Measurement-based classical computation

Matty J. Hoban,[1] Joel J. Wallman,[2] Hussain Anwar,[3] Naïri Usher,[3] Robert Raussendorf,[4] and Dan E. Browne[3]

[1]*ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, E-08860 Castelldefels (Barcelona), Spain*
[2]*Centre for Engineered Quantum Systems, School of Physics, The University of Sydney, Sydney, NSW 2006, Australia.*
[3]*Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom.*
[4]*Department of Physics and Astronomy, University of British Columbia, Vancouver, BC V6T 1Z1, Canada*

(Dated: December 16, 2013)

Measurement-based quantum computation (MBQC) is a model of quantum computation, in which computation proceeds via adaptive single qubit measurements on a multi-qubit quantum state. It is computationally equivalent to the circuit model. Unlike the circuit model, however, its classical analog is little studied. Here we present a classical analog of MBQC whose computational complexity presents a rich structure. To do so, we identify uniform families of quantum computations (refining the circuits introduced by Bremner, Jozsa and Shepherd in *Proc. R. Soc. A* **467**, 459 (2011)) whose output is likely hard to exactly simulate (sample) classically. We demonstrate that these circuit families can be efficiently implemented in the MBQC model without adaptive measurement, and thus can be achieved in a classical analog of MBQC whose resource state is a probability distribution which has been created quantum mechanically. Such states (by definition) violate no Bell inequality, but nevertheless exhibit non-classicality when used as a computational resource—an imprint of their quantum origin.

There is a strong belief that quantum computers can efficiently perform certain tasks that cannot be performed efficiently on a classical computer, such as integer factorization [1]. One of the central questions of quantum information theory is to better understand which aspects of quantum evolution are efficiently classically simulatable and which are not [2]. One important aspect of this investigation has been to learn when a computational model cannot possess a super-classical speed-up, by showing that it can be simulated efficiently on a classical computer. For example, Jozsa and Linden showed that in pure state circuit-model quantum computation, restricting the multi-partite entanglement in certain ways renders the model classically efficiently simulatable [3]. In contrast, a number of striking recent results [4–6] have given rigorous evidence that certain models of quantum computation (that have circuits with unrestricted entanglement) are unlikely to admit an efficient classical simulation.

A distinct way to question the role of entanglement in quantum computing is to consider it within the model of Measurement-based Quantum Computation (MBQC) [7]. In MBQC, computation proceeds via a sequence of single-site measurements on a (usually entangled) many qubit resource state. Certain entangled resource states, such as the cluster state [8] are known as universal resources since they enable universal quantum computation in this model. It has been shown that the computational properties of a resource state can be linked to its entanglement properties [9], and minimal criteria for a state to be a resource state for MBQC have been proposed [10]. Here, we consider the computations that can be performed in the MBQC framework when *no entanglement* is present in the resource state by developing and studying a classical analog of MBQC.

It is important to define clearly what we mean by *non-classical* in the context of computation. In this paper, we denote a standard classical computing device (formal definition in App. A) as a classical computer that has access to uniformly random bits (i.e. as is used to define the complexity class BPP). We then define non-classical computation as any family of computations which cannot be achieved efficiently (i.e. in polynomial time) with such a device.

The connections between MBQC and classical computation was studied from one perspective in [11], where it was shown that casting classical computations within the MBQC model illuminated a close connection between MBQC and GHZ-type paradoxes (see also [12]). Here we take an alternative approach. MBQC can be split into three components: a multi-qubit resource state; adaptive local measurements; and the classical side-computation which processes input and output and allows adaptive measurement [13]. In a full quantum realisation of MBQC, the first two components are quantum, and the latter classical. In this paper we consider the consequences of making all three components classical.

What is the classical analog of an entangled resource state? When we measure a quantum state, the output is usually random. Moreover, we can only make a measurement once—in entangled-state MBQC, measurement always changes the state. Due to the single-use property of the entangled resource states MBQC is often called the "one-way quantum computer" [7]. The classical object which shares these properties is a *single sample* from a multi-bit probability distribution. Like a set of single qubit measurements on an entangled state, it returns a random bit-string, similarly it supplies this only once. There are significant fundamental differences between a classical sample and an entangled state, however, both can be considered as resources in an MBQC-like framework. In this paper we define *measurement-based classical computation* (MBCC) as a model of computation consisting of polling a single sample from a multi-bit probability distribution and performing classical post-processing on these bits. Furthermore, we restrict classical post-processing to the sub-class of computations utilised in cluster state MBQC [13], linear computations (generated by XOR and NOT-gates alone).

