PHYSICAL REVIEW A **69**, 010301(R) (2004)

Universal quantum circuit for two-qubit transformations with three controlled-NOT gates

G. Vidal[1] and C. M. Dawson[2]

[1]*Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125, USA*

[2]*Center for Quantum Computer Technology and Department of Physics, The University of Queensland, Brisbane 4072, Australia*

(Received 12 August 2003; published 8 January 2004)

We consider quantum circuits made of controlled-NOT (CNOT) gates and single-qubit unitary gates and look for constructions that minimize the use of CNOT gates. We show, by means of an explicit quantum circuit, that three CNOT gates are necessary and sufficient in order to implement an arbitrary unitary transformation of two qubits. We also identify the subset of two-qubit gates that can be performed with only two CNOT gates and provide a simple characterization for them.

DOI: 10.1103/PhysRevA.69.010301 PACS number(s): 03.67.Lx, 03.67.Mn

In the context of establishing the existence of universal sets of two-qubit gates for quantum computation [1], Barenco et al. [2] showed that any unitary transformation on n qubits can be decomposed into a sequence of controlled-NOT (CNOT) and single-qubit gates. Since then it is customary in quantum information to use CNOT and single-qubit gates in order to express any unitary transformation in the quantum circuit model [3]. As a result, the CNOT gate has acquired a special status as the standard hallmark of multiqubit control. Among quantum information experimentalists, achieving a CNOT gate is one of the most coveted goals [4]. In turn, exhaustive theoretical studies on the optimal use of two-qubit interactions and of entangling gates to perform a CNOT gate have been conducted [5–8].

Here we shall consider the construction of quantum circuits that minimize the use of CNOT gates. Such optimal constructions are relevant in two separated scenarios. First, they play a role in determining the algorithmic complexity of a given quantum computation, that is, the number of elementary gates required to implement the corresponding n-qubit unitary evolution. A most remarkable result of Ref. [2] is the explicit decomposition of an arbitrary $U \in \mathrm{U}(2^n)$ as a sequence of CNOT and single-qubit gates. This general construction, however, unavoidably requires $\exp(n)$ CNOT gates, which renders the resulting quantum circuit inefficient, while the transformations relevant for quantum computation are precisely those that can be decomposed into only $\mathrm{poly}(n)$ elementary gates. Thus, given a unitary transformation $U \in \mathrm{U}(2^n)$, in quantum computation it is important to determine how many CNOT gates are required for its implementation.

Algorithmic complexity is typically concerned with the asymptotic scaling of computational resources, and thus with gates involving a large number of qubits. Here, instead, we shall analyze unitary gates of just two qubits, $n=2$. Quantum circuits that minimize the use of CNOT gates are also of interest in this case, but for another, more practical reason. In present day experiments, two-qubit gates as the CNOT gate are implemented in an imperfect way due to technological limitations. Therefore, in order to minimize the probability that an error occurs in performing a certain unitary evolution U on $n=2,3,\ldots$ qubits, it is instrumental that the number of times the qubits interact is as small as possible. Unfortunately, there is a general lack of results concerning how to optimally decompose $U \in \mathrm{U}(2^n)$ into CNOT and single-qubit gates.

In this paper we describe a *universal* quantum circuit for two-qubit unitary transformations $U \in \mathrm{SU}(4)$ consisting of only three CNOT gates and four rounds of local gates. The shortest circuit previously known requires four CNOT gates [9]. In addition, we show that three CNOT gates are necessary in order to perform a generic two-qubit gate, thereby establishing the optimality of the proposed universal quantum circuit. We also characterize the subset of two-qubit gates whose implementation requires only two CNOT gates and construct an alternative, smaller quantum circuit for them. In this way we give a complete classification of two-qubit gates in terms of their CNOT complexity.

