Most Quantum States Are Too Entangled To Be Useful As Computational Resources

D. Gross,[1] S. T. Flammia,[2] and J. Eisert[3,4]

[1]*Institut für Mathematische Physik, Technische Universität Braunschweig, 38106 Braunschweig, Germany*
[2]*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5 Canada*
[3]*Physics Department, University of Potsdam, 14469 Potsdam, Germany*
[4]*Institute for Mathematical Sciences, Imperial College London, London SW7 2PE, United Kingdom*

(Received 7 January 2009; published 11 May 2009)

It is often argued that entanglement is at the root of the speedup for quantum compared to classical computation, and that one needs a sufficient amount of entanglement for this speedup to be manifest. In measurement-based quantum computing, the need for a highly entangled initial state is particularly obvious. Defying this intuition, we show that quantum states can be too entangled to be useful for the purpose of computation, in that high values of the geometric measure of entanglement preclude states from offering a universal quantum computational speedup. We prove that this phenomenon occurs for a dramatic majority of all states: the fraction of useful n-qubit pure states is less than $\exp(-n^2)$. This work highlights a new aspect of the role entanglement plays for quantum computational speedups.

DOI: 10.1103/PhysRevLett.102.190501 PACS numbers: 03.67.Lx, 03.65.Ta, 03.65.Ud, 03.67.Ac

A classical computer endowed with the power to perform measurements on certain entangled many-body states is strongly believed to be exponentially more powerful than a classical machine alone. Indeed, a computer having access to local measurements on a cluster state [1–3] or the class of states identified in Refs. [4–8] can efficiently simulate any quantum computation. The best-known classical algorithm for this task requires superpolynomial run time, and it is strongly believed that no substantial improvement is possible. It is in this sense that certain many-body states possess strong computational power. More precisely, the particular states mentioned above are computationally universal in that they enable a classical machine to efficiently solve any problem in the complexity class BQP [9].

The key question that we ask in this work is: How common is the property of offering universal computational speedups and what is the role of entanglement in this context? All previous results which rule out computational universality of certain quantum systems seem to do so by either (i) showing that the systems are not entangled enough to support a universal quantum calculation [10–14] or (ii) relying on stringent symmetries [15–17]. It is therefore reasonable to conjecture, by extrapolating from the current lines of research, that in generic situations ‘‘more entanglement’’ will imply ‘‘more computational power.’’

Going further, it has been realized (using sundry techniques known under the label of the ‘‘probabilistic method’’ or the ‘‘concentration of measure phenomenon’’ [18,19]), that generic quantum states are extremely highly entangled from many points of view [20–22]. For example, a typical state is almost maximally entangled with respect to any partition of its systems into two parties. It follows that most states are excellent resources for some quantum information protocols, e.g., teleportation with respect to *any* bipartition. Thus, it is plausible to suspect that offering a computational speedup is a generic feature of quantum states, if only advanced enough classical control schemes could be devised to utilize their power.

Main result.—The arguments presented above turn out to be fallacies. In a first step, we will show that families of states with a high degree of geometric entanglement [23–25] cannot be universal. Recall that the geometric measure of entanglement $E_g(\Psi)$ is defined as

$$E_g(|\Psi\rangle) = -\log_2 \sup_{\alpha\in\mathcal{P}} |\langle\alpha|\Psi\rangle|^2,$$

where the supremum is taken over the set of all product states, $\mathcal{P}$. For the purpose of this Letter, we will always quantify entanglement by means of E_g. In a second step, we proceed to demonstrate that our criterion for large entanglement is fulfilled by typical quantum states with overwhelming probability: they are too entangled to be useful in this sense.

The proof involves substituting the quantum resource by a fair coin. In that sense, we show that even if one has complete knowledge about the state used and is capable of designing the most sophisticated measurement scheme specifically tailored to that state, the distribution of the measurement outcomes is not sufficiently different from that of a random string to afford a universal speedup. This observation is the basis for related results made independently in Ref. [26].

