

Discord in relation to resource states for measurement-based quantum computation

Eleanor G. Rieffel¹ and Howard M. Wiseman²

¹ *QuAIL, NASA Ames Research Center, Moffett Field, CA 94035*

² *Centre for Quantum Computation and Communication Technology (Australian Research Council),
Centre for Quantum Dynamics, Griffith University, Brisbane, QLD 4111, Australia*

(Dated: March 17, 2014)

We consider the issue of what should count as a resource for measurement-based quantum computation (MBQC). While a state that supports universal quantum computation clearly should be considered a resource, universality should not be necessary given the existence of interesting, but less computationally-powerful, classes of MBQCs. Here, we propose minimal criteria for a state to be considered a resource state for MBQC. Using these criteria, we explain why discord-free states cannot be resources for MBQC, contrary to recent claims [Hoban *et al.*, arXiv:1304.2667v1]. Independently of our criteria, we also show that the arguments of Hoban *et al.*, if correct, would imply that Shor’s algorithm (for example) can be implemented by measuring discord-free states.

I. INTRODUCTION

In measurement-based quantum computation (MBQC), computation is carried out by performing local measurements on an initial state. Classical processing of the results may take place in parallel, enabling the measurements to be performed adaptively. The foundational proposal [1] for MBQC introduced the class of cluster states for the initial states, but since then many other types of entangled states have been found that support universal quantum computation [2–4]. Universality is obviously a sufficient condition for a state to be a resource state for MBQC, but seems too strong as a necessary condition given the recent discovery of classes of MBQCs such as *IQP* [5]. This class includes only non-adaptive MBQCs, and so is unlikely to be universal, but nevertheless appears to give an advantage over classical computing. While it is generally believed that some entanglement (but not too much! [6–8]) is required for a state to be a resource for MBQC, that has yet to be established.

Recently, in their paper “Exact sampling and entanglement-free resources for measurement-based quantum computation,” Hoban *et al.* [9] challenged the notion that entanglement is necessary by proposing that there are resource states for certain types of MBQC that not only are entanglement free, but even discord free. The zero-discord claim is particularly surprising because discord-free states are “essentially classical” [9], as they comprise mixtures of locally orthogonal states. Prompted by their work, we address the question of how resource states for MBQC should be defined. We propose some minimal criteria, and come to conclusions contrary to those of Hoban *et al.* In particular, we argue that discord-free states *cannot* be resource states for MBQC. We leave open the question of whether other entanglement-free states could be resource states for MBQC.

Our paper is structured as follows. First, we propose the principle that for a state to be a resource state for MBQC, it must support computations that are inherently measurement based (Sec. II). In Sec. III, we give mini-

mal (i.e., weak) necessary conditions for a set of MBQCs to be inherently measurement based. We use these criteria in Sec. IV to consider the work of Hoban *et al.*, and explain why their arguments do not support their conclusion. We show that if one accepted their arguments, then one would also have to believe that Shor’s algorithm (for example) could be implemented in MBQC using discord-free resource states. In Sec. V, we propose a slightly stronger necessary condition, from which it follows that it would never make sense to claim that discord-free states are resources for MBQC. Finally, we summarize our findings. Readers interested only in our discussion of Hoban *et al.* could go straight to Sec. IV. Readers interested in the much broader question raised by our title should study Secs. II, III, and V.

II. A KEY PRINCIPLE

Throughout, we consider the standard model of MBQC [1, 10] in which single-qubit measurements on a ν -qubit quantum state ρ , together with a classical computational processor, are all that is needed to carry out the computation. In general, the measurements are adaptive [11, 12] (that is, the choice of measurement basis depends on the results of previous measurements), but some interesting MBQC algorithms, such as MBQC implementations of *IQP* computations [13], are non-adaptive.

To construct any argument that some given state is (or is not) a resource for MBQC, one must start with a sufficient (or necessary, respectively) criterion for the concept of “resource for MBQC”. Prior to this work, necessary criteria for a quantum state to be a resource for MBQC have not appeared in the literature, to our knowledge.

