# Optimal quantum circuits for general two-qubit gates

Farrokh Vatan* and Colin Williams†
*Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, Pasadena, California 91109-8099, USA*

(Received 13 August 2003; revised manuscript received 11 December 2003; published 22 March 2004)

In order to demonstrate nontrivial quantum computations experimentally, such as the synthesis of arbitrary entangled states, it will be useful to understand how to decompose a desired quantum computation into the shortest possible sequence of one-qubit and two-qubit gates. We contribute to this effort by providing a method to construct an *optimal* quantum circuit for a general two-qubit gate that requires at most 3 controlled-NOT (CNOT) gates and 15 elementary one-qubit gates. Moreover, if the desired two-qubit gate corresponds to a purely real unitary transformation, we provide a construction that requries at most 2 CNOT and 12 one-qubit gates. We then prove that these constructions are optimal with respect to the family of CNOT, $y$-rotation, $z$-rotation, and phase gates.

DOI: 10.1103/PhysRevA.69.032315 PACS number(s): 03.67.Lx, 03.65.Fd, 03.65.Ud

## I. INTRODUCTION

It is known that any $n$-qubit quantum computation can be achieved using a sequence of one-qubit and two-qubit quantum logic gates [1,2]. However, even for two-qubit gates, finding the *optimal* circuit with respect to a particular family of gates is not easy [3]. This is unfortunate because, at the current time, quantum computer experimentalists can only achieve a handful of gate operations within the coherence time of their physical systems [4]. Without a procedure for optimal quantum circuit design, experimentalists might be unable to demonstrate certain quantum computational milestones even though they ought to be within reach. For example, a current experimental goal is the synthesis of any two-qubit entangled state [5]. Although it is known, in principle, how to synthesize any such state [6], the resulting quantum circuits can be suboptimal, requiring excessive numbers of controlled NOT (CNOT) gates, if done injudiciously [7]. The current solution to this problem uses rewrite rules to recognize and eliminate redundant gates. However, a better solution would be to perform optimal design from the outset.

In this paper we give a procedure for constructing an optimal quantum circuit for achieving a general two-qubit quantum computation, up to a global phase, which requires at most 3 CNOT gates and 15 elementary one-qubit gates from the family $\{R_y, R_z\}$. We prove that this construction is *optimal*, in the sense that there is no smaller circuit, using the same family of gates, that achieves this operation. In addition, we show that if the unitary matrix corresponding to our desired gate is purely real, it can be achieved using at most 2 CNOT gates and 12 one-qubit gates.

A flurry of recent results on gate-count minimization for general two-qubit gates report similar findings to us. Vidal and Dawson proved that three CNOT's are sufficient to implement a general $U \in \mathbf{SU}(4)$ and that two-qubit controlled-$V$ operations require at most two CNOT's [8]. Vatan and Williams proved that any $U \in \mathbf{SU}(4)$ requires at most 3 CNOT's and 16 elementary one-qubit $\{R_y, R_z\}$ gates, that any $U \in \mathbf{SO}(4)$ (i.e., real gate) requires at most 2 CNOT's and 12 one-qubit $\{R_y, R_z\}$ gates, and that these constructions are optimal [9]. Later, Shende, Markov, and Bullock reported similar results on circuit complexity for $U \in \mathbf{SU}(4)$, and specialized the complexity bounds depending on which families of one-qubit gates were being used [10]. Fundamentally, all these results rest upon the decomposition of a general $U \in \mathbf{SU}(4)$ given in Refs. [11,12] and used in the GQC quantum circuit compiler [13].

The remainder of the paper is organized as follows. After introducing some notation in Sec. II, we discuss the *magic* basis [11] in Sec. III, and prove (in Theorems 1 and 2) its most important property, namely, that real entangling two-qubit operations become nonentangling in the magic basis. We also prove (via the circuit shown in Fig. 1, first introduced in Ref. [9]) that the magic basis transformations require at most *one* CNOT to implement them explicitly. This is in contrast to Fig. 3 in Ref. [15], which require three CNOT's. It turns out that this compact quantum circuit for the magic basis transformation is the cornerstone of our subsequent constructions for generic two-qubit gates, and our proofs of their optimality. In Sec. IV we present the first such construction, which proves that any two-qubit gate in $\mathbf{SO}(4)$ can be implemented in 12 elementary (i.e., $R_y, R_z$) gates and 2 CNOT's. Theorem 4 extends this result to any two-qubit gate in $\mathbf{O}(4)$ with determinant equal to $-1$, and proves that any such gate requires 12 elementary gates and 3 CNOT's. In Sec. V these results are generalized to the generic two-qubit gates in $\mathbf{U}(4)$ and we provide an explicit construction that requires 15 elementary gates and 3 CNOT's. Finally, in Sec. VI we prove that our construction for generic two-qubit gates is optimal by showing that there is at least one gate in $\mathbf{U}(4)$,