Intuitively, the strategy of proof in the first step is as follows: one realizes that a high value of E_g implies that every particular outcome in a local measurement scheme has low probability of occurring. Therefore—irrespective of the measurement strategy used—the distribution of outcomes will be ‘‘very random’’; so random indeed that one may sample from it efficiently using purely classical means.

To outline the proof in more detail: We assume that a classical computer assisted by local measurements on a highly entangled state can efficiently identify both the solution to a problem F in NP [27], and a certificate for the solution. Under this assumption, we construct a purely classical algorithm accomplishing the same task. Hence, highly entangled states cannot cause a significant speedup for these particular problems. For concreteness, one may think of F as the paradigmatic FACTORING problem: given an integer N and an interval $[k, l]$, decide whether N has a factor contained in $[k, l]$. A certificate for the solution is provided by the prime decomposition of N. Since there is an efficient quantum algorithm identifying the prime decomposition [28], it follows that highly entangled states cannot be universal (unless FACTORING is in P, which is generally believed to be highly unlikely).

Theorem 1 (Uselessness of quantum states).—Let $|\Psi_n\rangle$ be an n qubit state with geometric measure of entanglement $E_g(|\Psi_n\rangle) > n - \delta$. Consider a classical computer augmented by the power to perform local measurements on $|\Psi_n\rangle$. Assume this joint system is capable of finding and certifying a solution to an NP problem F after t time steps, with probability of success at least $1/2$. Then there exists a purely classical algorithm which identifies a solution to F after $C(n)2^{\delta+1}\ln(1/p_f)$ time steps with probability of success at least $1 - p_f$. Here, $C(n)$ is the time it takes to verify the certificate on a classical computer.

Note that C is a polynomial function of n (this being the defining property of NP problems). The theorem implies that a family of states $|\Psi_n\rangle$ cannot provide a superpolynomial speedup whenever their geometric measure is of the form $E_g(|\Psi_n\rangle) = n - O(\log_2(n))$. *A priori*, it is unclear that states with such an extreme geometric entanglement exist at all. It turns out that not only do they exist, but that this property is shared by the vast majority of all many-body states.

Theorem 2 (Almost all states are useless).—The fraction of state vectors on $n \geq 11$ qubits with geometric measure of entanglement less than $n - 2\log_2(n) - 3$ is smaller than e^{-n^2}.

It immediately follows that the fraction of universal resources among n qubit pure states is less than e^{-n^2}.

To prove Theorem 1, we assume that the classical part of the algorithm is deterministic, which does not restrict generality, since any probabilistic parts may be implemented by using quantum measurements as coins. In the course of the calculation, the computer will perform up to n local single-qubit projective measurements with two outcomes each, obtaining one of 2^n possible sequences of outcomes. There is a set G of "good" outcomes, which will cause the computer to output a valid solution to the problem F after $t \leq n$ time steps. By assumption, the probability of obtaining an outcome from G is larger than $1/2$. Each element of G is labeled by a product state $|\alpha\rangle$ corresponding to the local measurement outcomes. The probability of the event associated with $|\alpha\rangle$ to occur is $|\langle\alpha|\Psi\rangle|^2 \leq 2^{-E_g(|\Psi\rangle)} \leq 2^{-n+\delta}$. Hence,

$$1/2 \leq \mathrm{Prob}(G) \leq |G|2^{-n+\delta} \Rightarrow |G| \geq 2^{n-\delta-1}.$$

Thus, the ratio of good outcomes to the total number obeys

$$|G|/2^n \geq 2^{-\delta-1}. \tag{1}$$

To simulate the procedure on a classical computer, use the following algorithm: Instead of performing a physical measurement, choose the outcome of the measurements randomly using a fair coin, to generate a random string. This string is fed into the same classical postprocessing algorithm as before. If the random string causes the classical part of the computation to output a result after t time steps, check whether it solves the problem F. The problem being in NP, this is efficiently possible. If the result is valid, output it and abort. Otherwise, repeat the procedure with another random string. The probability of not having obtained a valid outcome after k trials is bounded above by $(1 - 2^{-\delta-1})^k < e^{-k2^{-\delta-1}}$, using Eq. (1) of the cardinality of the set of "good" outcomes. Set $k = 2^{\delta+1}\ln(1/p_f)$ to achieve a probability of failure smaller than p_f. The claim of Theorem 1 is now immediate. □