The term “resource” is used most frequently when discussing which states support universal MBQC and which do not (e.g., [2–4, 6–8]). Universality is certainly a sufficient condition, but seems too strong as a necessary condition for a state to be a resource for MBQC in light of results such as the following: (i) Anders and Browne [14] showed that single-qubit measurements on GHZ states can boost the extremely limited classical computational

class $\oplus L$ (parity- L) to P . (ii) Bremner *et al.* [5] showed that IQP contains computations not in P (unless the polynomial hierarchy collapses to the third level) while unlikely to give universal quantum computation. Here IQP is the class of “instantaneous quantum computations,” that is, those that can be carried out with non-adaptive measurements in the MBQC model. (iii) Hoban *et al.* [9] extended the last result to the class IQP^* .

At the other extreme, since any quantum state can be subjected to single-qubit measurements, one might say that every quantum state should be considered a resource for MBQC. On reflection, however, it is clear that this is too weak as a sufficient condition; it would remove any possibility of scientific advance on the question of resource states for MBQC. That the proper concept of a resource state for MBQC ought to require something between these two extremes should be a point of agreement between all researchers in the field.

One could try to characterize which resources support (or do not support) computationally interesting MBQC. The problem is that, almost certainly, not all of the interesting MBQC tasks are known. Instead, we concentrate on a weaker property, namely, what makes a set of MBQCs worthy of the name MBQC. That is, we introduce the notion of *inherently measurement-based computations*, and give a series of necessary conditions for sets of MBQCs to be considered inherently measurement-based.

We do not attempt to redefine MBQC itself to include only inherently measurement-based quantum computations. The reason is that this would be an impediment to discussing MBQC, just as excluding from quantum computations ones that are not inherently quantum would be an impediment to discussing quantum computation. By not using such exclusive language, the community is able to make useful statements such as “all reversible classical computations can be translated into a quantum computation of precisely the same efficiency.” The concept of “inherently quantum” is useful, just as is the concept of “inherently measurement based” (as we will see), but in neither case is it fruitful to exclude computations that are not inherently of the type under consideration.

We propose the following principle:

Principle II.1 *Any criterion for the resource status of a state that rests on its support for a set of MBQCs must require that set to be inherently measurement based.*

We highlight that in this principle, as in all such general propositions in this paper, it is necessary to consider a *set* of MBQCs, not merely a single MBQC. In keeping with Principle II.1, we also propose:

Principle II.2 *A state ρ is a resource for MBQC only if it supports a set of computations that is inherently measurement based.*

As a consequence of Principle II.1, to establish a state as a resource, it does not suffice to identify a set of

MBQCs it supports unless they are inherently measurement based.

The above principles do not involve any consideration of how ρ may be generated. This is quite deliberate. Whether a state can be efficiently generated is an interesting question, but one that should be kept separate from whether a state (even one that cannot be efficiently generated) should be considered a resource for MBQC. Maintaining this separation allows for discussion of distinctions between states in terms of their power for MBQC regardless of whether those states are practical. This stance is in keeping with discussions of universal resource states for MBQC. For example, Refs. [6, 7] consider the question of whether certain states are too entangled to be resources for MBQC without considering whether they can be efficiently generated. The question of whether there are states that can be efficiently generated that are too entangled was addressed separately [8]. More generally, when considering whether a state is a resource for any task, it should not matter where that state came from. In the current situation, for example, it should not matter whether a putative resource state for MBQC was generated via MBQC or not.

We now turn to the question of which computations are inherently measurement based.

