A practical scheme for quantum computation with any two-qubit entangling gate

Michael J. Bremner,1 Christopher M. Dawson,1,2 Jennifer L. Dodd,1 Alison Childs,1
Arnaud W. Harrow,2,3 Duncan Maitland,2,4 Michael A. Nielsen, and Tobias J. Osborne5

1Centre for Quantum Information and Foundational Physics, University of Cambridge, Cambridge CB3 0FD, UK
2Centre for Quantum Technologies, National University of Singapore, 117543 Singapore
3Centre for Quantum Technologies, National University of Singapore, 117543 Singapore
4Centre for Quantum Technologies, National University of Singapore, 117543 Singapore
5Department of Physics, Massachusetts Institute of Technology, Cambridge, MA 02139 USA

Abstract

We present a practical scheme for restricted class of symmetric Hamiltonians with no self-energy. This scheme is based on the equivalence of any two-qubit entangling gate with any two-qubit unitary operation. We show how to use this equivalence to design a practical scheme for any two-qubit entangling gate. The key idea is to use a two-qubit Hadamard gate and an arbitrary entangling gate to build a symmetric two-qubit state. We then use this symmetric state to perform a sequence of controlled-NOT operations, which can be used to perform any two-qubit operation.

Keywords: two-qubit entangling gate, Hamiltonian simulation, quantum computation.
Following [12], 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 ($\text{SWAP}$); 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 [12]:

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 non-trivial facts. The first is that $\text{CNOT}$ is universal [1]. The second is the canonical decomposition [13, 14] for any two-qubit gate $U$:

$$U = (A_1 \otimes B_1) e^{i(\theta_1 X \otimes X + \theta_2 Y \otimes Y + \theta_3 Z \otimes Z)} (A_2 \otimes B_2),$$

where $X, Y, Z$ are the Pauli sigma matrices, $A_1, B_1$ are one-qubit gates, and $-\frac{\pi}{4} < \theta_3 \leq \frac{\pi}{4}$ (see [13] 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, together with one-qubit gates, can be used to implement $W = e^{i(\phi Z \otimes Z)}$ where $0 < |\phi| < \frac{\pi}{4}$. We then show that $W$ can be used, together with one-qubit gates, to exactly implement $\text{CNOT}$, 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 $V = e^{i(\theta_2 X \otimes X + \theta_3 Y \otimes Y + \theta_4 Z \otimes Z)} \equiv U$. 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 $U \equiv \text{SWAP}$), so we need not consider these cases.

Suppose $U$ is imprimitive, in which case at least one of the $\theta_a$ is non-zero. We will show that in all cases $V$, and hence $U$, can be used with one-qubit gates to implement a $\text{CNOT}$ and is therefore universal. In each case, we use $V$ to obtain a gate of the form $V' = e^{i\phi Z \otimes Z}$, $0 < |\phi| < \frac{\pi}{4}$. Note that we may assume $|\theta_x| \geq |\theta_y| \geq |\theta_z|$ since the $\theta_a$ can 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 $S = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$.

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 $\theta_x = \frac{\pi}{4}$ and $\theta_y = \theta_z = 0$. Then $V = e^{i\frac{\pi}{4} X \otimes X}$ and is hence already of the required form. For the second special case, $\theta_x = \theta_y = \frac{\pi}{4}$ and $\theta_z = 0$. Noting that $V^8 = I$, and thus $V^7 = V^4$, we use the one-qubit gate $e^{i\frac{\pi}{4} X \otimes X}$ to obtain $V'^8 = e^{i\frac{\pi}{4} X \otimes X} V^8 = e^{i\frac{\pi}{4} X \otimes X} \equiv e^{i\frac{\pi}{4} Z \otimes Z}$, which is of the required form.

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

$$(I \otimes Z)(I \otimes Z)V = e^{i\theta_x Z \otimes Z} = e^{i\phi Z \otimes Z} = W$$

where $0 < |\phi| < \frac{\pi}{4}$, as required.

