Universal Quantum Computation with Little Entanglement

Maarten Van den Nest

Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, D-85748 Garching, Germany

(Received 11 July 2012; published 7 February 2013)

We show that universal quantum computation can be achieved in the standard pure-state circuit model while the entanglement entropy of every bipartition is small in each step of the computation. The entanglement entropy required for large-scale quantum computation even tends to zero. Moreover we show that the same conclusion applies to many entanglement measures commonly used in the literature. This includes e.g., the geometric measure, localizable entanglement, multipartite concurrence, squashed entanglement, witness-based measures, and more generally any entanglement measure which is continuous in a certain natural sense. These results demonstrate that many entanglement measures are unsuitable tools to assess the power of quantum computers.

DOI: 10.1103/PhysRevLett.110.060504 PACS numbers: 03.67.Ac, 03.65.Ud, 03.67.Lx

Introduction.—Quantum computers are believed to offer exponential computational advantages over classical computers. Understanding the essential features of quantum physics accounting for this increased power is a fundamental but largely unsolved problem. Perhaps the most natural candidate to which to attribute the power of quantum computers is entanglement [1]. Indeed entanglement has proved to be an essential resource in quantum information processing tasks such as teleportation [2], entanglement-based cryptography [3], and dense coding [4]. It is therefore natural to expect that entanglement plays an important role in quantum computation as well. However, in spite of significant insights [5–18], the question of whether entanglement will provide an understanding of quantum computing power in any decisive way (and if so, in which form) is to date unresolved.

In this Letter we investigate how much entanglement must be generated if a quantum computation is to achieve an exponential speed up (see also Refs. [8,9,13–17]). We focus on quantum computations operating on pure states. This setting is important when studying the power of quantum algorithms, because the latter are usually formulated in a pure-state framework. Perhaps contrary to common intuition, we will show that, throughout any quantum algorithm, states can remain slightly entangled without significantly compromising the efficiency of the computation. The result is proved for a major family of entanglement measures. It applies in particular to the fundamental measure of bipartite pure-state entanglement i.e., the entanglement entropy. More precisely, we show that classically simulating pure-state quantum circuits where the entanglement entropy of every bipartition is at most $O(\delta)$ at all times is as hard as classically simulating arbitrary i.e., universal quantum circuits. Here δ can be any parameter which scales inverse polynomially with the number of qubits n, say $\delta = 1/n$ or $\delta = 1/n^{1000}$. Note that such δ even tend to zero in the thermodynamic limit.

To prove the result, we show that a pure-state quantum computer restricted to operate within a small environment around the unentangled state $|0\rangle^n$ still has universal computational power (see Fig. 1). Because the entanglement entropy is continuous and equal to zero on product states, its value will be small for any state in such an environment. As continuity is the key quantity used in the argument, the result is by no means limited to the entanglement entropy. A fully analogous conclusion applies to every entanglement measure which is continuous in a certain natural

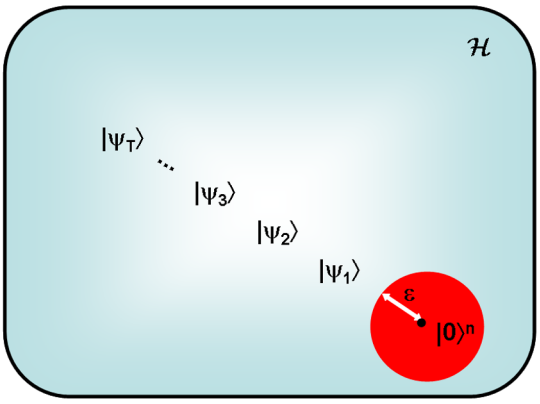

FIG. 1 (color online). Quantum computation in an ϵ neighborhood of $|0\rangle^n$. A quantum circuit composed of T gates starts with the input $|0\rangle^n$ and traces out some path $|0\rangle^n \to |\psi_1\rangle \to \cdots \to |\psi_T\rangle$ in the n-qubit Hilbert space $\mathcal{H}$. In principle the $|\psi_i\rangle$ may be highly entangled. Here we consider quantum computations QC_ϵ where the state of the computer is required to be ϵ close to $|0\rangle^n$ at all times. We show that a QC_ϵ still has universal quantum computing power, for any $\epsilon = 1/\mathrm{poly}(n)$. Every entanglement measure E which is sufficiently continuous will take on small values throughout the computation. Using this approach one shows that universal quantum computation is possible with vanishingly small amounts of entanglement; the argument applies to entanglement entropy and many other entanglement measures.

sense. This includes many commonly considered (bipartite and multipartite) measures.

