Novel Schemes for Measurement-Based Quantum Computation

D. Gross and J. Eisert

Blackett Laboratory, Imperial College London, Prince Consort Road, London SW7 2BW, United Kingdom
Institute for Mathematical Sciences, Imperial College London, Exhibition Rd, London SW7 2BW, United Kingdom

(Received 2 November 2006; revised manuscript received 29 January 2007; published 31 May 2007)

We establish a framework which allows one to construct novel schemes for measurement-based quantum computation. The technique develops tools from many-body physics—based on finitely correlated or projected entangled pair states—to go beyond the cluster-state based one-way computer. We identify resource states radically different from the cluster state, in that they exhibit nonvanishing correlations, can be prepared using nonmaximally entangling gates, or have very different local entanglement properties. In the computational models, randomness is compensated in a different manner. It is shown that there exist resource states which are locally arbitrarily close to a pure state. We comment on the possibility of tailoring computational models to specific physical systems.

DOI: 10.1103/PhysRevLett.98.220503 PACS numbers: 03.67.Mn, 03.67.Lx, 24.10.Cn

No classical method is known that is capable of efficiently simulating the results of measurements on a general many-body quantum system. What is a burden to computational physics can be made a virtue in quantum information science. Indeed, universal quantum computation is possible by first preparing a certain multipartite entangled resource—called a cluster state [1], which does not depend on the algorithm to be implemented—followed by local measurements on the constituents. This idea of a measurement-based "one-way computer" ($QC_{\mathcal{C}}$) [2] has attracted considerable attention in recent years. While a lot of progress has been made towards understanding this computational model [3–7], there is a surprising lack of new measurement-based computational models along these lines or new resource states. This contrasts with the surprising lack of development of new computational models or novel resource states. To our knowledge, no single model distinct from the $QC_{\mathcal{C}}$ has been developed based on local measurements on a fixed, algorithm-independent qubit resource state. Hence, questions of salient interest seem to be: Can we systematically find alternative schemes for measurement-based quantum computation? What are the properties that distinguish computationally universal resource states? These questions are clearly central when thinking of tailoring resource states to specific physical systems, e.g., to cold atoms in optical lattices, purely linear optical systems, or condensed-matter ground states. The problem is also relevant to many-body physics, when the question of efficient classical simulatability [8] is addressed: Quantum states may be thought of as being ordered according to their computational potency, universal and efficiently simulatable states forming the respective extremes.

In this Letter, we demonstrate how methods from many-body physics can be extended to develop schemes for measurement-based quantum computation (MBC). Starting from the concepts of matrix-product, projected entangled pair, and finitely correlated states [9,10], we develop a framework broad enough to allow for the construction of novel universal resources and models. The notion of universality in the context of one-way computing was recently addressed in Ref. [11]. A universal resource in their sense is a family of states out of which any other state can be obtained by local measurements on a subset of sites. It follows from the definition that many states cannot be universal: For example, states which are locally nonmaximally entangled have nonvanishing two-point correlation functions $\langle O_i O_{i+r}\rangle - \langle O_i\rangle\langle O_{i+r}\rangle$ or a nonmaximal localizable entanglement between any two constituents [11,12]. Complementary to this approach, we refer to a device as a universal quantum computer, if it can efficiently predict the outcome of any quantum algorithm. A state will hence be called a universal resource if one can, assisted by the results of local measurements on the state, efficiently predict the result of any quantum computation.

To exemplify the power of our framework, we describe three new models for MBC in quantum lattice systems. In all these models, the randomness is compensated in a manner different from the $QC_{\mathcal{C}}$. They highlight that, intriguingly, many properties of the original one-way computer may be relaxed: (i) We find resources exhibiting nonvanishing two-point correlations (which are typical for natural many-body ground states). The original discussion of the $QC_{\mathcal{C}}$ depended on the fact that the cluster can be prepared by mutually commuting unitaries (MCUs [13]) acting on small neighborhoods. Commutativity enables one to logically break down a $QC_{\mathcal{C}}$ calculation into small parts corresponding to individual gates; however, the use of MCUs implies severe restrictions, such as that the correlations vanish outside some neighborhood. Hence our framework can prove universality for states not amenable to any MCU-based technique. (ii) We treat a universal weighted graph state with partly weakly entangled bonds. (iii) We present universal states which are locally arbitrarily pure.