The proof of Theorem 2 requires two technical ingredients. The first is a concentration of measure result: Let $|\Phi\rangle$ be a normalized vector in $\mathbb{C}^d$, and let $|\Psi\rangle$ be drawn from the unit sphere according to Haar measure. Then,

$$\mathrm{Prob}\{|\langle\Phi|\Psi\rangle|^2 \geq \varepsilon\} < \exp[-(2d-1)\varepsilon]. \tag{2}$$

This statement follows easily from standard bounds to be found, e.g., in Refs. [29,30]. Second, we require the concept of an ε-net [18,20,21]. An ε-net $\mathcal{N}_{\varepsilon,k}$ on the set $\mathcal{P}$ of product states on k qubits is a set of vectors such that

$$\sup_{\alpha\in\mathcal{P}} \inf_{\tilde{\alpha}\in\mathcal{N}_{\varepsilon,k}} \| |\alpha\rangle - |\tilde{\alpha}\rangle \| < \varepsilon/2. \tag{3}$$

We claim such a net exists whose cardinality is bounded by $|\mathcal{N}_{\varepsilon,k}| \leq (5k/\varepsilon)^{4k}$. Indeed, from Ref. [20], we know that there is an (ε/k)-net $\mathcal{M}$ on the space of single qubit state vectors, where $|\mathcal{M}| \leq (5k/\varepsilon)^4$. Set $\mathcal{N}_{\varepsilon,k} = \{|\tilde{\alpha}_1\rangle \otimes \ldots \otimes |\tilde{\alpha}_k\rangle : |\tilde{\alpha}_i\rangle \in \mathcal{M}\}$. Now let $|\alpha\rangle = \bigotimes_i^k |\alpha_i\rangle$ be a product vector. By definition of $\mathcal{M}$, for every i, there exists $|\tilde{\alpha}_i\rangle \in \mathcal{M}$, such that $|\langle\alpha_i|\tilde{\alpha}_i\rangle|^2 \geq 1 - \varepsilon^2/4k$. Hence, for $|\tilde{\alpha}\rangle = \bigotimes_i |\tilde{\alpha}_i\rangle$,

$$|\langle\alpha|\tilde{\alpha}\rangle|^2 \geq \left(1 - \frac{\varepsilon^2}{4k}\right)^k \geq 1 - \frac{\varepsilon^2}{4},$$

which implies Eq. (3) [20].

Proceeding to prove Theorem 2, we let $\varepsilon = 2^{-l}$ for some yet-to-be-determined number l. Let $\mathcal{N}_{\varepsilon,n}$ be as above. Employing the standard union bound, we find

$$\mathrm{Prob}\{\sup_{|\tilde{\alpha}\rangle\in\mathcal{N}_{\varepsilon,n}} |\langle\tilde{\alpha}|\Psi\rangle|^2 \geq 2^{-l}\} < \exp[-(2^{n+1}-1)2^{-l}]|\mathcal{N}_{\varepsilon,n}|$$

$$< \exp(-2^{n-l} + 2nl) \tag{4}$$

$$< \exp(-2^{n-l} + 2n^2) \tag{5}$$

where the estimate (4) is valid if $2nl[1 - \ln(2)] > 4\ln(5n)$. Choosing $l = n - \log_2(3n^2)$, the condition above is satisfied when $n \geq 11$. Further, Eq. (5) becomes $\exp(-n^2)$. Now let $|\alpha\rangle$ be a general product vector and $|\tilde{\alpha}\rangle$ be the closest element in the ε-net. Then, using the operator norm $\|.\|_\infty$,

$$\begin{aligned} \left||\langle\alpha|\Psi\rangle|^2 - |\langle\tilde{\alpha}|\Psi\rangle|^2\right| &= |\mathrm{tr}[(|\alpha\rangle\langle\alpha| - |\tilde{\alpha}\rangle\langle\tilde{\alpha}|)|\Psi\rangle\langle\Psi|]| \\ &\leq \||\alpha\rangle\langle\alpha| - |\tilde{\alpha}\rangle\langle\tilde{\alpha}|\|_\infty \\ &\leq \||\alpha\rangle\langle\alpha| - |\tilde{\alpha}\rangle\langle\tilde{\alpha}|\|_1 \leq \varepsilon = 2^{-l}. \end{aligned}$$