These results demonstrate that the folklore intuition that ''weakly entangled pure quantum states represent little quantum computing power'' is in fact incorrect for a multitude of entanglement measures. This shows in particular that many entanglement measures are unsuitable tools to assess the power of quantum computers.

Quantum circuits and classical simulation.—We will consider the following (standard) pure-state quantum circuit model. The input is the n-qubit state $|0\rangle^n$ and circuits $\mathcal{C}$ consist of poly(n) elementary unitary gates acting on at most d qubits for some constant d. The computation is followed by a standard basis measurement on the first qubit. The complexity class BQP (bounded-error quantum polynomial time) represents all decision problems that are efficiently solvable on a quantum computer with bounded error probability.

We say that an n-qubit quantum circuit $\mathcal{C}$ can be simulated efficiently classically if there exists a polynomial-time classical algorithm with runtime poly(n, $1/\epsilon$) which allows us to estimate the probabilities $p(0)$ and $p(1)$ of measuring the outcome 0 and 1, respectively, up to error ϵ.

Entanglement and quantum computation.—Before proving our main results, we discuss some background related to the assertion that entanglement is a resource required for quantum computation.

First, it is important to recall that there is no unique way of quantifying how much entanglement is present in a many-body quantum system. There are infinitely many measures of entanglement [1,19] whose behavior may differ significantly, even qualitatively. In particular there exist scenarios where the same quantum state is found to be 'highly entangled' relative to one measure of entanglement whereas it is only 'slightly entangled' relative to another one (and indeed our results will provide a clear illustration of this). In short, *the* entanglement of a many-body quantum state does not exist.

Second, in the present context it is important to distinguish between pure- and mixed-state quantum computation. In the mixed state setting, several works have provided evidence that quantum computation operating with weakly entangled states is more powerful than classical computation [7,8,11,12]. This is essentially due to the fact that even nonentangled mixed states are nontrivial objects, being mixtures of potentially exponentially many separable pure states [8]. For quantum computations operating with pure states, the current view however seems to be different. Here it is often said that highly entangled quantum states must be generated if a quantum algorithm is to achieve an exponential speed up. This assertion is based on results such as those in Ref. [9] where this intuition is rigorously confirmed for one particular entanglement measure commonly used in the literature: the Schmidt rank. We briefly recall the result of Ref. [9], because an important point of the present work will be to contrast this result with various other entanglement measures. For a system of n qubits and a bipartition (A, B), denote $\chi^{A,B} = \log R^A$ where R^A is the Schmidt rank i.e., the rank of the reduced density operator of the qubits in A. Let χ be the maximal value of $\chi^{A,B}$ over all bipartitions. For any parameter γ, a quantum circuit where $\chi = O(\gamma)$ in every step of the computation will be called a (χ, γ) circuit. In Ref. [9] the following was proved [20]:

Theorem 1: Every $(\chi, \log n)$ quantum circuit operating on n qubits can be simulated efficiently classically.

Similar results have been proved for a few other entanglement measures. However they are also based on, or closely related to, the Schmidt rank [8,14–16].

Entanglement entropy.—In this Letter we demonstrate that for many commonly used entanglement measures we cannot hope for a result analogous to Theorem 1. This will hold in particular for the entanglement entropy. The entanglement entropy $E^{A,B}$ of an n-qubit state $|\psi\rangle$ for a bipartition (A, B) is given by the von Neumann entropy $S(\rho^A) = -\mathrm{Tr}\rho^A \log\rho^A$, where ρ^A is the reduced density operator of subsystem A. Let $\mathcal{E} = \max E^{A,B}$ denote the maximal entanglement entropy over all bipartitions. The notion of an $(\mathcal{E}, \gamma)$ quantum circuit is defined fully analogously to the (χ, γ) circuits considered above. A parameter δ is said to be polynomially small if $1/\delta = O(p(n))$ for some polynomial $p(n)$, where n is the number of qubits. We will show the following:

Observation 1: Consider any polynomially small δ. Then it is possible to efficiently solve every problem in BQP even when, throughout the entire computation, the entanglement entropy $\mathcal{E}$ is at most $O(\delta)$. Consequently, the task of classically simulating $(\mathcal{E}, \gamma)$ circuits is as hard as the task of simulating a universal quantum computer.

Note the very sharp contrast between Theorem 1 and Observation 1. In particular, whereas quantum circuits generating logarithmic amounts of Schmidt-rank entanglement can be simulated efficiently classically, δ amounts of entanglement entropy are generally as hard to simulate as universal quantum computation—note that δ tends to zero with growing n.