Matrix-product states.—The starting point is the familiar notion of a matrix-product state (MPS) [9]. We will first look at the simple case of a chain of n qubits. Its state is

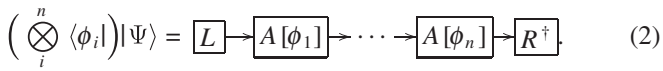
specified by (i) an auxiliary D-dimensional Hilbert space, called correlation space, (ii) two operators $A[0]$, $A[1]$ on $\mathbb{C}^D$, and (iii) two vectors $|L\rangle$, $|R\rangle$, representing boundary conditions. Explicitly

$$|\Psi\rangle = \sum_{s_1,\ldots,s_n=0,1} \langle R|A[s_n]\ldots A[s_1]|L\rangle |s_1,\ldots,s_n\rangle. \quad (1)$$

In order to generalize Eq. (1) to 2D lattices, we need to cast it into the form of a tensor network. Setting $L_i = \langle i|L\rangle$, $A[s]_{i,j} = \langle j|A|i\rangle$, we arrive at $\langle s_1,\ldots,s_n|\Psi\rangle = \sum_{i_0,\ldots,i_n}^{D} L_{i_0} A[s_1]_{i_0,i_1}\ldots A[s_n]_{i_{n-1},i_n} R^{\dagger}_{i_n}$.

Computational tensor networks.—We introduce a graphical notation which enables an intuitive understanding of Eq. (1) and its 2D equivalent. Tensors will be represented by boxes, indices by edges:

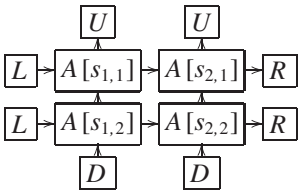
A single-index tensor can be interpreted as the expansion coefficients of either a "ket" or a "bra." Sometimes, we will indicate what interpretation we have in mind by placing arrows on the edges: outgoing arrows designating "kets", incoming arrows "bras." Connected arrows designate contractions of the respective indices. If $|\phi\rangle$ is a general state vector in $\mathbb{C}^2$, we abbreviate $\langle\phi|0\rangle A[0] + \langle\phi|1\rangle A[1]$ by $A[\phi]$. The overlap of $|\Psi\rangle$ with a local projection operator is easily derived:



(2)

Equation (2) should be read as follows: Initially, the correlation system is in the state $|L\rangle$. Subsequent measurements of local observables with eigenvectors $|\phi_i\rangle$ at the ith site induce the evolution $A[\phi_i]$, thereby "processing" the state in the correlation space. The probability of a certain sequence of measurements to occur is given by the overlap of the resulting state vector with $|R\rangle$. An appealing perspective on MBC suggests itself: Measurement-based computing takes place in correlation space; the gates acting on the correlation systems are determined by local measurements. The crucial new insight compared to previous treatments of MPS and PEPS in the context of many-body physics [9,10] or MBC [7] is that the matrices used in the parametrization of an MPS can be directly understood as quantum gates on a logical space. We will refer to this representation of MBC, as a computational tensor network (CTN).

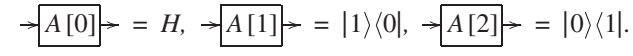
The graphical notation greatly facilitates the passage to 2D lattices. Here, the tensors $A[0/1]$ have four indices $A[s]_{l,d,r,u}$, which are contracted with the indices of the left, right, upper and lower neighbors, respectively:



