Practical Scheme for Quantum Computation with Any Two-Qubit Entangling Gate

Michael J. Bremner,[1] Christopher M. Dawson,[1] Jennifer L. Dodd,[1] Alexei Gilchrist,[1] Aram W. Harrow,[1,2]
Duncan Mortimer,[1] Michael A. Nielsen,[1] and Tobias J. Osborne[1]

[1]*Centre for Quantum Computer Technology and Department of Physics, The University of Queensland, QLD 4072, Australia*
[2]*MIT Physics, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139*

(Received 12 July 2002; published 25 November 2002)

Which gates are universal for quantum computation? Although it is well known that certain gates on two-level quantum systems (*qubits*), such as the controlled-NOT, are universal when assisted by arbitrary one-qubit gates, it has only recently become clear precisely what class of two-qubit gates is universal in this sense. We present an elementary proof that *any* entangling two-qubit gate is universal for quantum computation, when assisted by one-qubit gates. A proof of this result for systems of *arbitrary* finite dimension has been provided by Brylinski and Brylinski; however, their proof relies on a long argument using advanced mathematics. In contrast, our proof provides a simple *constructive* procedure which is close to *optimal* and experimentally practical.

DOI: 10.1103/PhysRevLett.89.247902 PACS numbers: 03.67.–a

A great deal of work has been done to determine what physical resources are capable of universal quantum computation. It is well known that certain gates on two-level quantum systems, such as the controlled-NOT (CNOT), are universal when assisted by arbitrary one-qubit gates [1]. It has also been shown that *almost any* gate on two d-level quantum systems (*qudits*), together with its swapped version, is universal for quantum computation without the aid of one-qudit gates [2,3]. However, this result does not explicitly specify which two-qudit gates are universal, requires the ability to apply the given gate in two different ways, and the resulting procedure is not practical, requiring large numbers of gates.

Recently, several authors have considered conditions for universality when only a single *fixed* multiqudit Hamiltonian interaction, together with one-qudit gates, is allowed [4–9]. They have shown that any interaction that can create entanglement between any pair of qudits is universal for quantum computation. Theoretical schemes for quantum computation based on this have been found, but they are not of practical utility. In order to make the simulations exact, the given interaction is modified by one-qudit gates which must be applied so that the period of evolution between them is infinitesimal. To simulate evolution for some noninfinitesimal time t, the error is controlled by concatenating a large number n of periods of evolution for a small time t/n. Although, in the qubit case, some such schemes minimize the amount of time required to do the simulation [7,8], the required number of one-qubit gates is enormous; an optimistic example of simulating a CNOT to accuracy only 10^{-3} [10] (less stringent than a commonly quoted estimate for the fault-tolerance threshold, 10^{-5}–10^{-6}—see references at the end of chapter 10 of [11]) requires approximately 10^4 one-qubit gates [4]. Thus, the one-qubit gates must be performed with rapidity and accuracy which are vastly more demanding than the standard requirements for quantum computation. We note, however, that Hammerer, Vidal, and Cirac [12] have obtained a practical scheme for a restricted class of symmetric Hamiltonians with no self-energy.

In contrast, the model we consider does not allow an interaction to be interrupted by one-qubit gates at arbitrary times. Following Brylinski and Brylinski [13], but restricting to the qubit case, we allow only a fixed entangling two-qubit *gate* U and arbitrary one-qubit gates between applications of U. Our proof that any such gate is universal provides an explicit method [14] for implementing a CNOT exactly, using a small number of one-qubit gates which is *fixed* for any given gate U. For the optimistic example mentioned above, this method requires only approximately ten one-qubit gates. This represents a savings of a factor of 10^3; typical savings will be much greater. The only limit to the accuracy achieved in practice is due to the accuracy with which the required one-qubit gates are calculated. This limit is inherent in any procedure for computation, but because of the constant number of one-qubit gates required by our scheme, the induced errors will depend only in a constant way on these inaccuracies. Combined with the fact that the number of uses of U is near optimal, this suggests that our scheme will be of practical utility.