III. SOME SIMPLE CRITERIA

As we noted above, there are different types of MBQC, with differing restrictions on the types of measurements and the types of classical computation that can be done, and still more types likely to be defined. For this reason, we do not give a full definition with necessary and sufficient conditions for a set of MBQCs to be inherently measurement based. We give a series of increasingly stringent requirements for a set of MBQCs to be inherently measurement based, expressed as a series of increasingly weak sufficient conditions for a set of MBQCs to be only superficially measurement-based, and therefore not inherently measurement based. Informally, all of these conditions say that for a quantum computation to be considered inherently measurement based, measurements must form a key part of the computation.

Consider a set S of MBQCs employing ρ , a pre-measurement state of ν qubits. We propose:

Criterion III.1 *A set S of MBQCs is only superficially measurement-based if, for every computation in S , the measurement of the pre-measurement state always yields the same classical ν -bit string \mathbf{m} .*

The reasoning here is that the quantum state ρ can be replaced by the more conveniently stored classical bit string $\mathbf{m} = m_\nu \dots m_1$ with no loss whatsoever. In fact, doing so saves the ultimate user the trouble of doing the measurements. Instead of performing a MBQC, the user performs only the classical computational part of the MBQC, substituting in the appropriate bit values

from the classical bit string instead of performing the measurements. The resulting output is indistinguishable from that of the MBQC. In such a computation, measurements are no longer needed, and the entire computation becomes completely classical. It seems fair to say that such a computation is not inherently measurement based or quantum.

This criterion, together with Principle II.1, allow us to make the following uncontroversial statement. On the basis of a set of MBQCs that always measure the state ρ in the computational basis, one cannot claim a state $\rho = |\mathbf{m}\rangle\langle\mathbf{m}|$, corresponding to the classical bit string $\mathbf{m} = m_\nu \dots m_1$, to be a resource for MBQC. Nobody has, to our knowledge, made precisely such a claim, but this is an important step towards our more substantial conclusions later in this section.

We now propose a stronger criterion.

Criterion III.2 *A set S of MBQCs is only superficially measurement-based if the ν -qubit pre-measurement state ρ can be measured locally (i.e., each qubit separately) ahead of time, without regard to which computation f in S will be carried out, and the resulting classical ν -bit string \mathbf{m} can be used to carry out any one of the computations in S .*

Again, the reasoning here is that the quantum state ρ can be replaced by a more conveniently stored classical bit string with no loss whatsoever, saving the ultimate user the trouble of doing the measurements, and turning the computation into a completely classical one. This criterion means that a set S of MBQCs in which the measurement basis for each qubit of ρ does not vary between elements of S should not be considered inherently measurement based. We stress that the classical bit string \mathbf{m} here is not required to be the same in every run of the algorithm. That is, the bit string \mathbf{m} replaces the pre-measurement state ρ in the sense that it can be used to yield (through purely classical processing, of course) a single output, exactly the same way that, in general, the pre-measurement state ρ only allows a MBQC to be run once. To state this more formally, Criterion III.2 can be rephrased as follows: A set S of MBQCs is only superficially measurement-based if, given a set of r copies of the pre-measurement state ρ , each can be measured locally ahead of time, without regard to which computations f in S will be carried out, and the resulting classical bit strings $\mathbf{m}_1, \mathbf{m}_2, \dots, \mathbf{m}_r$ can be used to carry out any set of r computations in S .

It is critical to recognize that Criterion III.2 does not imply that depth-1, or non-adaptive, MBQCs are only superficially measurement-based. A set S of non-adaptive MBQCs in which different members of the set S require the qubits to be measured in different bases avoids being classified as only superficially measurement-based by Criterion III.2 since the measurements cannot be made ahead of time, without regard to the specific $f \in S$ to be carried out. Criterion III.2 only rules out any set S of MBQCs in which the qubits are measured in the same

basis no matter what computation $f \in S$ is being carried out. That is, a distinction must be made between what we term *flexible* measurements of the initial state, in which the basis in which the qubits are measured depends on the specific computation to be performed, and adaptive measurements, in which the basis in which some of the qubits are measured depends on the outcome of previous measurements. Criterion III.2 does not require adaptive measurements, only flexible measurements, and for this reason (as we explain carefully in the next section) it does not imply that the MBQCs for IQP and IQP^* starting with graph states are only superficially measurement-based.