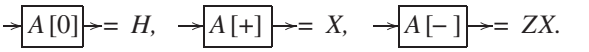
(3)

for various boundary conditions L, D, R, and U. Notably, simulating measurements on states as in Eq. (3) is notoriously hard for a classical computer [10]. This fact is an incarnation of the power of quantum computers and no problem to our approach. We will now describe several examples, demonstrating the versatility of our framework and showing how—surprisingly—many reasonable assumptions about universal resources turn out to be unnecessary. In what follows, we use the standard notation X, Y, Z for the Pauli operators, H for the Hadamard gate and $S = \mathrm{diag}(1, i)$ for the $\pi/4$-gate. The controlled ϕ-phase gate is $|0,0\rangle\langle 0,0| + |0,1\rangle\langle 0,1| + |1,0\rangle\langle 1,0| + e^{i\phi}|1,1\rangle\times\langle 1,1|$. Lastly, $|\pm\rangle = 2^{-1/2}(|0\rangle \pm |1\rangle)$.

AKLT-type states.—In this example, we consider ground states of nearest-neighbor spin-1 Hamiltonians of the AKLT-type, as they are well known in the context of condensed-matter physics [9]. To be brief, we first describe a 1D setting, turning to 2D structures later. More specifically, we investigate the state induced by



This is the exact unique ground state of a nearest-neighbor frustration-free gapped Hamiltonian [14]. One finds that the two-point correlation functions never vanish completely [9]. Still, all single-qubit unitaries on the correlation system can be realized by local physical measurements. We set $|\pm\rangle := 2^{-1/2}(|1\rangle \pm |2\rangle)$ and consider a measurement in the $\{|0\rangle, |+\rangle, |-\rangle\}$-basis. Ignoring global factors (as we will do whenever possible) one finds



Such measurements hence cause the state of the correlation system to be transported from left to right (up to local unitaries). Measuring several consecutive sites, the overall operator B applied to the correlation system is a product of H, X, and Z's. Assuming that we intended to just transport the information faithfully, we conceive B as an unwanted by-product. To understand this structure, we record two elementary observations: (i) The operators H, X, Z form a finite group $\mathcal{B}$ and (ii) Every element of $\mathcal{B}$ will occur as a by-product after a finite expected number of steps. The group property gives a possibility to cope with by-products [15]: Assume that at some point the state vector of the correlation system is given by $B|\psi\rangle$, for some unwanted $B \in \mathcal{B}$. We can rid ourselves of B by just transferring the state along the chain until B^{-1} occurs. This technique is completely general: It can deal with any finite by-product group (see further examples below). The probability of failure can be made exponentially small by adding a linear overhead to the resource. Moving on, a measurement in the $\{|0\rangle, 2^{-1/2}(|1\rangle \pm e^{i\phi}|2\rangle\}$-basis induces one of H, $S(\phi) := \mathrm{diag}(1, e^{i\phi})$, or $ZS(\phi)$ on the correlation system. Realizing that H, $Z \in \mathcal{B}$, we can use the method sketched above to implement both $S(\phi)$ and $HS(\phi)H$ using a finite expected number of steps. This is all we need, as these two families

generate all of $SU(2)$. Lastly, it is easy to see that measurements in the computational basis prepare a known state in the correlation system (in case $|1\rangle$ or $|2\rangle$ is measured) and can be used to read out the correlation system.

A qubit resource with nonvanishing correlations.—We turn to the state defined by $\rightarrow\boxed{A[s]}\rightarrow = G|s\rangle_r\langle s|_l, |L\rangle = |+\rangle, |R\rangle = G^{-1}|+\rangle$, where $G := \exp(i\pi/kX)$ for some integer $k > 2$. The number k specifies the amount of correlations in $|\Psi\rangle$: One finds $\langle Z_i Z_{i+n+1}\rangle - \langle Z_i\rangle\langle Z_{i+n+1}\rangle = [2\sin^2(\pi/k) - 1]^n$. To proceed with the analysis, we compute

$$\rightarrow\boxed{A[+]}\rightarrow = G, \rightarrow\boxed{A[-]}\rightarrow = GZ; \quad \rightarrow\boxed{A[X]}\rightarrow = GZ^x,$$

where the right-hand side is a compact notation for the two equations on the left: An observable as the argument to $A[]$ denotes a measurement in the corresponding eigenbasis. The outcome of the measurement is assigned to a variable; here $x = 0$ in case of the $+1$-eigenvalue and $x = 1$ in case of -1. From the previous equation, we find that G and Z generate the finite by-product group. Proceeding exactly as in the last example, it is easily seen that operations of the type $S(\phi)$ and $GS(\phi)G^\dagger$ can be realized, which is again enough the generate $SU(2)$.

