Fundamentals of universality in one-way quantum computation

M Van den Nest[1], **W Dür**[1,2], **A Miyake**[1,2] **and H J Briegel**[1,2]

[1] Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften, Innsbruck, Austria
[2] Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 25, A-6020, Innsbruck, Austria
E-mail: maarten.van-den-nest@uibk.ac.at, wolfgang.duer@uibk.ac.uk, akimasa.miyake@uibk.ac.at and hans.briegel@uibk.ac.at

Abstract. In this paper, we build a framework allowing for a systematic investigation of the fundamental issue: '*Which quantum states serve as universal resources for measurement-based (one-way) quantum computation?*' We start our study by re-examining what is exactly meant by 'universality' in quantum computation, and what the implications are for universal one-way quantum computation. Given the framework of a measurement-based quantum computer, where quantum information is processed by *local* operations only, we find that the most general universal one-way quantum computer is one which is capable of accepting arbitrary classical inputs and producing arbitrary quantum outputs—we refer to this property as CQ-universality. We then show that a systematic study of CQ-universality in one-way quantum computation is possible by identifying entanglement features that are required to be present in every universal resource. In particular, we find that a large class of entanglement measures must reach its supremum on every universal resource. These insights are used to identify several families of states as being not universal, such as one-dimensional (1D) cluster states, Greenberger–Horne–Zeilinger (GHZ) states, W states, and ground states of non-critical 1D spin systems. Our criteria are strengthened by considering the efficiency of a quantum computation, and we find that entanglement measures must obey a certain scaling law with the system size for all efficient universal resources. This again leads to examples of non-universal resources, such as, e.g. ground states of critical 1D spin systems. On the other hand, we provide several examples of efficient universal resources, namely graph states corresponding to hexagonal, triangular and Kagome lattices. Finally, we consider the more general

notion of encoded CQ-universality, where quantum outputs are allowed to be produced in an encoded form. Again we provide entanglement-based criteria for encoded universality. Moreover, we present a general procedure to construct encoded universal resources.

Contents

1. Introduction

1.1. Role of measurement-based quantum computation (MQC) in fundamental investigations

Quantum computers offer a promising new way of information processing, in which the distinguished features of quantum mechanics can fruitfully be exploited. The discovery of quantum algorithms, most notably Shor's factoring algorithm [1] and Grover's search algorithm [2], demonstrate that quantum computation can achieve a (possibly exponential) speed-up over classical devices. This has put quantum computation at the focus of contemporary research, and indeed, significant progress in the theoretical understanding of quantum information processing, as well as promising steps toward an experimental realization of large-scale quantum computation, have recently been reported. In spite of these exciting developments, the basic question: '*which features of quantum mechanics are responsible for the speed-up of quantum computation over classical devices?*' remains to date largely unanswered.

An indication that there might not be a straightforward answer to this fundamental but difficult question, is given by the fact that there exist various models for quantum computation, such the quantum Turing machine [3], the quantum circuit (or network) model [4], measurement-based models [5]–[12], as well as adiabatic quantum computation [13]. Although these models have been shown to be equivalent in a certain complexity-theoretic sense (colloquially speaking, any problem which can be solved efficiently in one of the above models, can also be solved efficiently by the others), the elementary concepts underlying these schemes may differ significantly.

Therefore, certain computational schemes may lend themselves more than others to understanding fundamental issues regarding the power of quantum as compared to classical computation. The new paradigm of *measurement-based quantum computation (MQC)*, with the one-way quantum computer [5, 6] and the teleportation-based model [7, 8] as the most prominent examples, has lead to fresh perspectives in these respects. While in, e.g. the circuit model quantum information is processed by coherent unitary evolutions, in MQC the processing of quantum information takes place by performing *sequences of adaptive measurements*. Teleportation-based models use joint (i.e. entangling) measurements on two or more qubits and thereby perform sequences of teleportation-based gates. In contrast, the one-way model uses a highly entangled state, the *cluster state* [14], as a universal resource which is processed by single-qubit measurements only.

The latter property provides a model of one-way quantum computation—which is the focus of this paper—with a very distinct feature, namely that the entire resource of the computation is provided by the entangled state in which the system is initialized. In particular, any computational

speed-up of such a model w.r.t. classical computation can be traced back entirely to the properties of the resource state.

What is more, in the one-way model the resource character of *entanglement* is particularly highlighted, as it is clearly separated from the processing of quantum information by local, single-qubit measurements. As the latter cannot increase any entanglement in the system, all entanglement required for quantum computation needs to be initially present in the system. The introductory question of this paper can therefore be rephrased in a more concise form, namely '*What are the essential entanglement features of a resource state for (one-way) MQC that are required to obtain a speed-up over classical computation?*' The present paper will be centred around this question.

We emphasize that, in the following, we will exclusively consider MQC in the sense of the one-way quantum computer, i.e. considering only local measurements; teleportation-based models will not be considered.

For proposed implementations of measurement-based computation see e.g. [6], [15]–[22] (further references can be found in [23]); for recent experimental developments see [24].

1.2. Universality in MQC—aim and contribution of this paper

In this paper, we will be interested in those resource states for MQC which possess the strongest computational power possible, namely those which enable *universal* quantum computation, as do the two-dimensional (2D) cluster states[3]. It is our aim to investigate under which conditions resource states, other than the 2D cluster states, are universal, and what the role of entanglement plays in this issue.

In order to study universality in MQC in detail, it is necessary to have a clear-cut definition of this notion. We will hence start our study (section 2) by re-examining what is exactly meant by 'universal quantum computation', and what the implications are for universality in MQC (section 3). We will find that the notion of universality strongly depends on whether the in- and outputs of a quantum computer are allowed to be either classical or quantum. Furthermore, we will argue that the most general universal one-way quantum computer is a device which accepts arbitrary classical (C) inputs and produces arbitrary quantum (Q) outputs—we will call such a device a *CQ-universal* one-way quantum computer. The property that a one-way quantum computer is restricted to accept classical information only, is essentially due to the fact that, after the resource state of the device has been prepared, the only allowed quantum operations are *local operations*, which do not allow one to couple in quantum input states. On the other hand, the generation of arbitrary quantum output states poses no problem (as is the case in the 2D cluster state model)—hence the notion of CQ-universality in MQC. As a standard example, the 2D cluster state model is CQ-universal.

After giving a formal definition of what constitutes a (CQ-) universal resource state for MQC, we develop a framework which allows a systematic investigation of the criteria which need to be met by every universal resource (section 5). Our approach, which has been initiated in [27], is centred around considerations regarding entanglement. In particular, we find that

---

[3] For completeness we mention that we will *not* investigate whether universal MQC can be simulated efficiently on a classical computer, which remains to date an unresolved issue. In other words, here we study universal resource states—having the maximal computational power which a quantum computer can have—but we do not investigate whether this maximal computational power is in fact stronger than classical computation. For studies of the possibility of classically simulating quantum computation, we refer to [25, 26].

every universal resource needs to be *maximally entangled*, in the sense that every entanglement measure (belonging to a well-defined class) must reach its supremum on every universal resource. This result subsequently leads to several criteria for universality, by applying the result to specific measures. We consider several examples and show that entropic entanglement width [27], Schmidt rank width [26], Schmidt measure [28], geometric measure of entanglement [29, 30] as well as measures describing the capability to generate Bell pairs, must grow unboundedly on every universal resource—thus, every resource which does not exhibit a divergence of the above measures, cannot be universal. This leads to several examples of states which are not universal, such as large families of graph states, the GHZ states, W states and ground states of non-critical strongly interacting 1D systems.

Along the way, we also take *efficiency* into account (section 6). In this case, we find that a necessary condition for efficient universality is that the growth of above mentioned entanglement measures must be sufficiently fast with the system size—in most cases faster-than-logarithmic. These results are again used to provide further examples of states which are not efficiently universal. Furthermore, we also construct examples of efficient universal resource states, namely graph states corresponding to 2D hexagonal, triangular and Kagome lattices (section 7). Here our proof consists of showing explicitly that all these resources can be transformed into each other (with a certain moderate overhead) by local operations and classical communication (LOCC)—and are therefore equally maximally entangled.

In section 8, we consider a weaker (i.e. more general) form of CQ-universality, namely *encoded universality*, where it is sufficient that the desired output states be generated in an *encoded* form (here the notion of 'encoding' is similar to e.g. schemes in fault-tolerance and quantum error-correction). After discussing encodings and providing a definition for encoded universality, we investigate to what extent entanglement-based criteria can be used to assess encoded non-universality. Most importantly, we show that the Schmidt measure and geometric measure, as well as all measures which are non-increasing under coarsening of partitions of the system, give rise to criteria for encoded universality. Furthermore, relying on an 'indirect' argument of classical simulatability of quantum computation, we also argue that the Schmidt rank width provides a criterion for encoded universality. We then also give general constructive results; most importantly, extending results put forward in [12], we find that any universal resource which is itself subsequently encoded in an arbitrary way, is an encoded universal resource—which is a nontrivial statement. This implies in particular that for *any* kind of encoding, an encoded 2D-cluster state is an encoded universal resource (up to logical Pauli operations). We provide extensions to encoded universality and discuss some examples of encoded universal resources presented in the literature.

Finally, a summary of our results and an outlook toward further investigations are formulated in sections 9 and 10.

Remark 1. The main text is supplemented with a number of remarks. Although these remarks provide information which is relevant to obtain a detailed understanding of the current investigation, they may be skipped in a first reading.

2. General considerations on universality

In this section, we discuss what a universal quantum computer should be capable of. Somewhat unexpectedly, this is not so trivial as one might think at first sight. In particular, we will argue

that there are several possible definitions, all of which are of natural interest depending on which application one might have in mind.

We will start our discussion by reviewing, in section 2.1, some important conceptual notions regarding the universality of the circuit model. In investigations of universality for general computational models, the circuit model will serve as a natural reference. This then leads us, in section 2.2, to consider four natural but distinct notions of universality of a quantum computer, namely *CC-*, *CQ-*, *QC-*, and *QQ-universality*. In each of those notions of universality it is specified whether the computer should accept quantum (Q) or classical (C) inputs, and produce quantum or classical outputs.

2.1. Circuit model

In the circuit model for quantum computation, quantum information is processed by applying sequences of unitary gates on quantum states. These gates are typically chosen from an elementary set. Universality in the circuit model is defined with respect to the possibility of generating arbitrary unitary operations by composition of such elementary gates. Namely, a gate set $\mathcal{S}$ is called *universal* if *any n*-qubit unitary operation $U \in SU(2^n)$, for every n, can be realized as a sequence of elementary gates taken from $\mathcal{S}$.

Notice that in principle the number of gates required to produce a given unitary may be unbounded. In practice, however, the number of gates that can be applied is limited, and one often considers only *n*-qubit unitary operations U that can be generated *efficiently*, i.e. with poly(n) elementary gates. An example of a universal gate set $\mathcal{S}_1$ is given by the two-qubit CNOT gate together with the group $SU(2)$ of arbitrary single-qubit gates [31], and this specific gate set usually serves as a reference set to distinguish between efficient and non-efficient gate sets. In particular, one says that a set of gates $\mathcal{S}$ is efficiently universal if any $U \in SU(2^n)$ that can be efficiently generated—i.e. with poly(n) gates—using the gate set $\mathcal{S}_1$, can also be efficiently generated using the gate set $\mathcal{S}$. This implies that efficient universal gate sets can simulate the set $\mathcal{S}_1$ with polynomial overhead.

For many practical applications, the exact generation of a unitary operator is not required, and an *approximate* application of U with a certain accuracy ϵ is sufficient. Such a finite accuracy shows up very naturally when considering discrete sets of elementary gates, such as the CNOT gate plus a finite set of single-qubit gates with certain rotational angles [31]. In fact, it turns out that an approximate generation of all unitary operations with arbitrary accuracy is possible for many discrete sets of elementary gates. The best known example is the set consisting of single- and two-qubit Clifford gates [32] together with a single-qubit $\pi/8$ rotation along the z-axis [31]. As established in the Solovay–Kitaev theorem, the overhead to approximate a sequence of m elementary gates from the set $\mathcal{S}_1$ with accuracy ϵ by gates from the discrete gate set specified above, scales as $O(m \log^c(m/\epsilon))$, i.e. poly-logarithmically in $1/\epsilon$ (where $1 \leqslant c \leqslant 2$) [31, 33].

It is evident from the above discussion that universality in the circuit model is concerned with the possibility of implementing arbitrary *unitary operations*. However, regarding the nature of a quantum computation in the circuit model, often additional (implicit) assumptions are made concerning both the *input* and *output* of a computation. Namely, it is often assumed that both the input and the output of a quantum computation are classical. This manifests itself in the fact that, firstly, the input state of a computation is typically a standard quantum state $|0\rangle^{\otimes n}$ and, secondly, the last step of the computation—after the unitary operation has been implemented—typically consists of a sequence of single-qubit measurements in the standard basis, destroying the final

quantum state (i.e. transforming it to a simple product state) and yielding the classical output. We emphasize that it is *not* necessary to restrict a quantum computation in the circuit model to this classical input–output scenario. In particular, arbitrary quantum inputs in the form of n-qubit quantum states $|\psi\rangle$ can naturally be processed by a (universal) circuit model quantum computer. In addition, it is not necessary to perform a final measurement. Without such final measurements, the quantum computation produces a quantum state as output, which might be used for other purposes. In this general scenario, a circuit model quantum computer might be considered as a device which accepts a quantum state as an input, processes it by applying a unitary operation (representing the program and possible classical input data), and finally produces an output quantum state (together with classical information resulting from possible measurements).

Thus, a (universal) circuit model quantum computer can be regarded as a device which accepts either a classical or quantum input, and which produces either a classical or quantum output. As we will discuss in more detail in section 2.2, the different choices one can make regarding the types of in- and outputs of a quantum computation have a significant impact on the definition(s) of universality one may consider. This will be a crucial point in defining and studying universality in MQC.

2.2. Different types of universality

As we have briefly reviewed in the previous section, universality in the circuit model is concerned with the possibility of implementing arbitrary *unitary operations*—be it exactly or with a certain precision.

When considering a quantum computational model other than the circuit model—such as the measurement-based model considered here—one can ask in which sense it may be called universal. In order to define universality, one typically takes the circuit model as a reference, and this is also the strategy which will be adopted here[4]. Colloquially speaking, a model is called universal *if it can perform the same tasks as a circuit model quantum computer*. In this section, we make this statement more precise (although we will stay at a qualitative level). In particular, we will argue that possible definitions of what a universal quantum computer is supposed to be capable of depend on the allowed input and output, which may either be of classical or quantum nature.

Regarding in- and outputs of a quantum computation, we have the following possibilities:

CC: both input and output are classical;
QC: the input is quantum and the output is classical;
CQ: the input is classical and the output is a quantum;
QQ: both input and output are quantum.

The notion of 'universal quantum computation' has different meanings depending on which of the above cases is considered. In each of these situations, a natural definition of universality can be formulated where the circuit model is used as a reference. Moreover, we emphasize that we will make a clear separation between universality of a quantum computer and the efficiency with

---

[4] This strategy is natural because all 'standard' models for QC are known to be equivalent, in a complexity-theoretic sense, to the circuit model.

which computations can be executed—i.e. we will regard *universality* and *efficient universality* as distinct notions (this point will be discussed further in section 2.3).

We now consider the cases CC, CQ, QC and QQ one by one.

CC. Here it is assumed that both input and output of the computation are *classical*, i.e. a quantum computer is considered to be a device that solves classical problems and provides the solution in the form of classical data. Only at an intermediate stage is the additional power of quantum mechanics used to achieve an enhanced processing of information. The final step of such a quantum computation is usually given by a sequence of (local) measurements performed on the output state, which ensures the transition from quantum information to classical information. An important example of this kind is given by Shor's factoring algorithm. One may call a quantum computer CC-universal if it can perform the same tasks as a circuit model quantum computer which accepts classical inputs and produces classical outputs. That is, for every unitary U, a CC-universal quantum computer must be capable of reproducing the statistics of local measurements performed on the state $U|0\rangle^{\otimes n}$. Note that, as we do not take efficiency into account yet, a CC-universal quantum computer is simply one which can perform universal classical computation (and is therefore not different from a classical computer). In order to distinguish a CC-universal quantum computer from classical computers, one needs to take efficiency into account and demand that the classical data is obtained in polynomial time for any unitary operations U that can be generated with a polynomial sized quantum circuit. We refer to remark 2 for further details regarding this issue.

QC. In this case, the output is still classical, i.e. the final step of the computation is given by a sequence of measurements. However, now the input can be an arbitrary quantum state $|\phi_{in}\rangle$ that is processed by the quantum computer. The input state may be the output state of a previous QQ-quantum computer (see the case QQ below), or the state of some physical system which one would like to study with the help of a (QC) quantum computer, e.g. the ground state of some spin system. For instance, one may wish to learn the value of some observable or entanglement measure, or whether a state (or density operator) has positive partial transposition [34]. Note that the input state may be known or unknown to the device. Finally, also in studies of quantum complexity classes such as QMA, situations are considered where devices can accept quantum states as inputs ('certificates') [35].

A quantum computer is then called QC-universal if it can perform the same tasks as a circuit model quantum computer which accepts quantum inputs and produces classical outputs. That is, *for every (possibly unknown) input state $|\phi_{in}\rangle$ and for every unitary operation U, a QC-universal quantum computer can reproduce the statistics of local measurements performed on the quantum state $|\phi_{out}\rangle = U|\phi_{in}\rangle$.* One may in addition take efficiency into account, in the same way as in the case of CC, demanding that the overhead with respect to the circuit model is polynomial[5].

CQ. Here the input is classical but the output of a quantum computation can now be a quantum state. Compared to a CC quantum computer, this device has the advantage that one can decide at a later stage whether one wishes to obtain classical information by performing measurements, or whether one wants to use the produced state as the input of a following quantum computation, or whether one wants to use this state for another quantum information task—the goal of a quantum computation might e.g. be to produce a quantum state which is

---

[5] However, for distinguishing such a device from classical computers this is not necessary (a classical computer cannot handle a quantum input).

subsequently distributed over several parties, and then used to establish a secret key, for secret sharing, or to perform (non-local) two-qubit gates.

Analogous to the previous cases, we will call a quantum computer CQ-universal if it can perform the same tasks as a circuit model quantum computer which accepts classical inputs and which produces quantum outputs. That is, *for every unitary operation U, a CQ-universal quantum computer is able to produce the quantum state* $|\phi_{\text{out}}\rangle = U|0\rangle^{\otimes n}$. This definition is equivalent to stating that that a CQ-universal quantum computer is capable of preparing an arbitrary quantum state. One may again add the requirement of efficiency here, calling a quantum computer efficiently CQ-universal if the overhead in the above state preparation compared to the circuit model is polynomial.