Two of us showed in [14] that, under this restriction, if an MBQC resource violates no Bell inequality then no non-linear

computation can be achieved. The computation is restricted to convex combinations of linear functions of the input bits. The expressiveness of MBCC (the types of computations it can perform), in which, as a classical model, no Bell inequality can be violated, is therefore limited in the same way. Can we then prove that MBCC can be simulated efficiently by a classical computer?

The resource in MBCC is a classical multi-bit probability distribution. Such distributions are of exponential size and include distributions unlikely to by efficiently realisable even by a quantum resources. We thus say that an n-bit distribution is *efficiently quantum preparable* when there exists a quantum circuit with a polynomial in n description, upon which the output of single qubit measurements can can prepare the distribution exactly. It follows that MBCC is equivalent to a quantum MBQC where all measurements are non-adaptive and of fixed basis.

In this paper, we give strong evidence that MBCC with an efficiently preparable resource can be computationally non-classical. More precisely we show that:

Theorem 1. *There exist uniform families of MBCC computations with efficiently quantum preparable resources which cannot be efficiently exactly simulated via a standard classical computing device unless the polynomial hierarchy collapses to the third level.*

By standard classical computing device we mean a classical Turing machine whose sole random element is a supply of uniformly random bits. This is a probabilistic Turing machine, and is used to define complexity classes BPP and PP. MBCC is also a fully classical computational model, but crucially the multi-bit probability distribution may have an (efficient) non-classical preparation.

The Polynomial Hierarchy is a family of classes in computational complexity theory [15]. It is believed, although not proven, that this family of classes is distinct. Aaronson and Arkipov (AA) recently called this a "generic, foundational" assumption of computer science [4], and this has been used to provide strong evidence that universal quantum computers [5], and certain restricted sub-classes of quantum computers [6] and quantum processes [4] are hard to exactly simulate on a classical computer.

Hypothesis 1. The third level of the polynomial hierarchy is strictly smaller than at least one other level in the hierarchy.

Under the assumption of Hypothesis 1, Bremner, Jozsa and Shepherd (BJS) showed that uniform families of a very restricted family of quantum circuits, Instantaneous Quantum Polytime (IQP) circuits, could not be exactly efficiently simulated on a standard classical computer, where by simulate we mean that the classical devices outputs a sample from an identical distribution to the simulated quantum circuit (*weak simulation* in Jozsa and Van Den Nest's classification [16]).

Our technical results include a strengthening of BJS's result by introducing a new and much stricter uniformity condition defining uniform families of circuits which we call (IQP*). We show that IQP*circuits also cannot be classically simulated unless Hypothesis 1 is violated. We then show that

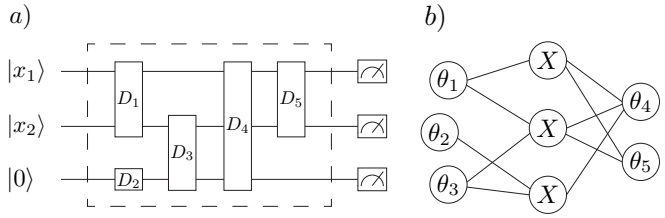

FIG. 1: a) Standard form of an IQP circuit, where each gate is diagonal in the Pauli-X basis and (x_1, x_2) is the two bit input string. All measurements are in the computational (Pauli-Z) basis. The boxed gates give the unitary D. b) A MBQC implementation of the circuit in a), where each circle represents a qubit prepared in the state $|+\rangle$ and edges between circles represent the application of a controlled-Z gate. The contents of the circles represent the basis in which the corresponding qubit is measured, where X represents the Pauli-X basis, and θ_j represents the basis $U_X(-\theta_j)ZU_X(\theta_j)$, where $U_X(\theta_j)$ is a rotation by θ_j about the Pauli-X axis. The angles θ_j are in one-to-one correspondence with the θ_z in the representation of D_j in Eq. (1). All of these measurements can be implemented simultaneously (non-adaptively) in MBQC.