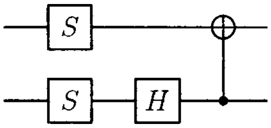

FIG. 1. A circuit for implementing the magic gate $\mathcal{M}$.

*Electronic address: Farrokh.Vatan@jpl.nasa.gov
†Electronic address: Colin.P.Williams@jpl.nasa.gov

namely the two-qubit SWAP gate, which cannot be implemented in fewer than three CNOT's.

## II. NOTATION

Throughout this paper we identify a quantum gate with the unitary matrix that defines its operation. We take rotations about the $y$ and $z$ axes, respectively, $R_y(\theta)$ and $R_z(\alpha)$, as our elementary one-qubit gates; i.e.,

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \quad R_z(\alpha) = \begin{pmatrix} e^{i(\alpha/2)} & 0 \\ 0 & e^{-i(\alpha/2)} \end{pmatrix}.$$

However, we also have three special one-qubit gates: the one-qubit identity matrix, $\mathbb{1}_2$, and the Hadamard gate $H$ and the phase gate $S$ defined as

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

We define two CNOT gates, CNOT1 a standard CNOT gate with the control on the top qubit and the target on the bottom qubit, and CNOT2 with the control and target qubits flipped. Thus

$$\text{CNOT1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \text{CNOT2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

We also use the two-qubit gate SWAP gate, which is defined as

$$\text{SWAP} = \text{CNOT1}\cdot\text{CNOT2}\cdot\text{CNOT1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We use the notation the $\wedge_1(V)$ for the controlled-$V$ gate, where $V \in \mathbf{U}(2)$. Throughout this paper we assume that for the $\wedge_1(V)$ gate the control qubit is the first (top) qubit. Therefore

$$\wedge_1(V) = \begin{pmatrix} \mathbb{1}_2 & \\ & V \end{pmatrix}.$$

In the special case of the $\wedge_1(\sigma_z)$ gate, we use the notation CZ. For any unitary matrix $U$, we denote its inverse, i.e., the conjugate transpose of $U$, by $U^*$.

## III. MAGIC BASIS

There are different ways to define the magic basis [12,14,16]. Here we use the definition used in Refs. [14,16]:

$$\mathcal{M} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 0 & i & 1 \\ 0 & 0 & i & -1 \\ 1 & -i & 0 & 0 \end{pmatrix}.$$

The circuit of Fig. 1 implements this transformation.

The following theorem presents the basic property of the magic basis. This result is already known (see, e.g., Ref. [19]), and we provide a proof for the sake of completeness.

*Theorem 1*. For every real orthogonal matrix $U \in \mathbf{SO}(4)$, the matrix of $U$ in the magic basis, i.e., $\mathcal{M}\cdot U\cdot\mathcal{M}^*$ is tensor product of two two-dimensional special unitary matrices. In other words, $\mathcal{M}\cdot U\cdot\mathcal{M}^* \in \mathbf{SU}(2)\otimes\mathbf{SU}(2)$.

*Proof*. We prove the theorem by showing that for every $A\otimes B \in \mathbf{SU}(2)\otimes\mathbf{SU}(2)$, we have $\mathcal{M}^*(A\otimes B)\mathcal{M} \in \mathbf{SO}(4)$. It is well known that every matrix $A \in \mathbf{SU}(2)$ can be written as the product $R_z(\alpha)R_y(\theta)R_z(\beta)$, for some $\alpha,\beta$, and $\theta$. Therefore any matrix $A\otimes B \in \mathbf{SU}(2)\otimes\mathbf{SU}(2)$ can be written as a product of the matrices of the form $V\otimes\mathbb{1}_2$ and $\mathbb{1}_2\otimes V$, where $V$ is either $R_y(\theta)$ or $R_z(\alpha)$. Thus the proof is complete if $\mathcal{M}^*(V\otimes\mathbb{1}_2)\mathcal{M}$ and $\mathcal{M}^*(\mathbb{1}_2\otimes V)\mathcal{M}$ are in $\mathbf{SO}(4)$. Elementary algebra shows that this is the case.