Weighted graph states.—Both previous examples can be embedded into 2D lattices, universal for computation [see Fig. 1(b)]. A general technique for coupling 1D chains to 2D universal resources will be discussed by means of a further example: the weighted graph state [3,16] shown in Fig. 1(a). In the figure, vertices denote physical systems initially in $|+\rangle$, solid edges the application of a controlled π-phase gate and dashed edges controlled $\pi/2$-phases, so some of the entangling gates do not have maximal entangling power. The resource's tensor representation (acting on a $D = 2$-dimensional correlation space) is given by

$$\boxed{A[s]} = S^s|+\rangle_{ru}\, S^s|+\rangle_{lu}\, Z^s|+\rangle_r\langle s|_{ld}\langle s|_{rd}\langle s|_l, \quad (4)$$

where $s \in \{0, 1\}$. Indices are labeled ru for "right-up" to ld for "left-down". Boundary conditions are $|0\rangle$ for the ru, lu, r directions, $|+\rangle$ otherwise. The broad setting for our scheme is the following: the correlation system of every

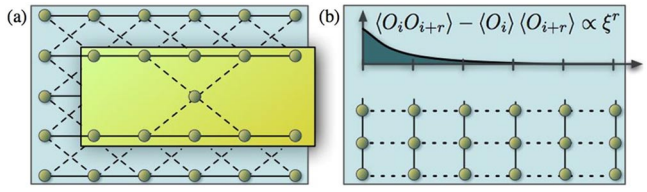


FIG. 1 (color online). Two resources for universal measurement-based quantum computing. (a) depicts a weighted graph state, where solid lines correspond to a controlled π-phase gate, dashed lines to $\pi/2$. (b) represents a scheme deriving from an AKLT-type model. Dashed lines represent a state with nonvanishing correlation functions, solid lines correspond to π-phase gates in $\{|1\rangle, |2\rangle\}$.

second horizontal line in the lattice is interpreted as a logical qubit. Intermediate lines will either be measured in the Z eigenbasis—causing the logical bits to be isolated—or in the Y basis—mediating an interaction between adjacent logical qubits.

We will first describe how to realize isolated evolutions of logical qubits. According to Eq. (4) the tensors $A[0/1]$ factor, allowing us to draw only the arrows corresponding to the factors of interest; so, e.g., $\boxed{A[s]}\rightarrow = Z^s|+\rangle_r$. We find

$$\begin{matrix} A[Z_{i-1,u}] & & A[Z_{i+1,u}] \\ \rightarrow & A[X_i] & \rightarrow \\ A[Z_{i-1,d}] & & A[Z_{i+1,d}] \end{matrix} = HS^{2x_i + z_i}, \quad (5)$$

where $z_i = z_{i-1,u} + z_{i-1,d} + z_{i+1,u} + z_{i+1,d}$. Eq. (5) is of the kind treated before in the case of 1D chains. Indeed, using the same techniques, one sees easily that general local unitaries can be implemented by measurements in the $2^{-1/2}(|0\rangle \pm e^{i\phi}|1\rangle)$ basis. The by-product group here is given by the full single-qubit Clifford group. Turning to two-qubit interactions, consider the schematics for a controlled-Z gate,

$$\begin{matrix} A[X] & A[X] & A[X] \\ & A[Y] & \\ A[X] & A[X] & A[X] \end{matrix} \quad . \quad (6)$$

