Optimal quantum circuit synthesis from controlled-unitary gates

Jun Zhang,[1,2] Jiri Vala,[2] Shankar Sastry,[1] and K. Birgitta Whaley[2]
[1]*Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, California 94720, USA*
[2]*Department of Chemistry and Pitzer Center for Theoretical Chemistry, University of California, Berkeley, California 94720, USA*
(Received 29 August 2003; published 16 April 2004)

Using a geometric approach, we derive the minimum number of applications needed for an arbitrary controlled-unitary gate to construct a universal quantum circuit. An analytic construction procedure is presented and shown to be either optimal or close to optimal. This result can be extended to improve the efficiency of universal quantum circuit construction from any entangling gate. In addition, for both the controlled-NOT (CNOT) and double-CNOT gates, we develop simple analytic ways to construct universal quantum circuits with three applications, which is the least possible for these gates.

DOI: 10.1103/PhysRevA.69.042309 PACS number(s): 03.67.Lx, 03.67.Pp

I. INTRODUCTION

Construction of a universal quantum circuit, i.e., a circuit that can implement any arbitrary unitary operation, is of central importance in the physical applications of quantum computation and quantum information processing [1]. Barenco *et al.* [2] proved the celebrated result that the controlled-NOT (CNOT) gate supplemented with single-qubit rotations is universal, which has become a *de facto* standard model of quantum computation. We have previously provided a generality beyond the standard model [3], namely, an analytic direct route to simulating any arbitrary two-qubit unitary operation from whatever entangling gate arises naturally in the physical applications. The ability to simulate an *arbitrary* two-qubit operation is particularly important for quantum simulations, where one wishes to use one readily controllable quantum system to simulate the behavior of another quantum system that may be hard to either realize or control.

Current experimental efforts are focused on realizing specific entangling gates. In order to be useful, these specific gates have to be able to generate any arbitrary two-qubit gate in an *efficient* manner. This is an extremely important question for experimental applications, where one seeks to reduce unwanted decoherence effects that inevitably increase with the total number of gates. In [3], we provided an upper bound for the applications of a given entangling gate, i.e., regardless of which two-qubit gate is to be implemented, we can always construct a quantum circuit with applications of the given gate not exceeding that upper bound. However, this upper bound is not tight because it may be possible to achieve universality with fewer applications of the given gate. For example, it was recently shown that just three applications of the CNOT gate together with local gates are universal [4].

The main contribution of this paper is a more general result for optimality, namely, the minimum number of applications needed for an arbitrary controlled-unitary (controlled-U) gate to construct a universal quantum circuit. We focus on the controlled-U gates because any entangling two-qubit gate can be used at most twice to simulate a controlled-U gate [3], and these gates can then be used as basic building blocks to construct universal quantum circuits [5,6]. Our main tool to derive the minimum upper bound for any controlled-U gate is the geometric representation of nonlocal two-qubit gates developed in [7], which provides an intuitive approach to this minimum upper bound. We also obtain a near optimal construction procedure that requires either the minimum applications of the given controlled-U gate, or one application more than the minimum, depending on the given gate. Moreover, for the CNOT and double-CNOT (DCNOT) gate [8] (which is locally equivalent to the iSWAP gate in [9]), we provide a simple analytic solution to simulating any two-qubit gate with at most three applications.

II. PRELIMINARIES

We first briefly review some relevant background knowledge [3,7,10–12]. Two quantum gates $U, U_1 \in \mathrm{SU}(4)$ are called *locally equivalent* if they differ only by local operations: $U = k_1 U_1 k_2$, where $k_1, k_2 \in \mathrm{SU}(2) \otimes \mathrm{SU}(2)$. Two gates are locally equivalent if and only if they have identical Makhlin local invariants [10]. From the Cartan decomposition on su(4), any two-qubit unitary operation $U \in \mathrm{SU}(4)$ can be written as

$$U = k_1 A k_2 = k_1 e^{c_1 (i/2)\sigma_x^1 \sigma_x^2} e^{c_2 (i/2)\sigma_y^1 \sigma_y^2} e^{c_3 (i/2)\sigma_z^1 \sigma_z^2} k_2, \qquad (1)$$

where $\sigma_\alpha^1 \sigma_\alpha^2 = \sigma_\alpha \otimes \sigma_\alpha$, σ_α are the Pauli matrices, and $k_1, k_2 \in \mathrm{SU}(2) \otimes \mathrm{SU}(2)$ are local gates. In [7] we found that the local equivalence classes of two-qubit gates are in one-to-one correspondence with the points in the tetrahedron $OA_1A_2A_3$ shown in Fig. 1, except on its base. For a general two-qubit gate U in Eq. (1), this geometric representation defines a set of parameters c_j satisfying $\pi - c_2 \geqslant c_1 \geqslant c_2 \geqslant c_3 \geqslant 0$.