Since the mapping $A\otimes B \mapsto \mathcal{M}^*(A\otimes B)\mathcal{M}$ is one to one and the spaces $\mathbf{SU}(2)\otimes\mathbf{SU}(2)$ and $\mathbf{SO}(4)$ have the same topological dimension, we conclude that this mapping is an isomorphism between these two spaces. ■

Note that the above theorem is not true for all orthogonal matrices in $\mathbf{O}(4)$. In fact, for every matrix $U \in \mathbf{O}(4)$, either $\det(U)=1$ for which the above theorem holds, or $\det(U)=-1$ for which we have the following theorem.

*Theorem 2*. For every $U \in \mathbf{O}(4)$ with $\det(U)=-1$, the matrix $\mathcal{M}U\mathcal{M}^*$ is a tensor product of two-dimensional unitary matrices and one SWAP gate in the form of the following decomposition: $\mathcal{M}\cdot U\cdot\mathcal{M}^* = (A\otimes B)\cdot\text{SWAP}\cdot(\mathbb{1}_2\otimes\sigma_z)$, where $A,B \in \mathbf{U}(2)$.

*Proof*. First note that $\det(\text{CNOT1})=-1$ and $\det(U\cdot\text{CNOT1})=1$. Then $\mathcal{M}(\text{CNOT1})\mathcal{M}^* = (S^*\otimes S^*)\text{SWAP}(\mathbb{1}_2\otimes\sigma_z)$. Since $\mathcal{M}U\mathcal{M}^* = [\mathcal{M}(U\cdot\text{CNOT}1)\mathcal{M}^*]\cdot[\mathcal{M}(\text{CNOT}1)\mathcal{M}^*]$, the theorem follows from Theorem 1. ■

## IV. REALIZING TWO-QUBIT GATES FROM O(4)

Let $U \in \mathbf{SO}(4)$. Then Theorem 1 shows that $\mathcal{M}U\mathcal{M}^* = A\otimes B$, where $A,B \in \mathbf{SU}(2)$. Therefore $U = \mathcal{M}^*(A\otimes B)\mathcal{M}$. We use the circuit of Fig. 1 for computing the magic basis transform $\mathcal{M}$ to obtain a circuit for computing the unitary operation $U$. This circuit can be simplified by using the decompositions $S = e^{i\pi/4}R_z(\pi/2)$ and $H = \sigma_z R_y(\pi/2)$. Note that $\mathbb{1}_2\otimes\sigma_z$ and the CNOT2 gates commute, and the overall phases $e^{i\pi/4}$ and $e^{-i\pi/4}$ from $S$ and $S^*$ cancel out. Hence we obtain the circuit of Fig. 2 for computing a general two-qubit gate from $\mathbf{SO}(4)$. Thus we have proved the following theorem.

*Theorem 3*. Every two-qubit quantum gate in $\mathbf{SO}(4)$ can be realized by a circuit consisting of 12 elementary one-qubit gates and 2 CNOT gates.

A similar argument and Theorem 2 imply the following construction for gates from $\mathbf{O}(4)$ with determinant equal to $-1$.

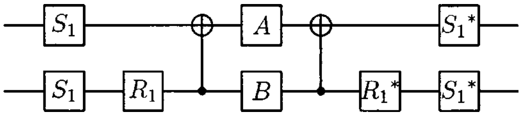

FIG. 2. A circuit for implementing a general transform in $\mathbf{SO}(4)$, where $A,B\in\mathbf{SU}(2)$, $S_1=R_z(\pi/2)$, and $R_1=R_y(\pi/2)$.

*Theorem 4.* Every two-qubit quantum gate in $\mathbf{O}(4)$ with determinant equal to $-1$ can be realized by a circuit consisting of 12 elementary gates and 2 CNOT gates and one SWAP gate (see Fig. 3).

Next, we generalize these results to construct circuits for gates in $\mathbf{U}(4)$.