In detail, we first perform the X measurements on the sites shown and the Z measurements on the adjacent ones. If any of these measurements yields the result "1", we apply a Z measurement to the central site labeled Y and restart the procedure three sites to the right [15]. If all outcomes are "0", a Y measurement is performed on the central site, obtaining the result y. For $c \in \{0, 1\}$,

$$\begin{matrix} A[X] & A[X] & A[X] \\ S^c|+\rangle & & S^c|+\rangle \end{matrix} = HZ^c,$$

$$\begin{matrix} & A[Y] & \\ S^c|+\rangle & & S^c|+\rangle \end{matrix} = (\mathbb{1} + (-1)^{c+y} iS^c \otimes S^c)|+\rangle_{lu}|+\rangle_{ru}$$

$$|c\rangle \rightarrow \boxed{A[X]}\boxed{A[X]}\boxed{A[X]} = S^c|+\rangle_{lu} S^c|+\rangle_{ru} H|c\rangle_r.$$

In summary, the evolution afforded on the upper line is $H(\mathbb{1} + (-1)^{c+y} iZ) \propto HSZ^{y+c}$, equivalent to Z^c up to by-products. This completes the proof of universality. Note that the expected number of steps for a gate does not depend on the overall number of logical qubits, as we never need all by-products to vanish simultaneously.

Entanglement properties.—In this section, we further investigate—using different methods—to what extent the entanglement properties of the cluster state can further be relaxed. We ask if there are resources that are (i) universal for $QC_{\mathcal{C}}$, (ii) translationally invariant, (iii) which have an arbitrarily small local entropy and

localizable entanglement (LE) [20], and (iv) from which not even a Bell pair can be deterministically distilled?

To show that—surprisingly—this is indeed the case, we will encode each logical qubit in a block of $2k+1$ horizontally adjacent physical qubits. Here, k is an arbitrary parameter. The first k qubits per block will take the role of "codewords", the final $k+1$ are "marker qubits" used in a construction to make the resource translationally invariant. We start by preparing a regular cluster state in the respective first qubit of each block. Then, we encode the states of each of these first qubits according to $|0\rangle \mapsto |O_k\rangle := |0\rangle^{\otimes k}$ and $|1\rangle \mapsto |W_k\rangle := k^{-1/2}(|0,\ldots,0,1\rangle + |0,\ldots,1,0\rangle + |1,\ldots,0,0\rangle)$. The rear $k+1$ qubits of each block are prepared in $|0,\ldots,0,1\rangle$. Call the resulting state vector $|\phi\rangle$. Finally, the resource is $|\Psi\rangle = \sum_{t=0}^{2k} \mathcal{T}^t|\phi\rangle$, where $\mathcal{T}$ is a cyclic translation of the lattice in the horizontal direction. To realize universal computing, pick one block and measure each of its qubits in the Z basis. In this way, one can distinguish the states $\mathcal{T}^t|\phi\rangle$ corresponding to different values of t. For definiteness, assume $t=0$. We then encounter a cluster state in the encoding $|O_k\rangle$ and $|W_k\rangle$. The key point is that, by Ref. [17], any two pure orthogonal states can be deterministically locally distinguished. Hence, one can translate any single-site measurement on a cluster state into a protocol for the encoded cluster. This shows that $|\Psi\rangle$ is universal for deterministic MBC. At the same time, the von Neumann entropy S_{vN} of any site is arbitrarily small for sufficiently large k: one finds that the entropy for a measurement in the computational basis reads $S_Z = H_b[3/(4k+2)]$, where H_b is the binary entropy function. Using the concavity of the entropy, we have that $LE \leq S_{vN} \leq S_Z$. It follows that not even a Bell pair can be deterministically created between any two fixed systems.

Outlook.—Until now, the only known scheme for MBC was the QC_C and slight variations. Entire classes of states with physically reasonable properties (e.g., nonmaximal local entanglement, long-ranged correlations) could not be dealt with. The framework presented opens up the possibility to adopt the computational model to specific physical systems and no longer vice versa. For example, in linear optics computing, bonds are the easier to create the lower the entanglement [18]. Under those circumstances, there may well be a trade-off between the effort used to prepare a resource and its efficiency for MBC [18]. In turn, for cold atoms in optical lattices, exploiting cold collisions [19], configurations as in Fig. 1(a) could possibly as feasibly be created as the cluster state, making use of a different interaction time for diagonal collisions. Other states may well be less fragile to finite temperature and decoherence effects. The presented tools open up a way to quantitatively explore such trade-offs.