We begin the description of our construction with some convenient definitions:

(i) We say that a two-qubit gate is *universal* if it can be used to perform universal quantum computation on two qubits when assisted by arbitrary one-qubit gates.

(ii) Suppose $U = (A_1 \otimes B_1)V(A_2 \otimes B_2)$. Since we have the ability to do arbitrary one-qubit gates, being able to perform U allows us to perform V, and vice versa. Whenever this is the case, we say that U and V are *equivalent* and write $U \equiv V$.

(iii) A gate U is *entangling* if it can create entanglement between two systems initially in a product state.

(iv) Following [13], we define U to be *primitive* if U is a product of one-qubit gates or if U is equivalent to the gate interchanging the two qubits (SWAP); otherwise U is *imprimitive*. We will see that, for two qubits, the class of imprimitive gates is exactly the class of entangling gates.

We now prove the qubit case of the result in [13].

Theorem: A two-qubit gate U is universal if and only if it is imprimitive, or, equivalently, if and only if it is entangling.

Proof: A brief summary of our proof is as follows: We use two nontrivial facts. The first is that CNOT is universal [1]. The second is the *canonical decomposition* [15,16] for any two-qubit gate U:

$$U = (A_1 \otimes B_1)e^{i(\theta_x X\otimes X+\theta_y Y\otimes Y+\theta_z Z\otimes Z)}(A_2 \otimes B_2), \quad (1)$$

where X, Y, Z are the Pauli sigma matrices, A_j, B_j are one-qubit gates, and $-\frac{\pi}{4} < \theta_\alpha \leq \frac{\pi}{4}$ (see [16] for a simple proof). Both of these facts have proofs which are somewhat detailed but elementary and constructive. Our strategy is to show that any imprimitive gate U, together with one-qubit gates, can be used to implement $W = e^{i\phi Z\otimes Z}$ where $0 < |\phi| < \frac{\pi}{2}$. We then show that W can be used, together with one-qubit gates, to exactly implement CNOT, which proves that W, and therefore U, is universal. Finally, since any universal gate is entangling, and any entangling gate is imprimitive, it follows that the class of entangling gates is exactly the class of imprimitive gates.

We define $V = e^{i(\theta_x X\otimes X+\theta_y Y\otimes Y+\theta_z Z\otimes Z)} \equiv U$. First, note that primitive gates have either $\theta_x = \theta_y = \theta_z = 0$ (corresponding to U being a product of one-qubit gates) or $\theta_x = \theta_y = \theta_z = \frac{\pi}{4}$ (corresponding to $U \equiv$ SWAP), so we need not consider these cases.

Suppose U is imprimitive, in which case at least one of the θ_α is nonzero. We will show that in all cases V, and hence U, may be used with one-qubit gates to implement a CNOT and is therefore universal. In each case, we use V to obtain a gate of the form $W = e^{i\phi Z\otimes Z}$, $0 < |\phi| < \frac{\pi}{2}$. Note that we may assume $|\theta_z| \geq |\theta_x| \geq |\theta_y|$ since the θ_α may be relabeled by conjugating V by the primitive gates $H \otimes H$ and $S \otimes S$ where $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.

First, consider the two special cases where either one or two of $\theta_x, \theta_y, \theta_z$ are $\frac{\pi}{4}$ and the remainder are 0. Suppose that $\theta_z = \frac{\pi}{4}$ and $\theta_y = \theta_x = 0$. Then $V = e^{i(\pi/4)Z\otimes Z}$ and is hence already of the required form. For the second special case, $\theta_z = \theta_x = \frac{\pi}{4}$ and $\theta_y = 0$. Noting that $V^8 = I$, and thus $V^7 = V^\dagger$, we use the one-qubit gate $e^{i(\pi/4)X\otimes I}$ to obtain $Ve^{i(\pi/4)X\otimes I}V^7 = e^{i(\pi/4)VX\otimes IV^\dagger} = e^{i(\pi/4)Y\otimes Z} \equiv e^{i(\pi/4)Z\otimes Z}$, which is of the required form [17].