IQP*circuits can be implemented in cluster-state MBQC using fixed-basis measurements. We thus demonstrate that the same computations can be implemented in MBCC, the classical analog of MBQC introduced above.

We begin by defining IQP (Instantaneous Quantum Polytime) circuits [17], introduced by BJS, which will play a central role in our argument.

Definition 1. An *IQP circuit* with classical input bit string x of size n acting on $q \geq n$ qubits consists of:

1. a quantum register prepared in the input state $|x\rangle|0\rangle^{\otimes q-n}$; and
2. the application of a unitary operator U to the register, where U is diagonal with respect to the eigenbasis of Pauli-X operators.

We denote the output of this computation, obtained via computational basis measurements on every qubit, by the q-bit string m, whose jth element $m_j \in \{0, 1\}$ is the outcome of the computational basis measurement on the jth qubit.

An example of an IQP circuit is illustrated in Fig. 1a. Such circuits are called *instantaneous* because D can be decomposed into a product of commuting gates, which can thus be applied in any order (or simultaneously) [17].

When studying the computational power of families of circuits, it is often useful to ensure that unreasonable computational power is not hidden in the description of the circuits themselves. This can be ensured via a *uniformity condition* which ensures that a description of each circuit in the family can be (classically) efficiently generated. While BJS introduce a uniformity condition in Ref. [6], we adopt a different one here, and we denote the set of uniform circuit families obtained under this condition by IQP*.

Definition 2. An IQP* circuit family is a family of IQP circuits, with input x and input size $n = |x|$, followed by computational basis measurements on every qubit, such that the

number of qubits q is polynomial in n, and where the unitary operator U_n (which has an explicit n-dependence) is a poly(n) product of gates of the form

$$D(\theta_z, z) = e^{i\theta_z X[z]}, \tag{1}$$

where each angle $\theta_z \in (0, 2\pi]$ has a description polynomial-size in n, z is a q-bit string, and we introduce the notation $X[z] = \bigotimes_j X^{z_j}$, where z_j is the jth bit of z. E.g. $D(\theta_{101}, 101) = \exp[i\theta_{101}(X \otimes \mathbb{1} \otimes X)]$.

In other words, the description of every member of an IQP* circuit family is a polynomial list L_n of q-bit strings z and corresponding angles θ_z. This list then defines the circuit for input size n. If we adopt the notational shorthand that $\theta_z = 0$ for all bit strings z not in L_n, then the unitary transformation for the circuit U_n is given by

$$U_n = \prod_{z \in Z_2^q} D(\theta_z, z). \tag{2}$$

Operators of this form have a useful symmetry in their matrix elements, which we will exploit below, namely,

$$\langle w \oplus y | D_n | w \rangle = \langle y | D_n | 0 \rangle \tag{3}$$

for all bit strings w and y, with $|0\rangle \equiv |0\rangle^{\otimes q}$ and where $\oplus$ represents a bit-wise sum modulo 2.

This is different from the uniformity condition introduced by BJS [6] in some significant ways. Most importantly, BJS' uniformity condition allows the circuit to depend on individual values of input string x, rather than (the more common choice of) the length of x. This means that the circuit construction itself can play a very siginificant role in the computation, for example evaluating an arbitrary polynomial-sized classical circuit. In contrast, due to their much weaker "pre-computation" stage, IQP* circuit families cannot even achieve a single non-linear logic Boolean function, such as AND. Lemma 1 is thus a considerable strengthening of the theorems in [6].

Lemma 1. *The output probability distributions generated by IQP* circuit families cannot be efficiently and exactly simulated on a standard classical computing device unless Hypothesis 1 is false.*

The full proof of Lemma 1 is presented in Appendix B. The technical definition of a classical computing device is provided in Appendix A along with other useful notions from computational complexity theory. To summarize the proof for readers familiar with Ref. [6], under postselection of measurement outcomes of a subset of qubits, the families of IQP* circuits can be mapped to general quantum circuits satisfying the standard uniformity condition for the complexity class BQP. We then utilize a similar proof technique to Ref. [6].