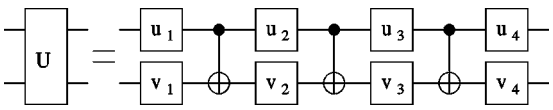
We consider two qubits, labeled A and B, and an arbitrary unitary transformation $U \in \mathrm{SU}(4)$. Let $u_l, v_l \in \mathrm{SU}(2)$ denote single-qubit unitary gates acting, respectively, on qubits A and B, and let U_{CNOT} denote a CNOT gate that has qubit A as control and qubit B as target,

$$U_{\mathrm{CNOT}}|^z m\rangle_A \otimes |^z n\rangle_B = |^z m\rangle_A \otimes |^z n \oplus m\rangle_B, \qquad m,n=0,1, \tag{1}$$

where $i \oplus j$ denotes sum modulo 2 and $|^z 0\rangle$ ($|^z 1\rangle$) is the eigenvector with eigenvalue 1 (-1) of the third of the Pauli matrices

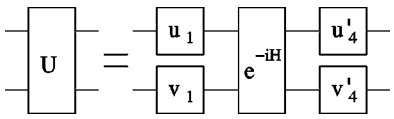
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2}$$

Theorem 1. An arbitrary unitary gate $U \in \mathrm{SU}(4)$ can be decomposed in terms of three CNOT gates and single-qubit unitary gates u_l, v_l (to be specified below) as



(3)

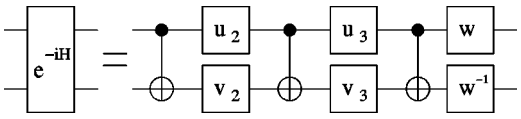
An important element in order to prove Theorem 1 is the decomposition of $U \in \mathrm{SU}(4)$ derived by Khaneja *et al.* [5] and Kraus *et al.* [10], namely,



(4)

$$H \equiv h_x \sigma_x \otimes \sigma_x + h_y \sigma_y \otimes \sigma_y + h_z \sigma_z \otimes \sigma_z , \tag{5}$$

where $\pi/4 \geqslant h_x \geqslant h_y \geqslant |h_z|$. An explicit protocol to extract the single-qubit gates $u_1, v_1, u_4', v_4' \in \mathrm{SU}(2)$ and the coefficients $h_x, h_y, h_z \in \mathcal{R}$ from U was presented in Ref. [10]. In what follows we show that e^{-iH} can be further decomposed as



(6)

where

$$u_2 \equiv \frac{i}{\sqrt{2}} (\sigma_x + \sigma_z) e^{-i(h_x - \pi/4)\sigma_x}, \quad v_2 \equiv e^{-i h_z \sigma_z}, \tag{7}$$

$$u_3 \equiv \frac{-i}{\sqrt{2}} (\sigma_x + \sigma_z), \quad v_3 \equiv e^{i h_y \sigma_z}, \tag{8}$$

$$w \equiv \frac{I - i\sigma_x}{\sqrt{2}}, \tag{9}$$

so that u_4 and v_4 in Eq. (3) are

$$u_4 = u_4' w, \qquad v_4 = v_4' w^{-1}. \tag{10}$$

Let us introduce the Bell basis

$$|\gamma_{00}\rangle \equiv \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle), \quad |\gamma_{01}\rangle \equiv \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle),$$

$$|\gamma_{10}\rangle \equiv \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle), \quad |\gamma_{11}\rangle \equiv \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle),$$

where $|mn\rangle$ denotes $|^z m\rangle_A \otimes |^z n\rangle_B$. Operator H in Eq. (5) can be rewritten as

$$H = \sum_{m,n=0}^{1} \lambda_{mn} |\gamma_{mn}\rangle\langle\gamma_{mn}|, \tag{11}$$

with λ_{mn} defined as

$$\lambda_{00} \equiv h_x - h_y + h_z, \quad \lambda_{01} \equiv h_x + h_y - h_z, \tag{12}$$

$$\lambda_{10} \equiv -h_x + h_y + h_z, \quad \lambda_{11} \equiv -h_x - h_y - h_z. \tag{13}$$

Then e^{-iH} becomes

$$e^{-iH} = \sum_{m,n=0}^{1} e^{-i\lambda_{mn}} |\gamma_{mn}\rangle\langle\gamma_{mn}|. \tag{14}$$