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

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

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 $n$,

$$U_n \equiv |0\rangle\langle 0| + |1\rangle\langle 1| \otimes \text{rot}^n(X, Y, Z). \quad (4)$$

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

In order to implement a $\text{CNOT}$, we need to use $U_{(0, 0, 2)[4]}$ to obtain a total rotation $U_{(0, 0, \pi/2)[4]} \equiv \text{CNOT}$. The first step is to use $U_{(0, 0, 0)[4]}$ a number of times $q = \lfloor \pi/2q \rfloor$. 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 $U_{(0, 0, 0)[2]}$ with $0 < |m| = \frac{\pi}{4} - 2|\phi| < 2|\phi|$. To do this, we note that we can easily obtain the following controlled rotations: the zero rotation, $U_{(0, 0, 0)[4]} = U_{(0, 0, 0)[4]}U_{(0, 0, -2)[4]}$, and $U_{(0, 0, 0)[4]} = U_{(0, 0, 2)[4]}U_{(0, 0, -2)[4]}$; Choose $n$ such that $|n| = 2|\phi|$ in which case $U_{(0, 0, 2)[4]}$ is equivalent to $U_{(0, 0, 2|\phi|)[4]}$. The product $U_{(0, 0, 0)[4]}U_{(0, 0, 2|\phi|)[4]}$ gives another controlled rotation $U_{(m, n)}$. The magnitude varies continuously as a function of $n$ and, 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 $n$ such that $|m| \equiv \frac{\pi}{4} - 2|\phi|$. For any given angle $\phi$, $m$ can be calculated numerically as the solution to a small set of equations (these can be found in exercise 4.15 in [15], see also [16]) [17]. Therefore, since $U_{(0, 0, 0)[4]} \equiv U_{(0, 0, 0)[4]}$, the final sequence is

$$U_{(0, 0, \pi/2)[4]} = U_{(0, 0, 2)[4]}(I \otimes A)U_{(0, 0, \pi/2)[4]}(I \otimes A^\dagger), \quad (5)$$

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 $\text{CNOT}$, which, in turn, can be used to perform universal quantum computation [18].

It is easy to explore some examples of our procedure using [11]. As an example, suppose we had a gate whose canonical decomposition yielded $U = e^{i\phi Z \otimes Z}$. Then $A_1 U_2 A_3 U_3 = \text{CNOT}$ where the gates $A_j$ are primitive:

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\phi B} \end{bmatrix}, \quad A_2 = I \otimes \begin{bmatrix} e^{i\phi Z} & e^{-i\phi Z} \\ e^{-i\phi Z} & e^{i\phi Z} \end{bmatrix}, \quad A_3 = I \otimes \begin{bmatrix} e^{-i\phi Z} & e^{i\phi Z} \\ e^{i\phi Z} & e^{-i\phi Z} \end{bmatrix}, \quad \text{where} \quad B = \begin{bmatrix} \sqrt{2} & -\sqrt{2} \\ \sqrt{2} & \sqrt{2} \end{bmatrix}.$$
where $\beta = \frac{1}{2} \cos^{-1} \frac{1}{2}$ and $\gamma = \frac{1}{2} \cos^{-1} \frac{1}{2^{\frac{1}{2}}}$. 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 number of times required to implement a CNOT, with arbitrary one-qubit gates. We will see that, although our scheme is slightly non-optimal 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 by the Hamiltonian simulation scheme described at the beginning of this Letter.

It follows from (10), (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 $\frac{U}{U_{\text{max}}} \max\{|\theta|, |\theta_q|, |\theta_p|\}$.

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 $U_{(\theta, \theta_q, \theta_p)} = \frac{U}{1+2\theta_{\text{max}}} \max\{|\theta|, |\theta_q|, |\theta_p|\}$ each of which takes $2q + 4$ times to implement a CNOT. (Recall that we take $\theta_{\text{max}} \geq \theta_{\text{max}}$.) Each control rotation uses $U_{(\theta, \theta_q, \theta_p)}$ in general (the special cases follow along similar lines with small changes in the number of uses of $U$).

The ratio of the number of uses of $U$ required by our scheme to the minimum possible number is therefore less than $1 + 16\theta_{\text{max}} / \pi$, which is between 1 (for small $\theta_{\text{max}}$) and 5 (for large $\theta_{\text{max}}$).

Returning to the comparison of our result with those on optimal simulation of Hamiltonians, [7, 8], note that our fixed-gate use $U$ can be thought of as a fixed-gate Hamiltonian which always evolves for the same amount of time between applications of one-qubit gates. Although one procedure slightly non-optimal in the number of uses of $U$ for large $\theta_{\text{max}}$, 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 4 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 [11] which provides a near-optimal way of using an arbitrary two-qubit entangling interaction to do universal quantum computation. Our scheme makes relatively lightweight demands on local control; and thus is likely to be experimentally practical. Our scheme inverts the usual challenge faced by 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 Tammya 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.