## V. REALIZING TWO-QUBIT GATES FROM U(4)

It is known that every $U\in\mathbf{U}(4)$ can be written as

$$U=(A_1\otimes A_2)\cdot N(\alpha,\beta,\gamma)\cdot(A_3\otimes A_4), \tag{1}$$

where $A_j\in\mathbf{U}(2)$ and

$$N(\alpha,\beta,\gamma)=\exp[i(\alpha\sigma_x\otimes\sigma_x+\beta\sigma_y\otimes\sigma_y+\gamma\sigma_z\otimes\sigma_z)],$$

for $\alpha,\beta,\gamma\in\mathbb{R}$ (see, e.g., Refs. [11,12,18]). Note that if $U\in\mathbf{SU}(4)$, then we can choose all operations $A_j$ in Eq. (1) from $\mathbf{SU}(2)$. Our construction is based on constructing an optimal circuit for computing $N(\alpha,\beta,\gamma)$. To this end, we first note that $D=\mathcal{M}^*\cdot N\cdot\mathcal{M}$ is a diagonal matrix of the form

$$\mathrm{diag}(e^{i(\alpha-\beta+\gamma)},e^{-i(\alpha-\beta-\gamma)},e^{i(\alpha+\beta-\gamma)},e^{-i(\alpha+\beta+\gamma)}).$$

Therefore $N(\alpha,\beta,\gamma)=\mathcal{M}\cdot D\cdot\mathcal{M}^*$. Utilizing the circuit of Fig. 1 for $\mathcal{M}$, we get the circuit of Fig. 4 for computing $N(\alpha,\beta,\gamma)$. Note that $(S\otimes S)\cdot D\cdot(S^*\otimes S^*)=D$. Then we substitute the right-hand side Hadamard gate of Fig. 4 by three gates, using the following identity: $\mathbb{1}_2\otimes H=$CNOT1$\cdot(\mathbb{1}_2\otimes H)\cdot$CZ. Now, the matrix $D_1=$CZ$\cdot D$ is a diagonal matrix, and

$$(\mathbb{1}_2\otimes H)\cdot D_1(\mathbb{1}_2\otimes H)=\wedge_1(V_2)\cdot(\mathbb{1}_2\otimes V_1), \tag{2}$$

where

$$V_1=\begin{pmatrix} e^{i\gamma}\cos(\alpha-\beta) & ie^{i\gamma}\sin(\alpha-\beta)\\ ie^{i\gamma}\sin(\alpha-\beta) & e^{i\gamma}\cos(\alpha-\beta)\end{pmatrix},$$

$$V_2=\begin{pmatrix} ie^{-2i\gamma}\sin 2\beta & e^{-2i\gamma}\cos 2\beta\\ e^{-2i\gamma}\cos 2\beta & ie^{-2i\gamma}\sin 2\beta\end{pmatrix}.$$

We have the following decompositions for $V_1$ and $\wedge_1(V_2)$ (see also Ref. [7]):

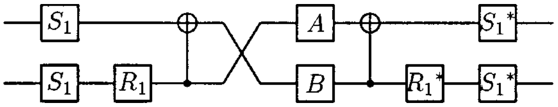

FIG. 3. A circuit for implementing a transform in $\mathbf{O}(4)$ determinant equal to $-1$, where $A,B\in\mathbf{SU}(2)$, $S_1=R_z(\pi/2)$, and $R_1=R_y(\pi/2)$.

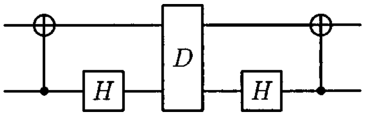

FIG. 4. A circuit for implementing $N(\alpha,\beta,\gamma)$; first version.

$$V_1=e^{i\gamma}R_z\left(-\frac{\pi}{2}\right)\cdot R_y[2(\beta-\alpha)]\cdot R_z\left(\frac{\pi}{2}\right), \tag{3}$$

and

$$\begin{aligned}\wedge_1(V_2)=e^{i(\pi/4-\gamma)}&\left[\mathbb{1}_2\otimes R_z\left(-\frac{\pi}{2}\right)\right]\cdot\text{CNOT1}\cdot\\ &\times\left[\mathbb{1}_2\otimes R_y\left(2\beta-\frac{\pi}{2}\right)\right]\cdot\text{CNOT1}\cdot\\ &\times\left\{R_z\left(2\gamma-\frac{\pi}{2}\right)\otimes\left[R_y\left(\frac{\pi}{2}-2\beta\right)\cdot R_z\left(\frac{\pi}{2}\right)\right]\right\}.\end{aligned} \tag{4}$$

By utilizing Eqs. (2)–(4), we can convert the circuit of Fig. 4 to the circuit of Fig. 5.