Consider an arbitrary single-qubit gate $U = \exp(n_x i\sigma_x + n_y i\sigma_y + n_z i\sigma_z)$. The controlled-$U$ operation U_f derived from this gate can be written as

$$U_f = (I \otimes e^{-\gamma (i/2)\sigma_z} U_1^\dagger) e^{\gamma (i/2)\sigma_z^1 \sigma_z^2} (I \otimes U_1), \qquad (2)$$

where $\gamma = \sqrt{n_x^2 + n_y^2 + n_z^2}$, and U_1 is a single-qubit gate given by Proposition 3 of [3]. By definition, $e^{\gamma (i/2)\sigma_z^1 \sigma_z^2}$ is locally equivalent to a controlled-U gate. Therefore, without loss of generality, we can use $U_f = e^{\gamma (i/2)\sigma_z^1 \sigma_z^2}$ to denote any

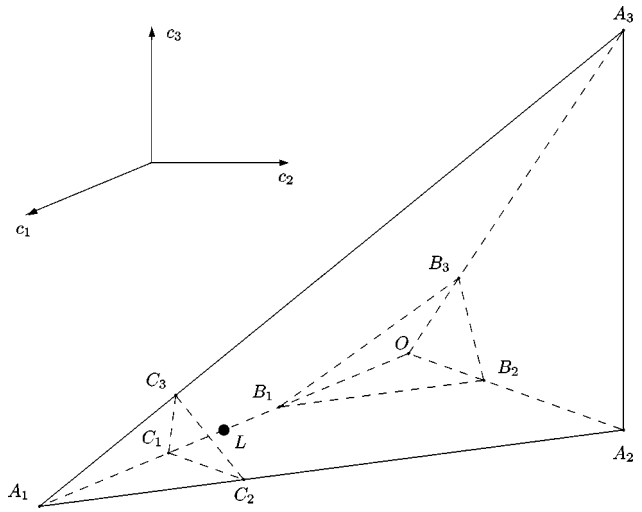


FIG. 1. Tetrahedron $OA_1A_2A_3$ contains all the local equivalence classes of nonlocal gates, where O ($[0,0,0]$) and A_1 ($[\pi,0,0]$) both correspond to local gates, L ($[\pi/2,0,0]$) to the CNOT gate, A_3 ($[\pi/2,\pi/2,\pi/2]$) to the SWAP gate, and the controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$ to the point $[\gamma,0,0]$ on OL [7]. Tetrahedra $OB_1B_2B_3$ and $A_1C_1C_2C_3$ contain all the local equivalence classes of the nonlocal gates that can be generated by n applications of U_f with local gates, where $B_1=[n\gamma,0,0]$, $B_2=[n\gamma/2,n\gamma/2,0]$, $B_3=[n\gamma/3,n\gamma/3,n\gamma/3]$, $C_1=[\pi-n\gamma,0,0]$, $C_2=[\pi-n\gamma/2,n\gamma/2,0]$, and $C_3=[\pi-n\gamma/3,n\gamma/3,n\gamma/3]$.

controlled-U gate. Since $e^{(\pi-\gamma)(i/2)\sigma_z^1\sigma_z^2}$ is locally equivalent to $e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$, we can always take the parameter $\gamma\in(0,\pi/2]$. Specifically, when $\gamma=\pi/2, U_f$ is locally equivalent to the CNOT gate.

III. MINIMUM UPPER BOUND FOR ANY CONTROLLED-*U* GATE

We have previously provided an upper bound for a given entangling gate to implement a universal quantum circuit [3]. For a controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$, this upper bound is $6\lceil\pi/4\gamma\rceil$, where the ceiling function $\lceil x\rceil$ is defined as a function that rounds x to the nearest integer toward infinity. This upper bound is not a tight one. We now use a geometric approach to show that the minimum upper bound for a controlled-U gate is $\lceil 3\pi/2\gamma\rceil$.

Any controlled-U gate U_f corresponds to a point on the line segment OL, as shown in Fig. 1. We now study the set of all the nonlocal gates that can be implemented by n applications of U_f. We first analyze the case $n\geqslant 3$ and then the case $n=2$. The following theorem shows that all gates that can be simulated by $n(\geqslant 3)$ applications of U_f together with local gates constitute two congruent tetrahedra in the tetrahedron $OA_1A_2A_3$, which is the geometric representation of all the nonlocal two-qubit operations [3].