Direct inspection shows that circuit (6) indeed acts on the Bell basis $|\gamma_{mn}\rangle$ as [11]

$$|\gamma_{mn}\rangle \to e^{-i\lambda_{mn}} |\gamma_{mn}\rangle. \tag{15}$$

Next we describe a way to check this fact. The first (leftmost) CNOT in Eq. (6) maps the Bell basis into a product basis, namely,

$$|\gamma_{mn}\rangle \to |^x m\rangle_A \otimes |^z n\rangle_B , \tag{16}$$

where $|^x 0\rangle \equiv (|^z 0\rangle + |^z 1\rangle)/\sqrt{2}$, $|^x 1\rangle \equiv (|^z 0\rangle - |^z 1\rangle)/\sqrt{2}$. The local transformations $u_2 \otimes v_2$ introduce convenient phases $e^{-i\phi_{mn}}$,

$$\phi_{mn} \equiv (-1)^m \left(h_x + \frac{\pi}{2} \right) + (-1)^n h_z , \tag{17}$$

into this product basis, and map the latter into a new product basis,

$$|^x m\rangle_A \otimes |^z n\rangle_B \to e^{-i\phi_{mn}} |^z m\rangle_A \otimes |^z n\rangle_B . \tag{18}$$

The second CNOT gate exchanges only two elements of the new product basis [recall Eq. (1)],

$$|^z 1\rangle_A \otimes |^z 0\rangle_B \leftrightarrow |^z 1\rangle_A \otimes |^z 1\rangle_B , \tag{19}$$

after which local gates $u_3 \otimes v_3$ switch back to the $|^x m\rangle_A \otimes |^z n\rangle_B$ basis and introduce more phases $e^{-i\phi_n'}$,

$$\phi_n' \equiv (-1)^{n+1} h_y . \tag{20}$$

The rightmost CNOT in Eq. (6) maps the basis $|^x m\rangle_A \otimes |^z n\rangle_B$ back into the original Bell basis,

$$|^x m\rangle_A \otimes |^z n\rangle_B \to |\gamma_{mn}\rangle, \tag{21}$$

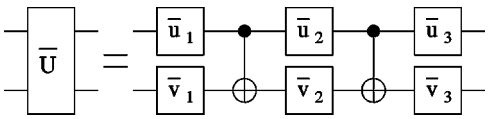
and the final local gates $w \otimes w^\dagger$ exchange vectors $|\gamma_{10}\rangle$ and $|\gamma_{11}\rangle$ in order to undo the permutation (19) [and also add a $\pi/2$ phase to each of them], so that circuit (6) implements transformation (15). This finishes the proof of Theorem 1.

As shown in Ref. [2], a nontrivial subset of two-qubit unitary transformations, namely, control-V transformations for $V \in \mathrm{U}(2)$, can be performed by using only two CNOT gates and single-qubit gates. For these gates, one finds $h_y = h_z = 0$ in its decomposition (4) and (5), so that they are locally equivalent to a control-phase gate U_φ,

$$U_\varphi |^z m\rangle_A \otimes |^z n\rangle_B = e^{-imn\varphi} |^z m\rangle_A \otimes |^z n\rangle_B , \tag{22}$$

for an arbitrary phase φ. Theorem 2 characterizes the set of *all* two-qubit transformations that can be performed with only two CNOT gates. They correspond to $h_z = 0$ in Eqs. (4) and (5), and are therefore a subset of zero measure in the space of two-qubit gates.

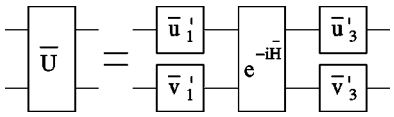
Theorem 2. A two-qubit gate $\overline{U} \in \mathrm{SU}(4)$ can be decomposed in terms of two CNOT gates and single-qubit gates $\overline{u_l}, \overline{v_l}$ as



(23)

if and only if $h_z=0$ in its decomposition (4) and (5).

