Are Random Pure States Useful for Quantum Computation?

Michael J. Bremner,[1] Caterina Mora,[2] and Andreas Winter[3,4]

[1]*Department of Computer Science, University of Bristol, Bristol BS8 1UB, United Kingdom**
[2]*Institute for Quantum Computation, University of Waterloo, 200 University Avenue W. N2L 3G1, Canada*
[3]*Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*
[4]*Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, 117542 Singapore*

(Received 21 January 2009; published 11 May 2009)

We show the following: a randomly chosen pure state as a resource for measurement-based quantum computation is—with overwhelming probability—of no greater help to a polynomially bounded classical control computer, than a string of random bits. Thus, unlike the familiar "cluster states," the computing power of a classical control device is not increased from P to BQP (bounded-error, quantum polynomial time), but only to BPP (bounded-error, probabilistic polynomial time). The same holds if the task is to sample from a distribution rather than to perform a bounded-error computation. Furthermore, we show that our results can be extended to states with significantly less entanglement than random states.

DOI: 10.1103/PhysRevLett.102.190502 PACS numbers: 03.67.Lx, 03.67.Ac, 89.70.Eg

In measurement-based (or "one-way") quantum computation, two very different resources are used: one is a multiqubit state $|\Psi\rangle$; the other is a classical algorithm used to determine how to measure the qubits, in which order and in which local basis [1]. This clear separation of quantum and classical resources gives rise to the question: Which combinations of quantum states and classical control algorithms yield an advantage over classical computation?

In this Letter, we show that the efficiency requirements on classical processing of measurement data in measurement-based models severely limits the class of quantum states which offer a computational speedup over classical computers. In particular, we demonstrate that the set of languages that can be decided by randomly chosen pure states together with polynomial-sized classical control circuits is the same (with high probability) as the set of languages that could be decided by polynomial-sized classical circuits and classical randomness alone [that is BPP (bounded-error, probabilistic polynomial time)]. Our intuition is that random pure states simply have too many uncorrelated parameters to allow for a computational speedup over classical processors. In support of this intuition, we extend our main theorem to cover states which do not share the entanglement properties of typical states.

Much of the literature has focused on identifying particular states, or classes of states, for which universal quantum computation can be performed by utilizing a small set of single-qubit measurements and a simple classical control algorithm. This is generally done by recognizing certain "nice" properties of a state which allow measurement outcomes to be interpreted as having applied a quantum gate to some predefined input state.

One can take a constructive approach, such as in [2,3] where the authors use techniques for the classical simulation of quantum systems to find simple rules that describe the effects of certain measurements. These rules apply to a wide range of entangled states and can be used to show that a large variety of systems can support measurement-based quantum computation. From a more physical perspective, other work has considered how ground or thermal states of natural systems can be used for measurement-based quantum computation [4–6].

Alternatively, one can identify general physical requirements that must be satisfied in order for it to be universal for quantum computation [7,8]. In these papers, the authors demonstrate that if the amount of entanglement in a family of states does not grow sufficiently quickly with the number of qubits, then there is no deterministic LOCC (local operations and classical communication) protocol that can prepare a family of cluster states.

The line of thinking in our paper is more in the vein of [9] where the authors examine how classical control computers of varying computational power are boosted by the addition quantum resources. For instance, they demonstrate GHZ (Greenberger-Horne-Zeilinger) states enhance classical control devices which are only capable of calculating parities to BPP.

Very recently Gross, Flammia, and Eisert [10] have also shown, like in the current Letter, that random states (in fact, *highly entangled* states) cannot be used for universal measurement-based quantum computation. They demonstrate this by proving that for certain problems in BQP (bounded-error, quantum polynomial time) which are thought to not be in BPP, highly entangled states offer no advantage over classical randomness even given an oracle which supplies the "best" set of single-qubit measurements to be performed.

Abstract measurement-based computation model.—We begin our analysis by defining the following general model of computation—one which seems to capture all computationally efficient possibilities of using measurements on a quantum state to drive a computation. See [11] for a formal exposition.

© 2009 The American Physical Society

Definition 1 A model of abstract measurement-based quantum computation (AMBQC) consists, for each n measuring the input length, of a pairs $(|\Psi\rangle, C)$, where $|\Psi_n\rangle$ is a state on q qubits, and C is a classical circuit on w bits and having at most v logical gates (each of which may involve up to 3 bits). In practice, we ask for q, v, and w to be polynomially bounded in n, but it will turn out that it is enough to require that they are not "too big."