QQ. This is the most powerful device, as it can accept quantum states as input and can produce quantum states as output. Apart from the applications mentioned in (ii) and (iii), such a quantum computer is *composable*, i.e. the output of a previous quantum computation can be used as the input of a subsequent quantum computation. In particular this allows one to use distributed quantum processors. We will call a quantum computer QQ-universal if it can produce the quantum state $|\phi_{\text{out}}\rangle = U|\phi_{\text{in}}\rangle$ for any given input state $|\phi_{\text{in}}\rangle$ and for any unitary operation U. Equivalently, one can say that any unitary operation U can be performed on an arbitrary input state. As before, the notion of efficiency can naturally be considered.

2.3. Some remarks

In this section, we give a number of remarks regarding the above types of universality.

Remark 2. *Separating universality and efficiency.* In the definitions of CC-, CQ-, QC- and QQ-universality we have deliberately separated the issue of universality from the issue of efficiency. The reason for this is that, in the present study of MQC, we will be interested in computational models having a quantum output. In such situations, we will argue that a lot can be learned by studying, say, CQ-universality, without considering efficiency. This will be in particular the case for the study of necessary conditions for CQ-universality: we will present systematic procedures for identifying large classes of resource states for MQC which are not CQ-universal, even though no considerations of efficiency are included. Finally, we note that in the case of CC-universality it is meaningless to separate universality from efficiency; as pointed out above, every classical computer is (inefficiently) CC-universal, such that nothing can be learned about the differences between classical and quantum computation by considering CC-universality without efficiency.

Remark 3. *Qubits, qudits and encodings.* In the above definitions of the different types of universalities, and in the discussion of the circuit model, we have always assumed that the physical systems involved are qubit systems (and qubit systems only). This does not represent a restriction if one considers classical inputs and outputs, as only the information is important in this case; the type and dimension of systems that carry the information is irrelevant[6]. The situation is different when considering also quantum inputs and/or outputs—i.e. in the CQ, QC, and QQ case. There, any computational model typically works with physical systems where the individual constituents are associated to a Hilbert space of fixed dimension, such

---

[6] We note that, in the CC case, the circuit model working with qudit systems has been shown to polynomially equivalent to the qubit circuit model [31].

IOP Institute of Physics Φ DEUTSCHE PHYSIKALISCHE GESELLSCHAFT

that the states which can be accepted and/or produced can only be multi-party d-dimensional systems, for some fixed d. For example, it is clear that, when local measurements are performed on a cluster state in the one-way model, only qubit states can be produced, and not e.g. qutrit states.

Notice, however, that in many cases it is sufficient to generate or provide quantum states in an *encoded* form. That is, the Hilbert space of a d-dimensional system can be embedded into the Hilbert space of $\lceil \log_2(d) \rceil$ qubits and in this sense any state of n d-dimensional systems can be generated in an encoded form with $n' = n \cdot \lceil \log_2(d) \rceil$ qubits. We will discuss the issue of encodings in more detail in section 8. Until then we will restrict our considerations to qubits, keeping in mind that higher dimensional systems can be produced in an encoded form.

Remark 4. *Known versus unknown quantum input.* A QC- or QQ-universal quantum computer must be capable of processing unknown inputs. Furthermore, although a CQ-universal computer can only accept classical inputs, it can simulate processes where a QC or QQ computer accepts a *known* quantum input: namely, suppose that a QQ-universal computer accepts a known input state $|\phi_{in}\rangle$ and performs a unitary operation U, producing the state $|\phi_{out}\rangle = U|\phi_{in}\rangle$. Then a CQ-universal computer can simulate this process by simply classically computing what the state $|\phi_{out}\rangle$ is, and by then preparing this state, which is possible from its CQ-universality. When efficiency is taken into account, an efficient CQ-universal computer can efficiently simulate any process $|\phi_{in}\rangle \rightarrow |\phi_{out}\rangle$ where (i) U is a poly-sized circuit, (ii) $|\phi_{in}\rangle$ can be prepared by a poly-sized circuit and (iii) this last circuit is known; for, in this case $|\phi_{out}\rangle$ is simply a state which can be prepared by a known poly-sized circuit, which any efficiently CQ-universal resource should be able to generate efficiently.

Remark 5. *Exact versus approximate universality.* In the qualitative treatment in section 2.2, we have considered an ideal situation and not talked about approximate universality. This is of course an important issue—cf e.g. the circuit model, where finite sets of elementary gates can only be approximately universal. Nevertheless, when considering MQC models, it is known that e.g. the 2D cluster states are exactly (CQ-) universal, and we will consider only this ideal situation in this paper. Approximate universality will be taken into account in upcoming work [36].

3. Universality in MQC

In this section, we move to our topic of interest, namely (one-way) measurement-based models of quantum computation. In section 3.1, we will consider the one-way model with a 2D cluster state as a resource state, and we will review in which ways it is universal. In fact, we will see that the 2D cluster state model is (efficiently) CQ-universal, and that this is the most powerful type of universality any MQC model can have (if we only consider local measurements and do not allow for additional resources). This leads us to introduce, in section 3.2, the definition of 'universal resource for MQC', which refers to CQ-universality. Afterward we discuss the notion of efficiency in universal MQC.

3.1. One-way model

In this section, we first briefly discuss the distinct features of the one-way model for MQC having a 2D cluster state as an entangled resource, and then consider in which way(s) it is universal.

The one-way quantum computer was introduced in [5, 6]. This computational model is in striking contrast to the circuit model, as the processing of quantum information is not realized by applying unitary gates (i.e. via physical interactions between the qubits), but it takes place solely by performing *single-qubit measurements*. The general procedure of a one-way quantum computation is the following.

(i) A classical input is provided which specifies the data and the program.

(ii) A 2D cluster state $|C_{d_1 \times d_2}\rangle$ of size $d_1 \times d_2$ is prepared, where d_1 and d_2 depend on the classical input data, the size of output and the length of the computation. A cluster state is a particular instance of a *graph state*. A graph state on m qubits is the joint eigenstate of m commuting correlation operators

$$K_a := \sigma_x^{(a)} \bigotimes_{b \in N(a)} \sigma_z^{(b)}, \tag{1}$$

where $N(a)$ denotes the set of neighbours of qubit a in the graph [23]; a 2D cluster state is obtained if the underlying graph is a $d_1 \times d_2$ rectangular lattice (thus $m = d_1 d_2$). The cluster state serves as the resource for the computation.

(iii) A sequence of adaptive one-qubit measurements is implemented on certain subsets of qubits in the cluster. In each step of the computation, the measurement bases depend on the program and on outcomes of previous measurements. A simple classical computer is used to compute which measurement directions have to be chosen in every step of the computation.

(iv) After the measurements have been implemented, the state of the system has the form $|\xi^\alpha\rangle|\psi_{\text{out}}^\alpha\rangle$, where α indexes the collection of measurement outcomes of the different branches of the computation. The states $|\psi_{\text{out}}^\alpha\rangle$ in all branches are equal up to a (local) discrete Pauli unitary operation, i.e. there exists a state $|\phi_{\text{out}}\rangle$ such that $|\psi_{\text{out}}^\alpha\rangle = \Sigma^\alpha |\phi_{\text{out}}\rangle$ for all α, where Σ^α is a multi-qubit Pauli operator, the so-called byproduct operator; the measured qubits are in a product state $|\xi^\alpha\rangle$ which also depends on the measurement outcomes.

Thus, in the one-way model every desired state $|\phi_{\text{out}}\rangle$ can be prepared deterministically up to a Pauli operator—even though the results of the measurements are random. Only the correction operations (i.e. the local Pauli operations) depend on the measurement outcomes, and can be determined via side-processing with a classical computer.

Let us now discuss the different types of universality for the one-way model.

QC, QQ. First, note that the one-way quantum computer in its above form cannot be QC- or QQ-universal by definition. This is because, in this scheme, one is given a 2D cluster state as a resource and the only allowed quantum operations are single-qubit measurements corresponding to the classical program. Such local operations do not allow the device to accept and process a quantum state.

CC. On the other hand, the one-way model is known to be *efficiently CC-universal*, as it was proven in [5, 6] that a one-way quantum computer can efficiently simulate any CC-computation in the circuit model. By 'efficiently' is meant here that the number of measurements as well as the

number of additional qubits and the temporal overhead required to simulate the transformation $|0\rangle^{\otimes n} \to U|0\rangle^{\otimes n}$ scale polynomially with the number of gates required to generate the unitary U (we refer the reader to section 3.3 for a deeper treatment of efficiency in MQC). Note also that the fact that, in the one-way model, output states can be prepared up to local Pauli operators does not cause any restriction, as these Pauli corrections can be incorporated by accordingly changing the final measurement bases in the algorithm.

CQ. Even stronger, with a slight modification the one-way model can be made to be *CQ-universal* and even *efficiently CQ-universal*. This is achieved by allowing as basic operations, next to the local measurements, also (local) Pauli operations. If such local unitaries are allowed, then it follows from the above that any multi-qubit state can deterministically be prepared by performing local measurements on a sufficiently large 2D cluster state, making the model CQ-universal. Efficient CQ-universality is obtained by again noting that the transformation $|0\rangle^{\otimes n} \to U|0\rangle^{\otimes n}$ can be simulated with polynomial overhead w.r.t. the circuit model.

Remark 6. *Making the one-way model QQ-universal.* As pointed out in remark 4, it follows from the efficient CQ-universality of the one-way model that it can efficiently simulate certain processes where a known input state is transformed by poly-sized unitary operation. Here we further remark that the one-way model can be made fully QQ-universal by allowing an additional resource, an 'input coupler', which allows one to couple in unknown quantum states[7]. When $|\phi_{in}\rangle$ is a (possibly unknown) input state on n qubits, this additional resource simply consists of n controlled phase gates $U_{PG} = diag(1, 1, 1, -1)$ which are applied—initially, and only once—pairwise between every qubit of $|\phi_{in}\rangle$ and every second qubit on the 'left side' of a $2n \times m$ cluster state (for some $m = \text{poly}(n)$). It was shown in [5, 6] that for every unitary operation U there exists a sequence of local measurements, implemented on the resulting state, which can generate the state $U|\phi_{in}\rangle$ on some subset of the cluster with polynomial overhead— making the model efficiently QQ-universal. Note that a particularly nice feature of this result is that the measurement protocol is independent of the input state and only depends on the unitary operation U. Finally, we emphasize that this scheme goes somewhat beyond the present investigation, as the controlled phase gates introduce additional entanglement in the system, going away from the LOCC-only scenario in which we are interested here (see, however, observation 3 in section 4.2)

3.2. General definition

We conclude from the above discussion that the most general universality exhibited by the one-way model is (efficient) CQ-universality. This is the situation we will have in mind when studying general universality in MQC—i.e. we will be interested in CQ-universality of general resource states. The main motivation for this is that CQ-universality is the most general and powerful type of universality any LOCC-based MQC model can have. In particular, any resource which is (efficiently) CQ-universal is also (efficiently) CC-universal, and, as we shall see in observation 3, it is efficiently QQ universal if supplemented with an input coupler. Furthermore, we will show in section 5 that a systematic study of the properties which make a resource CQ-universal, is possible, whereas systematic treatments of e.g. CC-universality in MQC are presently far less within reach. *Henceforth, when referring to 'universality' we will always mean 'CQ-universality'.*

---

[7] See also 'scheme 1' ($\cong$ QQ) versus 'scheme 2' ($\cong$ CQ) in [6].

We now have a computational model in mind where quantum algorithms are implemented by performing local measurements (or, more generally, LOCC—see remark 8) on a resource state, as in the cluster state model, and we will give a qualitative definition of a universal resource.

If one wants to avoid talking about infinitely large states, universality is to be regarded as a property that is attributed, not to a single state, but to a family of infinitely many states

$$\Psi = \{|\psi_1\rangle, |\psi_2\rangle, \ldots\}, \quad |\Psi| = \infty. \tag{2}$$

When considering the 2D cluster state model, it is indeed clear that it is not one cluster state which forms a universal resource, but rather the family of all 2D cluster states; this is most evident in step (ii) in section 3.1, where the size of the cluster state depends on which output state is to be prepared, or which quantum algorithm is to be executed.

Before stating the definition of universal resource, we will need the following notation. Let $|\psi\rangle$ be a multi-qubit state defined on a set of qubits $\{1, \ldots, N\}$, and let $|\phi\rangle$ be an n-qubit state, where $n \leqslant N$. We will use the expression $|\psi\rangle \geqslant_{\text{LOCC}} |\phi\rangle$ to denote that there exists a subset of qubits $A \subseteq \{1, \ldots, N\}$, where $|A| = n$, such that the transformation

$$|\psi\rangle \rightarrow |\phi\rangle^A |0\rangle^{\bar{A}} \tag{3}$$

(where $\bar{A} := \{1, \ldots, N\} \setminus A$) is possible by means of LOCC with unit probability.

We can now state the following definition of universal resource, first put forward in [27].

Definition 1 (Universal resource). *A family of states $\Psi = \{|\psi_1\rangle, |\psi_2\rangle, \ldots\}$ is called a universal resource for MQC if, for every n, and for every n-qubit quantum state $|\phi_{\text{out}}\rangle$, there exists a resource state $|\psi_i\rangle \in \Psi$ such that $|\psi_i\rangle \geqslant_{\text{LOCC}} |\phi_{\text{out}}\rangle$.*

Thus, we will e.g. say that the family of 2D cluster states

$$\Psi_{2D} := \{|C_{1\times1}\rangle, |C_{2\times2}\rangle, |C_{3\times3}\rangle, \ldots\}, \tag{4}$$

is a universal resource for MQC, as any multi-qubit state can be prepared (deterministically and exactly) by performing LOCC on 2D cluster state of appropriate size.

The above definition essentially expresses that a universal resource needs to be capable of preparing *any* quantum state. Note that we can associate the output quantum state $|\phi_{\text{out}}\rangle$ with a unitary operation U via

$$|\phi_{\text{out}}\rangle := U|0\rangle^{\otimes n}. \tag{5}$$

This association makes evident that the above definition is concerned with (CQ-)universal quantum computation, in the sense that a universal resource can simulate any unitary operation U acting on a fixed input state $|0\rangle^{\otimes n}$.

We now make several remarks regarding the above definition.

Remark 7. *Ignoring efficiency (see also Remark 2).* In definition 1, the issue of efficiency is deliberately omitted; for example, in this definition we do not put any restrictions on how large a resource state is allowed to be in order to prepare a desired output state. The reason for this is, as we will show in section 5, that several interesting aspects of universality can already be understood without taking the additional difficulty of efficiency into account. In particular,

this approach will show its merit when considering necessary conditions for universality. In section 5, we will present a systematic approach to obtaining many examples of non-universal resources—which *a fortiori* cannot be efficient universal resources either—without having to consider efficiency issues. Needless to say that efficiency is of course an important aspect of the investigation; we will treat this issue—separately—in the next section, where we provide a definition for an efficient universal resource.

Remark 8. *LOCC versus measurements only.* In definition 1, we slightly extend the framework of one-way quantum computation and allow for sequences of *arbitrary* LOCC, rather than only local measurements and local Pauli operations. In this way, the main feature of the one-way model is maintained, namely that resource states are processed by local operations. The resource character of entanglement is particularly highlighted, as LOCC operations are the most general operations which cannot increase entanglement. Hence the resource state includes all the necessary entanglement which is used up (in part) during the computation. Of course, it is clear that in realistic situations one would favour resources which are universal by local measurements (and some additional local corrections) only. Note that the examples of universal resources we will present in section 7, are all of this form.

Remark 9. *Exact deterministic universality.* Definition 1 represents an ideal situation, where we demand that states can be prepared exactly and with unit probability, i.e. it is a definition of exact, deterministic universality. In realistic conditions, it often suffices that output states can be prepared with an arbitrary high accuracy, and with a probability which is arbitrarily close to one. This realistic scenario (called *approximate, quasi-deterministic universality*) will not be treated in the present paper, where we stay with the ideal case in order to outline the main methods of this study. The reader is referred to a subsequent paper [36] for a treatment of approximate, quasi-deterministic universality.

Remark 10. *Fixed versus random output particles.* In the above definition for universality, it is assumed (as implicitly also done in [27]) that in all possible branches of the LOCC protocol, the output state $|\phi_{\text{out}}\rangle$ is prepared on the *same* output particles, see the discussion preceding definition 1. These output systems may in principle be unknown at the beginning of the LOCC protocol, but need to be the same for all branches of the protocol. Such a requirement is natural in the context of CQ-universality, where a quantum output can be further processed and used as a resource for some tasks that are specified at a later stage. One would like to know (favourably already in advance) on which particles the desired state is going to be prepared. A situation where this is necessary is e.g. given by the on-demand preparation of a certain resource state for distributed security applications that can be specified by the involved parties at some stage. In this case, every party holds one of the output particles, and the preparation of the desired state takes place by LOCC at some point.

The requirement of fixed output systems can in principle also be dropped. In this case, one demands instead that the output state can be generated between some, not previously specified, subset of particles. The subset of particles may even be random, depending e.g. on outcomes of measurements in the LOCC protocol. Note that in the context of CC-universality it is in fact natural that one does allow for random output systems (in fact, the classical output of a 'CC' cluster state quantum computation is derived by classical post-processing on the outcomes of measurements on all measured particles, so it is not clear that this output is localized on the qubits in a strict sense). In the following, we will *not* consider the possibility of random output

systems. We remark, however, that some of the results we obtain in the next sections crucially depend on the assumption of fixed output systems. We will again comment in remark 16 on the possibility of random output systems.

3.3. Efficient universality

In classical computation and quantum computation, efficiency is a central issue. Although the above definition of universality does not take efficiency issues into account, it is nevertheless useful. As we have argued to some extent in the previous section, and as will become more evident in the next one, it is not necessarily required to consider efficiency. Even when allowing for (exponential) overheads in temporal and spatial resources, and for unlimited classical computational power, one can still rule out large families of states as being not universal. Clearly, if one also considers efficiency, one obtains stronger criteria for non-universality, and from a practical perspective only resources which are (in the sense specified below) efficiently universal are useful.

3.3.1. Various efficiency issues. In MQC, the generation of a n-qubit state $|\phi_{out}\rangle$ takes place by performing sequences of single-qubit measurements, or, more generally, LOCC, on a resource state of $N \geqslant n$ qubits. In such a process, there are several efficiency issues that one needs to consider.

 (i) *Spatial overhead.* This refers to the required size N of the resource state, since at most $N - n$ qubits need to be measured in order to generate $|\phi_{out}\rangle$. We will say that the preparation of $|\phi_{out}\rangle$ by performing LOCC on a resource state is efficient with respect to spatial overhead if $N = \text{poly}(n)$, i.e. only polynomially many resource qubits are required.

 (ii) *Temporal overhead.* This refers to the required time steps to implement the sequence of LOCC. If one is restricted to projective measurements, then the number of time steps is at most $N - n$. As shown in [5, 6], many measurements can be performed simultaneously; e.g. all measurements devoted to implementing Clifford operations in the corresponding quantum circuit can be done in a single time step. For general LOCC, the situation is different. While it might still be possible to operate on several qubits simultaneously, sequences of adaptive local operations of arbitrary length are conceivable. We will say that the preparation of $|\phi_{out}\rangle$ by performing LOCC on a resource state is efficient with respect to temporal overhead, if the number of steps in the LOCC protocol that cannot be performed in parallel is $\text{poly}(n)$, i.e. only polynomially many time steps are needed.