Second, consider the more general case, $\theta_z \neq \frac{\pi}{4}$. Now

$$(I \otimes Z)V(I \otimes Z)V = e^{2i\theta_z Z\otimes Z} = e^{i\phi Z\otimes Z} = W, \quad (2)$$

where $0 < |\phi| < \frac{\pi}{2}$, as required.

Simple algebra shows that W is equivalent to a controlled rotation about the z axis:

$$\begin{aligned} e^{i\phi Z\otimes Z} &= |0\rangle\langle 0| \otimes e^{i\phi Z} + |1\rangle\langle 1| \otimes e^{-i\phi Z} \\ &\equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{2i|\phi|Z}. \end{aligned} \quad (3)$$

Note that, if necessary, we can obtain a positive exponent in the last line by conjugating by $I \otimes X$. We introduce the following notation for a controlled rotation about an arbitrary axis defined by a vector $\mathbf{n}$, with the direction specified by $\hat{\mathbf{n}} \equiv \mathbf{n}/|\mathbf{n}|$ and the angle of rotation determined by $|\mathbf{n}|$:

$$U_{\mathbf{n}} \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{i\mathbf{n}\cdot(X,Y,Z)}. \quad (4)$$

In particular, the controlled rotation (3) above is denoted $U_{(0,0,2|\phi|)}$. Conjugation by one-qubit gates on the second qubit changes the *axis* of rotation but not the *angle* of rotation: Given $\mathbf{n}'$ such that $|\mathbf{n}| = |\mathbf{n}'|$, we can find a one-qubit gate A such that $(I \otimes A)U_{\mathbf{n}}(I \otimes A^\dagger) = U_{\mathbf{n}'}$. A product of two rotations $U_{\mathbf{n}}$ and $U_{\mathbf{n}'}$ is clearly another controlled rotation $U_{\mathbf{m}}$. Both the direction of $\mathbf{m}$ and its magnitude vary depending on $\mathbf{n}$ and $\mathbf{n}'$.

In order to implement a CNOT, we need to use $U_{(0,0,2|\phi|)}$ to obtain a total rotation $U_{(0,0,\pi/2)} \equiv$ CNOT. The first step is to use $U_{(0,0,2|\phi|)}$ a number of times $q = \lfloor \frac{\pi/2}{2|\phi|} \rfloor$. If $\pi/2$ is an exact multiple of $2|\phi|$, then we are done. Otherwise, we must generate a gate to make up the difference; i.e., we need to obtain $U_{\mathbf{m}}$ with $0 < |\mathbf{m}| = \frac{\pi}{2} - 2q|\phi| < 2|\phi|$. To do this, we note that we can easily obtain the following controlled rotations: the zero rotation, $U_{(0,0,0)} = U_{(0,0,2|\phi|)}U_{(0,0,-2|\phi|)}$, and $U_{(0,0,4|\phi|)} = U_{(0,0,2|\phi|)}U_{(0,0,2|\phi|)}$. Choose $\mathbf{n}$ such that $|\mathbf{n}| = 2|\phi|$ in which case $U_{\mathbf{n}}$ is equivalent to $U_{(0,0,2|\phi|)}$. The product $U_{(0,0,2|\phi|)}U_{\mathbf{n}}$ gives another controlled rotation $U_{\mathbf{m}}$. $|\mathbf{m}|$ varies continuously as a function of $\mathbf{n}$ and so, by the intermediate value theorem, it must pass through all the angles between 0 and $4|\phi|$. As a consequence, it is possible to choose $\mathbf{n}$ such that $|\mathbf{m}| = \frac{\pi}{2} - 2q|\phi|$. For any given angle ϕ, $\mathbf{n}$ can be calculated numerically as the solution to a small set of equations (these can be found in exercise 4.15 in [11], see also [18]) [19]. Therefore, since $U_{(0,0,|\mathbf{m}|)} \equiv U_{\mathbf{m}}$, the final sequence is

$$U_{(0,0,\pi/2)} = U^q_{(0,0,2|\phi|)}(I \otimes A)U_{\mathbf{m}}(I \otimes A^\dagger), \quad (5)$$

where A is an appropriate one-qubit gate.