The purpose of the circuit C is twofold: First, during the computation, it acts as a control which determines, based on the input string x and previously generated measurement outcomes $m_1, \ldots, m_k$ on qubits $\ell_1, \ldots, \ell_k$, which qubit ℓ_{k+1} to be measured next and with which measurement POVM (positive operator valued measure) $(L_\mu^{(\alpha)})_\mu$. Second, at the end of the computation ($k = q$), to determine the output $y \in \{0, 1\}$ as a function of x and the $m_1, \ldots, m_q$, $\ell_1, \ldots, \ell_q$. The probability that $y = 1$ over all histories (i.e., the probability that the computation accepts) is denoted $C_x(\Psi)$.

Note that our state $|\Psi\rangle$ has q qubits, and exactly q measurements are made. We shall from now on implicitly restrict to AMBQCs $(|\Psi\rangle, C)$ in which all histories end up measuring all q qubits (or equivalently, there is no actually occurring history where some qubit is measured twice). An AMBQC obeying this condition we call *complete*; it is naturally fulfilled in all known specific models.

We say that $(|\Psi\rangle, C) = (|\Psi_n\rangle, C_n)$ computes a (partial) function f: $\{0, 1\}^n \rightarrow \{0, 1\}$ with bounded error, if

$$f(x) = 1 \Rightarrow C_x(\Psi) \geq 2/3, \qquad f(x) = 0 \Rightarrow C_x(\Psi) \leq 1/3.$$

Note that, even though in practice this will be an important restriction, we impose no uniformity on the C_n, nor on the states $|\Psi_n\rangle$.

If we are interested in collective properties of all AMBQCs with all possible inputs (as we shall be shortly), we may even disregard the n-bit input x, as a slightly longer control circuit starting off in the all-zero input can first prepare the input x and then do the actual computation described above.

These two points mean that we shall actually only look at particular finite sized n, q, v, and w.

Random states are not universal.—As promised, the question we want to address is whether a generic (i.e., randomly chosen) state $|\Psi\rangle$ is of any good use to an AMBQC? The way we think of this is a little different from the usual MBQC, where the resource state can typically be prepared easily in a quantum computer—since random states have enormous time complexity to prepare in a quantum computer [12] we think of $|\Psi\rangle$ as being handed to us by an all-powerful, Merlinesque character. Since we are similarly not even able to study a description of the state (as it is too long to read in time polynomial in n [12]), we cannot be expected to come up with the control circuit C on our own. Instead, it is described to us by a helpful Merlin, too, giving us the control circuit C that best exploits the properties of $|\Psi\rangle$.

In simple terms, our main result states that for a typical random state, there is *no* short control circuit that can do anything with $|\Psi\rangle$ which cannot be simulated to sufficient precision using classical random bits.

Theorem 2 For a random state $|\Psi\rangle$ on n qubits, consider classical Boolean control circuits C of width w and having at most v gates, let $C(\Psi)$ be the probability of acceptance of the AMBQC $(|\Psi\rangle, C)$, and similarly $C(2^{-q}\mathbb{1})$ the probability of acceptance when instead of Ψ the maximally mixed state $2^{-q}\mathbb{1}$ is used. Then, for any $\epsilon > 0$,

$$\Pr{}_\Psi\{\exists C|C(\Psi) - C(2^{-q}\mathbb{1})| > \epsilon\} \leq (8^8 w)^{3v} e^{-c\epsilon^2 2^q}, \quad (1)$$

where $c = \frac{1}{9\pi^3}$ is a universal constant. (Observe that the existential quantifier implicitly restricts to complete AMBQCs.)

So, whenever $v \ln w = o(2^q)$—e.g., for all polynomially bounded circuits—the right-hand side of Eq. (1) goes to zero exponentially, and hence for most states, the measurement results coming from Ψ can be replaced by classical independent randomness: this changing the acceptance probability by at most ϵ, regardless of the circuit used.

Proof For a given two-outcome POVM with operators $P \geq 0$ and $Q = \mathbb{1} - P \geq 0$ acting on $(\mathbb{C}^2)^{\otimes q}$, a straightforward application of Levy's Lemma [13] yields

$$\Pr{}_\Psi\{|\langle\Psi|P|\Psi\rangle - 2^{-q}\,\mathrm{Tr}P| > \epsilon\} \leq 4e^{-c\epsilon^2 2^q}, \quad (2)$$

where $c = \frac{1}{9\pi^3}$. The reason is that for any $0 \leq P \leq \mathbb{1}$, the function $|\Psi\rangle \mapsto \langle\Psi|P|\Psi\rangle$ has Lipschitz constant 1.