Here, we have used that for the trace norm $\|.\|_1$, $\||\alpha\rangle \times \langle\alpha| - |\tilde{\alpha}\rangle\langle\tilde{\alpha}|\|_1 \leq 2\||\alpha\rangle - |\tilde{\alpha}\rangle\|$ (see, e.g., Ref. [20]). It follows that $\sup_{\alpha\in\mathcal{P}}|\langle\alpha|\Psi\rangle|^2 \leq 2^{-l+1} < 2^{-n+2\log_2(n)+3}$ with probability greater than $1 - e^{-n^2}$. □

CQ universality and POSTBQP.—References [7,10] introduced a more stringent benchmark for universal resource states. The authors ascribe the quality of "*CQ* universality" to a resource state if—up to local unitary corrections—any pure state on k qubits can be prepared out of a sufficiently large $n > k$ qubit resource by means of local measurements on the remaining $n - k$ sites. As has been shown in Ref. [4,5], efficient *CQ* universality is a strictly stronger requirement than the notion of universality used in the present Letter. Hence, the results presented above already imply that generic states are not *CQ*-universal. However, we can strengthen the statement: Most states fail to be *CQ*-universal, even if we assume we had the power to *choose* the local measurement outcomes.

To put this into perspective, recall that models of quantum computing with the assumed capability of choosing the outcome of at least one measurement have been analyzed under the label of *post-selected* quantum computing [31]. The complexity class of decision problems efficiently decidable on post-selected computers is POSTBQP. It is known [31] that PostBQP $= PP \supseteq NP$—which implies that the capability to postselect dramatically increases the computational strength of quantum computers (unless $PP \subseteq$ BQP).

For generic states in the *CQ*-setting, however, postselection does not seem to help. Indeed, the dramatic majority of states are not efficiently *CQ*-universal, even if we (i) assume the power to choose the outcome of the local measurements, (ii) allow for any fixed error ε in the output fidelity, (iii) ask only for the capability to prepare a single product state, and (iv) make no *a priori* assumption on which sites the final state should end up in.

We proceed to prove the claim. Fix a subset K of k sites (the "output register") of a given n-qubit resource state $|\Psi\rangle$. Combining Lemma III.5 in Ref. [21] with Theorem 2 above, we find that for a random resource $|\Psi\rangle$ and fixed $\varepsilon > 0$,

$$\sup_{\alpha,\beta} \ln\frac{|(\langle\alpha| \otimes \langle\beta|)|\Psi\rangle|^2}{\|\langle\beta|\Psi\rangle\|^2} < 2\ln n - k - \ln(1-\varepsilon) + 3$$

with probability at least $1 - e^{-n^2} + e^{-c2^k\varepsilon^2}$. The supremum is over product states $|\alpha\rangle$ on K and $|\beta\rangle$ on K^C. There are fewer than n^k choices for $K \subset \{1, \ldots, n\}$ of cardinality k. Hence, the preceding bound is true for all such K simultaneously with probability no smaller than $1 - (e^{-n^2+k\ln n} + e^{-c2^k\varepsilon^2+k\ln n})$. The claim follows by taking $n \to \infty$ and $n = \mathrm{poly}(k)$.

Efficiently preparable states and concrete examples.—While conceptually relevant, generic Haar-random states on large systems cannot be efficiently prepared. In this section, we demonstrate that the effect that "too much entanglement" impedes computational efficiency can also be identified in more physically relevant states.