(iii) *Classical side-processing.* This is an essential part of the one-way model, where one needs to keep track of basis changes, and where one has to decide how measurements (or, more generally, local operations) are adapted depending on outcomes of previous measurements. Classical processing may also be required for other purposes (e.g. when considering error correction). We will say that the preparation of $|\phi_{out}\rangle$ by performing LOCC on a resource state is efficient with respect to classical side-processing if the overhead for classical computation is polynomially bounded in space and time. Notice that in the 2D cluster state model, the time complexity of classical side-processing only scales as $\log(n)$.

(iv) *Description and preparation complexity of resource states.* Throughout this paper, we will only be interested in whether (families of) resource states are universal for MQC or not,

and we will *not* be concerned with potential difficulties in *describing* the resource states efficiently, or whether they can be *prepared* efficiently [37]. We will rather assume that the resource states are provided.

Remark 11. *Description and preparation complexity.* For practical purposes, it may, however, be important to take issue (iv) into account. In particular, the possible efficient preparation of resource states might be crucial to determine whether MQC could be realized in practice with a given (family of) resource state(s). By efficient preparation it is meant that a resource state of N qubits can be prepared with the help of a quantum circuit with poly(N) elementary gates. Notice, however, that other ways of preparing resource states are conceivable. For instance, states that occur naturally as ground states of certain physical systems may be universal resource states. If one could find such universal resource states, then the problem of efficient generation by a quantum circuit becomes irrelevant.

Remark 12. We (implicitly) assume that the label k in a family of resource states $\Psi = \{|\psi_k\rangle\}_k$ only serves as some index to a set of quantum states (most of the time we will have some regular structure in mind and k is simply related to the size of the structure), and is not used to provide additional computational power.

3.3.2. Definition of efficient universality. Having the above efficiency issues in mind, the following question arises: *which states should be efficiently preparable from an efficient universal resource?* Evidently, there are many quantum states $|\phi_{\text{out}}\rangle$ that cannot be generated efficiently even in the circuit model. As already mentioned in section 2.2, in the definition of efficient universality for MQC, we will refer to the circuit model and demand that all states that can be *efficiently prepared in the circuit model should also be preparable efficiently in an MQC model.* Efficient generation of an n-qubit state $|\phi_{\text{out}}\rangle$ with n arbitrary in the circuit model means that there exists a polynomial-size quantum circuit, i.e. consisting of poly(n) elementary gates, which generates the family of these states with n increasing from a product state. Efficiency in the MQC model refers to efficiency with respect to spatial and temporal overhead and classical side-processing, all of which need to be poly(n). This is made precise in the following definition.

Definition 2 (Efficient universal resource). *A family of states Ψ is called an efficient universal resource for MQC if the following is true: for every family of states $\{|\phi_{\text{out}}^{(n)}\rangle\}_{n=1}^{\infty}$ which can be obtained by a poly(n)-sized family of quantum circuits, and where $|\phi_{\text{out}}^{(n)}\rangle$ is a state on n qubits, there exists a subfamily*

$$\{|\psi_{i_n}\rangle\}_{n=1}^{\infty} \subseteq \Psi, \tag{6}$$

where $|\psi_{i_n}\rangle$ is a state on at most $N = poly(n)$ qubits, such that the transformation

$$|\psi_{i_n}\rangle \rightarrow |\phi_{\text{out}}^{(n)}\rangle|0\rangle^{\otimes(N-n)}, \tag{7}$$

is possible by means of LOCC in poly(n) time, using classical side processing that is polynomially bounded in space and time.

Thus, as already stated in section 3.1, the set Ψ_{2D} of $d \times d$ cluster states is an efficient universal resource. Indeed, as pointed out earlier, every state which can be prepared by a poly-sized network, can also be prepared efficiently in the one-way model [to be precise, one can only meaningfully say that a *family* of states is generated by a poly-sized network, rather than a single state. Henceforth, whenever we refer to 'a state' which can be prepared by a poly-sized circuit', we will mean 'family of states'].

Remark 13. Equivalently to the above definition, one may define that an efficient universal resource is capable of efficiently preparing any state which can be efficiently prepared in the one-way model. In this way, one would obtain a definition of efficient universal resources for MQC which is stated entirely in terms of measurement-based schemes.

Remark 14. Note that the 2D cluster states can be described and, more importantly, prepared efficiently (as is the case for all graph states) [23, 38]. In particular, the preparation of an N-qubit 2D cluster state requires only $O(N)$ (more precisely: $2N$) phase gates, most of which can be performed in parallel. The 2D cluster state can hence be prepared in linear time in the circuit model.

4. Observations

In this section, we will present a number of straightforward observations which will turn out to be crucial to establish both necessary and sufficient criteria for (efficient) universality.

4.1. Universality and the 2D cluster states

We start with a key observation regarding universal resources which has already been presented in [27].

Observation 1. *A set of states Ψ is a universal resource if and only if all 2D cluster states $|C_{d \times d}\rangle$ (for all d) can be prepared (deterministically and exactly) from the set Ψ by LOCC.*

Necessity of the condition follows from the fact that a universal resource should be capable of preparing *any* quantum state, in particular an arbitrary 2D cluster state. Sufficiency follows from the fact that once a 2D cluster state of arbitrary size can be created, one can use the one-way model for quantum computation to generate *any* quantum state by LOCC [5, 6].

Note that a direct consequence of this observation is that every CQ-universal resource can immediately be made QQ-universal by reducing it to the 2D cluster state model. This can be seen as follows. Due to the fact that from any universal resource a 2D cluster state can be generated, a possible way to perform an arbitrary (CQ) quantum computation (i.e. to generate an n-qubit state $|\phi_{out}\rangle = U|0\rangle$) is to first generate a sufficiently large 2D cluster state, and then continue with the *same* LOCC protocol as in the one-way model. In particular, this allows one to use the same methods and techniques as in the one-way model for MQC to process classical inputs. What is more, in this way any CQ-universal resource Ψ can immediately be made QQ-universal by supplying Ψ with the same input coupler (i.e. an additional resource in the form of a simple round of n Bell measurements or controlled phase gates) as in the one-way model.

Observation 2. *Every CQ-universal resource can be made QQ-universal by allowing quantum inputs to be coupled into the resource by the same input coupler as in the one-way model, provided e.g. by n Bell measurements or phase gates.*

This observation illustrates in particular that there is no severe restriction in the fact that MQC schemes (within the framework 'resource state plus LOCC') can only be CQ-universal, since only a small step is required to go from CQ-universality to the most general notion of QQ-universality.

4.2. Efficient universality and the 2D cluster states

An observation for efficient universality is the following.

Observation 3. *A set of states Ψ is an efficient universal resource if and only if all 2D cluster states $|C_{d \times d}\rangle$ (for all d) can be efficiently prepared from the set Ψ by LOCC, i.e. with polynomial spatial and temporal overhead, and with polynomial classical side-processing.*

Necessity of the condition follows from the fact that an efficient universal resource must be capable of preparing the 2D cluster states efficiently, since these states can be prepared efficiently in the circuit model. Sufficiency follows from the fact that, once a 2D cluster state of arbitrary size can be created efficiently, one can use the one-way model to efficiently generate *any* quantum state that can be efficiently generated in the circuit model (as discussed in the previous section).

Again, this observation leads to one possible way of performing the computation by generating first a 2D cluster state and then using the corresponding LOCC protocol of the one-way model. Similar to the case where efficiency was not considered, it follows that any efficient CQ-universal resource is also efficiently QQ-universal when allowing for the same supplementary resource ('input coupler') as in the one-way model for MQC.

4.3. Equivalence of universal graph states

The next observation is concerned with a particular family of potential resource states, the graph states [23]. Consider a family Ψ where all members are graph states, and consider the case where we are interested only in preparing a specific quantum state. In principle it is conceivable that such a specific task can be performed more efficiently for certain graph resource states than for the 2D cluster state. The following observation, however, shows that this is not the case.

Observation 4. *Any quantum state that can be prepared from a graph state resource with polynomial temporal and spatial overhead by means of LOCC, can also be prepared from a 2D cluster state with polynomial temporal and spatial overhead.*

This observation implies that one cannot hope for an (exponential) speedup, even to prepare certain specific states $|\phi_{out}\rangle$ (or, equivalently, to perform some specific unitary operation, i.e. algorithm) within the measurement-based model if the resource states are general graph states. The one-way model based on the 2D cluster state is already optimal in this respect. The observation immediately follows from the fact that *any* graph state of n-qubits can be prepared efficiently in the circuit model with at most $n(n-1)/2$ two-qubit phase gates [23]. This implies that any graph state can also be prepared efficiently, i.e. with polynomial overhead in spatial and temporal resources, and in classical side-processing, from a 2D cluster state.

Note that the reverse of this observation is not necessarily true. One can imagine families of graph states that are designed in such a way that they include a useful part (e.g. some form of 2D cluster state of restricted size), but in addition there are a large number of useless 'dummy'-particles. If for a fixed number of qubits N the number of dummy-particles is

exponentially larger than the useful part of size n, then one will always have an exponential overhead in spatial resources, e.g. to prepare a n-qubit cluster state.

Nevertheless, if we restrict ourselves to efficient universal graph state resources, one finds that all such resources are equivalent, as they can be obtained from each other with polynomial spatial and temporal overhead.

Observation 5. *All efficient universal graph state resources can efficiently be obtained from each other by means of LOCC.*

This property follows from the fact that all graph states can be prepared efficiently in the circuit model.

5. Criteria for universality and no-go results

In this section, we formulate several requirements which every universal resource must meet. These necessary conditions are all formulated in terms of entanglement—as measured by certain appropriate entanglement measures—which needs to be present in every universal resource, hence emphasizing the role of entanglement as a resource for MQC.

In section 5.1, we give an outline of the general strategy which will be used to formulate criteria for universality. After this, in sections 5.2 through 5.5, we apply this approach. We formulate several necessary conditions for universality, and give numerous examples of resources which do not comply with these criteria, and which hence cannot be universal.

5.1. Type II entanglement monotones

In this section, the general strategy to obtain necessary conditions for universality is outlined. We emphasize that, at this point, we are only concerned with universality, and not with efficient universality. The additional aspect of efficiency will be treated in section 6.

First we need some definitions and notation. Let $E(|\psi\rangle)$ be a functional defined for all n-qubit states $|\psi\rangle$, for all natural numbers n. We denote by E^* the supremal value of E, when the supremum is taken over all possible n-qubit states, for all n (the case $E^* = \infty$ is allowed):

$$E^* := \sup_{\text{all } |\psi\rangle} E(|\psi\rangle). \tag{8}$$

Furthermore, letting $\Psi = \{|\psi_1\rangle, |\psi_2\rangle, \ldots\}$ be an arbitrary resource, we define $E(\Psi)$ to be the supremal value of E, when the supremum is taken over all states in the resource Ψ, i.e.

$$E(\Psi) := \sup_{|\psi_i\rangle \in \Psi} E(|\psi_i\rangle). \tag{9}$$

We are now interested in functionals E satisfying the following property:

(P1)$E(|\psi\rangle) \geqslant E(|\psi'\rangle)$ whenever $|\psi\rangle \geqslant_{\text{LOCC}} |\psi'\rangle$, for every N-qubit state $|\psi\rangle$ and n-qubit state $|\psi'\rangle$, and for every N, n with $N \geqslant n$.

Property (P1) states that E is a measure which is non-increasing under *deterministic* LOCC interconversion between (pure) quantum states. Measures satisfying this property are similar to entanglement monotones [39, 40], which are defined to be non-increasing *on average* under LOCC. A functional satisfying property (P1) will henceforth be called a *type II entanglement*

monotone in order to distinguish it from the standard notion of an entanglement monotone; the latter will be called a type I monotone. We refer the reader to the end of this section for a more thorough discussion concerning type I and type II monotones.

We can now formulate the following simple result, which will be central to our analysis.

Theorem 1. *Let Ψ be universal resource and let E be a type II entanglement monotone. Then $E(\Psi) = E^*$.*

Proof. As $\Psi = \{|\psi_1\rangle, |\psi_2\rangle, \ldots\}$ is universal resource, there exists, for every multi-qubit state $|\phi\rangle$, a state $|\psi_i\rangle \in \Psi$ (dependent on $|\phi\rangle$) such that $|\psi_i\rangle \geqslant_{\text{LOCC}} |\phi\rangle$. This implies that $E(|\psi_i\rangle) \geqslant E(|\phi\rangle)$), since E is a type II monotone. This immediately implies that

$$E(\Psi) \geqslant \sup_{|\phi\rangle} E(|\phi\rangle) = E^*. \tag{10}$$

Using the definition of E^* as a supremum then implies that $E(\Psi) = E^*$, yielding the desired result. □

As an immediate corollary to theorem 1 and the universality of the 2D cluster states, we find the following.

Corollary 1. *Let E be a type II monotone and let Ψ_{2D} be the family of 2D cluster states. Then $E(\Psi_{2D}) = E^*$.*

Theorem 1 states that all universal resources—such as e.g. the family of 2D cluster states—are *maximally entangled*, in the sense that every type II monotone E has to reach its supremum on every universal resource. Note that this implies that all universal resources have many entanglement features in common, namely all features quantified by type II monotones. In order to investigate the entanglement present in general universal resources, it therefore suffices to single out one such resource—say, the family of 2D cluster states—and study its entanglement features as measured by the functionals E. In this sense, the entanglement present in the 2D cluster states is representative for the entanglement present in all universal resources. We emphasize that the 2D cluster states *a priori* do *not* play a distinguished role in this context, as they can be replaced by any other universal resource. However, they usually form an appropriate test-bed, as many of their properties have already been established (see e.g. [23]), and since the fact that these states are graph states often allows one to use powerful tools from the stabilizer formalism [32] to investigate their properties.

Evidently, in order to show that a given family of states is *not* universal, it suffices to find a suitable measure E such that theorem 1 is violated.

Corollary 2. *Let Ψ be a resource, and suppose that there exists a type II monotone E, such that $E(\Psi) < E^*$. Then Ψ cannot be a universal resource.*

This corollary captures the main strategy which will be adopted in the following in order to obtain necessary conditions for universality. To arrive at a criterion, one simply has to specify a functional E, prove that it is a type II monotone, and finally compute its supremum E^*. Note that, in order to compute E^*, it suffices to compute the supremal value of E on the 2D cluster states, or any other universal resource. This is sometimes (but not always) more convenient than considering the definition of E^* as a supremum over all states, as we will see below.

Note that the definition of a type II monotone is related to, but slightly different from, the definition of a (type I) entanglement monotone as introduced in [39]. A (type I) entanglement monotone M is a functional defined on the set of n-qubit states such that M decreases *on average* under LOCC (where usually LOCC between states of the same system size are considered). That is, if an LOCC protocol is executed on an n-qubit input state $|\psi\rangle$, leading to n-qubit output states $\{|\psi_i\rangle\}$ in the different branches of the protocol, with probabilities $\{p_i\}$, then a monotone M by definition satisfies

$$M(|\psi\rangle) \geqslant \sum_i p_i M(|\psi_i\rangle). \tag{11}$$

This is slightly different from the requirement (P1) for two reasons. Firstly, in (P1) deterministic LOCC conversions between two states $|\psi\rangle$ and $|\psi'\rangle$ are considered, rather than protocols with different output states occurring with certain probabilities—hence, in (P1) there is no averaging as in (11). Secondly, in (P1) states of possibly different system sizes (N and n) are compared.

Despite of these differences, it is clear that there exists a large overlap between type I and type II monotones. In particular, note that, for every n-qubit type I monotone M, one has $M(|\psi\rangle) \geqslant M(|\psi'\rangle)$ for any pair of n-qubit states such that $|\psi\rangle$ can deterministically be transformed into $|\psi'\rangle$ by means of LOCC (note again that here states of the *same* system size are considered). Therefore, it comes as no surprise that several type I monotones are also type II monotones. The following result is easily verified.

Theorem 2. *Let $E(|\psi\rangle)$ be a functional defined for all n-qubit states $|\psi\rangle$, for all natural numbers n. Suppose that the following statements hold:*

(i) E is a type I entanglement monotone—i.e. E is non-increasing on average under LOCC, when states of the same system size are considered;

(ii) $E(|\psi\rangle|0\rangle) = E(|\psi\rangle)$ for every multi-qubit state $|\psi\rangle$—i.e. E is invariant under the addition of an uncorrelated one-qubit state (constituting an extra party).

Then E is a type II monotone.

Thus, all type I entanglement monotones which are invariant under the adding of uncorrelated single-qubit states, are also type II monotones, and thus are suitable measures to obtain necessary conditions for universality. We will encounter examples of this below.

On the other hand, we emphasize that several type I entanglement monotones do not meet requirement (ii) in theorem 2, and are therefore not useful to obtain necessary conditions for universality. Examples of such measures can straightforwardly be obtained as follows. Consider any type I monotone $\bar{E}$ which is defined by *averaging* a bipartite monotone E over all bipartitions of the system. It is clear that $\bar{E}$ then does not satisfy (ii), as appending one-qubit parties which are disentangled from the rest of the system will decrease the average entanglement. Therefore, the class of such 'averaging' type I monotones $\bar{E}$ do not give rise to suitable necessary conditions for exact deterministic universality. Other examples can easily be given.

Finally, we note that there exist type II entanglement monotones which are not type I monotones. We refer to e.g. the next section, where it is shown that the entropic entanglement width is a type II but not a type I monotone.

In the following sections (i.e. sections 5.2–5.5), we will follow the approach formulated after corollary 2 by applying it to several measures E. We will in particular consider the *entanglement*

width measures, several measures related to *localizable entanglement*, the *geometric measure* of entanglement and the *Schmidt measure*. Necessary conditions for universality will be obtained by showing that these measures are all type II monotones. Moreover, we will encounter examples of resources Ψ which violate at least one of the resulting criteria, such that these resources cannot be universal.

5.2. Entanglement width

In this section, we discuss two measures, introduced and investigated in [26, 27], namely the *entropic entanglement width* and the *Schmidt-rank width*. We will show that these measures are type II monotones, and hence give rise to criteria for universality. We will subsequently use these criteria to obtain several examples of non-universal resources.

5.2.1. Definitions. The entropic entanglement width $E_{\mathrm{wd}}(|\psi\rangle)$ of an multi-party state $|\psi\rangle$ is an entanglement measure introduced in [27]. This measure computes the minimal bipartite entanglement entropy in the state $|\psi\rangle$, where the minimum is taken over specific classes of bipartitions of the system. The precise definition is the following.

