showed that for measurement patterns with flow, with n inputs, n outputs and m total qubits, only minimum of $n+1$ and m qubits are required, while the number of required qubits can be as high as $m-2$ for measurement patterns with only gflow.

Our results provides a mechanism to take advantage of protocols naturally constructed in the measurement based model directly in the circuit model augmented with individual gate teleportations. As an application of our results, we consider the case of blind quantum computing (BQC) protocols natively derived in the measurement based model, introduced in Ref. [8] and Ref. [15]. In the UBQC protocol [8], a regular graph state, known as a brickwork state, of dimensions $N \times M$ is used where N and M are proportional to the dimensions of the quantum circuit corresponding to the desired computation. The open graph related to this brickwork state has flow and Theorem 4 provides a way to implement the BQC protocol using only $N+1$ qubits, instead of $N \times M$ qubits. In order to equip BQC with verification [15], randomly prepared single qubits (called traps), isolated from the actual computation are inserted blindly which act as a witness. The introduction of a trap qubits increases the size of the required brickwork state by $2 \times M$ in the most basic verification protocol of Ref. [15], while by converting to the circuit model, the minimal number of qubits to implement verification becomes $N+3$.

We also discussed the implications of removing the Clifford part of a measurement pattern, using well-established transformation rules for Pauli measurements, for the presence of flow versus gflow. We concluded that when certain measurements are fixed to a Pauli basis in measurement pattern, their removal can have either a positive or negative effect on the minimal physical qubit resources necessary to implement the pattern.

Acknowledgements – The authors thank Tommaso Demarie, Yingkai Ouyang, and Atul Mantri for useful comments on an earlier version of this paper. The second author is grateful to Eesa Nikahd for helpful discussions. The authors acknowledge support from Singapore's Ministry of Education and National Research Foundation, and the Air Force Office of Scientific Research under AOARD grant FA2386-15-1-4082. This material is based on research funded in part by the Singapore National Research Foundation under NRF Award NRF-NRFF2013-01.

[1] D. Deutsch, in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, Vol. 425 (The Royal Society, 1989) pp. 73–90.
[2] R. Raussendorf and H. J. Briegel, Physical Review Letters **86**, 5188 (2001).
[3] V. Danos, E. Kashefi, and P. Panangaden, Journal of the ACM (JACM) **54**, 8 (2007).
[4] In the rest of the paper, qubits and vertices in open graphs will be used interchangeably.
[5] V. Danos and E. Kashefi, Physical Review A **74**, 052310 (2006).
[6] D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix, New Journal of Physics **9**, 250 (2007).
[7] As gflow is more general than flow, in the rest of the paper we will use gflow only in reference to open

graphs which do not have flow.
[8] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS'09* (2009) pp. 517–526.
[9] M. A. Nielsen, Physical review letters **93**, 040503 (2004).
[10] D. E. Browne and T. Rudolph, Physical Review Letters **95**, 010501 (2005).
[11] S. C. Benjamin, D. E. Browne, J. Fitzsimons, and J. J. Morton, New Journal of Physics **8**, 141 (2006).
[12] R. Raussendorf, J. Harrington, and K. Goyal, New Journal of Physics **9**, 199 (2007).
[13] T. P. Friesen and D. L. Feder, Physical Review A **78**, 032312 (2008).
[14] P. Blythe and B. Varcoe, New Journal of Physics **8**, 231 (2006).
[15] J. F. Fitzsimons and E. Kashefi, arXiv preprint arXiv:1203.5217 (2012).
[16] T. Morimae and K. Fujii, Physical Review A **87**, 050301 (2013).
[17] M. Zwerger, H. Briegel, and W. Dür, Physical review letters **110**, 260503 (2013).
[18] M. Zwerger, H. Briegel, and W. Dür, Scientific reports **4** (2014).
[19] M. Hein, J. Eisert, and H. J. Briegel, Physical Review A **69**, 062311 (2004).
[20] E. Kashefi and P. Wallden, arXiv preprint arXiv:1510.07408 (2015).
[21] T. Morimae, Physical Review A **94**, 042301 (2016).
[22] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Nature **434**, 169 (2005).
[23] K. Chen, C.-M. Li, Q. Zhang, Y.-A. Chen, A. Goebel, S. Chen, A. Mair, and J.-W. Pan, Physical review letters **99**, 120503 (2007).
[24] R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger, Nature **445**, 65 (2007).
[25] G. Vallone, E. Pomarico, F. De Martini, and P. Mataloni, Physical review letters **100**, 160502 (2008).
[26] Y. Tokunaga, S. Kuwashiro, T. Yamamoto, M. Koashi, and N. Imoto, Physical review letters **100**, 210501 (2008).
[27] X.-C. Yao, T.-X. Wang, H.-Z. Chen, W.-B. Gao, A. G. Fowler, R. Raussendorf, Z.-B. Chen, N.-L. Liu, C.-Y. Lu, Y.-J. Deng, *et al.*, Nature **482**, 489 (2012).
[28] B. Lanyon, P. Jurcevic, M. Zwerger, C. Hempel, E. Martinez, W. Dür, H. Briegel, R. Blatt, and C. Roos, Physical review letters **111**, 210501 (2013).
[29] Y. Miwa, J.-i. Yoshikawa, P. van Loock, and A. Furusawa, Physical Review A **80**, 050303 (2009).
[30] R. Ukai, S. Yokoyama, J.-i. Yoshikawa, P. van Loock, and A. Furusawa, Physical review letters **107**, 250501 (2011).
[31] R. Pooser and J. Jing, Physical Review A **90**, 043841 (2014).
[32] N. De Beaudrap, Physical Review A **77**, 022328 (2008).
[33] A. M. Childs, D. W. Leung, and M. A. Nielsen, Physical Review A **71**, 032318 (2005).
[34] A. Broadbent and E. Kashefi, Theoretical computer science **410**, 2489 (2009).
[35] E. Nikahd, M. Houshmand, M. S. Zamani, and M. Sedighi, Microprocessors and Microsystems **39**, 210 (2015).
[36] M. Mhalla and S. Perdrix, in *International Colloquium on Automata, Languages, and Programming* (Springer, 2008) pp. 857–868.
[37] D. E. Browne and H. J. Briegel, arXiv preprint quant-ph/0603226 (2006).