First, we exhibit a family of efficiently preparable states $|\Phi_n\rangle$ on n qubits, for which $\lim_{n\to\infty} E_g(|\Phi_n\rangle)/n = 1$. These values of the geometric measure are high enough to rule out the possibility that such families offer an exponential speedup for the kind of problems considered above. Constructing explicit states which cannot cause even a superpolynomial increase in computational power remains an open problem. Fix a dimension d and choose a unitary $U \in U(\mathbb{C}^d)$. Define $V:\mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^d$ by $V|\beta\rangle = U|0\rangle \otimes |\beta\rangle$. For every k, we construct the state $|\Phi_k\rangle$ on $n = 2^k$ qudits by concatenating the maps V in a treelike fashion as shown in Fig. 1. Now set $d = \mathrm{poly}(k)$ and choose $U_k \in U(\mathbb{C}^d)$ randomly for every k. Recall that, by the Solovay-Kitaev theorem [32], general unitaries in $U(\mathbb{C}^m)$ can be efficiently approximated by a quantum circuit in a time polynomial in m and polylogarithmic in the error. Employing once more standard concentration of measure arguments [21], one easily finds that

$$\lim_{k\to\infty} \sup_{\alpha_1,\alpha_2,\beta} |\langle\alpha_1, \alpha_2|V_k|\beta\rangle|^2 = 1/d(k).$$

Thus, $V_k^\dagger$ maps any product state $|\alpha_1\rangle \otimes |\alpha_2\rangle$ to a vector $|\beta\rangle$ with $\||\beta\rangle\|^2 \leq 1/d(k)$ (asymptotically). It follows that the lowest layer of $V^\dagger$'s in the definition of $|\Phi_k\rangle$ sends any unit-norm product vector on n qudits to a product vector on $n/2$ qudits, with squared norm at most $d(k)^{-n/2}$. Inducting over all layers and using the appropriate base-d logarithm in the definition of geometric measure, we conclude

$$\lim_{k\to\infty} \frac{-1}{n(k)} \log_{d(k)} \sup_{\alpha\in\mathcal{P}} |\langle\alpha|\Phi_k\rangle|^2 = \sum_{i=1}^{\infty} 2^{-i} = 1.$$

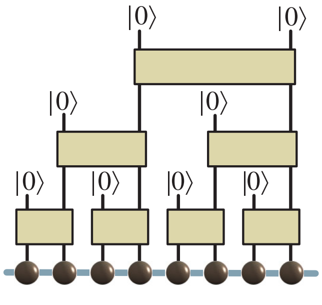

FIG. 1 (color online). The tree-tensor network [11,13,34] that gives rise to states with high geometric entanglement. Each of the boxes represents a unitary.

Turning to the CQ setting, it is easy to identify states whose efficiency as a resource is limited by the presence of correlations which can, on average, not be removed by means of local measurements. Consider the ground state $|\Psi\rangle$ of a *critical model* with two-point correlation functions between the sites j, k fulfilling $\langle\Psi|M_j \otimes M_k|\Psi\rangle - \langle\Psi|M_j|\Psi\rangle\langle\Psi|M_k|\Psi\rangle > f[\mathrm{dist}(j, k)]$, with $f(x) = 1/\mathrm{poly}(x)$. Assume we could prepare a three-qubit cluster state $|Cl_3\rangle\langle Cl_3|$ on some "output register." We allow for local unitary corrections and an average trace-norm error of ε so that with $\sigma = p_l U_j^{(l)} \otimes U_i^{(l)} \otimes U_k^{(l)}|Cl_3\rangle\langle Cl_3|(U_j^{(l)} \otimes U_i^{(l)} \otimes U_k^{(l)})^\dagger$, it holds that $\|\mathrm{tr}_{\setminus\{j,i,k\}}(|\Psi\rangle\langle\Psi|) - \sigma\|_1 \leq \varepsilon$. Here, p_l is the probability of obtaining a certain sequence of measurement outcomes. Noting that the qubits associated with sites j, k are uncorrelated for $|Cl_3\rangle$, one easily derives that the size of the resource must scale as $O[f^{-1}(\varepsilon)]$. This observation complements the results of Ref. [7], where different arguments for the fact that critical ground states may not be well-suited as CQ resources were presented.