Let $|\psi\rangle$ be an N-qubit pure state. A *tree* is a graph with no cycles. Let T be a *subcubic* tree, which is a tree such that every vertex has exactly 1 or 3 incident edges. The vertices which are incident with exactly one edge are called the *leaves* of the tree. We consider trees T with exactly N leaves $V := \{1, \ldots, N\}$, which are identified with the N qubits of the system. Letting $e = \{i, j\}$ be an arbitrary edge of T, we denote by $T \setminus e$ the graph obtained by deleting the edge e from T. The graph $T \setminus e$ then consists of exactly two connected components (see figure 1), which naturally induce a bipartition (A_T^e, B_T^e) of the set of qubits V. We denote the bipartite entanglement entropy of $|\psi\rangle$ with respect to the bipartition (A_T^e, B_T^e) by $E_{A_T^e, B_T^e}(|\psi\rangle)$, where $E_{A,B}(|\psi\rangle) = -\mathrm{Tr}(\rho_A \log_2 \rho_A)$ with $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. The *entropic entanglement width* of the state $|\psi\rangle$ is now defined by

$$E_{\mathrm{wd}}(|\psi\rangle) := \min_T \max_{e \in T} E_{A_T^e, B_T^e}(|\psi\rangle), \tag{12}$$

where the minimization is taken over all subcubic trees T with N leaves, which are identified with the N parties in the system. Thus, for a given tree T we consider the maximum, over all edges in T, of the quantity $E_{A_T^e, B_T^e}(|\psi\rangle)$; then the minimum, over all subcubic trees T, of such maxima is computed.

Similarly, one can use the Schmidt rank, i.e. the number of nonzero Schmidt coefficients, instead of the bipartite entropy of entanglement as a basic measure. One then obtains the *Schmidt-rank width*, or *χ-width*, denoted by $\chi_{\mathrm{wd}}(|\psi\rangle)$ [26]. The precise definition is the following. Let $\chi_{A_T^e, B_T^e}(|\psi\rangle)$ denote the number of nonzero Schmidt coefficients of $|\psi\rangle$ with respect to a bipartition (A_T^e, B_T^e) of V as defined above i.e. $\chi_{A,B}(|\psi\rangle) = \mathrm{rank}(\rho_A)$. The χ-width of the state $|\psi\rangle$ is defined by

$$\chi_{\mathrm{wd}}(|\psi\rangle) := \min_T \max_{e \in T} \log_2 \chi_{A_T^e, B_T^e}(|\psi\rangle). \tag{13}$$
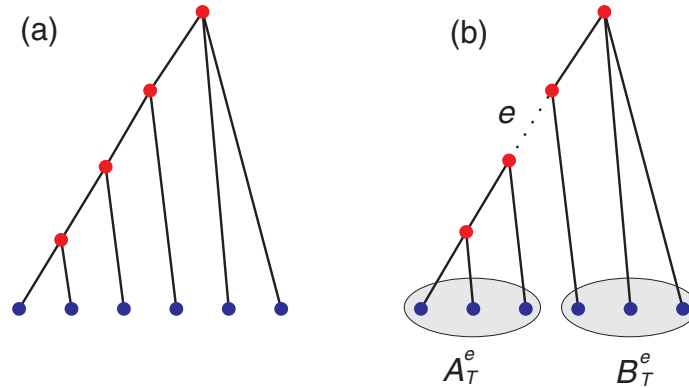
Figure 1. (a) Example of a subcubic tree T with six leaves (indicated in blue). (b) Tree $T \setminus e$ obtained by removing edge e and induced bipartition (A_T^e, B_T^e).

Note that, since the inequality

$$\log_2 \chi_{A,B}(|\psi\rangle) \geqslant E_{A,B}(|\psi\rangle) \tag{14}$$

holds for any bipartition (A, B) of the system and for any state $|\psi\rangle$, we have

$$\chi_{\mathrm{wd}}(|\psi\rangle) \geqslant E_{\mathrm{wd}}(|\psi\rangle). \tag{15}$$

The entanglement width measures are extensively studied in [26, 27], to which we refer the interested reader for more details. In particular, it was shown that the Schmidt-rank width can be given a natural interpretation, as this measure quantifies the optimal description of a state in terms of a tree tensor network.

5.2.2. Formulation of the universality criterion. Next we prove that E_{wd} and χ_{wd} are type II monotones. First we focus on the entropic entanglement width.

Theorem 3. *The entropic entanglement width $E_{wd}(|\psi\rangle)$ is a type II monotone.*

Proof. Let $|\phi\rangle$ and $|\phi'\rangle$ be two n-qubit states, such that $|\phi\rangle$ is (deterministically) convertible by LOCC into $|\phi'\rangle$. Let T_0 be a subcubic tree such that

$$\max_{e \in T_0} E_{A_{T_0}^e, B_{T_0}^e}(|\phi\rangle) = E_{\mathrm{wd}}(|\phi\rangle). \tag{16}$$

Moreover, let e_0 be an edge of T_0 such that

$$E_{A_{T_0}^{e_0}, B_{T_0}^{e_0}}(|\phi'\rangle) = \max_{e \in T_0} E_{A_{T_0}^e, B_{T_0}^e}(|\phi'\rangle). \tag{17}$$

We then have:

$$E_{\mathrm{wd}}(|\phi\rangle) = \max_{e \in T_0} E_{A_{T_0}^e, B_{T_0}^e}(|\phi\rangle),$$
$$\geqslant E_{A_{T_0}^{e_0}, B_{T_0}^{e_0}}(|\phi\rangle), \tag{18}$$

$$\geqslant E_{A_{T_0}^{e_0}, B_{T_0}^{e_0}}(|\phi'\rangle), \tag{19}$$

$$= \max_{e \in T_0} E_{A_{T_0}^e, B_{T_0}^e}(|\phi'\rangle), \tag{20}$$

$$\geqslant E_{\text{wd}}(|\phi'\rangle). \tag{21}$$

Further, suppose that $|\psi\rangle$ and $|\psi'\rangle$ are N-qubit and n-qubit states, respectively, such that $|\psi\rangle \geqslant_{\text{LOCC}} |\psi'\rangle$. Then the above implies that

$$E_{\text{wd}}(|\psi\rangle) \geqslant E_{\text{wd}}(|\psi'\rangle|0\rangle^{N-n}). \tag{22}$$

The result is obtained if $E_{\text{wd}}(|\psi\rangle|0\rangle) = E_{\text{wd}}(|\psi\rangle)$ for all states $|\psi\rangle$. This is essentially implied by the following property. Suppose that $|\psi\rangle$ is an N-qubit state defined on a set of qubits $V := \{1, \ldots, N\}$, and suppose that $|\psi\rangle|0\rangle$ is defined on the set $V' := \{1, \ldots, N, N+1\} = V \cup \{N+1\}$. Letting (A, B) be an arbitrary bipartition of V and writing $A' := A \cup \{N+1\}$, we have $E_{A,B}(|\psi\rangle) = E_{A',B}(|\psi\rangle|0\rangle)$. This property can straightforwardly be used to show that the entropic entanglement width is the same for the states $|\psi\rangle$ and $|\psi\rangle|0\rangle$. $\qquad\square$

Notice, however, that the entropic entanglement width is *not a type I entanglement monotone*. Despite the fact that (P1) is satisfied, this measure can increase on average under LOCC. This is most easily verified by considering the example of a three-qubit W state [41], from which maximally entangled pairs shared between random pairs of parties can be generated with probability arbitrarily close to one [42]. While the entropic entanglement width of the W state is smaller than one, the entanglement width of the output Bell pairs is equal to one.

An argument similar to the proof of theorem 3 can be used to prove that the Schmidt-rank width also satisfies (P1), i.e. this measure is a type II monotone. In fact, as is e.g. shown in [43], the Schmidt rank is non-increasing under stochastic LOCC (SLOCC). It follows that in contrast to the entropic entanglement width, the Schmidt rank width is a type I entanglement monotone, and even satisfies a stronger condition.

Theorem 4. *Consider and N-qubit state $|\psi\rangle$ and an n-qubit state $|\psi'\rangle$ with $N \geqslant n$, such that $|\psi\rangle$ can be transformed into $|\psi'\rangle|0\rangle^{N-n}$ by SLOCC with some nonzero probability. Then $\chi_{\text{wd}}(|\psi\rangle) \geqslant \chi_{\text{wd}}(|\psi'\rangle)$. As a corollary, the Schmidt-rank width is a type I and type II monotone.*

In order to formulate the criteria for universality associated to the entanglement width measures, we now compute the supremal values of these measures. We will prove that both of these suprema are unbounded, i.e. $E_{\text{wd}}^* = \chi_{\text{wd}}^* = \infty$. To obtain these results, it will suffice to show that the entropic entanglement width of the 2D cluster states is unbounded[8]. Notice that the infinity of E_{wd} on the 2D cluster states implies the infinity of E_{wd}^*. Moreover, the latter implies infinity of χ_{wd}^* via equation (15).

In order to prove that 2D cluster states have an unbounded entropic entanglement width, we need to evaluate this measure on graph states. Here we use a result established in [26, 27],

---

[8] In fact, any randomly chosen state has the property that the entropy of any reduced density operator is almost maximal (see [44]), and hence also the entropic entanglement width is unbounded.

stating that the entropic entanglement width of a graph state is equal to the *rank width* of the underlying graph. The rank width is a graph invariant defined in [45]. One then uses the property that the rank width of the $(2l + 1) \times (2l + 1)$ grid graph is lower bounded by $l - 1$ ([46] see also [45]), showing that this measure is indeed unbounded in the limit of infinitely many qubits. This shows that $E^*_{\mathrm{wd}} = \chi^*_{\mathrm{wd}} = \infty$.

Combining the above argument with theorems, we arrive at the following criterion for universality.

Theorem 5. *Let Ψ be a universal resource. Then $E_{\mathrm{wd}}(\Psi) = \chi_{\mathrm{wd}}(\Psi) = \infty$. Hence, any resource with a bounded E_{wd} or χ_{wd} cannot be universal.*

Although the definitions of the entanglement width measures involve highly nontrivial combinatorial optimization problems, these measures can efficiently be evaluated (or approximated) on several families of states—and hence the corresponding criteria for universality can be employed. In particular, the entanglement width criteria prove to be very powerful to investigate the universality of graph state resources. This is illustrated in the following example.

Example. It was shown in [26, 27] that both the entropic entanglement width and the Schmidt-rank width of an arbitrary graph state coincide with the rank width of the underlying graph. Together with theorem 5, this implies that every graph state resource where the rank width of the underlying graphs is *bounded*, cannot be a universal resource. This criterion leads to many examples of graph state resources which are not universal, as several examples of families of graphs are known where the rank width measure is bounded—in fact, efficient algorithms exist to compute (or approximate) the rank width of any graph [45]. Examples of graphs of bounded rank width, giving rise to non-universal resources, have been given in previous work, see [26, 27]. These examples include

1. tree graphs,
2. cycle graphs,
3. co-graphs,
4. graphs locally equivalent to trees,
5. distance-hereditary graphs,
6. graphs of bounded tree width,
7. graphs of bounded clique width,
8. ...

We refer to the graph theory literature for definitions. Note that two interesting examples of non-universal resources are the linear cluster states (which are instances of tree graphs) and the GHZ states (corresponding to complete graphs), or any family of $k \times l$ lattices where k is constant (and l grows with the system size).

A second application of theorem 5 is obtained by considering ground states of strongly correlated spin systems associated to a 1D geometry.

Example. Consider ground states of strongly correlated spin systems with nearest-neighbour interaction associated to a 1D geometry. When such systems are in the *non-critical* phase, one

typically finds that the bipartite entropy of entanglement between a subchain of spins and the rest of the chain, is bounded from above by a constant. See e.g. [47]. For all ground states where this property holds, one can easily show that the entropic entanglement width is bounded. To do so, let $|\psi_N\rangle$ be such a ground state of a system of N particles, and consider the subcubic tree T depicted in figure 1, where the leaves 1 to N correspond to the natural linear ordering of the system. As all bipartitions (A_T^e, B_T^e) are such that some connected subchain of particles $\{a, a+1, \ldots, a+k\}$ is separated from the rest of the system, one finds that the quantity

$$\max_{e \in T} E_{A_T^e, B_T^e}(|\psi\rangle) \tag{23}$$

is bounded from above by a constant (independent of N). As (23) is by definition an upper bound to the entropic entanglement width, one finds that this measure is bounded on the resource $\Psi := \{|\psi_N\rangle\}_N$. This implies that Ψ cannot be universal. We have therefore found that any resource of ground states of (non-critical) 1D spin systems where the block-wise entanglement entropy is bounded, cannot be a universal resource.

Below (see section 6) we will see that a similar result typically holds for ground states of *critical* 1D systems, and we will prove that such ground states cannot be *efficient* universal resources.

5.3. Localizable entanglement

Next we discuss a second class of measures which gives rise to criteria for universality. These measures will be centred around the possibility or impossibility of preparing Bell states by performing LOCC on resource states.

Consider the following simple measure E_{Bell}: for an arbitrary N-qubit state $|\psi\rangle$, define $E_{\text{Bell}}(|\psi\rangle) := 1$ if

$$|\psi\rangle \geqslant_{\text{LOCC}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{24}$$

i.e. if it is possible to deterministically create a Bell pair between a predefined pair of qubits in the system, and $E_{\text{Bell}}(|\psi\rangle) := 0$ if this is not possible. Clearly, one has $E_{\text{Bell}}^* = 1$, and E_{Bell} is a type II monotone. Therefore, every universal resource Ψ must satisfy $E_{\text{Bell}}(\Psi) = 1$. This is nothing but stating that a universal resource—i.e. a resource capable of preparing *arbitrary* states—must be able to prepare Bell states, which is a trivial observation. Nevertheless, this simple criterion allows one to conclude that many resources are not universal. For instance, one can consider the following example.

Example. The family of W states $\{|W_N\rangle\}_N$ is not universal, as it has been shown that Bell state cannot be prepared deterministically by performing LOCC on W states [42]. Here we have used the definition

$$|W_N\rangle := \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |e_{N,i}\rangle, \tag{25}$$

where $|e_{N,i}\rangle$ is defined to be the N-qubit computational basis state with a $|1\rangle$-state on the ith position in the tensor product, and $|0\rangle$ everywhere else (for example $|e_{3,1}\rangle = |100\rangle$, $|e_{3,2}\rangle = |010\rangle$, ...).

Using this idea, a slightly more involved but substantially more powerful criterion can be obtained as follows. Let $|\psi\rangle$ be a state on N qubits $V := \{1, \ldots, N\}$ and let α and β be two qubits in the system. Define

$$E_{\text{Bell}}^{\alpha,\beta}(|\psi\rangle) := 1, \tag{26}$$

if it is possible to deterministically create a Bell pair on the qubits α and β by performing LOCC on $|\psi\rangle$, and this measure is zero otherwise. Then define the measure $\mathcal{N}_{\text{LE}}(|\psi\rangle)$ to be the maximal size $|A|$ of a subset of qubits $A \subseteq V$ such that $E_{\text{Bell}}^{\alpha,\beta}(|\psi\rangle) = 1$ for all α and β in A where $\alpha \neq \beta$. Thus, $\mathcal{N}_{\text{LE}}(|\psi\rangle)$ is the largest size of a subset of qubits, such that a Bell state can be created deterministically between any two qubits in this subset, by performing LOCC on $|\psi\rangle$.

It is again clear from the definition that the measure $\mathcal{N}_{\text{LE}}$ is a type II monotone. To compute the supremum $\mathcal{N}_{\text{LE}}^*$, we again consider the 2D cluster states. It is well known that when a system of qubits is in a 2D cluster state, then a Bell pair can be created between any pair of qubits by LOCC [14, 23]. Therefore, $\mathcal{N}_{\text{LE}}(|C_{d \times d}\rangle) = d^2$, which shows that $\mathcal{N}_{\text{LE}}^* = \infty$. This leads to the following result.

Theorem 6. *Let Ψ be a universal resource. Then $\mathcal{N}_{LE}(\Psi) = \infty$.*

In order to obtain examples of no-go results, we again turn to ground states of strongly correlated spin systems.

Example. In the context of spin systems, the entanglement measure *localizable entanglement*, introduced in [48], is often considered. This measure, which will be connected to $\mathcal{N}_{\text{LE}}$, is defined as follows. Let $|\psi\rangle$ be an N-qubit state, and let α and β denote two arbitrary qubits in the system. The localizable entanglement between these qubits, denoted by $L^{\alpha\beta}(|\psi\rangle)$, is defined to be maximal entanglement (measured by the concurrence) of the subsystem of qubits $\{\alpha, \beta\}$, which can be created *on average* by performing LOCC on the other qubits in the system. This quantity is an entanglement monotone for $2 \times 2 \times l$ systems [49] and also fulfils property (P1). Note that $L^{\alpha\beta}$ is maximal (i.e. equal to one) if and only if a Bell pair can deterministically be created between the qubits α and β by LOCC—in other words, $L^{\alpha\beta}(|\psi\rangle) = 1$ if and only if $E_{\text{Bell}}^{\alpha,\beta}(|\psi\rangle) = 1$. In ground states of strongly correlated spin systems which are organized according to some geometry (such as a d-dimensional lattice), $L^{\alpha\beta}$ is typically a decreasing function of the distance between the spins α and β [48, 50]. Note that, whenever such a decay law of the localizable entanglement exists, the measure $\mathcal{N}_{\text{LE}}$ must be bounded. This implies that, if the ground state of a spin system exhibits a decay of the localizable entanglement with the distance between spins, then this resource cannot be universal.

Remark 15. *Extension to approximate quasi-deterministic universality.* We note that, contrary to the results obtained for the entanglement width measures, one cannot extend theorem 6 to the case of approximate and/or quasi-deterministic universality (see our upcoming work [36]). Hence, it will be restricted to the case of exact deterministic universality as studied in the present paper.

Remark 16. *Fixed versus random output particles.* Notice that the above arguments are based on the assumption (as already discussed earlier) that the output particles belong to a fixed set A in all branches of the LOCC protocol. If one is allowed to generate the desired output state between *some*, not previously specified, subset of qubits, which might be different for different output branches, the situation changes. As shown in [42], in this case maximally entangled pairs

can be created from the W state quasi-deterministically and one finds that the above criteria can no longer be applied. This is true for any 'local' measure (such as the localizable entanglement), while 'global' measures (e.g. entropic entanglement width, Schmidt rank width, Schmidt number, geometric measure of entanglement) can still be used.

5.4. Geometric measure of entanglement

As a third measure we consider the *geometric measure* of entanglement E_g, a multipartite entanglement (type I) monotone introduced in [29], and show that also E_g can be used to obtain a criterion for universality. This measure is defined as follows. Let $|\psi\rangle$ be an N-qubit state, and let $\pi(|\psi\rangle)$ denote the maximal modulus squared of the overlap between $|\psi\rangle$ and a complete product state on N qubits,

$$\pi(|\psi\rangle) = \max_{|\varphi\rangle = |\varphi_1\rangle \otimes \ldots \otimes |\varphi_N\rangle} |\langle \psi | \varphi \rangle|^2. \tag{27}$$

Then the geometric measure is defined by

$$E_g(|\psi\rangle) := -\log_2 \pi(|\psi\rangle). \tag{28}$$

It was proven in [29] that E_g is a type I entanglement monotone. Moreover, this measure trivially satisfies property (ii) stated in theorem 2, i.e. one has $E_g(|\psi\rangle|0\rangle) = E_g(|\psi\rangle)$. Therefore, one finds that E_g is also a type II monotone. In order to compute the supremum E_g^*, we use that the geometric measure of the $d \times d$ cluster states grows as $O(d^2)$ [51], which implies that $E_g^* = \infty$. This leads to the following criterion.