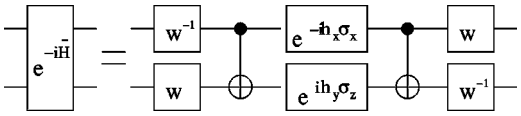
First we prove that if $h_z=0$, then $\overline{U}$ can be decomposed as in Eq. (23). Decomposition (4) and (5) becomes



(24)

$$\overline{H} \equiv h_x \ \sigma_x \otimes \sigma_x + h_y \ \sigma_y \otimes \sigma_y, \quad h_x \geq h_y \geq 0. \tag{25}$$

One can now express $e^{-i\overline{H}}$ as



(26)

where w has been defined in Eq. (9) and where $\overline{u_l}, \overline{u_l'}, \overline{v_l}, \overline{v_l'}$ in Eqs. (23) and (24) are related through

$$\overline{u}_1 = w^\dagger \overline{u_1'}, \quad \overline{v}_1 = w \overline{v_1'}, \quad \overline{u}_3 = \overline{u_3'} w, \quad \overline{v}_3 = \overline{v_3'} w^\dagger. \tag{27}$$

The validity of circuit (26) can be checked by reasoning similarly as we did in the proof of Theorem 1. In particular, the first local gates $w_A^\dagger \otimes w_B$ permute vectors $|\gamma_{10}\rangle$ and $|\gamma_{11}\rangle$. Then the leftmost CNOT gate maps the Bell basis $|\gamma_{mn}\rangle$ into the product basis $|^x m\rangle_A \otimes |^z n\rangle_B$. Gates $\overline{u}_2 \otimes \overline{v}_2$ introduce convenient phases $e^{-i\overline{\phi}_{mn}}$ to $|^x m\rangle_A \otimes |^z n\rangle_B$,

$$\overline{\phi}_{mn} \equiv (-1)^m h_x - (-1)^n h_y. \tag{28}$$

Finally, the rightmost CNOT and $w_A \otimes w_B^\dagger$ gates map the local basis back into the original Bell basis. This shows that any $\overline{U}$ with $h_z=0$ in its decomposition (4) and (5) can be implemented with local gates and two CNOT gates.

To prove the converse we will argue that circuit (26) is, up to local unitary gates, the most general form of a gate implementable with two CNOT gates, as that in Eq. (23). The initial and final gates $\overline{u}_1, \overline{v}_1, \overline{u}_3, \overline{v}_3$ in circuit (23) do not change the parameters h_x, h_y, h_z for $\overline{U}$ and may be ignored. As a rotation on the Bloch sphere, single-qubit gates can be written as a series of three rotations around two perpendicular axes. In particular we may write

$$\overline{u}_2 = e^{-ia_1\sigma_z} e^{-i\alpha\sigma_x} e^{-ia_2\sigma_z}, \tag{29}$$

$$\overline{v}_2 = e^{-ib_1\sigma_x} e^{i\beta\sigma_z} e^{-ib_1\sigma_x} \tag{30}$$

(see, for example, Theorem 4.1 in Ref. [3]). Recalling that the CNOT gate (1) can be expressed as

$$U_{\mathrm{CNOT}} = \frac{I+\sigma_z}{2} \otimes I + \frac{I-\sigma_z}{2} \otimes \sigma_x, \tag{31}$$

TABLE I. Number of CNOT gates necessary and sufficient for the implementation of a two-qubit gate $U \in \mathrm{SU}(2)$, in terms of the vector of coefficients (h_x, h_y, h_z) of Eq. (5), where $\pi/4 \geq h_x \geq h_y \geq |h_z|$. We use h^+ and $h^\pm$ to denote $h>0$ and $|h| \neq 0$, respectively.

(h_x, h_y, h_z)	CNOT complexity
$(\pi/4,0,0)$	1
$(h_x^+, h_y, 0)$[a]	2
$(h_x^+, h_y^+, h_z^\pm)$	3

[a]Except for $(\pi/4,0,0)$.

it is clear that the leftmost and rightmost exponentials in Eqs. (29) and (30) commute with the contiguous CNOT gates in circuit (26). This implies that the h_x, h_y, h_z parameters of $\overline{U}$ are the same as those of the gate,

$$U_{\mathrm{CNOT}} (e^{-i\alpha\sigma_x} \otimes e^{i\beta\sigma_z}) U_{\mathrm{CNOT}}. \tag{32}$$

But up to local gates this is circuit (26) with $\alpha = h_y$ and $\beta = h_x$. Therefore $\overline{U}$ has $h_z=0$ in the decomposition (4) and (5), completing the proof of Theorem 2.