This completes our proof, since it demonstrates that the imprimitive gate U together with one-qubit gates can be used to implement a CNOT, which, in turn, can be used to perform universal quantum computation [20]. ■

It is easy to explore some examples of our procedure using [14]. As an example, suppose we had a gate whose canonical decomposition yielded $U = e^{i(\pi/6)Z\otimes Z}$. Then $A_1UA_2UA_3 =$ CNOT where the gates A_j are *primitive*:

$$\begin{aligned} A_1 &= \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} \otimes (e^{-i\gamma B}e^{i\beta Y}), \\ A_2 &= I \otimes (e^{-i(\pi/6)Z}e^{-i\beta Y}), \qquad A_3 = I \otimes (e^{-i(\pi/6)Z}e^{i\gamma B}), \\ B &= \left(\sqrt{\tfrac{3}{5}}Z - \sqrt{\tfrac{2}{5}}Y\right), \end{aligned} \quad (6)$$

where $\beta = \frac{1}{2}\cos^{-1}\frac{1}{3}$ and $\gamma = \frac{1}{2}\cos^{-1}\frac{1}{\sqrt{6}}$.

We conclude with a discussion of the optimality of the scheme for universal quantum computation described in our proof. We need to answer two questions: What is the

"optimal" use of a given gate U? How optimal is our scheme? We define a scheme to be *optimal* if it uses U the minimal number of times required to implement a CNOT, with arbitrary one-qubit gates. We will see that, although our scheme is slightly nonoptimal in usage of the two-qubit interaction, the number of one-qubit gates used by our scheme is many orders of magnitude smaller than the number required to achieve accuracies sufficient for fault-tolerant quantum computation in the Hamiltonian simulation schemes described at the beginning of this Letter.

It follows from [12] (section D1) that the number of uses of U required to implement the CNOT in *any* protocol using only U and one-qubit gates is bounded below by $\frac{\pi}{4\theta_{\max}}$ where $\theta_{\max} = \max\{|\theta_x|, |\theta_y|, |\theta_z|\}$.

To compare with our scheme, we obtain an estimate of the number of uses of U required to implement a CNOT using our scheme. Recall that we use a controlled rotation $U_{(0,0,2|\phi|)}$ $q = \lfloor \frac{\pi}{8\theta_{\max}} \rfloor$ times to implement a CNOT. (Recall that we take $\theta_z = \theta_{\max}$.) Each controlled rotation uses U twice, in general (the special cases follow along similar lines with small changes in the number of uses of U), and the corrections at the end can require up to four uses of U. Thus, the CNOT uses U $2q + 4$ times. The ratio of the number of uses of U required by our scheme to the minimum possible number is therefore less than $1 + 16\theta_{\max}/\pi$, which is between 1 (for small $\theta_{\max}$) and 5 (for large $\theta_{\max}$). Numerical results suggest that, in practice, the number of uses of U in our scheme is either exactly optimal or one greater than the optimal number.

Returning to the comparison of our result with those on optimal simulation of Hamiltonians [7,8], note that our fixed given gate U can be thought of as a fixed given Hamiltonian which always evolves for the same amount of time between applications of one-qubit gates. Although our procedure is slightly nonoptimal in the number of uses of U for large $\theta_{\max}$, the payoff in terms of error control is enormous. In general, we require only approximately $6q$ one-qubit gates, and q depends only on the gate U, not on the desired accuracy. In the example given above, only four one-qubit gates are required, compared to the unbounded number required to achieve arbitrary accuracy in the Hamiltonian simulation procedures.