As in Ref. [6], Lemma 1 may be generalized to include multiplicative error up to a certain factor on the individual probabilities. However, we shall not consider such multiplicative error here. We discuss the issue of approximate simulations and finite numbers of samples at the end of this paper. Lemma 1 presents strong evidence that IQP* circuit families may not be efficiently and exactly simulated on a classical computer.

Before proceeding to our main result, we note a related phenomenon in Corollary 1, namely that there exist efficiently-preparable families of quantum states for whom the statistics of computational basis measurements are unlikely to be efficiently and exactly simulated on a classical computer.

Definition 3. An IQP* *zero-input state family* is the set of quantum states created by an IQP* circuit family, when the input is set to the all zeros string $0 \ldots 0$.

Corollary 1. *The statistics of computational basis measurements on* IQP* *zero-input state families cannot be efficiently and exactly simulated on a standard classical computer unless Hypothesis 1 is false.*

Proof. We use a special property of IQP circuits, namely that the output statistics of an IQP circuit with input x, defined according to Definition 1, may be realized by the same IQP circuit acting on the n-bit all-zeros string by performing some simple extra post-processing of the output bits of the measurements.

Observe that the probability that the measurement output string is a bit string m given input x is

$$\begin{aligned} \text{Prob.}(m|x) &= |\langle m | D_n | \bar{x} \rangle|^2, \\ &= |\langle m \oplus \bar{x} | D_n | 0 \rangle|^2, \\ &= \text{Prob.}(m \oplus \bar{x}|0), \end{aligned} \tag{4}$$

where $\bar{x}$ is x appended by $q - n$ zeros and we obtained the second line from Eq. (3).

Thus identical output statistics to an IQP circuit given input x can be obtained via the same circuit with input 0 and post-processing of the output bit string m to string $m \oplus \bar{x}$. This post-processing comprises at most n bit-flips and can be (trivially) efficiently performed on a classical device. From this, the corollary follows directly from Lemma 1. □

Corollary 1 is an important preface to our main result, and captures many of its features. Note that the subject of the corollary is a classical probability distribution. Even though the distribution is *classical*, its statistics have inherited the (likely) hardness of exact simulation of the IQP**quantum* circuit families.

We now turn to MBQC (and then MBCC) implementations of IQP*circuit families. We show the general result that any MBQC which can be achieved using measurements in a fixed basis can be achieved in MBCC (though possibly requiring a resource state that cannot be efficiently generated classically).

IQP circuits have a special form in MBQC, first derived in [18] and illustrated in Fig. 1. We will show below that IQP*families also have the property that they can be achieved in MBQC with a non-adaptive fixed measurement basis.

Lemma 2. For every instance of MBQC on an n-qubit resource, where every measurement basis is fixed, there is a corresponding instance of MBCC with an n-bit resource, whose output statistics simulate it exactly.

The proof of Lemma 2 follows immediately from the fact that the statistics of any projective measurement upon a quantum state relies solely on matrix elements which are diagonal with respect to the measured basis. Given the state, a fully dephasing channel in this eigenbasis may be applied, which sets all off-diagonal elements to zero. This channel will not change the statistics of the measurement which follows but outputs a state which is separable and discord-free [19]. Measurements on a separable and discord-free quantum state define a multi-bit probability distribution. MBCC utilising a sample of this distribution will exactly simulate an instance of the MBQC.

The final step in the proof of Theorem 1 is to show that IQP*circuits can be implemented in MBQC with fixed measurements.

Lemma 3. Given a member of an IQP*circuit family, there is an efficient implementation in MBQC whose measurements are fixed and non-adaptive.

Proof. From Eq. (4), we can place all of the dependence on x into classical post-processing. For convenience, we insert $H^2 = \mathbb{1}$ between every state, unitary and measurement in an IQP*circuit to change the input state from $|0\rangle^{\otimes q}$ to $|+\rangle^{\otimes q}$, the final measurements into Pauli-X measurements and to make all gates diagonal in the Pauli-Z basis (rather than the Pauli-X basis). Then, noting that $CZ^2 = \mathbb{1}$, where CZ is the controlled-phase gate, we can add CZ gates after each input state, so that the IQP*circuit is equivalent to preparing a cluster state, applying gates that are diagonal in the Pauli-Z basis and then measuring in the Pauli-X basis.