Theorem 1. For a controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$, every gate generated by n ($\geqslant 3$) applications of U_f together with local gates is locally equivalent to a gate $e^{c_1(i/2)\sigma_x^1\sigma_x^2}e^{c_2(i/2)\sigma_y^1\sigma_y^2}e^{c_3(i/2)\sigma_z^1\sigma_z^2}$, with the parameters c_j satisfying either $0\leqslant c_1+c_2+c_3\leqslant n\gamma$ or $c_1-c_2-c_3\geqslant\pi-n\gamma$.

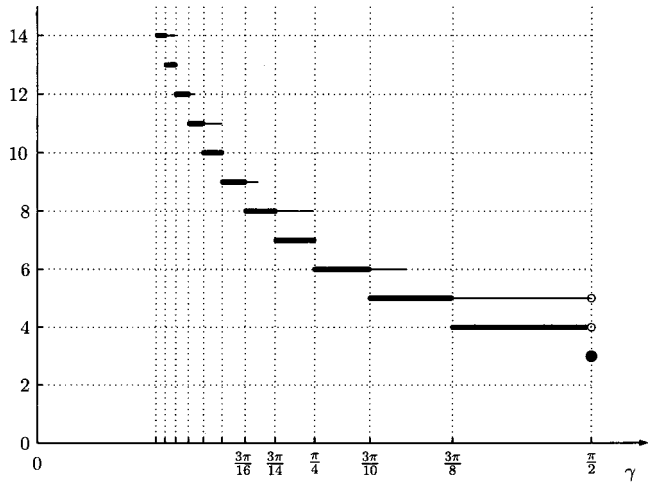


FIG. 2. Upper bound of applications needed for an arbitrary controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$ to construct a universal quantum circuit. Thick lines, minimum number; thin lines, number from our constructive procedure.

See Appendix A for a proof. Theorem 1 tells us that all the gates that can be generated by n applications of U_f with local gates can be represented by two tetrahedra $OB_1B_2B_3$ and $A_1C_1C_2C_3$ in Fig. 1. Note that these two tetrahedra are congruent, and the equations describing the faces $B_1B_2B_3$ and $C_1C_2C_3$ are $c_1+c_2+c_3=n\gamma$ and $c_1-c_2-c_3=\pi-n\gamma$, respectively. These two faces are the boundaries of all those points that can be generated by n applications of U_f.

It is clear that as$n$ grows each of these two tetrahedra $OB_1B_2B_3$ and $A_1C_1C_2C_3$ expands with consecutive faces of each tetrahedron remaining parallel. To obtain the minimum number of applications needed for a given controlled-U gate U_f to implement any arbitrary two-qubit operation, we only need to find the least integer n such that the union of the two tetrahedra $OB_1B_2B_3$ and $A_1C_1C_2C_3$ can cover the whole tetrahedron $OA_1A_2A_3$ as n grows. Since this is convex, we can further restrict our attention to covering all its vertices. As seen from Fig. 1, this is equivalent to the condition that one of the two tetrahedra contains the point A_3 ($[\pi/2,\pi/2/\pi/2]$) i.e., the SWAP gate. From Theorem 1, we require only that $n\gamma\geqslant 3\pi/2$, which leads to $n=\lceil 3\pi/2\gamma\rceil$. This provides the minimum upper bound for an arbitrary controlled-U gate to implement a universal quantum circuit, and is summarized in the following theorem.

Theorem 2. For an arbitrary controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$, the minimum application required to implement any arbitrary two-qubit gate together with local gates is $\lceil 3\pi/2\gamma\rceil$.

In Fig. 2, the minimum upper bound for any controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$ is shown as a function of γ and depicted by thick lines. The thin lines represent the number of applications needed by a near optimal construction procedure we present below. Note that the single point at $\gamma=\pi/2$ with value 3 indicates that three applications of the CNOT gate with local gates suffice to implement any arbitrary two-qubit gate. The CNOT gate is therefore the most efficient gate among all the controlled-U gates.

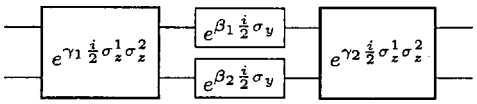
IV. NEAR OPTIMAL UNIVERSAL QUANTUM CIRCUIT

In real physical applications, it is desirable to have a constructive procedure to implement a universal quantum circuit. At this time, there is no explicit way to construct a universal quantum circuit that exactly achieves the minimum upper bound for an arbitrary controlled-U gate U_f. However, we have found a construction procedure for a near optimal universal quantum circuit from an arbitrary controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$ combined with local gates. Depending on the value of γ, the upper bound of this construction is either equal to the minimum or just one more than the minimum applications of U_f as shown in Fig. 2.