The proof of Observation 1 will be obtained by combining Steps 1 and 2 below. First, for any $\epsilon > 0$ the set $\mathcal{S}_\epsilon$ consists of all n-qubit states $|\psi\rangle$ which are ϵ close to $|0\rangle^n$ in trace distance. We denote by QC_ϵ a restricted quantum computer where only those quantum circuits are allowed for which the state of the n-qubit register belongs to $\mathcal{S}_\epsilon$ in each step of the computation.

Step 1: Consider any polynomially small ϵ. Having access to a QC_ϵ allows one to solve every problem in BQP in polynomial time. In particular, the task of classically simulating a QC_ϵ is as hard as the task of simulating a universal quantum computer.

This claim is proved as follows: Let $\mathcal{C}$ denote an arbitrary polynomial-size m-qubit quantum circuit composed

from a universal gate set (say CNOT gates, Hadamard gates, and $\frac{\pi}{8}$-phase gates). Suppose that $\mathcal{C}$ acts on the input $|0\rangle^m$ and is followed by measurement of the first qubit in the computational basis. Let p denote the probability of measuring 1. Then the following problem is well known to be BQP complete: given the promise that either $p \geq 2/3$ or $p \leq 1/3$, determine which of these possibilities is the case. Next we show that this BQP-complete problem can be solved efficiently by means of a transformed quantum circuit operating within the QC_ϵ model. The input of the new circuit is the n-qubit state $|0\rangle^n$ where $n := m + 1$. First a single-qubit rotation on qubit $m + 1$ is performed to generate the state

$$|0\rangle^m \otimes (\sqrt{1-\epsilon}|0\rangle + \sqrt{\epsilon}|1\rangle). \tag{1}$$

Then each gate G in the circuit $\mathcal{C}$ is applied controlled on qubit $m + 1$ being in the state $|1\rangle$ (i.e., we apply the operation which acts as $|\psi\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |0\rangle$ and $|\psi\rangle \otimes |1\rangle \rightarrow G|\psi\rangle \otimes |1\rangle$). Letting $\mathcal{C}_t$ denote the product of the first t gates in $\mathcal{C}$, it follows that after t gates, the quantum register is in the state

$$|\psi_t\rangle = \sqrt{1-\epsilon}|0\rangle^m \otimes |0\rangle + \sqrt{\epsilon}\mathcal{C}_t|0\rangle^m \otimes |1\rangle. \tag{2}$$

After all gates have been applied, a standard basis measurement on the first qubit is performed. The probability q of measuring 1 is given by $q = \epsilon p$. Repeating the computation $\mathrm{poly}(n)$ times allows us to estimate q with an accuracy of $1/\mathrm{poly}(n)$. Because ϵ is polynomially small, this allows one to determine in polynomial time whether $p \geq 2/3$ or $p \leq 1/3$. Finally, we remark that the overlap between $|\psi_t\rangle$ and $|0\rangle^n$ is $\sqrt{1-\epsilon}$ for every t. Therefore the entire computation operates within $\mathcal{S}_{\bar{\epsilon}}$ with $\bar{\epsilon} = \sqrt{\epsilon}$ (see the Supplemental Material [21]). The result now readily follows.

Step 2: Given any polynomially small δ, there exists a suitable polynomially small ϵ such that $\mathcal{E} = O(\delta)$ for every state in $\mathcal{S}_\epsilon$.

To prove Step 2, consider an n-qubit state $|\psi\rangle$ in $\mathcal{S}_\epsilon$ where ϵ will be determined later. For a bipartition (A, B) of the qubits, let ρ^A and $|0\rangle^A$ denote the states obtained from $|\psi\rangle$ and $|0\rangle^n$, respectively, by tracing out all qubits in B. We now recall the following continuity property [22] of the von Neumann entropy S. Let ρ and σ be two arbitrary density operators on a d-dimensional Hilbert space and denote by T their trace distance. Then, as long as $T \leq 1/(2e)$, one has

$$|S(\rho) - S(\sigma)| \leq 2T\log_2(d) - 2T\log_2(2T). \tag{3}$$

Because $T(|\psi\rangle, |0\rangle^n) \leq \epsilon$ and because the trace distance is contractive, this implies that $T(\rho^A, |0\rangle^A) \leq \epsilon$. Using Eq. (3) and the fact that $|0\rangle^A$ has zero entropy, it follows that

$$E^{A,B}(|\psi\rangle) = S(\rho^A) \leq 2\epsilon|A| - 2\epsilon\log_2(2\epsilon), \tag{4}$$

for every $\epsilon \leq 1/(2e)$, where $|A|$ denotes the number of qubits in A. It follows that, given any polynomially small δ, there exists a suitable polynomially small ϵ such that $E^{A,B}(|\psi\rangle) = O(\delta)$. This proves Step 2.