Motivated by current experimental difficulties in the realization of CNOT gates, in this work we have analyzed the construction of quantum circuits that achieve two-qubit unitary transformations by using the smallest number of CNOT gates possible. For an arbitrary n-qubit unitary transformation $U \in \mathrm{U}(2^n)$, both characterizing its exact CNOT complexity and constructing an optimal quantum circuit seem very ambitious tasks, even by numerical analysis. Surprisingly, in the case of two-qubit transformations it has been possible to characterize the CNOT complexity of an arbitrary gate analytically, and to express this complexity just in terms of the coefficients (h_x, h_y, h_z) of the decomposition presented in [5,10], as summarized in Table I.

A possible extension of the present analysis is to also optimize the use of single-qubit unitary transformations in the above constructions. However, in order to perform this optimization, a sensible cost function for single-qubit gates is first required. In a given experimental setup it could well happen that rotations in the Bloch sphere around, say, axis x are simpler to perform than around axis y; or it could be easier to perform rotations by a fixed angle and axis than by arbitrary ones. All these details need to be properly reflected in a cost function, to be optimized in order to obtain the most convenient quantum circuit for the given experimental setup. However, the following two facts in such optimization are independent of the specific experimental details: (i) 15 independent angles must be specified by means of local operations in the case of an arbitrary transformation $U \in \mathrm{SU}(4)$, and (ii) at least three of these angles correspond to local gates that are performed between the three CNOT gates.

Finally, one may also seek to generalize the present results by considering the CNOT complexity of *specific* transformations of $n>2$ qubits. In the case of three qubits, for instance, the Toffoli gate is known to require at most six CNOT gates [3], but only five CNOT gates have so far been proved to be necessary [12]. In order to study this problem, techniques different from the ones employed in this work

are required, since no decomposition analogous to decomposition (4) and (5) is known for unitary transformations involving more than two qubits.

G.V. thanks J. I. Cirac and J. Pachos for comments and for hospitality at the Max Planck Institute for Quantum Optics, Garching, Germany, December 2001, and Debbie Leung for important corrections in an earlier version of this paper. C.D. acknowledges the Institute for Quantum Information, California Institute of Technology for hospitality. This work was supported by the National Science Foundation of USA under Grant No. EIA–0086038.

[1] D.P. Divincenzo, Phys. Rev. A **51**, 1015 (1995); T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995); A. Barenco, Proc. R. Soc. London, Ser. A **449**, 678 (1995); S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995); D. Deutsch *et al.*, Proc. R. Soc. London, Ser. A **449**, 669 (1995).

[2] A. Barenco *et al.*, Phys. Rev. A **52**, 3457 (1995).

[3] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[4] Fortschr. Phys. **48**(9–11) (2000).

[5] N. Khaneja, R. Brockett, and S.J. Glaser, Phys. Rev. A **63**, 032308 (2001).

[6] G. Vidal, K. Hammerer, and J.I. Cirac, Phys. Rev. Lett. **88**, 237902 (2002).

[7] M.J. Bremner *et al.*, Phys. Rev. Lett. **89**, 247902 (2002).

[8] J. Zhang, J. Vala, S. Sastry, and K.B. Whaley, e-print quant-ph/0212109.

[9] S.S. Bullock and I.L. Markov, Phys. Rev. A **68**, 012318 (2003).

[10] B. Kraus and J.I. Cirac, Phys. Rev. A **63**, 062309 (2001).

[11] In Eq. (15) we have neglected a physically irrelevant, global phase $e^{i\pi/4}$ originating in that $\det(U_{\mathrm{CNOT}}) = -1$ in Eq. (1), i.e., $U_{\mathrm{CNOT}} \notin \mathrm{SU}(4)$.

[12] J.L. Dodd and G. Vidal (unpublished).