Theorem 7. *Let Ψ be a universal resource. Then $E_g(\Psi) = \infty$.*

Thus, any resource with a bounded geometric measure, cannot be universal.

Example. The geometric measure of the N-qubit W state is equal to [30]

$$E_g(|W_N\rangle) = (N-1)\log_2 \frac{N}{N-1}, \tag{29}$$

which, for large N, tends to $(\ln 2)^{-1} \sim 1.44$. This shows that E_g is bounded for the W-states, such that these states cannot form a universal resource.

5.5. Schmidt measure

Finally, as a fourth measure we consider the Schmidt measure, a (type I) entanglement monotone introduced in [28]. The Schmidt measure $E_s(|\psi\rangle)$ of an N-qubit state $|\psi\rangle$ is defined as the logarithm to base two of the minimal number K of N-qubit complete product states $\{|\alpha_1\rangle, \ldots, |\alpha_K\rangle\}$, such that $|\psi\rangle$ can be written as a linear combination

$$|\psi\rangle = \sum_{i=1}^{K} a_i |\alpha_i\rangle, \tag{30}$$

for some complex coefficients a_i. As it can easily be shown that $E_s(|\psi\rangle|0\rangle) = E_s(|\psi\rangle)$ and as E_s is a genuine (type I) entanglement monotone, it follows that the Schmidt measure is a

type II monotone. Moreover, one has calculated the Schmidt measure of the 2D cluster states in [52], yielding $E_s(|C_{d \times d}\rangle) = O(d^2)$, which shows that $E_s^* = \infty$. We can therefore conclude the following.

Theorem 8. *Let Ψ be a universal resource. Then $E_s(\Psi) = \infty$.*

Example. Consider the GHZ states

$$|\psi_{\text{GHZ}}\rangle := \frac{1}{\sqrt{2}} \left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n} \right). \tag{31}$$

By definition, these states have a constant Schmidt measure (equal to $\log_2(2) = 1$), showing that also by this criterion (see also section 5.5) these states cannot yield universal resource.

6. Efficient universality and scaling of entanglement

In order to obtain criteria for universality, so far we have not considered *efficient* universality, as defined in section 3.3.2. Evidently, every efficient universal resource must also satisfy theorem 1, and, conversely, any resource which is identified by corollary 2 as not being a universal resource, *a fortiori* cannot be efficiently universal. However, when efficient universality is taken into account, the criterion in corollary 2 can considerably be strengthened, as we will show in this section.

6.1. General strategy

Our approach will be illustrated by the following example, where we focus on the entropic entanglement width. Consider an efficient universal resource

$$\Psi := \{|\psi_1\rangle, |\psi_2\rangle, \ldots\}, \tag{32}$$

where $|\psi_i\rangle$ is a state on N_i qubits, for every $i = 1, 2, \ldots$. For every $d \times d$ cluster state on $n = d^2$ qubits, there exists a state $|\psi_{f(n)}\rangle \in \Psi$ in the resource Ψ (where $f(n) \in \{1, 2, \ldots\}$), such that $|\psi_{f(n)}\rangle \geqslant_{\text{LOCC}} |C_{d \times d}\rangle$, thus showing that

$$E_{\text{wd}}(|\psi_{f(n)}\rangle) \geqslant E_{\text{wd}}(|C_{d \times d}\rangle) \geqslant O(\sqrt{n}). \tag{33}$$

In the last equality we have used that the rank width of the $(2l + 1) \times (2l + 1)$ grid graph is larger than $l - 1$, as proven by Oum [46]. This implies that the entropic entanglement width of the $d \times d$ cluster states scale (at least) as $O(d) = O(\sqrt{n})$. As Ψ is an efficient universal resource, the number of qubits $N_{f(n)}$ on which $|\psi_{f(n)}\rangle$ is defined, only grows polynomially with the size n of the 2D cluster states (see observation 3 in section 4.2). Thus, there exists a polynomial $p(n)$ such that $N_{f(n)} \leqslant p(n)$. Conversely, for large n (where we only consider the leading order, denoted by k, of the polynomial $p(n)$), one has $n \geqslant O((N_{f(n)})^{1/k})$, thus showing that

$$E_{\text{wd}}(|\psi_{f(n)}\rangle) \geqslant O((N_{f(n)})^{1/(2k)}). \tag{34}$$

We therefore find a necessary condition on the *scaling behaviour* of the entanglement measure E_{wd} on any efficient universal resource Ψ: equation (34) shows that $E_{\text{wd}}(|\psi_i\rangle)$ must grow as $O((N_i)^{1/(2k)})$ for some k, which is essentially equivalent to stating that this measure must grow

faster-than-logarithmically with the system size on Ψ. Hence, resources where the entropic entanglement width grows at most as the logarithm of the system size, cannot be efficient universal resources (in particular, resources with bounded entanglement width are covered by this result).

The argument of the above example can be repeated for all type II monotones E. In every case, *a necessary condition on the scaling behaviour of E for efficient universal resources is obtained*. More formally, one has the following.

Theorem 9. *Let $\Psi := \{|\psi_1\rangle, |\psi_2\rangle, \ldots\}$, be a resource, where $|\psi_i\rangle$ is a state on N_i qubits, for every i. Let E be a type II monotone, and let φ be a function such that, for every[9] 2D cluster state $|C_{d\times d}\rangle$ on $n = d^2$ qubits, one has*

$$E(|C_{d\times d}\rangle) \geqslant \varphi(n). \tag{35}$$

If $E(|\psi_i\rangle)$ scales as $\log \varphi(N_i)$, then Ψ cannot be an efficient universal resource.

This result should be regarded as a strengthening of theorem 1. We emphasize again that the 2D cluster states in principle do not play a distinguished role in theorem 9, in the sense that they can be replaced—without weakening or strengthening the result—by arbitrary efficient universal resources or, in fact, any family of states *which themselves also can efficiently be prepared*. However, as pointed out before, being graph states, the 2D cluster states usually form a suitable test-bed also in this case.

Specializing these considerations to entanglement width, localizable entanglement, geometric measure and Schmidt measure, one finds the following.

Theorem 10. *Let Ψ be a resource. If one of the measures E_{wd}, χ_{wd}, $\mathcal{N}_{LE}$, E_g or E_s scales at most logarithmically with the system size on Ψ, then Ψ cannot be an efficient universal resource.*

The proof of this result simply follows from the fact that all these measures scale as $O(n^{1/k})$, for some k, for the 2D cluster states on n qubits.

When considering entanglement width, the above criterion allows one to determine new examples of no-go results which were not detected by theorem 1.

Example. Consider, as at the end of section 5.5.2, a family of ground states $\{|\phi_N\rangle\}$ of a 1D spin system, where $|\phi_N\rangle$ is a state of N spins. Investigating now the *critical* phase, one typically has that the block entanglement entropy of a subchain of spins of length $L \leqslant N$ scales as $\log L$ [47]. Similar to the example in section 5.5.2, one then finds that the entanglement width of such a ground state can at most scale as the logarithm of the system size. This shows that *any resource of ground states of 1D (critical) spin systems where the block entanglement of a subchain scales as the logarithm of the length of the subchain, cannot be an efficient universal resource.* Thus, together with the example in section 5.2.2, we find that ground states of critical or non-critical 1D spin systems can typically not be efficient universal resources.

Another interesting no-go result is obtained using the Schmidt measure.

Example. One easily finds that the Schmidt measure can grow at most logarithmically with the system size for the W states (this immediately follows from the definition of these states). This implies that the W states cannot be efficient universal resources. In contrast to the argument

---

[9] Here, the words 'for every 2D cluster state' can be replaced by 'for infinitely many 2D cluster states' in order to yield a slightly stronger result.

based on localizable entanglement (see also section 5.3), the argument presented here is also valid when considering the possibility of random output particles. Note also that by considering the geometric measure, as in section 5.4, one can conclude that the W states do not form an (efficient) universal resource.

6.2. Efficient universality and classical simulation of MQC

It is instructive to point out a relation between efficient (exact deterministic) universality of a resource Ψ and the problem of efficiently (i.e. with polynomial overhead) classically simulating MQC on this resource. When a resource is identified as *not* being an efficient universal resource, one may wonder whether an efficient classical simulation of MQC on this resource becomes possible. Although one can of course not expect that such a result would hold in general, here we note that such a property is valid if one considers the criteria for efficient universality corresponding to the Schmidt-rank width and the Schmidt measure. In particular, in previous work [26] we showed that MQC can be simulated on every resource where the Schmidt-rank width grows only logarithmically with the system size. This shows that any resource which is ruled out by the Schmidt-rank width criterion in theorem 9 as an efficient universal resource, allows an efficient classical simulation of MQC.

A similar remark can be made regarding the Schmidt measure. Suppose that Ψ is a resource where the Schmidt measure grows at most logarithmically with the system size. Equivalently, every state in the family Ψ can be written as a linear combination of polynomially many (w.r.t. the number of qubits) complete product states. One then easily verifies that any LOCC on such states can be simulated with polynomial overhead by a classical computer. In particular, the expectation value of a local observable $O := O_1 \otimes \cdots \otimes O_n$ can be efficiently computed when an n-qubit system is in a state $|\psi\rangle$ with logarithmically scaling Schmidt rank: writing

$$|\psi\rangle = \sum_{i=1}^{K} a_i|\alpha_i\rangle, \tag{36}$$

where the $\{|\alpha_i\rangle\}$ are $K = \mathrm{poly}(n)$ complete product states, the expectation value

$$\langle\psi|O|\psi\rangle = \sum_{i,j=1}^{K} a_i\bar{a}_j\langle\alpha_i|O|\alpha_j\rangle, \tag{37}$$

can efficiently be computed, as every term $\langle\alpha_i|O|\alpha_j\rangle$ can be efficiently computed and as there are only $\mathrm{poly}(n)$ such terms in the above sum. Similarly, a state obtained after performing a local projection on $|\psi\rangle$ can efficiently be determined (note that such states can have a Schmidt measure of at most $\log_2 K$). One can therefore conclude that any resource which fails to pass the Schmidt measure criterion in theorem 9, even allows an efficient classical simulation of MQC.

Thus, it is interesting to find that in the issue of efficient universality, as well as in the context of efficient simulation of MQC, the *scaling* of entanglement with the system size plays an important role.

7. Examples of efficient universal resources

To provide examples of universal resource states, our strategy is to establish an equivalence, up to a polynomial overhead, among (efficient) universal resources. The proof of efficient universality of the 2D cluster states [5, 6] means an efficient capability to simulate any circuit model by LOCC and, in particular, to prepare any other resource state by LOCC. Thus, all we have to show for other resource states is that the opposite transformation is also efficiently possible.

Theorem 11. *The graph states corresponding to the 2D square, hexagonal, triangular and Kagome lattices are efficient universal resources for MQC.*

Proof. According to our strategy, a proof is given in the form of an explicit deterministic LOCC protocol which transforms such other candidate states into the 2D cluster state with a polynomial overhead in resources and operations (see figure 2).

As LOCC, we translationally apply σ_y and σ_z measurements, which are known to correspond to simple update rules of the graph, namely local complementation (inversion of the neighbourhood subgraph) and vertex deletion, respectively [23]. We will get a resulting graph state *deterministically* after applying local Clifford unitary corrections $u_{y,k}$ and $u_{z,k}$ on neighbouring qubits (with help of classical communication), such as

$$u_{y,k} = \sqrt{(-1)^k(-i\sigma_z)} = \frac{1}{\sqrt{2}}\left(\mathbf{1} - (-1)^k i\sigma_z\right), \quad u_{z,k} = \sigma_z^k,$$

which depend on the measurement outcomes $k = \{0, 1\}$.

Let us illustrate such graph transforms to prove the theorem. Our LOCC protocol transforms (a) hexagonal-lattice graph state into (d) the 2D cluster state via (b) the triangular-lattice and (c) the Kagome-lattice graph state sequentially. When we apply the σ_y measurements on vertices of the hexagonal lattice in figure 2(a), we will have a triangle around the measured qubits by the local complementation. The resulting graph turns out to be a triangular lattice (b). Next, we apply the σ_z measurements on vertices marked by $\diamond$, which simply deletes the measured qubits along with the attached edges. The graph now becomes a so-called Kagome lattice, which has degree 4 uniformly in a similar manner as the square lattice. The last step is a bit involved, but straightforward by applying σ_y and σ_z measurements according to the ordering of figure 2. Accordingly, we finally obtain a square lattice, i.e. a 2D cluster state. The total spatial overhead is eight in that a unit square on (d) is obtained from eight hexagons in (a). Since the overhead is constant, all resource states are efficient universal. $\qquad\square$

Note that, since these other resource states can be transformed into the 2D cluster state always by *adaptive local projective measurements* assisted with classical communication, and local (Clifford) operations, they are also universal in the sense of a conventional one-way quantum computation.

It is interesting to observe that the square lattice, together with the hexagonal and triangular lattices are the only possibilities to obtain a regular tiling of the 2D plane. Furthermore, the Kagome lattice is an example of a uniform semiregular 2D tiling with 2 basic tiles (the triangle and the hexagon). The hexagonal lattice has vertex degree 3, which leads to an increased robustness against local noise as compared to the 2D cluster state [53]. Since the 1D cluster state (with uniform vertex degree 2) has been proved not to be universal [27], the vertex degree 3 is minimal for universal resource on *uniform* lattice structures.
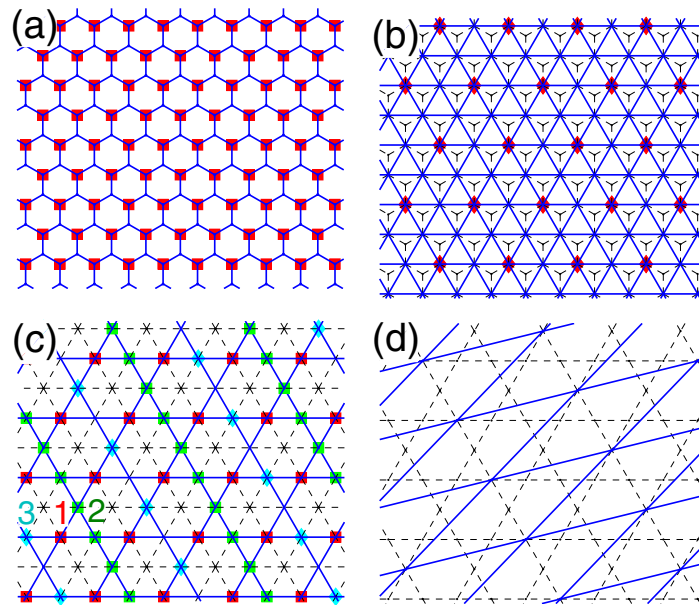
IOP Institute of Physics **Φ** DEUTSCHE PHYSIKALISCHE GESELLSCHAFT

Figure 2. Examples of efficient universal resource for MQC. These are graph states corresponding to (a) hexagonal, (b) triangular and (c) Kagome lattices. Deterministic LOCC transformation from (a) to (d) (2D cluster state) via (b) and (c) is indicated, where simple graph rules can be used sequentially (σ_y and σ_z measurements are displayed by □ and ◇, respectively). The spatial overhead for the transformation is constant.

We remark that other universal resource states have been presented [54] based on non-uniform lattice structures (see also [55]), where each gate in a universal set of unitary gates can be implemented by local measurements on an elementary unit and these units are combined (bottom-up approach). Here we took, in contrast, a top-down approach, where we prove universality by explicitly constructing LOCC protocols that yield the 2D cluster state.

Of course, we can simulate *directly* any circuit model on such new universal resources in practice, without transforming them into the 2D cluster state of the 2D square lattice. Let us illustrate this by a hexagonal lattice (due to its potential advantage for the local decoherence compared with a square lattice). In figure 3, we show a direct simulation of the circuit model on the 2D hexagonal lattice, after deleting uncoloured qubits by the σ_z measurements. We consider each snaking horizontal path running from the left to the right as a quantum wire which corresponds to an evolution of a logical single qubit in the circuit model.

Here we give an alternative proof of its efficient exact deterministic universality in a similar manner as the proof of the 2D cluster state [5, 6] (see also [54] for other resources). Namely, we take a bottom-up approach by showing two (sufficient) conditions are fulfilled for our family of resource states.

1. *Simulation of a universal set of elementary gates*: it is capable of implementing a set of universal gates on logical qubits with at most polynomial overhead.
2. *Composability*: the simulation (1) of elementary gates is composable between any neighbouring pair of logical qubits, as well as repeatable.
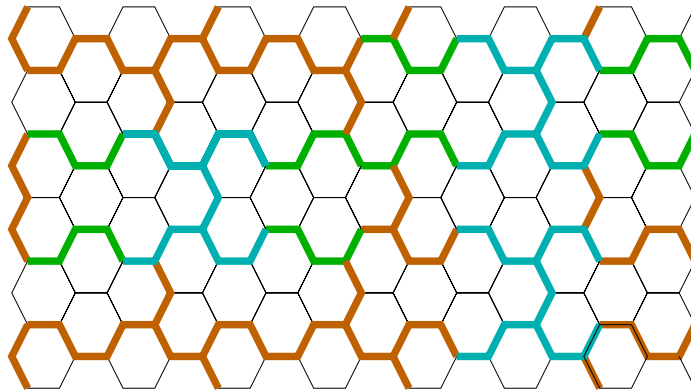
Figure 3. A direct simulation of the circuit model on the hexagonal lattice. After measuring uncoloured qubits in the σ_z direction, the resource state is capable of simulating a set of universal gates between any neighbouring two quantum wires (snaking horizontal paths) and to compose them into an arbitrary unitary operation. Here we illustrate an implementation (with the same measurement pattern of [5, 6]) of CNOT and of arbitrary $SU(2)$ rotation with the Euler decomposition by the 15-qubit 90° rotated H part (blue) and the five-qubit chain part (green), respectively.

Here we follow the implementation (measurement pattern) of [5, 6] of CNOT and of arbitrary $SU(2)$ rotation with the Euler decomposition in terms of the 15-qubit 90° rotated H part (blue) and the five-qubit chain part (green), respectively. The capability of implementing such gates as often as required follows immediately from its periodic structure. The length of an extra 1D path can be adjusted, if necessary, by the σ_y measurement.