IV. DISCUSSION OF HOBAN *ET AL.*'S CLAIMS

In Ref. [9], Hoban *et al.* claim to “show that there exist computations which cannot be efficiently and exactly performed on a classical computer, but can be performed in standard measurement-based quantum computation (MBQC) using resource states with zero entanglement and zero discord.” In this section, we examine their arguments and explain why they do not support this conclusion. In Sec. V, we present a more general argument that shows that discord-free states cannot be resources for MBQC.

The MBQCs on which Hoban *et al.* base their claim that discord-free states can be resources for MBQC involve measurement in only the eigenbasis of the discord-free state ρ . Thus, Criterion III.2 is strong enough to establish that these sets are not inherently measurement based, and therefore, by Principle II.1, cannot be used to establish that a type of quantum state is a resource for MBQC.

Before presenting our argument in more detail, it is worth mentioning that we have no disagreement with the other main claim of Hoban *et al.* [9], namely their Lemma 1, in which they have applied similar proof techniques to those in [5] to show that efficient classical sampling of the output of IQP^* circuits, a subclass of IQP circuits with a more standard uniformity condition, implies the collapse of the polynomial hierarchy to the third level, just as it does for IQP circuits [5]. Other sampling problems that can be achieved efficiently using quantum means and are unlikely to be efficiently achievable classically are known [15–17].

First, we review the construction of Hoban *et al.* [9], so that we can discuss issues specific to their arguments. They define an IQP^* circuit family to be a family of quantum circuits $C_{Z,\Theta}$, indexed by the integers n , acting on a register of ν qubits and taking as input an n -bit string $\mathbf{x} = x_n \dots x_1$. The family must be uniform, meaning that there exists a Turing machine that can output a description of the quantum circuit in polynomial time given input n . For IQP^* , that description specifies (i) how $\nu > n$ depends polynomially on n ; (ii) Z , a set of polynomially-many ν -bit strings $\mathbf{z} = z_\nu \dots z_1$; and (iii)

Θ , a set of angles θ_z , one for each string $z \in Z$, such that each $\theta_z \in (0, 2\pi]$ has a polynomial-sized description. The circuit consists of a polynomial sequence of gates of the form $e^{i\theta_z X[z]}$, where $X[z] = \bigotimes_{j=1}^{\nu} X^{z_j}$. The register is initialized to the n -qubit state $|x\rangle$ followed by $(\nu - n)$ qubits initialized to $|0\rangle$. The ν -bit output m is obtained by measuring all of the qubits in the computational basis at the end of the computation.

Hoban *et al.* prove that efficiently and exactly simulating the output of such circuits classically would imply the collapse of the polynomial hierarchy to the third level. They have thereby proven their first result, Lemma 1 – an interesting result, with which, as we said, we have no quarrel.

They further show that all of the computational difficulty in simulating the output of these circuits classically is in the simulation of the output for any one particular input x . For example, one can restrict to the $\mathbf{0}$ input state in which the input is a string of n zeros, as can be seen from the following symmetry argument. Let \bar{x} be the ν -bit string consisting of x followed by $\nu - n$ zeros. The probability $P(m|x)$ that output string m is obtained, given input string x , is equal to $P(m \oplus \bar{x} | \mathbf{0})$. Thus, given a way to obtain samples for the probability distribution for input $\mathbf{0}$, samples for the probability distribution for input x can be obtained trivially.