In [18], it is shown that any unitary gate of the form

$$D_z(\theta_z, z) = e^{i\theta_z Z[z]}, \tag{5}$$

where $Z[z] = \bigotimes_j Z^{z_j}$ and z_j is the jth bit of z, can be achieved in MBQC with simultaneous measurements, and with byproduct operators which are a tensor product of Z and $\mathbb{1}$. Since the byproduct operators commute with the logical gates (5), they can be applied at the end of the computation and measurements do not need to be adaptive. Therefore all the gates in an IQP*circuit can be implemented in MBQC without adaptivity. □

Combining Lemma 2 with Lemma 3 implies that IQP*circuit families can be realized in MBCC, with a resource distribution which is efficiently quantum preparable. Together with Lemma 1 this proves Theorem 1.

Discussion. What is the relationship between MBCC and MBQC - its fully quantum counterpart? From one perspective, MBCC can be seen as a special case of MBQC, since dephased states are a sub-set of quantum states. In both models the classical side-processing is of secondary importance (and of weak computational power) and the driver of the computation is the correlations in the measurement outcomes.

In other aspects the two models are strikingly different. In response to an early pre-print of this present work, Rieffel and Howard introduce criteria which divides MBQC instances into *superficial* and *inherently measurement based* [10]. Using their criteria, MBCC would be superficially measurement-based. We agree that MBCC is of an intrinsically different nature to universal MBQC. It is thus all the more remarkable that it exhibits non-classical computational attributes.

Can we identify further instances of MBCC which achieve hierarchy collapse, or other evidence of non-classical computation? Rieffel and Howard [10] note that the output distribution of Shor's algorithm might be of this category, since it is very likely that Shor's algorithm cannot be efficiently simulated by a classical computing device. However, such a distribution is very different to those considered above. Firstly, the simplicity of this distribution (peaked at integer multiples of the inverse order r^{-1}) means that post-selection is unlikely to enable strong computations that collapse the polynomial hierarchy. Second, given a single piece of classical information, (the order r), the Shor algorithm distribution can be efficiently classically generated [23] – whereas no equivalent simulation method is known for IQP*output distributions. Finally, a single instance of Shor's algorithm has a fixed input whereas a single distribution allows for IQP*computations via MBCC on any input bitstring (of a particular length). We emphasise that the dependence on input for IQP*is simple (due to equation 4) it is far from trivial under post-selection, enabling highly non-trivial computations on that input.

Conclusions. Theorem 1 gives strong evidence that MBCC cannot be simulated efficiently on a gate-model classical computer whose sole randomness source is a supply of uniformly random bits. The MBCC model can exploit the correlations in probability distributions to achieve non-classical computation. This seems paradoxical, since MBCC is described in fully classical terms. The resolution of this apparent paradox is that this probability distribution can be created by quantum means. From a computational perspective, any family of distributions which do not have an efficient classical implementation have a non-classical character. For a probability distribution, the key marker of non-classicality is typically the violation of a Bell inequality. MBCC reminds us that distributions which violate no Bell inequality may still possess a non-classical character.

From the perspective of quantum information, these results have direct implications for MBQC. They provide a concise argument that adaptive measurement is necessary for universal MBQC (otherwise MBQC and MBCC would be equivalent), and demonstrate that, in spite of this, adaptive measurement is not required for the model to exhibit characteristics of non-classical computation.

Does this work have experimental relevance? Can one *verify* that the desired probability distribution has been produced? This question has been considered for boson sampling [4, 21] and needs to be addressed in our future work. However, for a small-scale demonstration experiment a convincing verification procedure would be to implement the post-selection and confirm a non-trivial computation. Another important issue associated with experimental realizations is that of approximation. While the approximation model (multiplicative errors on individual probabilities) considered in Ref. [6] can be immediately applied here, it does not provide an analysis of the most physically relevant error model, namely, additive error on the whole probability distribution. We note that AA [4] have made progress in this direction.