A slightly more economical simulation can also be done by selecting the controlled-phase gate and the set $SU(2)$ of single-qubit rotations as a set of elementary gates for the circuit model. By measuring the middle qubit of the 'bridge between quantum wires' (i.e. the centre qubit in the blue part) in the σ_y direction, we can simply implement a logical 'remote' controlled-phase gate (cf [54]), without additional measurements along the quantum wires.

8. Encoded universality

So far we have restricted our attention to situations where the resource states consist of systems with fixed dimension d, and where the desired target states are multipartite states of d-dimensional systems. We have concentrated on $d = 2$, i.e. qubit systems, and have provided definitions and criteria when such a family of resource states is capable of producing any other quantum state of n qubits. In this section we will show how to extend our results in order to take higher-dimensional systems, generation of systems with different dimensions, and *encoded* quantum states into account. We will first specify what we mean by encoding, and then put forward a definition for encoded (CQ-)universality in MQC, based on different notions of *locality*. We will finally discuss the applicability of entanglement criteria developed in the previous sections, and discuss examples of encoded universal resources.

8.1. Encoded quantum states

We start with some general considerations on encoded quantum states.

8.1.1. Qubits and qudits. In the measurement-based model for quantum computation, a resource state constituting of N two-dimensional systems is processed by sequences of LOCC. It is clear that the physical systems remain the same throughout the procedure, and hence the resulting quantum state is also one consisting of qubits. It is *impossible* to generate a state of d-dimensional systems (qudits) from a qubit system. More generally, if the system constituting the resource state is k-dimensional, and the states to be generated consist of d-dimensional systems, then one cannot generate any such state whenever $k \neq d$. What is, however, possible, is to generate the desired state in an *encoded* form. In almost all conceivable cases, the generation of a quantum state in such an encoded form is sufficient.

The most natural kinds of encoding are the following.

1. If $k \geqslant d$, then ideally one encodes $m = \lfloor \log(k)/\log(d) \rfloor$ d-level systems into one k-level system.
2. If $k < d$, then ideally one uses $m = \lceil \log(d)/\log(k) \rceil$ k-level systems to encode one d-level system.

In neither of these two cases are additional levels used. One may also consider more complex encodings, e.g. any encoding that can be generated by a poly-sized quantum circuit. However, in this case quantum information corresponding to a d-level system may be distributed among *all* k-level systems. In the following, we will restrict ourselves to the kinds of encodings specified above, where a natural association with physical systems is maintained. This restriction allows us to use entanglement-based criteria for universality also for encoded systems.

8.1.2. General encodings. The treatment of systems of different dimensionality is not the only case where encodings are useful. Even if one is restricted to qubits, it is natural to consider the question of whether states can be generated in an encoded way. Encoded states appear naturally in e.g. quantum computation once error-correction is considered. In particular, any fault-tolerant implementation of quantum computation actually generates states in an encoded form, and performs unitary operations on the encoded states. In this case the (redundant) encoding serves to protect quantum information against the influence of errors. One may consider encodings also for different reasons. For instance, for certain physical set-ups it may be impossible (or very hard) to perform arbitrary single-qubit operations and two-qubit gates. However, for certain encodings the implementation of logical single- and two-qubit gates i.e. gates acting on the encoded or logical systems, is possible. Such a situation occurs for instance in charge-controlled quantum dots, where despite the difficulties in obtaining inhomogeneous single-spin rotations, processing of encoded quantum information is possible [56]–[58]. Finally—and this brings us back to the present study of universality—if one is ultimately interested in a CC computational scheme, it is often sufficient that a quantum computer is capable of generating states in an encoded form. In particular, we will see below that any encoded CQ-universal resource for MQC is also CC-universal.

For simplicity, in the following we will restrict ourselves to the case where $k = d = 2$. Generalization to $k \neq d \geqslant 2$ is, however, straightforward.

Next we define what is meant by 'encoded qubits' and 'encoded quantum states'. First we consider encodings of one-qubit systems and states.

Definition 3 (Encoded qubit). *An m-qubit encoding $\mathcal{E} := (\mathcal{H}, \{|\mathbf{0}\rangle, |\mathbf{1}\rangle\})$ of a one-qubit system is specified by:*

1. *a Hilbert space $\mathcal{H} \cong \mathbb{C}^{2^m}$, representing a system of m qubits, and*
2. *two (fixed) orthogonal states $|\psi_0\rangle, |\psi_1\rangle \in \mathcal{H}$. We use the shorthand notation $|\mathbf{0}\rangle := |\psi_0\rangle$ and $|\mathbf{1}\rangle := |\psi_1\rangle$.*

Let $|\phi\rangle = a|0\rangle + b|1\rangle$ be an arbitrary one-qubit state. The encoded version of $|\phi\rangle$ with respect to the encoding $\mathcal{E}$ is the state $|\boldsymbol{\phi}\rangle := a|\mathbf{0}\rangle + b|\mathbf{1}\rangle \in \mathcal{H}$.

This definition is now generalized to encompass encodings of many-qubit systems and states.

Definition 4 (Encoded qubit *n* qubit system). *An m-qubit encoding $\mathcal{E} := (\mathcal{H}^E, \mathcal{P}, \{|\mathbf{0}\rangle, |\mathbf{1}\rangle\})$ of an n-qubit system is specified by:*

1. *a Hilbert space $\mathcal{H}^E \cong \mathbb{C}^{2^{mn}}$, representing a system of $m \cdot n$ qubits labeled by a set $E = \{1, \ldots, m \cdot n\}$,*
2. *a partition $\mathcal{P} := \{A_1, \ldots, A_n\}$ of E, where every A_k denotes a set of m qubits of E, and*
3. *two (fixed) orthogonal m-qubit states $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$.*

Consider an n-qubit state

$$|\phi\rangle = \sum_{i_1, i_2, \ldots i_n \in \{0,1\}^n} c_{i_1 i_2 \ldots i_n} |i_1\rangle |i_2\rangle \ldots |i_n\rangle. \tag{38}$$

The encoded version of $|\phi\rangle$ w.r.t. the encoding $\mathcal{E}$ is the state

$$|\boldsymbol{\phi}\rangle = \sum_{i_1, i_2, \ldots i_n \in \{0,1\}^n} c_{i_1 i_2 \ldots i_n} |\boldsymbol{i_1}\rangle_{A_1} |\boldsymbol{i_2}\rangle_{A_2} \ldots |\boldsymbol{i_n}\rangle_{A_n} \in \mathcal{H}^E.$$

Here the subscripts A_k denote on which qubits the states $|\boldsymbol{i_k}\rangle$ are defined.

For notational simplicity, in the definition above we have considered the same encoding for every qubit. Generalization to different encodings for different qubits is straightforward.

Similarly, for $k \neq d \geqslant 2$ an encoded qudit can be defined by a set of d orthogonal states of m k-level systems, and the definition of an encoded state follows immediately. The case of generating d-level systems using k-level systems is also covered, where the encoding corresponds to (i) or (ii) specified in section 8.1.1.

8.2. Local operations on encoded systems

The notion of *locality* is central in MQC. In particular, entangled quantum states are processed by LOCC. This allows one to attribute entanglement as a resource to the initial state of the system, and only in this context criteria based on entanglement properties of resource states as presented in section 5 become meaningful. When considering systems with a fixed dimension e.g. qubits, as we did in the previous sections, the notion of locality is unique and simply corresponds to single-qubit operations. When considering encoded systems as we do here, one may, however, consider two different notions of locality, and the corresponding classes of 'local' operations assisted by classical communication.

 (i) Local with respect to physical systems constituting the resource state: LOCC.
 (ii) Local with respect to the encoded systems: **LOCC**.

It depends on the context at hand which of these two notions of locality is of interest. The first notion, associating locality to the physical systems constituting the quantum state, seems to be the most natural one. However, in some cases one might also naturally consider (ii), i.e. locality with respect to logical or encoded system. Notice that in the case of **LOCC**, joint operations on certain groups of physical qubits are allowed. Hence, if we consider LOCC in the definition for universality, we obtain a more stringent requirement as when using **LOCC**. Usage of **LOCC** will turn out to be useful when considering entanglement-based criteria for encoded universality.

8.3. Definition of encoded universality

In this section, we precisely define what is meant by an 'encoded universal resource for MQC'. In order to do so, we first need to specify the notion of a 'consistent family of encodings', which is the following. In the present study, the role of an infinitely large resource is played by a family of states $\Psi = \{|\psi_1\rangle, |\psi_2\rangle, \ldots\}$, where $|\psi_i\rangle$ is a state on N_i qubits and where $N_i \leqslant N_{i+1}$ for every i. More precisely, the state $|\psi_i\rangle$ belongs to a Hilbert space $\mathcal{H}^{E_i}$, where E_i denotes a set of N_i qubits, such that $E_i \subseteq E_{i+1}$, for every i. We will say that $\{\mathcal{H}^{E_1}, \mathcal{H}^{E_2}, \ldots\}$ is a *nested* family of Hilbert spaces. Now, suppose that, for every Hilbert space $\mathcal{H}^{E_i}$ an encoding $\mathcal{E}_i = \{\mathcal{H}^{E_i}, \mathcal{P}_i, \{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}\}$ is given. Since a resource Ψ plays the role of an infinitely large state, when considering encodings—together with the corresponding partitions of the systems $\mathcal{H}^{E_i}$ into logical qubits as specified by the encodings $\mathcal{E}_i$—it is natural to impose a certain degree of consistency of these encodings. In particular, we will require that the way in which the Hilbert space $\mathcal{H}^{E_i}$ is partitioned into logical qubits, should be consistent with the way in which $\mathcal{H}^{E_{i+1}}$ is partitioned, i.e. $\mathcal{P}_i \subseteq \mathcal{P}_{i+1}$ for every i. In such case, we will call $\mathcal{F} := \{\mathcal{E}_1, \mathcal{E}_2, \ldots\}$ a *consistent family of encodings*.

We are now in a position to give a definition of encoded universal resource for MQC.

Definition 5 (Encoded universality). *Consider a nested family of Hilbert spaces $\{\mathcal{H}^{E_i}\}_i$, and let $\Psi = \{|\psi_1\rangle, |\psi_2\rangle, \ldots\}$ be a family of states such that $|\psi_i\rangle \in \mathcal{H}^{E_i}$, for every i. Let $\mathcal{F} := \{\mathcal{E}_1, \mathcal{E}_2, \ldots\}$ be a consistent family of m-qubit encodings of this family of Hilbert spaces. The family Ψ is called an encoded universal resource for MQC with respect to $\mathcal{F}$, if for every n and for every n-qubit quantum state $|\phi_{\mathrm{out}}\rangle$, there exists a state $|\psi_i\rangle \in \Psi$ such that $|\psi_i\rangle \geqslant_{\mathrm{LOCC}} |\boldsymbol{\phi}_{\mathrm{out}}\rangle$, where $|\boldsymbol{\phi}_{\mathrm{out}}\rangle$ is the encoded version of $|\phi_{\mathrm{out}}\rangle$ w.r.t. the encoding $\mathcal{E}_i$.*

The family Ψ is said to be an encoded universal resource for MQC if there exist a consistent family of encodings with respect to which Ψ is universal.

IOP Institute of Physics Φ DEUTSCHE PHYSIKALISCHE GESELLSCHAFT

Remark 17. General comments regarding definition.

  (i) Any resource that is universal is also encoded universal, although the opposite is not necessarily true. We will discuss examples for such cases later in this section.
 (ii) Although we allow for an arbitrary one-qubit encoding, the encoding needs to be fixed, i.e. it needs to be the same for all output states.
(iii) As in the case of non-encoded universality, we also assume here that the output state is prepared on the same output particles in all branches of the LOCC protocol (an extension to random output particles is possible in the same way as in the non-encoded case).
 (iv) In the definition we refer to LOCC, i.e. operations on the individual physical systems (see (i) in the preceding section). One may also consider a weaker form of universality with respect to **LOCC**.
  (v) In the above definition, the same encoding is used for every qubit. This restriction can easily be lifted without changing the results to be presented in the following. We have adopted this version of the definition for notational convenience.
 (vi) In this paper, we do *not* consider general encodings by means of arbitrary poly-sized quantum circuits. This is a restriction in the sense that the latter leads to a more general definition of encoded universality (i.e. it is likely that there exist encoded universal resources w.r.t. such general codings which are not covered by the present theory). The reason for this is that it is not clear how criteria stated in terms of entanglement can be formulated for such general encodings, whereas this will be possible for the current definition. However, it is clear that general encodings by poly-sized quantum circuits deserve further attention.

We will sometimes consider a slightly weakened version of encoded universality, in the following sense. Let $\{|0\rangle, |1\rangle\}$ be an (m-qubit) encoding of a one-qubit system, let $|\phi\rangle$ be an encoded version of an n-qubit state $|\phi\rangle$ with respect to this encoding (see definition), and let $U = U_1 \otimes \ldots \otimes U_n$ be an n-qubit local operation, where

$$U_k := a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|, \tag{39}$$

(for every $k = 1, \ldots, n$). Then the encoded version $\boldsymbol{U} = \boldsymbol{U}_1 \otimes \cdots \otimes \boldsymbol{U}_n$ of this operator is defined by

$$\boldsymbol{U}_k := a|\boldsymbol{0}\rangle\langle \boldsymbol{0}| + b|\boldsymbol{0}\rangle\langle \boldsymbol{1}| + c|\boldsymbol{1}\rangle\langle \boldsymbol{0}| + d|\boldsymbol{1}\rangle\langle \boldsymbol{1}|, \tag{40}$$

and naturally acts as

$$\boldsymbol{U}|\boldsymbol{\phi}\rangle = \sum_{i_1,i_2,\ldots i_n=0}^{1} c_{i_1 i_2 \ldots i_n} \boldsymbol{U}_1 |\boldsymbol{i}_1\rangle_{A_1} \cdots \boldsymbol{U}_n |\boldsymbol{i}_n\rangle_{A_n}.$$

For example, given an encoding $\{|\boldsymbol{0}\rangle, |\boldsymbol{1}\rangle\}$ the logical single-system Pauli operations are defined by

$$\boldsymbol{\sigma}_z = |\boldsymbol{0}\rangle\langle \boldsymbol{0}| - |\boldsymbol{1}\rangle\langle \boldsymbol{1}|, \quad \boldsymbol{\sigma}_x = |\boldsymbol{0}\rangle\langle \boldsymbol{1}| + |\boldsymbol{1}\rangle\langle \boldsymbol{0}|, \quad \boldsymbol{\sigma}_y = -i|\boldsymbol{0}\rangle\langle \boldsymbol{1}| + i|\boldsymbol{1}\rangle\langle \boldsymbol{0}|. \tag{41}$$

Note that an operation which is local in the sense of logical qubits need not be local at the level of the physical qubits in the system, i.e. it may act jointly on several physical qubits.

We will sometimes consider resources which are encoded universal in the restricted sense that it is possible to prepare an encoded version of any state *up to logical local operations*. Notice that a resource which is universal in this (restricted) sense with respect to CQ is, however, fully CC-universal. That is, if we are only interested in obtaining classical outputs, such logical local operations do not play a role as we simply have to adapt the basis of the final measurements. We also note that the 2D cluster states are CQ-universal under projective local measurements up to Pauli operations; this property, together with the above restricted notion of encoded universality, will play a role in the next section.

8.4. Encoded universality and the 2D cluster states

In this section, it is our aim to relate encoded universal resources to (encoded versions of) the 'standard' universal resource, the family of 2D cluster states i.e. this section will contain a result analogous to observation in section 4. Although this result will be highly analogous to observation, its proof will not be as straightforward and will require some extra work. The result is the following.

Theorem 12. *A family of states Ψ is an encoded universal resource with respect to a specific encoding (more precisely: w.r.t. a consistent family of encodings) up to logical Pauli operators, if and only if encoded 2D cluster states $|C_{d \times d}\rangle$ of arbitrary size d with respect to the same encoding can be generated by means of LOCC, up to logical Pauli operations.*

A family of states Ψ is an encoded universal resource up to logical Pauli operators if and only if there exists an encoding (more precisely: a consistent family of encodings) such that encoded 2D cluster states $|C_{d \times d}\rangle$ of arbitrary d can be generated by means of LOCC, up to logical Pauli operations.

Proof. Necessity of the condition is obvious, as an encoded universal resource must be capable of producing an encoded version of any state, in particular an encoded 2D cluster state. Sufficiency of the condition is based on the fact that an encoded 2D cluster state is an encoded universal resource under LOCC up to logical Pauli operations for *any* encoding. The proof of the latter statement is postponed until theorem 16. □

Note that it is by no means trivial that local operations on physical qubits allow one to process encoded quantum information. For example as already indicated above, logical local operations need not act locally on the physical qubits, i.e. one may not be able to realize logical local operations as physical local operations. For example, consider a three-qubit encoding where $|\mathbf{0}\rangle := |000\rangle$ and $|\mathbf{1}\rangle := |W_3\rangle$, where the latter is the W state on three-qubits. It is clear that in this case a logical σ_x operation, i.e.

$$\boldsymbol{\sigma}_x := |000\rangle\langle W_3| + |W_3\rangle\langle 000| \tag{42}$$

acts non-locally on the physical qubits.

However, we will find that it is always possible to realize logical projective two-outcome measurements (which are the basic ingredient of the one-way 2D cluster state model) by physical local operations. We again refer to theorem 16.

8.5. Criteria for universality

We have discussed entanglement-based criteria for non-encoded universality in section 5 and 6. Here we discuss to which extent these criteria can be applied—either directly or in an adapted form—in the context of *encoded universality*[10].

8.5.1. Criteria at the level of encoded systems. The first observation is that one can use exactly the same criteria for universality when considering encoded universality, if one applies them at the level of encoded systems. This is expressed in the following.

Theorem 13. *Consider a fixed (consistent family of) encoding(s), which also implies a partition of the system. Any entanglement-based criterion for universality formulated for non-encoded systems using LOCC leads to a criterion for the encoded system by considering the corresponding entanglement measures where locality is defined with respect to the partition of the system, i.e. LOCC.*

The proof of this theorem is straightforward, as one can treat any logical qubit as a two-level system if **LOCC** are allowed.

Remark 18. *Entanglement with respect to partitions.* For a *fixed* encoding, one considers local operations with respect to this encoding, i.e. **LOCC**. Entanglement is defined relative to the partitions induced by the encoding. For instance, one says that $E_{\text{Bell}}(|\phi\rangle) = 1$ if an encoded entangled pair $(|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$ can be created between some pair of encoded systems. In the case of entanglement width measures, they are now defined with respect to the fixed partition. That is, entanglement between blocks of qubits is considered, where each block consists of several physical qubits specified by the encoding. Entanglement within each block is irrelevant and absorbed into the encoding. Notice that in this way one still obtains a set of powerful criteria to assess whether a given state is encoded universal with respect to a fixed encoding. In particular, *any* encoded universal resource still needs to have unbounded entanglement width (defined via **LOCC**).