Now, observe that every control circuit effectively describes such a two-outcome POVM: the circuit starts making measurements on the system, and for each sequence of previous outcomes decides on the next measurement; at the end, the complete data obtained—the sequence $\ell = \ell_1 \ldots \ell_q$ of qubits measured, the local measurements $\alpha = \alpha_1 \ldots \alpha_q$ and the outcomes $m = m_1 \ldots m_q$—is used to decide acceptance or rejection. Thus, we find the accepting and rejecting operators,

$$P = \sum_{\substack{(\ell,\alpha,m)\\ \text{acc.history}}} \bigotimes_{k=1}^{q} (L_{m_k}^{(\alpha_k)})^{\ell_k},$$

and $Q = \mathbb{1} - P$. In this way, clearly, $C(\Psi) = \langle\Psi|P|\Psi\rangle$.

The number of possible circuits to consider is at most $[8^8\binom{w}{3}]^v \leq \frac{1}{6}(8^8 w)^{3v}$, so we put together Eq. (2) with the union bound to obtain Eq. (1), observing the simple equation $C(2^{-q}\mathbb{1}) = 2^{-q}\,\mathrm{Tr}P$.

Finally, we have to explain why the latter probability can be sampled efficiently classically. But that is straightforward, since the maximally mixed state $2^{-q}\mathbb{1}$ is a tensor product of single-qubit maximally mixed states $\frac{1}{2}\mathbb{1}$, so indeed each measurement result of a local POVM $(L_\mu)_\mu$ may be sampled independently with probability $\frac{1}{2}\,\mathrm{Tr}L_\mu$ for outcome μ, which can be done efficiently thanks to the classical description of the POVM.

Remark.— For traditional MBQC, the local measurements are simply von Neumann measurements, i.e., consisting of two orthogonal basis projectors. In that case, the measurement outcomes are simply replaced by independent random bits.

It is clear that the above can be generalized without any difficulty to qudits as elementary systems. Equivalently, models that consider measurements on bounded-sized sets of qubits could also be considered.

Note furthermore that the step-by-step simulation above produces a probability distribution over the same computational histories as the original AMBQC. We do not claim, however, that these two distributions are close (which is not true in general), but only that the efficient coarse grainings represented by the output bit y are.

Sampling of a t-bit string.—If the object of the computation is to produce a sample from distribution on, say, t-bit strings, we denote by $C(\Psi)$ the resulting distribution. If $t \ll q$, we can apply Levy's Lemma to all 2^t probability values of $C(\Psi)$—and in a generalization of Theorem 2 we can show via the same counting argument as in Theorem 2, enhanced by an additional union over all sample strings y, that

$$\Pr{}_{\Psi}\{\exists C \| C(\Psi) - C(2^{-q}\mathbb{1})\|_1 > \epsilon\} \leq 2^t(8^8 w)^{3v} e^{-c\epsilon^2 2^{q-2t}}, \tag{3}$$

where $c = \frac{1}{9\pi^3}$ is as before.

In other words, as long as $2^{2t} t v \ln w = o(2^q)$, it is exponentially unlikely for a random state to provide any advantage for AMBQC over a maximally mixed state. We note that this condition is typically fulfilled in "traditional" cluster state models, where both t and the depth of the quantum circuit are polynomial in the input size n, so q is a higher order polynomial in n than t.

Schmidt-rank-K states.—It is natural to wonder which exact property makes a random state so particularly useless for AMBQC. Two answers might come to mind: first, random states have, with high probability, almost maximal description complexity [12]. Another is that typical random states are highly entangled: indeed, Gross *et al.* [10] show that the geometric measure of entanglement on $q = q(n)$ qubits,

$$E_g(|\Psi\rangle) = -\log \max_{|\varphi\rangle = \bigotimes_j |\varphi^{(j)}\rangle} |\langle\varphi|\Psi\rangle|^2,$$

is with high probability $\geq q - 2\log q - O(1)$. Then they show (similar to our approach above) that in performing a computation with only one-sided and bounded error, the measurement outcomes of such states may be replaced by independent random bits. The resulting probabilistic computation still has bounded, one-sided error.

This motivates the following definition and theorem.