The relationship between entanglement and quantum computational speed-up has been debated since the early days of quantum computing theory. These results emphasize the intricacies of this question. They illustrate that the quantum speed up in Shor's algorithm is of a qualitatively different character to the hardness of the sampling distributions in this paper, and show that even an ostensibly fully classical model, such as MBCC, can have a quantum computational character if its resource distribution is quantum mechanically generated. The relationship between quantum computational power and correlations appears even more subtle than previously thought.

Acknowledgements—We thank Jonathan Oppenheim, Richard Jozsa, Fernando Brandão for insightful comments, Eleanor Rieffel and Howard Wiseman for stimulating correspondence and Jens Eisert and Michael Bremner for helpful discussions. MJH acknowledges funding from CHIST ERA (DIQIP), JJW was supported by the IARPA MQCO program and by the ARC via EQuS project number CE11001013, HA and NU are funded by the EPSRC, RR acknowledges support from NSERC, MITACS and Cifar and DEB is supported by the Leverhulme Trust.

[1] P. Shor, *SIAM Rev.* **41**, 303 (1999).
[2] M. Van den Nest, Quant. Inf. Comp. **11**, 784 (2011).
[3] R. Jozsa and N. Linden, *Proc. R. Soc. A* **459**, 2011 (2003).
[4] S. Aaronson and A. Arkhipov, *Proc. of ACM STOC*, 333-342, (2011).
[5] B. M. Terhal and D. P. DiVincenzo, *Quantum Information and Computation* **4**, 2, 134 (2004).
[6] M. J. Bremner, R. Jozsa, and D. J. Shepherd, *Proc. R. Soc. A* **467**, 459 (2011).
[7] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
[8] H.J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
[9] M. Van Den Nest, *et al*, Phys. Rev. Lett. 97, 150504 (2006).
[10] E. G. Rieffel, H. M. Wiseman, arXiv:1307.1083 (2013).
[11] J. Anders and D. E. Browne, *Phys. Rev. Lett.* **102**, 050502 (2009).
[12] R. Raussendorf, Phys. Rev. A 88, 022322 (2013).
[13] R. Raussendorf, D. E. Browne and H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
[14] M. J. Hoban and D. E. Browne, *Phys. Rev. Lett.* **107**, 120402 (2011).
[15] C.H. Papadimitriou, *Computational Complexity*, Addison Wesley, Boston (1993).
[16] R. Jozsa and M. Van Den Nest, arXiv:1305.6190v1.
[17] D. J. Shepherd and M. J. Bremner, *Proc. R. Soc. A* **465**, 1413 (2009).
[18] D. E. Browne and H. J. Briegel, *Lectures on Quantum Information, D. Bruß, G. Leuchs (Ed.)*, Wiley-VCH, Berlin, 359 (2006).
[19] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, *Rev. Mod. Phys.* **84**, 1655 (2012).
[20] S. Aaronson, *Proc. R. Soc. A* **461**, 3473 (2005).
[21] C. Gogolin, M. Kliesch, L. Aolita and J. Eisert, arXiv:1306.3995 (2013).
[22] M. A. Broome et al, *Science* **339**, 794 (2013); M. Tillmann et al, *Nature Photonics* **7**, 540 (2013); J. B. Spring et al, *Science* **339**, 798 (2013); A. Crespi et al, *Nature Photonics* **7**, 545 (2013).
[23] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

Appendix A: Some computational complexity definitions

It is important that we define what we mean by "classical computing devices". By this expression we include general probabilistic processes since quantum circuits will, in general, not give deterministic outcomes and we want to simulate the statistics of quantum circuits. We follow [6] in making the following definition (where Boolean circuits are defined in [15]):

Definition 4. A **standard classical computing device** takes an input $x \in \{0,1\}^n$ of size n and produces a bit string $y \in \{0,1\}^s$ of size s by performing the following operations:

1. Flip r_1 fair coins to produce a random bit string $z \in \{0,1\}^{r_1}$ of size r_1 where we make the assignment "heads" to 0 and "tails" to 1;
2. Prepare the bit string $x' = (x, \tilde{0}, z)$ where $\tilde{0}$ is the bit string of size r_2 with all elements equal to 0; and
3. Apply a Boolean circuit B_n that takes bit string x' of size $n + r_1 + r_2$ as an input and outputs the bit string $y \in \{0,1\}^s$ of size s, where the description of B_n is generated in poly(n) by a classical Turing Machine.