An arbitrary two-qubit operation $U\in \mathrm{SU}(4)$ can be written as in Eq. (1), with the parameters c_j in the tetrahedron $OA_1A_2A_3$. Since we have easy access to all the local gates [3,5], we need to implement only the nonlocal part A in Eq. (1). We do this in the following two steps: (1) Apply $e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$ at most $\lceil \pi/2\gamma \rceil$ times to simulate the third component $e^{c_3(i/2)\sigma_z^1\sigma_z^2}$ of A (see Proposition 2 of [3]); (2) Apply $e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$ at most $\lceil \pi/\gamma \rceil$ times to simulate the first two components $e^{c_1(i/2)\sigma_x^1\sigma_x^2}e^{c_2(i/2)\sigma_y^1\sigma_y^2}$ of A (Theorem 3).

The first step follows directly from Proposition 2 in [3]. The construction procedure therein takes at most $\lceil \pi/2\gamma \rceil$ applications when $\gamma\in(0,\pi/2)$, and only two applications when $\gamma=\pi/2$, i.e., for the CNOT gate. We therefore need to realize only the second step. The next theorem identifies all nonlocal gates that can be implemented by two controlled-U gates together with local gates.

Theorem 3. Given two controlled-U gates $e^{\gamma_1(i/2)\sigma_z^1\sigma_z^2}$ and $e^{\gamma_2(i/2)\sigma_z^1\sigma_z^2}$ with $\gamma_1,\gamma_2\in(0,\pi/2]$, all the local equivalence classes of two-qubit gates that can be implemented by these two gates together with local gates can be described as $e^{c_1(i/2)\sigma_x^1\sigma_x^2}\cdot e^{c_2(i/2)\sigma_y^1\sigma_y^2}$ with $0\leqslant c_1+c_2\leqslant \gamma_1+\gamma_2$. Furthermore, we can implement such a gate by the following quantum circuit:



where $\cos\beta_1$ and $\cos\beta_2$ are the two roots of the quadratic equation

$$\begin{aligned}\sin\gamma_1\sin\gamma_2\,x^2+[&\cos^2 c_1+\cos^2 c_2-\cos^2\gamma_1-\cos^2\gamma_2\\&+2(\cos\gamma_1\cos\gamma_2-\cos c_1\cos c_2)\cos(\gamma_1-\gamma_2)]^{1/2}x\\&+\cos\gamma_1\cos\gamma_2-\cos c_1\cos c_2=0.\end{aligned}\tag{3}$$

See Appendix B for a proof. This theorem can be illustrated by Fig. 3, in which the triangle OA_1A_2 is the base of the tetrahedron $OA_1A_2A_3$ and the controlled-U gates $e^{\gamma_1(i/2)\sigma_z^1\sigma_z^2}$ and $e^{\gamma_2(i/2)\sigma_z^1\sigma_z^2}$ correspond to points $[\gamma_1,0]$ and $[\gamma_2,0]$ on OA_1, respectively. The nonlocal gates that can be generated by these two controlled-U gates are shown as the shaded area in Fig. 3. Since the gate $[c_1,c_2,0]$ is locally equivalent to the gate $[\pi-c_1,c_2,0]$, the shaded area consists of two symmetric triangles. (Note that Proposition 2 in [3] is a special case of this theorem by setting $\beta_1=4\pi$ and $\gamma_1=\gamma_2$.) When $\gamma_1=\gamma_2=\pi/2$, i.e., both gates are CNOT gates, the above quantum circuit can implement any gate in the triangle OA_1A_2. In other words, two applications of the CNOT gate can implement those two-qubit gates that are located on the base of the tetrahedron $OA_1A_2A_3$ and only those gates. This result was also implied by Vidal and Dawson [4].

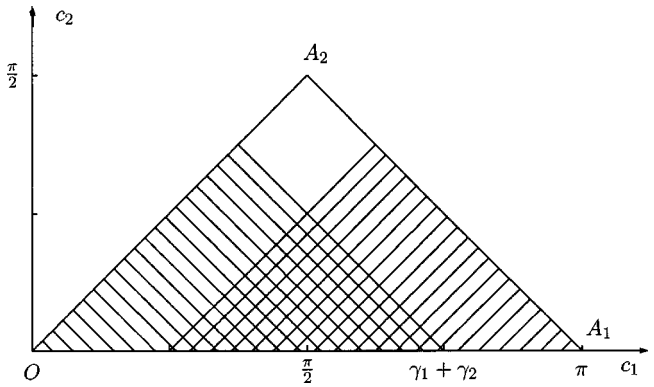


FIG. 3. Nonlocal gates that can be generated by two given controlled-U gates $e^{\gamma_1(i/2)\sigma_z^1\sigma_z^2}$ and $e^{\gamma_2(i/2)\sigma_z^1\sigma_z^2}$.