Support was provided by the DFG (SPP 1116), EU (QAP), EURYI, EPSRC, QIP-IRC, and Microsoft Research.

[1] H.-J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
[2] R. Raussendorf and H.-J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[3] M. Hein *et al.*, arXiv:quant-ph/0602096.
[4] M. A. Nielsen, Rep. Math. Phys. **57**, 147 (2006); R. Jozsa, arXiv:quant-ph/0508124; D. E. Browne and H.-J. Briegel, arXiv:quant-ph/0603226; V. Danos, E. Kashefi, and P. Panangaden, arXiv:quant-ph/0412135.
[5] M. Hein, J. Eisert, and H.-J. Briegel, Phys. Rev. A **69**, 062311 (2004); R. Raussendorf, D. E. Browne, and H.-J. Briegel, *ibid.* **68**, 022312 (2003); D. Schlingemann and R. F. Werner, *ibid.* **65**, 012308 (2001).
[6] M. S. Tame *et al.*, Phys. Rev. A **73**, 022309 (2006).
[7] F. Verstraete and J. I. Cirac, Phys. Rev. A **70**, 060302(R) (2004).
[8] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003); R. Jozsa, arXiv:quant-ph/0603163; I. Markov and Y. Shi, arXiv:quant-ph/0511069; Y.-Y. Shi, L.-M. Duan, and G. Vidal, Phys. Rev. A **74**, 022320 (2006); M. Van den Nest *et al.*, *ibid.* **75**, 012337 (2007).
[9] M. Fannes, B. Nachtergaele, and R. F. Werner, Commun. Math. Phys. **144**, 443 (1992); I. Affleck, *et al.*, *ibid.* **115**, 477 (1988); S. Östlund and S. Rommer, Phys. Rev. Lett. **75**, 3537 (1995); J. Eisert, *ibid.* **97**, 260501 (2006); D. Perez-Garcia *et al.*, arXiv:quant-ph/0608197.
[10] F. Verstraete and J. I. Cirac, arXiv:cond-mat/0407066; S. Richter, Ph.D. thesis, Osnabrück, 1994; F. Verstraete *et al.*, Phys. Rev. Lett. **96**, 220601 (2006); N. Schuch *et al.*, *ibid.* **98**, 140506 (2007).
[11] M. Van den Nest *et al.*, Phys. Rev. Lett. **97**, 150504 (2006).
[12] Consider a state with nonvanishing two-point correlations between any two sites. Since local measurements cannot, on average, decrease the correlations between unmeasured systems, it is impossible to deterministically prepare uncorrelated outputs.
[13] B. Schumacher and R. F. Werner, arXiv:quant-ph/0405174.
[14] In the original AKLT model, $A[0] = 2^{1/2}Z$. We have replaced Z by H as a possible slight variant, as $\{Z, |1\rangle\langle 0| + e^{i\phi}|0\rangle\langle 1|\}$ alone does not generate all of $SU(2)$.
[15] This scheme can be vastly optimized. In the present work, we are only interested in proofs of principle.
[16] W. Dür *et al.*, Phys. Rev. Lett. **94**, 097203 (2005); S. Anders *et al.*, *ibid.* **97**, 107206 (2006); E. T. Campbell *et al.*, Phys. Rev. A **75**, 042303 (2007).
[17] J. Walgate *et al.*, Phys. Rev. Lett. **85**, 4972 (2000).
[18] D. Gross, K. Kieling, and J. Eisert, Phys. Rev. A **74**, 042343 (2006); D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005); J. Eisert, *ibid.* **95**, 040502 (2005).
[19] D. Jaksch *et al.*, Phys. Rev. Lett. **82**, 1975 (1999); O. Mandel *et al.*, Nature (London) **425**, 937 (2003).
[20] M. Popp *et al.*, Phys. Rev. A **71**, 042306 (2005).