Combining Steps 1 and 2 immediately yields the proof of Observation 1.

Continuous measures.—The only properties of the entanglement entropy used to prove Observation 1 are that (a) this function vanishes on the product state $|0\rangle^n$ and (b) it is sufficiently continuous, in the sense of Step 2. Such continuity is rather natural and thus exhibited by various other well known entanglement measures; this includes bipartite measures as well as various true multipartite measures. As a result, Observation 1 can readily be generalized (see the Supplemental Material [21]):

Observation 2: Consider any polynomially small δ. Then it is possible to efficiently solve every problem in BQP even when, throughout the entire computation, E is $O(\delta)$. Here E is any entanglement measure from the following list: (a) α-Renyi entropy for any $\alpha \geq 1$, (b) geometric measure [23], (c) relative entropy of entanglement [24], (d) squashed entanglement [25], (e) localizable entanglement of every qubit pair [26], (f) multipartite concurrence [27], and (g) n-Tangle [28]. Consequently, the task of classically simulating (E, δ) quantum circuits is as hard as the task of simulating a universal quantum computer.

The list of entanglement measures in Observation 2 can be made considerably longer. Whereas we will not attempt to make this list complete, it is interesting to note that analogous conclusions to Observation 2 can be reached in one go for generally defined families of measures. We give a sketch of the results; details are given in the Supplemental Material [21].

A first natural example is the family of distance measures, which have the form

$$D(|\psi\rangle) = \inf\{d(|\psi\rangle, \sigma)\colon \sigma \text{ is unentangled}\}. \tag{5}$$

Here $d(\cdot, \cdot)$ is some notion of distance and the minimization is either taken over all pure or mixed separable states σ, depending on the definition of D. Thus D measures the distance to the nearest unentangled state. Examples are the geometric measure and the relative entropy of entanglement. Clearly, any other distance measure can be added to Observation 2 as long as the measure d is sufficiently well behaved; that is, by choosing ϵ polynomially small one can ensure that the d distance between any $|\psi\rangle$ in $\mathcal{S}_\epsilon$ and $|0\rangle^n$ is at most δ.

A second example is the family of epsilon measures [29]. If E is an entanglement measure and $\epsilon > 0$ then the associated ϵ measure is defined as

$$E_\epsilon(|\psi\rangle) = \inf\{E(\rho)\colon \rho \text{ s.t.} T(|\psi\rangle, \rho) \leq \epsilon\}, \tag{6}$$

where ρ may generally be a mixed state and where $T(\cdot, \cdot)$ denotes the trace distance. Thus E_ϵ measures the minimal entanglement guaranteed to present in an ϵ ball around $|\psi\rangle$. This construction gives a technique to obtain a smooth function E_ϵ even when the original measure E is not [29]. Step 1 immediately implies that universal quantum

computation can be achieved with zero ϵ entanglement, for every underlying entanglement measure E and for every polynomially small ϵ. An interesting example is the Schmidt rank: universal quantum computation is possible with zero Schmidt rank ϵ measure for all bipartitions—note the sharp contrast with Theorem 1.

A third family regards measures related to polynomial functions in the entries of a state. Consider the quantities

$$\langle\psi|^{\otimes k} A |\psi\rangle^{\otimes k} \quad \text{and} \quad \langle\psi|^{\otimes k} A |\psi^*\rangle^{\otimes k}, \tag{7}$$

where $k = \text{poly}(n)$, where A is an nk-qubit operator, and where $|\psi^*\rangle$ denotes the complex conjugate of $|\psi\rangle$ in the standard basis. The quantities of Eq. (7) define polynomials in the coefficients of $|\psi\rangle$ and their complex conjugates. Several entanglement measures are given by expressions of the form of Eq. (7) or as simple functions thereof. Consider e.g., the multipartite concurrence and the n-tangle, as well as the general family of comb-based measures [30]. Another class related to Eq. (7) with $k = 1$ regards witness-based measures of the form

$$E_{\mathcal{C}}(|\psi\rangle) = \max\{0, -\max_{W\in\mathcal{C}} \langle\psi|W|\psi\rangle\}, \tag{8}$$

where $\mathcal{C}$ denotes a subfamily of entanglement witness operators [31]. Provided that the operator norm of A scales at most polynomially with the number of qubits, every quantity of the form of Eq. (7) is sufficiently continuous for our purposes. As a result, for a large class of entanglement measures based on such quantities a result similar to Observation 2 will hold. This is, e.g., the case for the multipartite concurrence, n-tangle, and witness-based measures $E_{\mathcal{C}}$ for which the operator norm of each $W \in \mathcal{C}$ scales at most polynomially with the system size.