Definition 3 (Random Schmidt-rank K states) Construct the following random state Ψ on $q = q(n)$ qubits, called *random Schmidt-rank K state*. We define its distribution by a sequence of random experiments: let

$$R := \sum_{j=1}^{K} |\psi_j^{(1)}\rangle\langle\psi_j^{(1)}| \otimes \cdots \otimes |\psi_j^{(q)}\rangle\langle\psi_j^{(q)}|, \tag{4}$$

where all the qK unit vectors $|\psi_j^{(\ell)}\rangle$ are chosen independently at random from any measure on the pure states of $\mathbb{C}^2$ such that $\mathbb{E}\psi_j^{(\ell)} = \frac{1}{2}\mathbb{1}$. Now pick a unit vector $|\Psi_0\rangle$ from the support of R according to the unitary invariant measure, and finally let

$$|\Psi\rangle = \frac{1}{\sqrt{\langle\Psi_0|R|\Psi_0\rangle}}\sqrt{R}|\Psi_0\rangle. \tag{5}$$

Theorem 4 For a random Schmidt-rank K state $|\Psi\rangle$ on q qubits, with $64 \leq K \leq 2^q$ (which implies $q \geq 6$), consider classical Boolean control circuits C of width w and having at most v gates. Then, for any $\epsilon > 0$,

$$\Pr{}_{\Psi}\{\exists C|C(\Psi) - C(2^{-q}\mathbb{1})| > \epsilon\} \leq (2^q + (8^8 w)^{3v}) \times e^{-c'\epsilon^2 K^{1/3}}, \tag{6}$$

and where $c' = \frac{1}{1296\pi^3}$ is a universal constant.

In other words, whenever $q + v \ln w = o(K^{1/3})$—e.g. for all polynomially bounded circuits and superpolynomial K—the right-hand side of Eq. (4) goes to zero exponentially, and hence, for most Schmidt-rank K states, the measurement results coming from Ψ can be replaced by classical independent randomness: this changes the acceptance probability by at most ϵ, regardless of the circuit used.

To prove this, we shall use Levy's Lemma [13] once again, but we also need two further concentration results, which we only state, referring to [11] for proofs:

Lemma 5 For the random operator R in Eq. (4) such that $K \geq 4.2^k$ and $2 \leq k \leq q$,

$$\Pr{}_R\left\{\|R\|_\infty > 2\frac{K}{2^k}\right\} \leq 2^q e^{-K2^{-k}/3}.$$

Lemma 6 For the random operator R in Eq. (4), and $0 \leq P \leq \mathbb{1}$,

$$\Pr{}_R\left\{\left|\frac{1}{K}\mathrm{Tr}RP - \frac{1}{2^q}\mathrm{Tr}P\right| > \epsilon\right\} \leq 2e^{-2\epsilon^2 K}.$$

We are now ready for the *Proof of Theorem 4.* Picking the random state $|\Psi\rangle$, we have implicitly already constructed the operator R in Definition 3.

First, according to Lemma 5, and choosing $k = \lfloor\frac{2}{3} \times \log K\rfloor$, we get

$$\|R\|_\infty \leq 4K^{1/3}, \tag{7}$$

except with probability $\leq 2^q e^{-K^{1/3}/3}$.

Second, according to Lemma 6, we have for all measurement POVMs $(P, \mathbb{1} - P)$ constructed by the allowed classical control circuits [of which there are $M \leq \frac{1}{6}(8^8 w)^{3v}$—see the proof of Theorem 2,

$$\left|\frac{1}{K}\mathrm{Tr}RP - 2^{-q}\mathrm{Tr}P\right| \leq \epsilon, \tag{8}$$

except with probability $\leq 2Me^{-2\epsilon^2 K}$.

Third, assuming Eq. (7) holds for a particular R, application of Levy's Lemma [13] to the same POVM elements

P is possible, noting that the Lipschitz constant of the function $|\Psi_0\rangle \mapsto \mathrm{Tr}\sqrt{R}\Psi_0\sqrt{R}P$ is $\Lambda \leq 8K^{1/3}$. We find that for all these P,

$$\left|\mathrm{Tr}\sqrt{R}\Psi_0\sqrt{R}P - \frac{1}{K}\,\mathrm{Tr}RP\right| \leq \epsilon, \tag{9}$$

except with probability $\leq 4Me^{-c\epsilon^2K/\Lambda^2}$, with $c = \frac{1}{9\pi^3}$, as in Theorem 2. The special case $P = \mathbb{1}$ is trivially included:

$$|\mathrm{Tr}\sqrt{R}\Psi_0\sqrt{R} - 1| \leq \epsilon; \tag{10}$$

i.e., $\sqrt{R}|\Psi_0\rangle$ is already almost normalized.