Now we focus on the sequence CNOT1$\cdot[\mathbb{1}_2\otimes R_z(-\pi/2)]\cdot$CNOT1 of operations. We have the following identity:

$$\text{CNOT1}\cdot[\mathbb{1}_2\otimes R_z(\theta)]\cdot\text{CNOT1}=\text{CNOT2}\cdot[R_z(\theta)\otimes\mathbb{1}_2]\cdot\text{CNOT2}.$$

After applying this rule, the two consecutive CNOT2 gates on the right-hand side of the circuit reduce to the identity. Also note that, on the left-hand side of the circuit, we can apply the rule

$$[\mathbb{1}_2\otimes R_z(\theta)]\cdot\text{CNOT1}=\text{CNOT1}\cdot[\mathbb{1}_2\otimes R_z(\theta)].$$

Thus the circuit of Fig. 5 can be converted to the circuit of Fig. 6. Note that the operation defined by this circuit has determinant equal to $-1$, thus we need to add a global $e^{i(\pi/4)}$ phase to get the special unitary operation $N(\alpha,\beta,\gamma)$ exactly. Now utilizing the circuit of Fig. 6 and the canonical decomposition (1) we could get a circuit to realize the operation $U\in\mathbf{U}(4)$. Note that in this process, the left- and right-hand side operations $R_z(\pi/2)$ and $R_z(-\pi/2)$ of Fig. 6 will be "absorbed" by adjacent $A_j$. The final result is the circuit of Fig. 7, and we have proved the following theorem.

*Theorem 5.* Every two-qubit quantum gate in $\mathbf{U}(4)$ can be realized, up to a global phase, by a circuit consisting of 15 elementary one-qubit gates and 3 CNOT gates.

The construction given in Theorem 5 is *optimal*. To prove this it is sufficient to place a lower bound on the number of CNOT gates needed to implement a generic two-qubit gate. This is because Ref. [15] already shows that we need at least

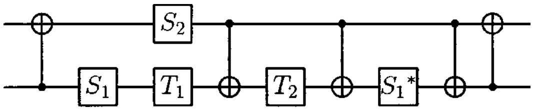

FIG. 5. A circuit for implementing $N(\alpha,\beta,\gamma)$; second version. Here $S_1=R_z(\pi/2)$, $S_2=R_z(2\gamma-\pi/2)$, $T_1=R_y(\pi/2-2\alpha)$, and $T_2=R_y(2\beta-\pi/2)$.

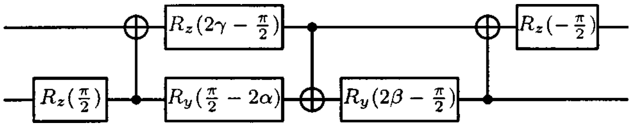
$R_z(2\gamma-\frac{\pi}{2})$
$R_z(-\frac{\pi}{2})$
$R_z(\frac{\pi}{2})$
$R_y(\frac{\pi}{2}-2\alpha)$
$R_y(2\beta-\frac{\pi}{2})$

FIG. 6. A circuit for implementing $N(\alpha,\beta,\gamma)$; third version. A global $e^{i(\pi/4)}$ phase is missing here.

15 elementary one-qubit gates to implement a generic two-qubit gate. So we need only concern ourselves with the minimum required number of CNOT gates. We prove in the next section that three CNOT gates are needed in the general case.

We wish to emphasize that our decomposition is *constructive*. To see this, note that we can use Kraus and Cirac's methods [12] to decompose any desired two-qubit gate into the form given by Eq. (1). All parameters in this decomposition may be determined constructively. Thereafter, it only remains to reduce the $N(\alpha,\beta,\gamma)$ matrix to an explicit quantum circuit. This we can do immediately using the circuit template in Fig. 6. By concatenating these two processes we can find the optimal circuit for any generic two-qubit operation constructively.