Since the second step of the procedure is indeed equivalent to implementing any gate in the triangle OA_1A_2, we can now realize it by using Theorem 3. From a given controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$, it is easy to obtain an n-fold product gate $e^{n\gamma(i/2)\sigma_z^1\sigma_z^2}$ by n applications of U_f. We then take $\gamma_1=n\gamma$ and $\gamma_2=m\gamma$. From Theorem 3, to ensure that $e^{n\gamma(i/2)\sigma_z^1\sigma_z^2}$ and $e^{m\gamma(i/2)\sigma_z^1\sigma_z^2}$ can simulate any gate in the triangle OA_1A_2 we require only that the shaded area in Fig. 3 covers the point A_2. This is equivalent to $(m+n)\gamma\geqslant\pi$, whence $m+n=\lceil \pi/\gamma \rceil$. We can therefore choose any positive integers m and n, as long as they satisfy this equality. Moreover, the parameters β_1 and β_2 of the local gates can be determined by solving Eq. (3). Hence we can explicitly simulate any nonlocal gate $e^{c_1(i/2)\sigma_x^1\sigma_x^2}e^{c_2(i/2)\sigma_y^1\sigma_y^2}$ by applying the controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$ at most $\lceil \pi/\gamma \rceil$ times.

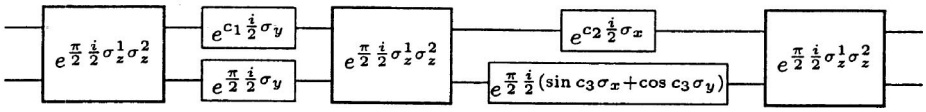
Combining these two steps together, for a given controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$, the constructive approach presented above needs at most $\lceil \pi/\gamma \rceil+\lceil \pi/2\gamma \rceil$ applications for the case $\gamma\in(0,\pi/2)$, or four applications for the case $\gamma=\pi/2$, to implement any arbitrary two-qubit operation. In Fig. 2, the upper bound of this construction procedure is shown as thin lines. It is evident that our procedure is near optimal—it implements a universal quantum circuit with either minimum possible applications of U_f or one more than the minimum.

In [3] we provided an upper bound of $6\lceil \pi/4\gamma \rceil$ applications for an arbitrary controlled-U gate U_f. Since $\lceil \pi/\gamma \rceil+\lceil \pi/2\gamma \rceil\leqslant 6\lceil \pi/4\gamma \rceil$, it is clear that the construction presented here is more efficient by up to five gate applications. Furthermore, since U_f is a basic building block for implementing a universal quantum circuit, this construction also implies improved efficiency (a smaller number of gates) to achieve universality from any arbitrary entangling gate [2,3,5,6].

V. UNIVERSAL QUANTUM CIRCUIT FROM THREE CNOT OR DCNOT GATES

The explicit construction procedure presented above requires four applications of the CNOT gate to implement any arbitrary two-qubit gate. From Theorem 2, we know that the minimum upper bound for the CNOT gate is 3 (see also Fig. 2). Since the CNOT gate with local gates is widely adopted as the standard model of universal quantum computation, it is especially important to find an attractive construction with a minimum number of applications. Recent work has provided constructions with three applications of CNOT [4]. We have found the following simple analytic route to construct a universal quantum circuit from three applications of the CNOT gate with local gates.

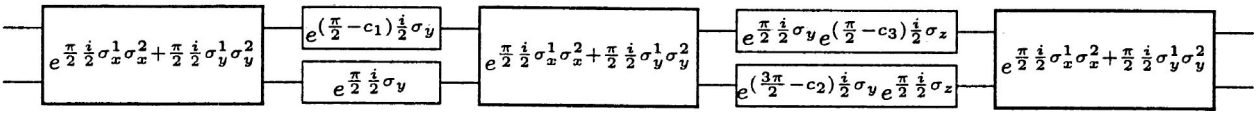
Theorem 4. The following quantum circuit is locally equivalent to a generic nonlocal gate $A = e^{c_1 \frac{i}{2}\sigma_x^1\sigma_x^2} e^{c_2 \frac{i}{2}\sigma_y^1\sigma_y^2} e^{c_3 \frac{i}{2}\sigma_z^1\sigma_z^2}$:



Proof. By direct algebraic computation, we can show that Makhlin's local invariants [10] of the above quantum circuit are identical to those of the nonlocal gate A [See Eq. (25) in [7]]. Therefore this quantum circuit implements a generic nonlocal gate A.