Insufficiently continuous measures.—It is interesting to note that the continuity argument used to prove Observations 1 and 2 does not apply to the Schmidt rank: indeed the latter is a discrete measure. This is in nice agreement with Theorem 1 and clarifies the special nature of $(\chi, \log n)$ quantum circuits and their efficient classical simulation. Other measures of interest to which the continuity argument does not apply are the Renyi α entropies with $\alpha < 1$ (see the Supplemental Material [21]).

Concluding remarks.—An implication of our results is that many pure-state entanglement measures used in the literature give little information about the performance of (pure-state) quantum algorithms. What could be more appropriate tools to this end? Note that, whereas the entanglement entropy $\mathcal{E}$ (say) throughout a QC_ϵ computation will be polynomially small, the success probability π that the algorithm outputs the corrects result is polynomially small as well. However, it is likely that their ratio $\mathcal{E}/\pi$ will be large. The latter quantity could therefore be a better measure of quantum computing power than how much entanglement is actually present in the system.

I thank H. J. Briegel, I. Cirac, M. Christandl, D. Browne, W. Dür, G. Giedke, R. Jozsa, B. Kraus, M. Piani, R. Renner, G. Vidal, and T.-S. Wei for discussions.

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[5] R. Jozsa, in *The Geometric Universe*, edited by S. Huggett, L. Mason, K. P. Tod, S. T. Tsou, and N. Woodhouse (Oxford University, Oxford, 1998).
[6] D. Gottesman, in *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, MA, 1999), pp. 32–43.
[7] N. Linden and S. Popescu, Phys. Rev. Lett. **87**, 047901 (2001).
[8] R. Jozsa and N. Linden, Proc. R. Soc. A **459**, 2011 (2003).
[9] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
[10] R. Orus and J. I. Latorre, Phys. Rev. A **69**, 052308 (2004).
[11] E. Biham, G. Brassard, D. Kenigsberg, and T. Mor, Theor. Comput. Sci. **320**, 15 (2004).
[12] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).
[13] M. Van den Nest, A. Miyake, W. Dür, and H. Briegel, Phys. Rev. Lett. **97**, 150504 (2006).
[14] R. Jozsa, arXiv:quant-ph/0603163.
[15] M. Van den Nest, W. Dür, G. Vidal, and H. J. Briegel, Phys. Rev. A **75**, 012337 (2007).
[16] I. L. Markov and Y. Shi, SIAM J. Comput. **38**, 963 (2008).
[17] N. Yoran, arXiv:0802.1156.
[18] D. Gross, S. T. Flammia, and J. Eisert, Phys. Rev. Lett. **102**, 190501 (2009).
[19] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
[20] In Ref. [9] a stronger form of classical simulation was achieved than the one defined in the previous section. However here we adopt the latter because we will show that, even for this weaker form, no analogue of Theorem 1 can exist for many entanglement measures (unless BQP = BPP).
[21] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.110.060504 for technical details and mathematical proofs.
[22] M. Fannes, Commun. Math. Phys. **31**, 291 (1973).
[23] A. Shimony, Ann. N.Y. Acad. Sci. **755**, 675 (1995).
[24] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
[25] M. Christandl and A. Winter, J. Math. Phys. (N.Y.) **45**, 829 (2004).
[26] F. Verstraete, M.-A. Martin-Delgado, and J. I. Cirac, Phys. Rev. Lett. **92**, 087201 (2004).
[27] A. R. R. Carvalho, F. Mintert, and A. Buchleitner, Phys. Rev. Lett. **93**, 230501 (2004).
[28] A. Wong and N. Christensen, Phys. Rev. A **63**, 044301 (2001).
[29] M. Piani, C. Mora, and H. J. Briegel, New J. Phys. **10**, 083027 (2008).
[30] A. Osterloh and J. Siewert, Phys. Rev. A **72**, 012337 (2005).
[31] F. G. S. L. Brandao, Phys. Rev. A **72**, 022310 (2005).