Hoban *et al.* exhibit a way to implement the circuits $C_{Z,\Theta}$ acting on input $x = \mathbf{0}$ using MBQC. The MBQC uses a graph state ρ_Z with $r = \nu + |Z|$ qubits where $|Z|$ is the number of elements $z \in Z$ or, equivalently, the number of gates applied in the original circuit. We will use c_j , with $j \in \{1, \dots, \nu\}$ for the computational qubits, and q_z for the additional $|Z|$ qubits. Edges go from a qubit q_z to exactly the subset of the ν qubits c_j such that the j th bit of z , z_j , is 1. To perform the computation, each of the $|Z|$ qubits q_z is measured in the basis corresponding to its associated angle θ_z yielding $|Z|$ bit values b_z . To complete the computation, the remaining ν qubits c_j are all measured in the X -basis $\{|+\rangle, |-\rangle\}$, and on the resulting bit values a classical computation determined by the $\{b_z\}$ is performed to obtain the ν -bit outcome m . To obtain results for a circuit $C_{Z,\Theta}$ acting on input $x \neq \mathbf{0}$, one can simply (classically) compute $m \oplus \bar{x}$. The full computations just described are undoubtably true MBQCs. Each graph state ρ_Z can support any computation in IQP^* with the same set Z but differing θ_z . For this reason, they are *not* found to be only superficially measurement-based according to our Criteria III.1, III.2, and V.1. Indeed, this construction provides a measurement-based quantum computational means to efficiently sample a distribution that is strongly suspected not to be able to be sampled efficiently classically.

Hoban *et al.* then point out that, starting with the graph state ρ_Z , one can dephase all of the qubits, the q_z in the θ_z basis and the c_j in the X basis, to obtain the

discord-free [18, 19] state

$$\rho_{Z,\Theta} = \sum_{\mathbf{y}}^{2^r-1} P(\mathbf{y}|\mathbf{x}) |\mathbf{y}\rangle \langle \mathbf{y}| \quad (1)$$

where here $|\mathbf{y}\rangle = |y_r\rangle \cdots |y_1\rangle$, and \mathbf{y} is the bit string $y_r \cdots y_1$. That is, the state is “essentially a classical probability distribution” [9] and obviously is unentangled. Measuring each of the qubits in the basis in which it was dephased, and then performing a classical computation on the resultant bits – exactly the computation that would have been performed on the measurement outcomes in the original MBQC – yields output m , a sample from the distribution $P(m|x)$ corresponding to the original circuit $C_{Z,\Theta}$. Note that the state in Eq. (1) is specific to the circuit $C_{Z,\Theta}$, which we have emphasized by denoting it $\rho_{Z,\Theta}$. Thus, measuring $\rho_{Z,\Theta}$ yields samples from only this one distribution, though bit-wise addition of \bar{x} enables sampling from the trivially related distributions obtained by applying $C_{Z,\Theta}$ to input $x \neq \mathbf{0}$.

We fully agree with the correctness of these statements, but we disagree markedly with Hoban *et al.* in the interpretation of this procedure. They claim that $\rho_{Z,\Theta}$ is a resource for MBQC. However, it is clear that there is no reason to stop their procedure after creating the discord-free state $\rho_{Z,\Theta}$. One can simply measure it and obtain a classical bit string \mathbf{y} that can be stored classically without requiring quantum storage. Indeed, any computation that uses a quantum state as a resource only to measure each of its qubits in a fixed basis could be performed identically and more conveniently using a classically stored bit string. Thus, by Criterion III.2 and Principle II.1, it is clear that this set of computations does not support Hoban *et al.*’s claim that ρ is a resource for MBQC.

It is important to understand why Criterion III.2 implies that the computations starting with a discord-free state $\rho_{Z,\Theta}$ are only superficially measurement-based, while the computations starting with a graph state ρ_Z are not so categorized. A single initial graph state ρ_Z can support a set of computations $S_Z = \{f_\Theta\}$ for all possible sets of measurement angles Θ . Criterion III.2 does not classify S_Z as only superficially measurement-based because ρ_Z cannot be measured ahead of time and still support the computation of all $f_\Theta \in S_Z$; the measurements to be performed depend on which f_Θ is to be carried out. In the language of Sec. III, while all of the MBQCs in this set are non-adaptive, the set does require flexible measurements.