Moreover, we have a similar result for the DCNOT gate, which is defined as the quantum gate performing the operation $|m\rangle \otimes |n\rangle \rightarrow |n\rangle \otimes |m \oplus n\rangle$ [8]. It is easy to prove that the DCNOT gate is locally equivalent to the gate $e^{(\pi/2)(i/2)\sigma_x^1\sigma_x^2+(\pi/2)(i/2)\sigma_y^1\sigma_y^2}$, which corresponds to A_2 ($[\pi/2, \pi/2, 0]$) in Fig. 1.

Theorem 5. The following quantum circuit is locally equivalent to a generic nonlocal gate $A = e^{c_1 \frac{i}{2}\sigma_x^1\sigma_x^2} e^{c_2 \frac{i}{2}\sigma_y^1\sigma_y^2} e^{c_3 \frac{i}{2}\sigma_z^1\sigma_z^2}$:



This theorem can also be proved by direct algebraic computation of Makhlin's invariants, as for Theorem 4. Note that this is not a controlled-U gate. In fact, it is locally equivalent to the iSWAP gate in the computational basis:

$$\text{iSWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

which can be generated naturally by the XY interaction [9]. Theorem 5 thus provides a route to universal quantum circuits from XY coupled qubits that is at least as efficient as any CNOT-based circuit.

VI. CONCLUSION

In summary, we have found the minimum upper bound to construct a universal quantum circuit from any controlled-U gate together with local gates. This minimum upper bound depends only on the single controlled-U parameter γ, as shown in Fig. 2. It shows that among all the controlled-U gates, the CNOT gate is the most efficient, a fact not evident from the previous upper bound result in [3]. An explicit construction of universal quantum circuits from a given controlled-U gate was provided and shown to be close to optimal, i.e., it implements a universal quantum circuit with either minimum applications, or one more than the minimum. In addition, we developed simple analytic ways for both the CNOT and DCNOT (not a controlled-U) gates to construct universal quantum circuits with exactly three applications, which is the least possible for these gates.

ACKNOWLEDGMENTS

We thank the NSF for financial support under ITR Grant No. EIA-0205641. The effort of J.Z., J.V., and K.B.W. is also sponsored by the Defense Advanced Research Projects Agency (DARPA) and the Air Force Laboratory, Air Force Material Command, USAF, under Contract No. F30602-01-2-0524.

APPENDIX A: PROOF OF THEOREM 1

From Refs. [7,11], we know that the Lie algebra $\mathfrak{g}=\mathrm{su}(4)$ has a direct sum decomposition $\mathfrak{g}=\mathfrak{p}\oplus\mathfrak{k}$, where

$$\mathfrak{k}=\mathrm{span}\frac{i}{2}\{\sigma_x^1,\sigma_y^1,\sigma_z^1,\sigma_x^2,\sigma_y^2,\sigma_z^2\},$$

$$\mathfrak{p}=\mathrm{span}\frac{i}{2}\{\sigma_x^1\sigma_x^2,\sigma_x^1\sigma_y^2,\sigma_x^1\sigma_z^2,\sigma_y^1\sigma_x^2,\sigma_y^1\sigma_y^2,\sigma_y^1\sigma_z^2,\sigma_z^1\sigma_x^2,\sigma_z^1\sigma_y^2,\sigma_z^1\sigma_z^2\}. \tag{A1}$$

Note that the Abelian subalgebra

$$\mathfrak{a}=\mathrm{span}\frac{i}{2}\{\sigma_x^1\sigma_x^2,\sigma_y^1\sigma_y^2,\sigma_z^1\sigma_z^2\} \tag{A2}$$

is contained in $\mathfrak{p}$ and is a Cartan subalgebra of the pair $(\mathfrak{g},\mathfrak{k})$. Consider the following adjoint control system defined on $\mathrm{SU}(4)/\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ [11]:

$$\dot{P}=XP,\quad X\in \mathrm{Ad}_{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}\,H_d, \tag{A3}$$

where $P(0)=e$ and $H_d=(i/2)\sigma_z^1\sigma_z^2$. Here H_d is the Hamiltonian that can generate a controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$ directly. Let $a(t)$ be the trajectory generated by $P(t)$ in a Weyl chamber $\mathfrak{a}^+$ that is defined by the tetrahedron $OA_1A_2A_3$ in Fig. 1. It can be shown that

$$\dot{a}(t)=\Gamma(Ad_k(H_d)), \tag{A4}$$

where $\Gamma:\mathfrak{p}\to\mathfrak{a}^+$ is the orthogonal projection onto $\mathfrak{a}^+$ and $k\in\mathrm{SU}(2)\otimes\mathrm{SU}(2)$. From Kostant's convexity theorem [13], we can rewrite Eq. (A4) as

$$\dot{a}(t)=\sum_j \beta_j(t)H_d^j, \tag{A5}$$

where $\Sigma_j\beta_j(t)=1$ with $\beta_j(t)\geqslant 0$, and H_d^j is on the Weyl orbit of H_d. Integrating Eq. (A5) from 0 to $n\gamma$, where γ is determined by the given controlled-U gate $U_f=e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$, we obtain