All variables n, s, r_1, r_2 are positive integers. If the computational resources of this device are polynomial in n then i.e. $s = \text{poly}(n)$, $r_1 = \text{poly}(n)$, and $r_2 = \text{poly}(n)$.

There is a classical computational complexity class associated with these devices if the computational resources they use are polynomial in n, and this is the class of decision problems known as BPP. Since these classical computing devices involve nondeterministic processes, the correct answer to a decision problem may not be obtained deterministically; there is a probability of giving the wrong answer. A problem is in BPP if this error probability is less than or equal to some constant $c < 1/2$. A related and potentially larger complexity class of probabilistic classical computations is PP where the error probability is bounded from above by $1/2$ but may not be a constant, i.e. can depend on the input size n. This last class will also be important in later discussion.

Similar to BJS [6] and AA [4], our proof makes use of complexity classes defined using *post-selection*. Post-selection cannot be achieved deterministically in a physical realization, but is an extremely useful technical concept. Post-selection is the act of demanding that the outcome of a quantum measurement is a fixed value, and that the state of the system then evolves via a fixed projector and a renormalization. Aaronson introduced the class POSTBQP, which, loosely speaking, represents the problems solvable on a quantum computer given polynomial resources if we were given the extra power of post-selecting measurement outcomes. BJS introduced the complexity class POSTIQP, which applies a similar treatment to their uniform IQP circuits.

The formal definitions of the classes POSTBQP, POSTIQP and POSTIQP* are as follows.

Definition 5. A **BQP circuit family** $\{C_n : n \in \mathbb{N}\}$ is a set of quantum circuits such that for each input bit string x of size $n \in \mathbb{N}$, C_n is a quantum circuit acting on $q = \text{poly}(n)$ qubits (initiated in the state $|x\rangle|0\rangle^{\otimes q-n}$) with a sequence of gates chosen from the universal gate set $\{CZ, H, Z, P\}$ which has a description generated in poly(n) time by a classical Turing Machine.

Here CZ is the controlled-Z gate, H is the Hadamard gate, Z is the Pauli-Z gate and $P = e^{i\frac{\pi}{8}Z}$. We now define the aforementioned complexity classes under post-selection utilizing the definitions above and following the work of Aaronson in [20].

Definition 6. A language $L \subseteq \{0,1\}^*$ is in POSTBQP iff there exists a BQP circuit family $\{C_n | n \in \mathbb{N}\}$ such that for all inputs $x \in \{0,1\}^n$:

1. after C_n is applied to the state $|x\rangle|0\rangle|0\rangle...|0\rangle$, there is a non-zero probability that a qubits (excluding the last qubit) at the end of the circuit are in the state $|0\rangle^{\otimes a}$ for $a = poly(n)$;
2. if $x \in L$ and these a qubits are in the state $|0\rangle^{\otimes a}$, the last qubit when measured in the computational basis is $|1\rangle$ with probability $\geq 2/3$;
3. if $x \notin L$ and these a qubits are in the state $|0\rangle^{\otimes a}$, the last qubit when measured in the computational basis is $|1\rangle$ with probability $\leq 1/3$;

where the last qubit is the bottom qubit line in a quantum circuit diagram such as in Fig. 1. These are postselected circuits because we postselect on a number of qubits all being in the state $|0\rangle$, and then accept the outcome of a measurement on the last qubit. Therefore, the set of qubits upon which we postselect never includes the last qubit.

To define POSTIQP, BJS use a near identical definition, replacing "a BQP circuit family" with their definition of "a uniform IQP circuit family" in Definition 6. Similarly, we define POSTIQP* by replacing, "a BQP circuit family" in this definition by "an IQP* circuit family".

Appendix B: Proof of Lemma 1

In this section we provide a proof of Lemma 1. This section utilizes some of the technical concepts defined in Appendix A. To prove Lemma 1 we use the arguments presented in [6].