Remark 19. *Simultaneous treatment of different encodings.* Notice that above criterion automatically provides a test for all encodings that lead to the same partition of the system, i.e. the same notion of **LOCC**, independent of the choice of the two-orthogonal states constituting the logical qubit. However, it would still be desirable to obtain a more general statement about non-universality with respect to *all* possible encodings. Although many encodings are treated simultaneously, one still needs to check for all possible partitions of the system and determine the corresponding measures, which is impractical.

In the following, we utilize entanglement-based criteria at the level of physical systems to infer statements about encoded universality. This turns out to be possible, although only under certain circumstances and for certain entanglement measures.

8.5.2. Schmidt measure and geometric measure. In this section, we will show that every encoded universal resource must have an unbounded Schmidt measure and geometric measure i.e. $E_s(\Psi) = \infty = E_g(\Psi)$ for every encoded universal resource Ψ.

---

[10]We remark that this terminology must not be confused with the notion of encoded universality used in [56].

We start by considering the geometric measure. Let $|\psi\rangle$ be a state defined on a set of qubits $S := \{1, \ldots, n\}$, and let $\mathcal{P} := \{A_1, \ldots, A_l\}$ be any partition of the set S into l subsets A_i. One can regard $|\psi\rangle$ as an l-party state, where every subset A_i is associated to a party. At this coarse-grained level one can also define the geometric measure $E_g^{\mathcal{P}}$ in a natural way, where now locality is defined with respect to these l parties. An important property is now that $E_g^{\mathcal{P}}(|\psi\rangle) \leqslant E_g(|\psi\rangle)$ for any partition $\mathcal{P}$, i.e. the geometric measure is *non-increasing under coarsening of the partition* [28].

This property will be crucial for proving that $E_g(\Psi) = \infty$ for every encoded universal resource Ψ. Let $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$ be an m-qubit encoding with respect to which Ψ is encoded universal, and let $|\phi\rangle = \sum c_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle$ be an arbitrary n-qubit state. By the encoded universality of Ψ, there exists a state $|\psi_i\rangle \in \Psi$ and an encoded version $|\boldsymbol{\phi}\rangle$ of $|\phi\rangle$ such that $|\psi_i\rangle \geqslant_{\text{LOCC}} |\boldsymbol{\phi}\rangle$. As E_g is a type II entanglement monotone, this implies that $E_g(|\psi_i\rangle) \geqslant E_g(|\boldsymbol{\phi}\rangle)$. Let $S := \{1, \ldots, m \cdot n\}$ be the set of qubits on which $|\boldsymbol{\phi}\rangle$ is defined, and $\mathcal{P}$ be the partition of S which is naturally associated with the encoded state. Using now the property that E_g is non-increasing under coarsening, one finds that $E_g(|\boldsymbol{\phi}\rangle) \geqslant E_g^{\mathcal{P}}(|\boldsymbol{\phi}\rangle)$. Now, let U be an m-qubit unitary operation such that

$$U|\mathbf{0}\rangle = |0\rangle^{\otimes m} \text{ and } U|\mathbf{1}\rangle = |1\rangle|0\rangle^{\otimes(m-1)}, \tag{43}$$

implying that $U^{\otimes n}|\boldsymbol{\phi}\rangle$ is equal to

$$\sum c_{i_1 \ldots i_n} \left\{ |i_1\rangle|0\rangle^{\otimes(m-1)} \right\} \ldots \left\{ |i_n\rangle|0\rangle^{\otimes(m-1)} \right\}. \tag{44}$$

This equation should be read in the sense that the state $|\phi\rangle$ is distributed over n single-qubit parties, where every party supplemented with an uncorrelated ancilla of $m-1$ qubits in the state $|0\rangle^{\otimes(m-1)}$. As such ancillas cannot change the value of any type I entanglement monotone [39], one finds that $E_g^{\mathcal{P}}(U^{\otimes n}|\boldsymbol{\phi}\rangle) = E_g(|\phi\rangle)$. Moreover, as $U^{\otimes n}$ is a local operation with respect to the partition $\mathcal{P}$, one has $E_g^{\mathcal{P}}(U^{\otimes n}|\boldsymbol{\phi}\rangle) = E_g^{\mathcal{P}}(|\boldsymbol{\phi}\rangle)$. This proves that $E_g(|\psi_i\rangle) \geqslant E_g(|\phi\rangle)$. As this result holds for arbitrary $|\phi\rangle$, we find that $E_g(\Psi) = \infty$, as desired.

Note that in the proof of the above result we have only used that (i) E_g is a type II entanglement monotone, (ii) E_g is a type I entanglement monotone, and (iii) E_g is non-increasing under coarsening. Therefore, the same arguments hold for the Schmidt measure E_s, and we can immediately formulate the following general result.

Theorem 14. *Let E be a measure which is a type I and type II entanglement monotone and which is non-increasing under coarsening. Then $E(\Psi) = E^*$ for every encoded universal resource Ψ. In particular, $E_s(\Psi) = E_g(\Psi) = \infty$ for every encoded universal resource.*

Note that the above result is general in that it is formulated independent of any specific encoding. It allows to rule out e.g. the W states as resources which are certainly not encoded universal (see also section 5.7).

8.5.3. Localizable entanglement.   We now turn to the criteria based on the ability of creating Bell pairs between qubits in the system. Recall that we have seen in section 5.3 that for any universal resource it must be possible to create a Bell state between some pair of qubits in the system (recall also that we consider fixed output particles, i.e. the same for all branches of the protocol). The results of [12] show that this criterion cannot be suitable to assess universality

of encoded resources (if one applies it at the level of physical qubits). Although [12] is only concerned with CC-universality, one can lift their results to the more general level of encoded CQ-universality, as we will see in this section.

The failure of the above measure is already evident when considering the following simple example based on the results of [12]. Suppose one has the encoding

$$|\mathbf{0}\rangle = |0\rangle^{\otimes m}, \quad |\mathbf{1}\rangle = |W_m\rangle, \tag{45}$$

where $|W_m\rangle$ is a W state of m qubits, for some fixed m. A state

$$|\phi\rangle = 1/\sqrt{2}(|\mathbf{0}\rangle|\mathbf{0}\rangle + |\mathbf{1}\rangle|\mathbf{1}\rangle) \tag{46}$$

is evidently maximally entangled at the encoded level, although at the level of the physical qubits only a certain (arbitrary small) amount of (entropic) entanglement is present. This can be seen by considering the reduced density operator of a single individual particle k, which is given by

$$\rho_k = \frac{2m - 1}{2m}|0\rangle\langle 0| + \frac{1}{2m}|1\rangle\langle 1|. \tag{47}$$

Clearly, the entropy of entanglement can go to zero as $m \to \infty$. The entanglement of assistance (and therefore also the localizable entanglement) between any pair of qubits is upper bounded by $S(\rho_k)$ [42], and hence also goes to zero for $m \to \infty$. However, maximal entanglement between *blocks of qubits*, i.e. at the encoded level, is naturally present.

As it was proven in [12] that the 2D cluster states encoded with respect to the encoding specified in equation (45) form a CC-universal resource (in fact, we will prove below that this resource is also encoded CQ-universal), one can conclude that measures related to the possibility of creating Bell pairs are *not* suitable to study encoded universality. In particular, such a resource is not CQ-universal, even though it is encoded CQ-universal.

8.5.4. Entanglement width. We now turn to the entanglement width measures. We will use the result of [26] to establish a criterion for encoded universality (at the level of physical qubits). The criterion will be stated independent of any encoding, as is the case with theorem 14.

As discussed earlier, in [26] it was shown that LOCC protocols on all (families of) states with at most logarithmically growing χ-width can be simulated efficiently on a classical computer. This implies that, for these resource states, measurement-based quantum computation on encoded qubits can be simulated efficiently on a classical computer for *any* choice of encoding. This result does, strictly speaking, not exclude the possibility that states with logarithmically bounded χ-width constitute a universal encoded resource, as it has to date not been proven that an efficient classical simulation of (CC-)universal quantum computation is impossible. However, under the assumption that one will not be able to efficiently simulate quantum computation, one can conclude the following from the theorem above.

Theorem 15. *Let Ψ be a family of states such that the χ-width grows at most logarithmically with the system size on the set Ψ. Then, under the assumption that (CC) quantum computation cannot be simulated efficiently by classical computers, the resource Ψ cannot be encoded universal.*

Remark 20. *Direct use of entanglement width.* So far we have not been able to directly prove (or disprove) that every encoded universal resource should have an unbounded entropic entanglement width and/or Schmidt-rank width. This is mainly due to the fact that these measures do not seem to exhibit a 'non-increasing under coarsening' property. In particular, it seems that these measures can (significantly) increase due to the use of encodings. Therefore, we leave this issue as an interesting open problem.

8.6. Encoded universal resources

In this section, we prove a general result on encoded universality up to logical local operations, which immediately provides a large number of encoded universal resources.

Theorem 16. *Let Ψ be a family of states that is a universal resource under local projective measurements, up to local unitary operations. Then, for any encoding $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$, the encoded version of the family, denoted by $\mathbf{\Psi}$, is an encoded universal resource under LOCC up to logical local unitary operations.*

The proof of this theorem is a straightforward generalization of a particular example of an encoded universal resource presented in [12]. We use a result of Walgate *et al* [59], stating that any two orthogonal multi-qubit quantum states can be distinguished by LOCC deterministically. As a consequence, for any choice of encoding $\{|\mathbf{0}\rangle = |\psi_0\rangle, |\mathbf{1}\rangle = |\psi_1\rangle\}$, any two-outcome projective measurement within the logical subspace can be performed by means of LOCC, i.e. by operating on the physical qubits independently. To see this, consider a two-outcome projective measurement specified by the projectors on to the two orthogonal states $\{|\phi_0\rangle, |\phi_1\rangle\}$. Let $|\boldsymbol{\phi}_0\rangle, |\boldsymbol{\phi}_1\rangle$ be encoded versions of these states (which are therefore also orthogonal). Any encoded version $|\boldsymbol{\psi}\rangle$ of a state $|\psi\rangle$ can be written as

$$|\boldsymbol{\psi}\rangle = |\boldsymbol{\phi}_0\rangle|\boldsymbol{\chi}_0\rangle + |\boldsymbol{\phi}_1\rangle|\boldsymbol{\chi}_1\rangle, \tag{48}$$

where $|\boldsymbol{\chi}_0\rangle, |\boldsymbol{\chi}_1\rangle$ are non-normalized, possible non-orthogonal, encoded states of the remaining system. Since one can deterministically distinguish $|\boldsymbol{\phi}_0\rangle$ and $|\boldsymbol{\phi}_1\rangle$ by performing local measurements only on the particles corresponding to these states, the state of the remaining (i.e. unmeasured) particles is given by $|\boldsymbol{\chi}_0\rangle/\sqrt{p_0}$ or $|\boldsymbol{\chi}_1\rangle/\sqrt{p_1}$, depending on the measurement outcome. The success probabilities for the two branches are given by $p_0 := |\langle \boldsymbol{\chi}_0 | \boldsymbol{\chi}_0 \rangle|^2$ and $p_1 := |\langle \boldsymbol{\chi}_1 | \boldsymbol{\chi}_1 \rangle|^2$. Note that the unmeasured system is in the same state as if the logical projective measurement had been performed on the logical system, and the corresponding probabilities to obtain the outcomes are also the same. Note also that the measured system is not in an eigenstate of the measured logical observable. However, this is irrelevant as we are no longer interested in states of measured systems but rather in state of the remaining ones. Consider now a sequence of projective measurements that would produce a certain output state $|\phi_{\text{out}}\rangle$ up to local (i.e. single qubit) operations from a given resource state. If we perform the encoded versions of this sequence of measurements on the encoded state, i.e. measurements on the logical subspace, we obtain as output state an encoded version of the state $|\boldsymbol{\phi}_{\text{out}}\rangle$ up to logical single system operations, as desired.

Notice that the result is general in the sense that it covers *all* possible encodings, and for any encoding it is sufficient to perform only *local* operations on the physical qubits. As an immediate consequence, we obtain the following.

Theorem 17. *For any encoding, the family of encoded 2D-cluster states $\{|\boldsymbol{C}_{d \times d}\rangle\}$ is an encoded universal resource up to single system logical Pauli operations under LOCC. Any family of encoded 2D-cluster states is also CC-universal under LOCC.*

The proof is again straightforward. We apply the same sequence of single qubit measurements as in the one-way model for MQC on the level of encoded, i.e. logical system. This can be done by using only LOCC as shown above. If the initial state was an encoded 2D-cluster state, the resulting state $|\boldsymbol{\phi}_{\text{out}}\rangle$ is an encoded version of the desired output state $|\phi_{\text{out}}\rangle$ up to logical single system Pauli operations, similar as in the one-way model.

Remark 21. *Performing logical Pauli operations by LOCC.* We remark that it is necessary to consider (logical single system) correction operations at the end of the process, as is e.g. required in the one-way model. Otherwise it may often not be possible to generate the desired output state deterministically. Notice that it is not always possible to perform the logical Pauli operations, i.e. the final basis change, by means of LOCC. This is also the reason why the above theorems can only be stated up to logical Pauli operations. However, if we are interested in classical output data only (CC-universality), these logical Pauli operations correspond to a known basis change and do not play a role. They simply correspond to an adjustment of the final measurement basis, where again the same techniques to perform projective measurements on logical systems by means of LOCC can be used.

An example of an encoding where logical Pauli operations cannot be performed locally is given by equation (45). In this case, $\boldsymbol{\sigma}_x$ would need to map a product state on to an entangled state, which is clearly impossible by LOCC. For certain encodings, logical Pauli operations *can* however be implemented by LOCC. For such encodings, the resulting resource is fully CQ-encoded universal. An example for such an encoding is provided by

$$|\boldsymbol{0}\rangle = |0\rangle^{\otimes m}; \quad |\boldsymbol{1}\rangle = |1\rangle^{\otimes m}. \tag{49}$$

Here we have $\boldsymbol{\sigma}_x = \sigma_x^{\otimes m}$, $\boldsymbol{\sigma}_z = \sigma_z^{(1)}$, $\boldsymbol{\sigma}_y = \sigma_y^{(1)} \sigma_x^{\otimes(m-1)}$. It might be interesting to look for other encodings where this is the case. Natural candidates are encodings where the logical basis states are obtained from each other by LOCC i.e. have the same type of entanglement.

8.7. Discussion of encoded universal resources in the literature

Some examples of encoded universal resources, often as proposals for physical implementation of one-way computation, have been discussed previously in the literature. In this subsection we focus on encodings that are naturally covered in our framework. We do not intend to review all potential implementations here; a brief summary is available in section 5 of [23].

In [12], Gross and Eisert describe a specific example of an encoded universal resource using the encoding (44). The focus of their investigations lies on CC-universality, and only the classical information of measurement outcomes performed at the end of a one-way computation is considered. These authors use a different terminology to describe MQC computation, and methods from many-body physics (such as matrix product states and their generalizations to

2D systems) are used and extended. The above mentioned example the authors propose fits into the general framework described in the present paper. In particular, as one finds (see theorem 1) for general encodings, the resource is also CQ-universal up to logical Pauli operations. Additional examples of universal resources based on weighted graph states are put forward in [12]. The example presented in figure 1(a) of [12] fits into the framework we consider as well, and this resource fulfills the entanglement-based criteria for CQ-universality we presented above, even without considering encodings. The relation, if there is any, between the other examples given in [12] and the current investigation, is at present unclear, and understanding whether there is a connection between the two approaches would be an interesting topic for further research.

The authors of [12] stress that their resources have radically different entanglement properties than the (unencoded) cluster state. This is, however, only true when considering 'local' entanglement features with respect to physical qubits. 'Global' entanglement properties (such as entanglement width, geometric measure, Schmidt measure) as well as entanglement width respect to the proper encoding (i.e. **LOCC**) seem to be in fact the *same* as of a 2D cluster state, as we have illustrated in this section.

Another example of an encoded universal resources is given in [60], where Bartlett and Rudolph show how to obtain encoded graph states corresponding to square and hexagonal lattices as the (approximate) ground state of a nearest-neighbour two-body interaction Hamiltonian. The encoding they use is given by equation (49), and they show that MQC can proceed on the encoded cluster states under LOCC (i.e. by physical single-qubit measurements). The focus of [60] lies on the realization of an encoded universal resource state by means of two-body Hamiltonians with a constant gap between the ground state and excited states, regardless of the system size. Note that, in contrast, the generation of a non-encoded graph states as the exact ground state of a two-body Hamiltonian is impossible (see [61]).

Encodings into quantum error correction codes are naturally utilized for fault-tolerant computation, and the simulation of fault-tolerant circuits (i.e. circuits on the encoded logical qubits by quantum codes) with 2D cluster states has been discussed in [62]. Recently, in [63], fault-tolerant quantum computation with an encoded 2D cluster state is discussed. The scheme is based on a high degree of verification in terms of error-detection (and post-selection) using a Calderbank–Shor–Steane code. Hence, the logical qubits are themselves stabilizer states, so that this specific encoding allows implementation of logical σ_z measurements by (transversal) single qubit measurements, and logical Clifford gates by (transversal) single-qubit gates. The latter property makes arbitrary logical Clifford measurements possible. The missing gate for universality, a $\pi/8$ gate, is provided by preparing a logical qubit in the corresponding site in a specific state, namely $\cos(\pi/8)|\mathbf{0}\rangle + \sin(\pi/8)|\mathbf{1}\rangle$, together with (transversal) single-qubit measurements. We remark that our approach (via theorem 17) in principle provides an alternative way to perform the required logical single-system measurements and hence universal MQC, although it is not clear whether fault-tolerance is guaranteed. In [64], entirely new schemes for fault-tolerant quantum computation using topologically protected quantum information (surface codes) have been proposed. We remark that such types of global encodings may not be treated in a straightforward manner by the methods developed in this paper.

9. Summary

In this paper, we have investigated which states constitute universal resources for MQC, and what the role of entanglement is in this issue.

9.1. Considerations regarding universality in QC and MQC

Sections 2 and 3 were dedicated to investigating what is exactly meant by 'universal quantum computation', and, more specifically, 'universal *one-way* quantum computation'. We argued that a distinction needs to be made between several types of universality—called CC-, QC-, CQ- and QQ-universality—depending on whether the input and output of a quantum computer are allowed to be either classical (C) or quantum (Q). In the current investigation of universality in MQC, we focused on *CQ-universality*, due to the following reasons.

(i) Among the above four types of universality, CQ-universality is the most general type any (one-way) MQC model can have. In particular, any CQ-universal resource is also CC-universal. The reason that, e.g. QQ-universality is not possible, is essentially due to the fact that in one-way models, where resource states are processed with *local* operations only, it is not possible to have quantum states as inputs; only classical inputs are possible.

(ii) Although the most general property of QQ-universality is not achievable in any MQC model where resource states can be processed by LOCC only, we have shown that a small modification of the scheme—a supplementary 'input coupler' in the form of a sequence of phase gates or Bell measurements, which is used only at the beginning of an algorithm to read in quantum inputs—suffices to make any CQ-universal MQC model also QQ-universal.