Summary and outlook.—We have shown that entanglement for universal resource states must "come in the right dose." Future work should aim to identify a greater variety of physically relevant states exhibiting the phenomenon of being "too entangled." For example, it would be interesting to quantify to which degree output states of random, polynomially sized quantum circuits are subject to this effect. Also, the results underscore the importance of systematically understanding relevant classes of the few states that are in fact universal. This work highlights the quite intriguing role entanglement plays in quantum computing: As with most good things, it is best consumed in moderation.

The authors thank M. Bremner, C. Mora, and A. Winter for discussions. D. G. and J. E. were supported by the EU (COMPAS, CORNER, QAP), the EPSRC, EURYI, and Microsoft Research; S. T. F. by the Perimeter Institute for Theoretical Physics. Research at Perimeter is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research & Innovation.

[1] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001); R. Raussendorf and H. J. Briegel, Quantum Inf. Comput. **6**, 443 (2002); P. Walther *et al.*, Nature (London) **434**, 169 (2005).

[2] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004); R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003); D. Schlingemann and R. F. Werner, Phys. Rev. A **65**, 012308 (2001).

[3] S. Popescu, Phys. Rev. Lett. **99**, 250501 (2007).

[4] D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).

[5] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, Phys. Rev. A **76**, 052315 (2007).

[6] D. Gross and J. Eisert, arxiv:0810.2542.

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

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

[9] BQP is the set of decision problems solvable by a polynomial-sized uniform quantum circuit with bounded error probability.

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

[11] M. Van den Nest, W. Dür, G. Vidal, and H. J. Briegel, Phys. Rev. A **75**, 012337 (2007).

[12] G. Vidal, Phys. Rev. Lett. **98**, 070201 (2007).

[13] I. L. Markov and Y. Shi, SIAM J. Comput. **38**, 963 (2008).

[14] M. Fannes, B. Nachtergaele, and R. F. Werner, Commun. Math. Phys. **144**, 443 (1992).

[15] D. Gottesman, Ph.D. thesis, CalTech, 1997.

[16] S. Clark, R. Jozsa, and N. Linden, arXiv:quant-ph/0701103.

[17] R. Jozsa and A. Miyake, Proc. R. Soc. A **464**, 3089 (2008).

[18] V. D. Milman and G. Schechtman, *Asymptotic Theory of Finite-Dimensional Normed Spaces* (Springer, New York, 1986).

[19] N. Alon and J. H. Spencer, *The Probabilistic Method* (Wiley-Interscience, New York, 2000).

[20] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).

[21] P. Hayden, D. W. Leung, and A. Winter, Commun. Math. Phys. **265**, 95 (2006).

[22] E. Lubkin, J. Math. Phys. (N.Y.) **19**, 1028 (1978); D. N. Page, Phys. Rev. Lett. **71**, 1291 (1993); S. K. Foong and S. Kanno, *ibid.* **72**, 1148 (1994).

[23] A. Shimony, Ann. N.Y. Acad. Sci. **755**, 675 (1995).

[24] H. Barnum and N. Linden, J. Phys. A **34**, 6787 (2001).

[25] T.-C. Wei and P. M. Goldbart, Phys. Rev. A **68**, 042307 (2003).

[26] M. Bremner, C. Mora, and A. Winter, following Letter, Phys. Rev. Lett. **102**, 190502 (2009).

[27] O. Goldreich, *Computational Complexity* (Cambridge University Press, Cambridge, 2008).

[28] P. Shor, SIAM J. Comput. **26**, 1484 (1997).

[29] F. Hiai and D. Petz, "The Semicircle Law, Free Random Variables and Entropy," Mathematical Surveys and Monographs 77, Amer. Math. Soc., 2000 (to be published).

[30] D. Petz and J. Reffy, arXiv:math/0310338.

[31] S. Aaronson, Proc. R. Soc. A **461**, 3473 (2005).

[32] C. M. Dawson and M. A. Nielsen, Quantum Inf. Comput. **6**, 81 (2006).

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

[34] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).