On the other hand, a single discord-free state $\rho_{Z,\Theta}$ obtained by dephasing as described above, supports a much smaller set of the above computations than the graph state ρ_Z . It supports only the set of above computations in which each of the qubits q_z is measured in the basis associated with θ_z , where Θ contains the angles θ_z , one for each qubit q_z . For this set of computations, flexible measurements are not required; one can still perform all of the computations in the set after measuring in the eigenbasis of ρ_Z . One does not need to know which com-

putation is desired before measuring all of the qubits. Thus, this smaller set of computations is only superficially measurement-based by Criterion III.2.

One can gain further insight by recognizing that Hoban *et al.*'s construction of an MBQC to obtain their discord-free state is completely unnecessary: they could just as well have dephased the state obtained in their original quantum circuit model prior to the final measurement of all of the qubits c_j in the standard (logical) basis. This would yield the even simpler discord-free state

$$\rho'_{Z,\Theta} = \sum_{\mathbf{m}=0}^{2^\nu-1} P(\mathbf{m})|\mathbf{m}\rangle\langle\mathbf{m}|. \quad (2)$$

where $P(\mathbf{m}) = P(\mathbf{m}|\mathbf{x})$ is the desired probability distribution for the “measurement output string $\dots \mathbf{m}$ ” [9]. In deciding whether or not a state should be considered a resource state for MBQC, it should not matter how the state was obtained. In particular, it should not matter whether it was obtained through MBQC or through some other means.

The same construction can be applied to many quantum computations. In the following subsection, we consider Shor's factoring algorithm [10, 20] as an example.

A. An analogous “resource” for factoring

Suppose F is a uniform family of integers M_n , by which we mean that a Turing machine can output M_n , an integer of bit length n , in polynomial time given input n . For example, we may use a cryptographic grade pseudorandom number generator to output a series of integers of increasing length. The expected runtime of any known classical factoring algorithm is superpolynomial in n , and it is strongly suspected that any classical approach to factoring is superpolynomial. For this reason, most of the numbers in these uniform families will be hard to factor classically.

Next we introduce, as is standard for Shor's algorithm, another efficient pseudorandom number generator G that outputs another uniform family of integers $a_n < M_n$. We define uniform Shor circuit families to be families in which each circuit is a concatenation of the following: (i) a quantum (though it may as well be classical) circuit that upon input n computes M_n and a_n ; (ii) a quantum circuit that takes as input M_n and a_n and a register of size $\nu + n$, where $M_n^2 \leq 2^\nu < 2M_n^2$, prepared as an equal superposition of all logical values x for $0 \leq x \leq 2^\nu - 1$ in the first ν bits of the register, and computes the function $f_n(x) = a_n^x \bmod M_n$ in a quantum parallel sense into the remaining n bits of the register; and (iii) a quantum circuit of sufficient size (polynomial in n) that it can carry out Shor's algorithm for this input. Finally, a read-out is, of course, performed to obtain, nondeterministically, an estimate of the period of f_n , which, with high probability, provides a key to factorizing M_n .

Now, instead of performing this final measurement, one could dephase the final quantum state in the computational basis, obtaining a discord-free state ρ . Since, with high probability, a factor of M_n can be obtained from a sample of the classical probability distribution associated with ρ , such probability distributions in general cannot be sampled efficiently classically given input n and the description of the circuit, unless there is a classical factoring algorithm of expected polynomial runtime.

Should such a ρ be considered a resource for MBQC? Just as we do not believe that Hoban *et al.*'s arguments support their Theorem 2, we do not believe that the analogous argument we have just given supports the analogous theorem, *Shor's algorithm may be implemented in MBQC using resource states with zero entanglement and zero discord*. Similarly, we do not believe such arguments support their Corollary 2 or its analog, *Shor's algorithm may be implemented in MBQC using correlations which do not violate any Bell inequalities*. Criterion III.2 together with Principle II.1 explain why.