Putting the three steps together, we find that if Eqs. (7)–(10) hold, then for all eligible control circuits,

$$|C(\Psi) - C(2^{-q}\mathbb{1})| \leq 3\epsilon.$$

As noted above, however, this will be the case except with probability bounded above by

$$2^q e^{-K^{1/3}/3} + 2Me^{-2\epsilon^2K} + 4Me^{-c\epsilon^2K/\Lambda^2}.$$

Redefining $\epsilon \mapsto \epsilon/3$ concludes the proof. □

It is intuitive (and not difficult to show) that with high probability, a random Schmidt-rank K state satisfies $E_g(|\Psi\rangle) \leq \log K + O(1)$, and since $|\Psi\rangle$ is always a superposition of K product states, also the descriptive (quantum Kolmogorov) complexity of the state is bounded by an exponential in K (this follows from a straightforward counting argument, cf. [12]). Hence, even these states, though failing the criterion of [10], are useless for AMBQC. We would like to say that this is due to the complexity of a random choice of pure state, but have to stress that it is not the descriptive complexity of [12]. Rather, it is the fact that all degrees of freedom given to the state are exhausted uniformly.

Note that the number of degrees of freedom sufficient for this is anything growing superpolynomially in n, if the control circuit and q are polynomially bounded. But it is also necessary, because if K is polynomial, then $|\Psi\rangle$ always has an efficient classical description, and so have all the states occurring through the course of the computation; in other words, the state is useless for AMBQC for another reason, as it is simulable in P.

Conclusion.—We have shown that for decision problems with bounded-error probability (and more generally for the task of approximately sampling a distribution on "few" bits), a generic quantum state is (with overwhelming probability) not more useful as a resource to a classical control mechanism for a generalized measurement-based model, than a random bit string. The only condition on the classical control is that it can be built as a Boolean circuit of subexponential depth. In other words, unless BQP = BPP, such states will not yield universal quantum computation when used in any reasonable environment controlling the sequence of measurements. However, the result is not limited to BQP, it also encompasses promise problems, as long as the AMBQC is supposed to be polynomially efficient and has bounded error; furthermore, the complexity may essentially be anything strictly smaller than exponential. (Observe that an exponential classical control could simulate the whole state, so its power is also not increased by having access to $|\Psi\rangle$.)

Finally, even decidedly "nonrandom" states (in the sense that their distribution is not unitary invariant) still have the same property if only they are drawn from a large enough manifold, as we have demonstrated with random states of bounded Schmidt rank.

We acknowledge insightful and interesting discussions with David Gross, Steve Flammia, and Jens Eisert; we also thank Ashley Montanaro for important suggestions. M. B. and A. W. are supported by the EC-FP6-STREP network QICS. C. M. acknowledges support by the IQC, QuantumWorks NSERC Innovation Platform, and Ontario Centres of Excellence. A. W. is supported by the U.K. EPSRC through the "QIP IRC," by the Royal Society, and by the European Commission through IP "QAP." The Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

*michael.bremner@bris.ac.uk

[1] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001); R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).

[2] D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007); D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, Phys. Rev. A **76**, 052315 (2007).

[3] D. Gross and J. Eisert, arXiv:0810.2542.

[4] S. D. Barrett, S. D. Bartlett, A. C. Doherty, D. Jennings, and T. Rudolph, arXiv:0807.4797.

[5] G. K. Brennen and A. Miyake, Phys. Rev. Lett. **101**, 010502 (2008).

[6] A. C. Doherty and S. D. Bartlett, arXiv:0802.4314.

[7] M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel, Phys. Rev. Lett. **97**, 150504 (2006).

[8] M. Van den Nest, W. Dür, A. Miyake, and H. J. Briegel, New J. Phys. **9**, 204 (2007).

[9] J. Anders and D. E. Browne, Phys. Rev. Lett. **102**, 050502 (2009).

[10] D. Gross, S. Flammia, and J. Eisert, preceding Letter, Phys. Rev. Lett. **102**, 190501 (2009).

[11] M. Bremner, C. E. Mora, and A. Winter, arXiv:0812.3001.

[12] C. E. Mora and H. J. Briegel, Phys. Rev. Lett. **95**, 200503 (2005); C. E. Mora, H. J. Briegel, and B. Kraus, arXiv: quant-ph/0610109.

[13] V. D. Milman and G. Schechtman, *Asymptotic Theory of Finite Dimensional Normed Spaces* (Springer Verlag, Berlin, New York, 1986) (With an Appendix by M. Gromov), LNM 1200.