(iii) Furthermore, as we have shown here, a systematic treatment of CQ-universality—i.e. formulation of criteria for CQ-universality as well as construction of new universal resource states—is possible. Such an investigation reveals the central role of entanglement.

Nevertheless, it is clear that other types of entanglement also deserve a detailed investigation. In particular, if one is interested in quantum computers as devices which only provide solutions to classical problems (such as, e.g. prime factoring), one is evidently interested in CC-universality in MQC, rather than CQ- or QQ-universality. However, systematic treatments of CC-universality, and the role of entanglement in such issues, seem much less clear.

9.2. Criteria for universality

In sections 4, and 6, we have developed a framework to investigate (CQ-)universality in MQC. We have analysed which entanglement features any (efficient) universal resource must have. We considered type II monotones E, which are non-increasing under deterministic LOCC conversion, and found that every universal resource must reach the supremum of any such measure E. Thus, universal resources are maximally entangled if entanglement is quantified by such measures E. This insight leads to a class of criteria for universality, as any resource which does not exhibit such a maximal entanglement, cannot be universal. We have illustrated this strategy by considering the entanglement width measures, measures related to localizable entanglement, the geometric measure and the Schmidt measure, and have obtained the following criteria for universality (theorems 5–7, 8).

9.2.1. Criteria for universality.   For every universal resource, the following measures must be unbounded:

1. entropic entanglement width E_{wd};
2. Schmidt-rank width χ_{wd};
3. maximal size $\mathcal{N}_{\mathrm{LE}}$ of a set of qubits with pairwise unit localizable entanglement;
4. geometric measure E_{g}, and
5. Schmidt measure E_{s}.

   Subsequently, several examples of non-universal resources have been given. We name the 1D cluster states, W states, GHZ states and ground states of non-critical 1D spin systems, as the most important examples.

   When efficiency is additionally required, the above criteria can be strengthened, as one finds that the scaling behaviour (with respect to the number of qubits) of all measures E on efficient universal resources must be sufficiently strong.

9.2.2. Criteria for efficient universality.   For any efficient universal resource, the measures E_{wd}, χ_{wd}, $\mathcal{N}_{\mathrm{LE}}$, E_{g} and E_{s} must scale faster than logarithmically with the number of qubits.

   We noted that these results agree with recent results stating that MQC can in fact be classically simulated efficiently on all resources where the Schmidt-rank width grows at most logarithmically with the system size.

   It is important to make the following comment. When assessing the universality or non-universality of a given resource, the choice of suitable entanglement measures E may strongly depend on the resource which is studied. In other words, every measure has a regime of (families of) states in the Hilbert space, where it is most powerful. This is most distinctly illustrated when assessing the universality of graph state resources. One finds that e.g. the measures related to localizable entanglement are *not* useful to investigate universality of graph states—since all (fully entangled) graph states have maximal localizable entanglement between every pair of qubits in the system [23], and therefore localizable entanglement does not distinguish between, e.g. the 1D and the 2D cluster states. Similarly, the geometric measure and the Schmidt measure fail to detect the 1D cluster states as being non-universal, as these measures grow unboundedly on these states. This reflects the fact that all graph states are highly entangled in several ways. On the other hand, the entanglement width measures do turn out to be very powerful to classify graph states in the context of universality, and are e.g. able to identify 1D cluster states (and several other examples) as non-universal. Hence, we can conclude that an important aspect of this study is to map out, for a given measure E, the regime where this measure is useful to detect non-universal resources. Conversely, it is important, for a given resource or class of resources, to identify those measures E which are useful to asses their universality.

9.3. Examples of universal resources

In section 7, we have presented examples of efficient universal resources (see also [27]), namely the graph state resources associated to the 2D hexagonal, triangular and Kagome lattices. We have provided explicit LOCC protocols which efficiently transform these states to the 2D cluster states.

9.4. Encoded universality

In section 8, we considered a more general notion of CQ-universality, called *encoded CQ-universality*, in MQC. A resource is called encoded universal if it is possible to generate arbitrary encoded states by performing LOCC on the resource. There are several reasons for considering encoded universality.

 (i) For many applications (e.g. situations where qudit states are represented by encoded qubit states, as well as in fault tolerant schemes), it is sufficient—and even preferred—that output states are generated in encoded form.
 (ii) Encoded universality is a weaker notion of CQ-universality than the one considered above— i.e. every CQ-universal resource is also encoded CQ-universal. In particular, by considering encoded universality in MQC one comes closer to the notion of CC-universality, such that insight into the former might lead to insights into the latter.
(iii) A systematic investigation of encoded CQ-universality using considerations regarding entanglement, leading both to criteria for encoded universality and to new constructions of universal resources, is possible.

We subsequently studied which criteria have to be fulfilled by any encoded universal resource. Most importantly, we found that the Schmidt measure and geometric measure of entanglement must be unbounded on every encoded universal resource.

Finally, we provided a class of constructions of encoded universal resources, by showing that every CQ-universal resource, which is subsequently encoded, is also an encoded universal resource (up to logical Pauli operations). In particular, such resources are also fully CC-universal.

10. Outlook and open problems

In this paper, we have treated 'exact and deterministic universality', i.e. we have considered the case where the desired output states are created with unit probability (i.e. deterministically) and with unit accuracy (i.e. exactly). In the present study, we have not considered the—from a practical perspective—relevant case of *approximate* and *non-deterministic* generation of the output states. In a forthcoming paper [36], we will extend the definition of universality to take these weaker requirements into account, and investigate to what extent the entanglement-based criteria established for exact deterministic universality can be transferred to this more general case. While some measures (most notably local measures such as localizable entanglement) can no longer be used, many of the present results carry over to this more general case. In [36], we will also provide examples of approximate quasi-deterministic universal resources that are not exact deterministic universal, including states different from graph states.

We remark that several questions in the present study remain to date unanswered, most notably the issue of whether the entanglement width measures can be used directly to assess encoded universality. Furthermore, additional insights are needed regarding the scaling of entanglement in efficient encoded universal resources. In a broader scope, it would be interesting to understand whether criteria for efficient CC-universality differ from the criteria for efficient (encoded) CQ-universality, i.e. whether there exist efficient CC-universal resources that are not (encoded) CQ-universal.

IOP Institute of Physics ⏀ DEUTSCHE PHYSIKALISCHE GESELLSCHAFT

We are convinced that insights gained in the investigation of the universality of resources for MQC allow us to deepen our understanding of the nature and the potential of quantum computation.

Acknowledgments

References

[1] Shor P W 1994 *Proc. 35th Annu. Symp. on the Foundation of Computer Science* (Los Alamitos: IEEE Computer Society) p 124
[2] Grover L K 1997 *Phys. Rev. Lett.* **79** 325
[3] Deutsch D 1985 *Proc. R. Soc. Lond.* A **400** 97
   Bernstein E and Vazirani U 1993 *Proc. 25th Annu. ACM Symp. on Theory of Computing* (New York: ACM) p 11
[4] Deutsch D 1989 *Proc. R. Soc. Lond.* A **425** 73
   Yao A C-C 1993 *Proc. 34th Annu. Symp. on the Foundation of Computer Science* (Los Alamitos: IEEE Computer Society) p 352
   Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P W, Sleator T, Smolin J A and Weinfurter H 1995 *Phys. Rev.* A **52** 3457
[5] Raussendorf R and Briegel H J 2001 *Phys. Rev. Lett.* **86** 5188
   Raussendorf R and Briegel H J 2002 *Quantum Inform. Comput.* **2** 443
[6] Raussendorf R, Browne D E and Briegel H J 2003 *Phys. Rev.* A **68** 022312
[7] Gottesman D and Chuang I 1999 *Nature* **402** 390
[8] Nielsen M A 2003 *Phys. Lett.* A **308** 96
   Leung D 2004 *Int. J. Quantum Inform.* **2** 33
[9] Perdrix S and Jorrand P 2004 *Preprint* quant-ph/0404146
[10] Danos V, Kashefi E and Panangaden P *Preprint* quant-ph/0412135
   de Beaudrap N, Danos V and Kashefi E 2006 *Preprint* quant-ph/0603266
[11] Verstraete F and Cirac J I 2004 *Phys. Rev.* A **70** 060302 (R)
   Aliferis P and Leung D W 2004 *Phys. Rev.* A **70** 062314
   Jorrand P and Perdrix S *Preprint* quant-ph/0404125
[12] Gross D and Eisert J 2007 *Phys. Rev. Lett.* **98** 220503 (*Preprint* quant-ph/0609149)
[13] Farhi E, Goldstone J, Gutmann S, Lapan J, Lundgren A and Preda D 2001 *Science* **292** 472
[14] Briegel H J and Raussendorf R 2001 *Phys. Rev. Lett.* **86** 910
[15] Briegel H J, Raussendorf R and Schenzle A 2002 Optical lattices as a playground for studying multiparticle entanglement *Laserphysics at the Limit* ed H Figger, D Meschede and C Zimmermann (Berlin: Springer) p 433
[16] Borhani M and Loss D 2005 *Phys. Rev.* A **71** 034308
   Weinstein Y S, Hellberg C S and Levy J 2005 *Phys. Rev.* A **72** 020304 (R)
[17] Clarks R, Moura Alves C and Jaksch D 2005 *New J. Phys.* **7** 124
   Tame M S, Paternostro M, Kim M S and Vedral V 2005 *Phys. Rev.* A **72** 012319
   Kay A, Pachos J K and Adams C S 2006 *Phys. Rev.* A **73** 022310

IOP Institute of Physics Φ DEUTSCHE PHYSIKALISCHE GESELLSCHAFT

[18] Barrett S D and Kok P 2005 *Phys. Rev.* A **71** 060310 (R)
      Cho J and Lee H-W 2005 *Phys. Rev. Lett.* **95** 160501
      Benjamin S C, Eisert J and Stace T M 2005 *New J. Phys.* **7** 194
      Lim Y L, Barrett S D, Beige A, Kok P and Kwek L C 2006 *Phys. Rev.* A **73** 012304
      Benjamin S C, Browne D E, Fitzsimons J and Morton J 2006 *New J. Phys.* **8** 141
[19] Tanamoto T, Liu Y-X, Fujita S, Hu X and Nori F 2006 *Phys. Rev. Lett.* **97** 230501
[20] Yoran N and Reznik B 2003 *Phys. Rev. Lett.* **91** 037903
      Nielsen M A 2004 *Phys. Rev. Lett.* **93** 040503
      Browne D E and Rudolph T 2005 *Phys. Rev. Lett.* **95** 010501
      Louis S G R, Nemoto K, Munro W J and Spiller T P 2006 *Preprint* quant-ph/0607060
[21] Menicucci N C, van Loock P, Gu M, Weedbrook C, Ralph T C and Nielsen M A 2006 *Phys. Rev. Lett.*
      97 110501
[22] Duan L-M and Raussendorf R 2005 *Phys. Rev. Lett.* **95** 080503
      Varnava M, Browne D E and Rudolph T 2005 *Preprint* quant-ph/0507036
      Gross D, Kieling K and Eisert J 2006 *Phys. Rev.* A **74** 042343
      Kieling K, Rudolph T and Eisert J 2006 *Preprint* quant-ph/0611140
      Dawson C M, Haselgrove H L and Nielsen M A 2006 *Phys. Rev. Lett.* **96** 020501
      Rohde P P, Ralph T C and Munro W J 2007 *Phys. Rev.* A **75** 010302 (R)
[23] Hein M, Dür W, Eisert J, Raussendorf R, Van den Nest M and Briegel H J 2005 *Quantum Computers,*
      Algorithms and Chaos ed G Casati D L Shepelyansky P Zoller G Benenti (Italy: Varenna) p 115 (*Preprint*
      quant-ph/0602096)
[24] Mandel O, Greiner M, Widera A, Rom T, Hänsch T W and Bloch I 2003 *Nature* **425** 937
      Walther P, Resch K J, Rudolph T, Schenck E, Weinfurter H, Vedral V, Aspelmeyer M and Zeilinger A 2005
      Nature **434** 169
      Prevedel R, Walther P, Tiefenbacher F, Böhil P, Kaltenbaek R, Jennewein T and Zeilinger A 2007 *Nature*
      445 65–69
      Lu C-Y, Zhou X-Q, Gühne O, Gao W-B, Zhang J, Yuan Z-S, Goebel A, Yang T and Pan J-W 2007 *Nat.*
      Phys. **3** 91
      Tame M S, Prevedel R, Paternostro M, Bohi P, Kim M S and Zeilinger A 2006 *Preprint* quant-ph/0611186
[25] Nielsen M A 2006 *Rep. Math. Phys.* **57** 147 (*Preprint* quant-ph/0504097)
      Markov I and Shi Y 2005 *Preprint* quant-ph/0511069
      Jozsa R *Preprint* quant-ph/0603163
      Shi Y, Duan L and Vidal G 2005 *Preprint* quant-ph/0511070
      Yoran N and Short A J 2006 *Phys. Rev. Lett.* **96** 170503
      Bravyi S and Raussendorf R 2006 *Preprint* quant-ph/0610162
      Yoran N and Short A J *Preprint* quant-ph/0611241
      Aharonov D, Landau Z and Makowsky J 2006 *Preprint* quant-ph/0611156
      Browne D E 2006 *Preprint* quant-ph/0612021
[26] Van den Nest M, Dür W, Vidal G and Briegel H J 2007 *Phys. Rev.* A **75** 012337
[27] Van den Nest M, Miyake A, Dür W and Briegel H J 2006 *Phys. Rev. Lett.* **97** 150504
[28] Eisert J and Briegel H J 2001 *Phys. Rev.* A **64** 022306
[29] Shimony A 1995 *Ann. N.Y. Acad. Sci.* **755** 675
      Barnum H and Linden N 2001 *J. Phys. A: Math. Gen.* **34** 6787
[30] Wei T-C and Goldbart P M 2003 *Phys. Rev.* A **68** 042307
[31] Nielsen M A and Chuang I L 2000 *Quantum computation and quantum information* (Cambridge: Cambridge
      University Press)
[32] Gottesmann D 1997 *PhD Thesis* Caltech
[33] Dawson C M and Nielsen M A 2005 *Preprint* quant-ph/0505030

[34] Peres A 1993 *Phys. Rev. Lett.* **77** 1413
Horodecki M, Horodecki P and Horodecki R 1996 *Phys. Lett.* A **223** 1

[35] As a review, Aharonov D and Naveh T 2002 *Preprint* quant-ph/0210077

[36] Mora C *et al* unpublished

[37] Mora C and Briegel H J 2005 *Phys. Rev. Lett.* **95** 200503
Mora C, Briegel H J and Kraus B 2006 *Preprint* quant-ph/0610109

[38] Mhalla M and Perdrix S 2004 *Preprint* quant-ph/0412071

[39] Vidal G 2000 *J. Mod. Opt.* **47** 355

[40] Plenio M B and Virmani S 2007 *Quantum Inform. Comput.* **7** 1

[41] Dür W, Vidal G and Cirac J I 2000 *Phys. Rev.* A **62** 062314

[42] Fortescue B and Lo H-K 2006 *Preprint* quant-ph/0607126

[43] Miyake A 2003 *Phys. Rev.* A **67** 012108

[44] Page D N 1993 *Phys. Rev. Lett.* **71** 1291
Hayden P, Leung D W and Winter A 2006 *Commun. Math. Phys.* **265** 95
Calsamiglia J, Hartmann L, Dür W and Briegel H J 2005 *Phys. Rev. Lett.* **95** 180502

[45] Oum S-I 2005 *PhD Thesis* Princeton University

[46] Oum S-I private communication, see also [45]

[47] Vidal G, Latorre J I, Rico E and Kitaev A 2003 *Phys. Rev. Lett.* **90** 227902
Latorre J I, Rico E and Vidal G 2004 *Quantum Inform. Comput.* **4** 48
Verstraete F and Cirac J I 2006 *Phys. Rev.* B **73** 094423
Verstraete F, Wolf M M, Perez-Garcia D and Cirac J I 2006 *Phys. Rev. Lett.* **96** 220601
Eisert J and Osborne T J 2006 *Phys. Rev. Lett.* **97** 150404
Bravyi S, Hastings M B and Verstraete F 2006 *Phys. Rev. Lett.* **97** 050401
Cramer M, Eisert J, Plenio M B and Dreissig J 2006 *Phys. Rev.* A **73** 012309
Plenio M B, Eisert J, Dreissig J and Cramer M 2005 *Phys. Rev. Lett.* **94** 060503

[48] Verstraete F, Popp M and Cirac J I 2004 *Phys. Rev. Lett.* **92** 027901

[49] Gour G, Meyer D A and Sanders B C 2005 *Phys. Rev.* A **72** 042329

[50] Popp M, Verstraete F, Martin-Delgado M A and Cirac J I 2005 *Phys. Rev.* A **71** 042306
Verstraete F, Martin-Delgado M A and Cirac J I 2004 *Phys. Rev. Lett.* **92** 087201
Pachos J K and Plenio M B 2004 *Phys. Rev. Lett.* **93** 056402

[51] Markham D, Miyake A and Virmani S 2006 *Preprint* quant-ph/0609102

[52] Hein M, Eisert J and Briegel H J 2004 *Phys. Rev.* A **69** 062311

[53] Dür W and Briegel H J 2004 *Phys. Rev. Lett.* **92** 180403

[54] Childs A M, Leung D W and Nielsen M A 2005 *Phys. Rev.* A **71** 032318

[55] Tame M S, Paternostro M, Kim M S and Vedral V 2006 *Phys. Rev.* A **73** 022309

[56] DiVincenzo D P, Bacon D, Kempe J, Burkard G and Whaley K B 2000 *Nature* **408** 339

[57] Taylor J M, Dür W, Zoller P, Yacoby A, Marcus C M and Lukin M D 2005 *Phys. Rev. Lett.* **94** 236803

[58] Taylor J M, Engel H-A, Dür W, Yacoby A, Marcus C M, Zoller P and Lukin M D 2005 *Nat. Phys.* **1** 177

[59] Walgate J, Short A J, Hardy L and Vedral V 2000 *Phys. Rev. Lett.* **85** 4972

[60] Bartlett S D and Rudolph T 2006 *Phys. Rev.* A **74** 040302 (R)

[61] Van den Nest M, Luttmer J, Dür W and Briegel H-J 2006 *Preprint* quant-ph/0612186

[62] Raussendorf R 2003 *PhD Thesis* Ludwig-Maximillians University München
Nielsen M A and Dawson C M 2005 *Phys. Rev.* A **71** 042323
Aliferis P and Leung D W 2006 *Phys. Rev.* A **73** 032308

[63] Fujii K and Yamamoto K 2006 *Preprint* quant-ph/0611160
Danos V, Kashefi E, Ollivier H and Silva M 2006 *Preprint* quant-ph/0611273

[64] Raussendorf R, Harrington J and Goyal K 2006 *Ann. Phys.* **321** 2242 (*Preprint* quant-ph/0510135)
Raussendorf R and Harrington J 2007 *Phys. Rev. Lett.* **98** 190504