We now turn to showing why discord-free states could never be resources for MBQC.

V. GENERAL ARGUMENT

In this section, we give a third, broader criterion that encompasses additional sets of MBQCs that, we argue, should be considered only superficially measurement-based. We use this third criterion to establish that discord-free states cannot be considered resources for MBQC. Before motivating the broader criterion we will define, we first recall the definition of a discord-free state [18, 19]. For ν qubits, it is any state that can be written, for a suitable definition of basis $\{|0\rangle, |1\rangle\}$ for each qubit, in the form of Eq. (2), where $P(\mathbf{m})$ is an arbitrary probability distribution.

A state of this form is not only “essentially a classical probability distribution” $P(\mathbf{m})$ [9]; it is experimentally indistinguishable from a pre-existing basis state $|\mathbf{m}\rangle$ with the bit string \mathbf{m} drawn at random from that distribution [11]. As an obvious consequence, any computation that can be done with a discord-free state ρ is indistinguishable from one done with a sample $|\mathbf{m}\rangle$ from the probability distribution represented by the discord-free state ρ .

Suppose one starts with a sample $|\mathbf{m}\rangle$ from the probability distribution represented by the discord-free state ρ . Instead of making the single-qubit measurements on state $|\mathbf{m}\rangle$ (according to whatever putative MBQC algorithm is to be implemented), one could generate results with the same statistics as these measurement results using the classical bit string \mathbf{m} and classical computation on each of the ν bits of \mathbf{m} individually, independent of the values of any of the other bits. Specifically, for each qubit j , given m_j and the measurement basis, one can trivially calculate the probability distribution from which the output bit may be generated.

Note that a single discord-free state can be measured only once, so a discord-free state is not a black box that provides samples from a distribution, but rather one that yields only a single sample. Perhaps it will help the reader to understand if we restate this in the style of the discussion following Criterion III.2. A set of 100 discord-free states ρ , all of which are measured in the eigenbasis of ρ , can be replaced by a set of 100 samples from the distribution. Thus, a set of discord-free states can be replaced by a bit string containing the same number of samples as the number of discord-free states one is replacing.

These considerations motivate

Criterion V.1 *A set S of MBQCs should be considered only superficially measurement-based if the ν -qubit state ρ can be measured locally ahead of time, without regard to which computation f in S will be carried out, and the resulting classical ν -bit string \mathbf{m} can be used, together with classical (possibly non-deterministic) computation on each bit of \mathbf{m} separately, to carry out any one of the computations in S .*

For the same reasons explained with respect to Criterion III.2, Criterion V.1 does not imply that the MBQCs for IQP and IQP^* starting with graph states are only superficially measurement-based. The paragraph prior to stating Criterion V.1 shows that any set of MBQCs supported by a discord-free state satisfies Criterion V.1 and is therefore not inherently measurement based. This statement, together with Principle II.1, implies that discord-free states cannot be resources for MBQC. This completes our argument for why it would never make sense to claim that a discord-free state could be a resource for MBQC.

As a final note, we remark that more stringent conditions than the ones we have given are likely called for. It seems reasonable, for example, that if, in a set of MBQCs, the pre-measurement state could be replaced by a classical bit string with only linear classical computational overhead, then said set is not inherently measurement based. Some readers may worry that such a principle would rule out graph states as a resource for MBQC, because in many cases graph states can be generated from a classical description using only linear computation. However, the computation required is quantum, not classical. Thus, while a graph state may be a resource state for MBQC, its classical description

is not; nor do Refs. [10, 11], however useful, constitute resources for quantum computation. Other readers may wonder why we restrict the amount of classical computation. If we were to allow unlimited classical computation, all measurement-based computation, and in fact, all quantum computation, could be carried out since BQP is in $PSPACE$. For this reason, limiting the amount of classical computation is necessary.