We have given a simple algorithm [14] which provides a near-optimal way of using an *arbitrary* two-qubit entangling interaction to do universal quantum computation. Our scheme makes relatively undemanding requirements on local control and, thus, is likely to be experimentally practical. Our scheme inverts the usual challenge facing the designer of a quantum computer: Instead of having to do delicate, system-specific theoretical calculations to engineer systems to perform gates such as the CNOT, it will now be possible for physicists to experimentally determine the character of the available interaction and then apply our algorithm to use that interaction to do universal quantum computation.

We thank Tamyka Bell, Carl Caves, Tim Ralph, and Rüdiger Schack for helpful comments and suggestions. A.W.H. thanks the Centre for Quantum Computer Technology at the University of Queensland for its hospitality and acknowledges support from Army Research Office. A.G. was supported by The New Zealand Foundation for Research, Science and Technology.

[1] A. Barenco, C. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[2] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[3] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London A **449**, 669 (1995).
[4] J. L. Dodd, M. A. Nielsen, M. J. Bremner, and R. T. Thew, Phys. Rev. A **65**, 040301(R) (2002).
[5] W. Dür, G. Vidal, J. I. Cirac, N. Linden, and S. Popescu, Phys. Rev. Lett. **87**, 137901 (2001).
[6] P. Wocjan, D. Janzing, and T. Beth, Quantum Inf. Comput. **2**, 117 (2002).
[7] C. H. Bennett, J. I. Cirac, M. S. Leifer, D.W. Leung, N. Linden, S. Popescu, and G. Vidal, Phys. Rev. A **66**, 012305 (2002).
[8] G. Vidal and J. I. Cirac, Phys. Rev. A **66**, 022315 (2002).
[9] M. A. Nielsen, M. J. Bremner, J. L. Dodd, A. M. Childs, and C. M. Dawson, Phys. Rev. A **66**, 022317 (2002).
[10] The accuracy is measured by the metric induced by the operator norm—see [4] for details.
[11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, Cambridge, 2000).
[12] K. Hammerer, G. Vidal, and J. I. Cirac, quant-ph/0205100.
[13] J. L. Brylinski and R. Brylinski, in *Mathematics of Quantum Computation*, edited by R. K. Brylinski and G. Chen, Computational Mathematics (Chapman & Hall/CRC Press, Boca Raton, 2002), Chap. II.
[14] C. M. Dawson and A. Gilchrist, online implementation of the procedure described herein, http://www.physics.uq.edu.au/gqc/
[15] N. Khaneja, R. Brockett, and S. J. Glaser, Phys. Rev. A **63**, 032308 (2001).
[16] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[17] Noting that $V^6 = Y \otimes Y$ allows the number of uses of V to be reduced to 2: $Ve^{i(\pi/4)X\otimes I}V^7 = V[e^{i(\pi/4)X\otimes I}(Y \otimes Y)]V$.
[18] J. Preskill, *Physics 229: Advanced Mathematical Methods of Physics—Quantum Computation and Information* (California Institute of Technology, Pasadena, CA, 1998), http://www.theory.caltech.edu/people/preskill/ph229/
[19] The equations are $\cos(|\mathbf{m}|) = \cos^2(2\phi) - \sin^2(2|\phi|)\hat{\mathbf{z}} \cdot \hat{\mathbf{n}}$ and $\sin(|\mathbf{m}|)\hat{\mathbf{m}} = \sin(2|\phi|)\cos(2\phi)(\hat{\mathbf{z}} + \mathbf{n}) - \sin^2(2|\phi|)\hat{\mathbf{n}} \times \hat{\mathbf{z}}$. These are easily solved using standard numerical techniques.
[20] Note that our construction could be easily modified in order to simulate any desired two-qubit gate.