$$a(n\gamma)=\sum_j \lambda_j n\gamma H_d^j, \tag{A6}$$

where $\lambda_j=(1/n\gamma)\int_0^{n\gamma}\beta_j(t)dt$ and $\Sigma_j\lambda_j=1$. Therefore, the point $a(n\gamma)$ lies in the convex hull of the Weyl orbit of $n\gamma H_d$. This convex hull can be represented by the two tetrahedra $OB_1B_2B_3$ and $A_1C_1C_2C_3$ in Fig. 1. We therefore obtain that every gate generated by n applications of $e^{\gamma(i/2)\sigma_z^1\sigma_z^2}$ together with local gates is locally equivalent to a gate $e^{c_1(i/2)\sigma_x^1\sigma_x^2}e^{c_2(i/2)\sigma_y^1\sigma_y^2}e^{c_3(i/2)\sigma_z^1\sigma_z^2}$, with the parameters c_j satisfying either $0\leqslant c_1+c_2+c_3\leqslant n\gamma$ or $c_1-c_2-c_3\geqslant\pi-n\gamma$.

APPENDIX B: PROOF OF THEOREM 3

A general two-qubit quantum circuit that consists of two controlled-U gates $e^{\gamma_1(i/2)\sigma_z^1\sigma_z^2}$ and $e^{\gamma_2(i/2)\sigma_z^1\sigma_z^2}$ together with local gates can be described as

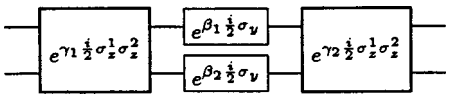
$$e^{\gamma_2(i/2)\sigma_z^1\sigma_z^2}(k_1\otimes k_2)e^{\gamma_1(i/2)\sigma_z^1\sigma_z^2}. \tag{B1}$$

Recall that the local gates k_1 and k_2 can be written in Euler's ZYZ decomposition as

$$k_1=e^{\alpha_1 i\sigma_z}e^{\beta_1 i\sigma_y}e^{\gamma_1 i\sigma_z},$$

$$k_2=e^{\alpha_2 i\sigma_z}e^{\beta_2 i\sigma_y}e^{\gamma_2 i\sigma_z}. \tag{B2}$$

Substituting Eq. (B2) into Eq. (B1), and taking into account the fact that σ_z^1 and σ_z^2 both commute with $\sigma_z^1\sigma_z^2$, we obtain the following quantum circuit that is locally equivalent to Eq. (B1):



We want to find all the nonlocal gates that can be generated by the above quantum circuit by tuning the parameters β_1 and β_2 of the local gates. Following the procedure in [10], we find that Makhlin's local invariants for this quantum circuit are

$$\begin{aligned} g_1&=\cos r_1\cos r_2-\sin r_1\sin r_2\cos\beta_1\cos\beta_2,\\ g_2&=0,\\ g_3&=2(\cos\beta_1+\cos\beta_2)^2\sin^2\gamma_1\sin^2\gamma_2+2\cos^2\gamma_1\\ &\quad+2\cos^2\gamma_2-1-4\cos\beta_1\cos\beta_2\sin\gamma_1\sin\gamma_2\\ &\quad\times\cos(\gamma_1-\gamma_2). \end{aligned} \tag{B3}$$

From. [7], we know that these Makhlin's invariants can also be written as functions of the parameters c_j in the geometric representation:

$$\begin{aligned} g_1&=\cos c_1\cos c_2\cos c_3,\\ g_2&=\sin c_1\sin c_2\sin c_3, \end{aligned} \tag{B4}$$

$$g_3 = 2(\cos^2 c_1 + \cos^2 c_2 + \cos^2 c_3) - 3.$$

To find the corresponding point $[c_1, c_2, c_3]$ of this quantum circuit in the geometric representation, we only need to equate Eqs. (B3) and (B4), and thereby obtain

$$c_3 = 0,$$

$$\cos c_1 \cos c_2 = \cos r_1 \cos r_2 - \sin r_1 \sin r_2 \cos \beta_1 \cos \beta_2, \tag{B5}$$

$$\cos^2 c_1 + \cos^2 c_2 = (\cos \beta_1 + \cos \beta_2)^2 \sin^2 \gamma_1 \sin^2 \gamma_2 + \cos^2 \gamma_1 + \cos^2 \gamma_2 - 2 \cos \beta_1 \cos \beta_2 \times \sin \gamma_1 \sin \gamma_2 \cos(\gamma_1 - \gamma_2).$$