VI. CONCLUSION

We have proposed the principle that a state should be considered a resource for MBQC only if it supports inherently measurement-based quantum computations. We have also provided necessary criteria for MBQCs to be inherently measurement based, criteria which are so weak as to be, we hope, uncontroversial. Building from this principle and these criteria, we have explained why it could never be correct to consider discord-free states as resources for MBQC, and we have specifically addressed the arguments of Hoban *et al.* that suggested otherwise.

We leave the problem of fully characterizing what it means for a state to be a resource state for MBQC, and what it means for a MBQC to be inherently measurement based, as future work.

Note added: Subsequent to the the submission of our paper, Hoban *et al.* have revised their paper, removing the claim that discord-free states can be resources for MBQC and changing their title [21]. Nevertheless, their arguments remain much as they were, so most of the detailed critique we give in Sec. IV applies just as much to their revised version as to the original. In particular, our criticism in Sec. IV still holds: the class of problems solved by any one of their discord-free resource states is a trivial class quite distinct from IQP^* ; moreover, their dephasing procedure has nothing to do with IQP^* , but rather could be applied to any quantum algorithm (including Shor's, as we discuss) to produce a resource of similarly limited utility.

Acknowledgements

Both authors would like to thank Dan Browne for stimulating e-mail exchanges.

-
- [1] R. Raussendorf and H. J. Briegel, Physical Review Letters **86**, 5188 (2001).
 - [2] M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel, Physical Review Letters **97**, 150504 (2006).
 - [3] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, Physical Review A **76**, 052315 (2007).
 - [4] H. Briegel, D. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, Nature Physics **5**, 19 (2009).
 - [5] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science **467**, 459 (2011).
 - [6] D. Gross, S. T. Flammia, and J. Eisert, Physical Review Letters **102**, 190501 (2009).
 - [7] M. J. Bremner, C. Mora, and A. Winter, Physical Review Letters **102**, 190502 (2009).
 - [8] R. A. Low, Proceedings of the Royal Society A: Math-

- ematical, Physical and Engineering Science **465**, 3289 (2009).
- [9] M. J. Hoban, J. J. Wallman, H. Anwar, N. Usher, R. Raussendorf, and D. E. Browne, *Exact sampling and entanglement-free resources for measurement-based quantum computation*, arXiv:1304.2667v1 (2013).
 - [10] E. G. Rieffel and W. Polak, *A Gentle Introduction to Quantum Computing* (MIT Press, Cambridge, MA, 2011).
 - [11] H. M. Wiseman and G. J. Milburn, *Quantum Measurement and Control* (Cambridge University Press, Cambridge, UK, 2010).
 - [12] R. Raussendorf and H. J. Briegel, *Computational model for the one-way quantum computer: Concepts and summary*, arXiv preprint quant-ph/0207183 (2002).
 - [13] D. Browne, E. Kashefi, and S. Perdrix, in *Theory of Quantum Computation, Communication, and Cryptography* (Springer, 2011), pp. 35–46.
 - [14] J. Anders and D. E. Browne, Physical Review Letters **102**, 050502 (2009).
 - [15] S. Aaronson and A. Arkhipov, in *Proceedings of STOC'11* (2011), pp. 333–342.
 - [16] S. Aaronson and A. Arkhipov, *BosonSampling is far from uniform*, arXiv:1309.7460 (2013).
 - [17] B. M. Terhal and D. P. DiVincenzo, Quantum Information & Computation **4**, 134 (2004).
 - [18] H. Ollivier and W. H. Zurek, Physical Review Letters **88**, 017901 (2001).
 - [19] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
 - [20] P. W. Shor, in *Proceedings of FOCS'94* (1994), pp. 124–134.
 - [21] M. J. Hoban, J. J. Wallman, H. Anwar, N. Usher, R. Raussendorf, and D. E. Browne, *Measurement-based classical computation*, arXiv:1304.2667v3 (To appear in PRL.) (2014).