One of the key lemmas which underpin BJS's main result (see Corollary 3.3 in [6]) is the complexity class equation:

Lemma 4. POSTIQP = POSTBQP = PP

where POSTIQP, POSTBQP and PP are defined in Appendix A and in [6]. The right-hand equation is due to Aaronson [20].

To prove Lemma 1, we need to show that:

Lemma 5. POSTIQP*=POSTBQP=PP.

Lemma 1 then follows directly from all other steps of the proof of Corollary 3.3 in [6]. We shall not reproduce those steps of the proof here.

In order to prove POSTIQP* = POSTBQP, it is necessary to prove that POSTIQP* $\subseteq$ POSTBQP and that POSTBQP $\subseteq$ POSTIQP*. It is clear that the former is true. To prove the latter, recall that any BQP circuit can be expressed in the formalism of MBQC [13]. The physical realization of any BQP circuit family in MBQC comprises the generation of a graph state of sufficient size and appropriate structure, followed by adaptive single-qubit measurements in the bases X, Y and $(X \pm Y)/\sqrt{2}$.

Graph state generation comprises:

1. preparation of a set of qubits in state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$; and
2. implementation of CZ gates between certain qubits.

The measurements can be implemented by rotating about the Z axis by 0, $\pi/4$, $-\pi/4$ or $\pi/2$ followed by a measurement in the X basis.

The sequence of measurements corresponds to the chosen BQP circuit. Notice that from Definition 6 the initial state and the gates depend on n and not the specific value of x. The dependence on x is introduced by having measurements of the following form (via a simple application of gate identities in [13]): there are n qubits that each correspond to each element x_j of x, and if $x_j = 0$ we make the measurement in the X basis, and if $x_j = 1$ then we implement a π-rotation about the Z axis and measure in the X basis. Since the rotation commutes with the CZ gates, it can be incorporated into the preparation of that qubit by preparing $|+\rangle$ if $x_j = 0$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ otherwise. For the rest of the qubits in the graph state, the rotation about the Z axis and measurement in the X basis is only defined by size n, the size of x.

If we could post-select on measurement outcomes in MBQC then we remove the need for adaptive measurements—computations are accepted only if certain outcomes occur. We now show that non-adaptive computations in MBQC are instances of IQP* circuits. This can be easily shown if one writes out the computation in MBQC as a quantum circuit, and for all qubits after preparation of states $|+\rangle$ and $|-\rangle$ and before measurements in the X basis two Hadamard gates are applied, yielding exactly the same circuit. The action of a Hadamard on these state preparations gives the mapping $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_j}|1\rangle) \to |x_j\rangle$. In a computation in MBQC all unitaries prior to measurement are diagonal in the Z basis, so the action of a Hadamard on every qubit prior to and after these unitaries maps these unitaries diagonal in the Z basis to unitaries that are diagonal in the X basis; those unitaries that appear in IQP* circuits. Finally the action of a Hadamard prior to measurement in the X basis results in a measurement in the computational basis. In Fig. 2 we give an example of this equivalence between MBQC circuits without adaptivity and IQP circuits.

Therefore, under the action of post-selection MBQC computations are instances of IQP* circuits. To complete the proof of Lemma 1 we insert Lemma 5 into the proofs of Theorem 3.2 in [6] and Corollary 3.3 in [6].

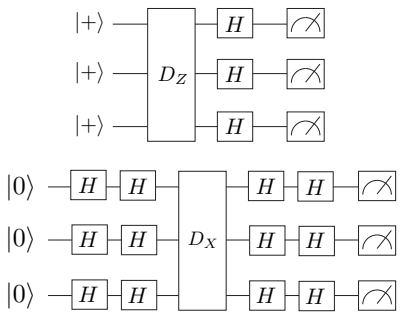

FIG. 2: The top circuit where D_Z is a unitary that is diagonal in the Pauli-Z basis is equal to the bottom circuit where D_X is a unitary that is diagonal in the Pauli-X basis. The top circuit is of the form of a circuit in MBQC but without adaptivity. Since $H \cdot H = \mathbb{1}$ we immediately see that the bottom circuit is an example of an IQP circuit.