After some algebraic derivations, we obtain the following equations for the tuning parameters β_1 and β_2:

$$\cos \beta_1 + \cos \beta_2 = \frac{\sqrt{\cos^2 c_1 + \cos^2 c_2 - \cos^2 \gamma_1 - \cos^2 \gamma_2 + 2(\cos \gamma_1 \cos \gamma_2 - \cos c_1 \cos c_2)\cos(\gamma_1 - \gamma_2)}}{\sin \gamma_1 \sin \gamma_2}, \tag{B6}$$

$$\cos \beta_1 \cos \beta_2 = \frac{\cos \gamma_1 \cos \gamma_2 - \cos c_1 \cos c_2}{\sin \gamma_1 \sin \gamma_2}.$$

It is clear that $\cos \beta_1$ and $\cos \beta_2$ can be viewed as two roots of the following quadratic equation:

$$f(x) = \sin \gamma_1 \sin \gamma_2 x^2 + [\cos^2 c_1 + \cos^2 c_2 - \cos^2 \gamma_1 - \cos^2 \gamma_2 + 2(\cos \gamma_1 \cos \gamma_2 - \cos c_1 \cos c_2)\cos(\gamma_1 - \gamma_2)]^{1/2} x + \cos \gamma_1 + \cos \gamma_2 - \cos c_1 \cos c_2 = 0. \tag{B7}$$

Since $\gamma_1, \gamma_2 \in (0, \pi/2]$, we have $\sin \gamma_1 \sin \gamma_2 > 0$. To guarantee the existence of two roots in the interval $[-1, 1]$, we need the following three conditions to be satisfied: $f(1) \geqslant 0$, $f(-1) \geqslant 0$ and $\Delta \geqslant 0$, where Δ is the discriminant of the quadratic equation. It is not hard to see that the first two conditions $f(1) \geqslant 0$ and $f(-1) \geqslant 0$ are equivalent to the following inequality:

$$(\sin \gamma_1 \sin \gamma_2 + \cos \gamma_1 \cos \gamma_2 - \cos c_1 \cos c_2)^2 \geqslant \cos^2 c_1 + \cos^2 c_2 - \cos^2 \gamma_1 - \cos^2 \gamma_2 + 2(\cos \gamma_1 \cos \gamma_2 - \cos c_1 \cos c_2)\cos(\gamma_1 - \gamma_2). \tag{B8}$$

After some algebraic derivations, Eq. (B8) can be simplified to $\sin^2 c_1 \sin^2 c_2 \geqslant 0$, which always holds true. Therefore, the conditions $f(1) \geqslant 0$ and $f(-1) \geqslant 0$ are automatically satisfied for any parameters β_1 and β_2. For the third condition, we have

$$\Delta = [\cos c_1 \cos(\gamma_1 + \gamma_2) - \cos c_2]^2 - \sin^2(\gamma_1 + \gamma_2)\sin^2 c_1. \tag{B9}$$

To ensure $\Delta \geqslant 0$, we only need that $0 \leqslant c_1 + c_2 \leqslant \gamma_1 + \gamma_2$. Therefore, all the local equivalence classes that can be generated by these two (controlled-U gates and local gates can be described as $e^{c_1(i/2)\sigma_z^1\sigma_z^2} \cdot e^{c_2(i/2)\sigma_z^1\sigma_z^2}$, where $0 \leqslant c_1 + c_2 \leqslant \gamma_1 + \gamma_2$.

[1] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).
[2] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[3] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. Lett. **91**, 027903 (2003).
[4] G. Vidal and C. M. Dawson, Phys. Rev. A **69**, 010301 (2004); see also F. Vatan and C. Williams, e-print quant-ph/0308006; and V. V. Shende, S. S. Bullock, and I. L. Markov, e-print quant-ph/0308045.
[5] M. J. Bremner, C. M. Dawson, J. L. Dodd, A. Gilchrist, A. W. Harrow, D. Mortimer, M. A. Nielsen, and T. J. Osborne, Phys. Rev. Lett. **89**, 247902 (2002).
[6] D. P. DiVincenzo, Proc. R. Soc. London, Ser. A **454**, 261 (1998).
[7] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. A **67**, 042313 (2003).
[8] D. Collins, N. Linden, and S. Popescu, Phys. Rev. A **64**, 032302 (2001).
[9] N. Schuch and J. Siewert, Phys. Rev. A **67**, 032301 (2003).
[10] Y. Makhlin, Quantum Inf. Process. **1**, 243 (2002).
[11] N. Khaneja, R. Brockett, and S. J. Glaser, Phys. Rev. A **63**, 032308 (2001).
[12] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[13] B. Kostant, Ann. Sci. Ec. Normale Super. **6**, 413 (1973).