## VI. THREE CNOT GATES ARE NEEDED

To show that the construction of Theorem 5 is optimal, we prove that there is at least one gate in $\mathbf{U}(4)$, namely the two-qubit SWAP gate, a real unitary matrix having a determinant of −1, which requires no less than three CNOT gates.

In the proof of the following theorem we utilize the notion of *entangling power* introduced in Ref. [17]. For a unitary operation $U\in\mathbf{U}(4)$, the entangling power of $U$ is defined as

$$\mathrm{EP}(U)=\underset{|\psi_1\rangle\otimes|\psi_2\rangle}{\mathrm{average}}[E(U|\psi_1\rangle\otimes|\psi_2\rangle)],$$

where the average is over all product states $|\psi_1\rangle\otimes|\psi_2\rangle\in\mathbb{C}^2\otimes\mathbb{C}^2$ distributed according to the uniform distribution (in general, we can define EP with regards to any distribution, but here we only consider the uniform distribution). In the above formula $E$ is the linear entropy *entanglement measure* defined for $|\psi\rangle\in\mathbb{C}^4$ as follows:

$$E(|\psi\rangle)=1-\mathrm{tr}_1\rho^2,$$

where $\rho=\mathrm{tr}_2|\psi\rangle\langle\psi|$ and $\mathrm{tr}_j$ denotes the result of tracing out the $j$th qubit. Note that $0\leqslant E(|\psi\rangle)\leqslant\frac{3}{4}$, and the lower or upper bound is obtained if $|\psi\rangle$ is a product state or a maximally entangled state, respectively. In Ref. [17] the following simple formula for calculating EP is presented:

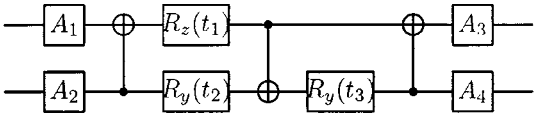

FIG. 7. A circuit for implementing a transform in $\mathbf{U}(4)$.

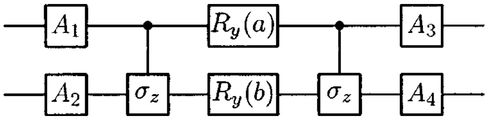

FIG. 8. A circuit consisting of two CNOT gates in terms of CZ gates.

$$\mathrm{EP}(U)=\frac{5}{9}-\frac{1}{36}[\langle U^{\otimes 2},T_{1,3}U^{\otimes 2}T_{1,3}\rangle + \langle(\mathrm{SWAP}\cdot U)^{\otimes 2},T_{1,3}(\mathrm{SWAP}\cdot U)^{\otimes 2}T_{1,3}\rangle],$$

where the Hilbert-Schmidt scalar product $\langle A,B\rangle$ is defined as $\langle A,B\rangle=\mathrm{tr}(A^{\dagger}B)$ and the permutation $T_{1,3}$ on $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ is the transposition $T_{1,3}|a,b,c,d\rangle=|c,b,a,d\rangle$ on the system of four qubits.

We will utilize the following basic properties of the function EP:

(i) For every $U\in\mathbf{U}(4)$ we have $0\leqslant\mathrm{EP}(U)\leqslant\frac{2}{9}$.
(ii) For every $A,B\in\mathbf{U}(2)$ we have $\mathrm{EP}(A\otimes B)=0$.
(iii) For every $U\in\mathbf{U}(4)$ and $A,B\in\mathbf{U}(2)$ we have $\mathrm{EP}[(A\otimes B)\cdot U]=\mathrm{EP}[U\cdot(A\otimes B)]=\mathrm{EP}(U)$.
(iv) $\mathrm{EP}(U)=\mathrm{EP}(U^*)$.
(v) $\mathrm{EP}(\mathrm{CNOT})=\frac{2}{9}$ and $\mathrm{EP}(\mathrm{SWAP})=0$.

We will also use the simple fact that SWAP cannot be written as $\mathrm{SWAP}=A\otimes B$, where, $A,B\in\mathbf{U}(2)$.

*Theorem 6.* To compute the SWAP at least three CNOT gates are needed.

*Proof.* We construct a proof by contradiction. Suppose that there is a circuit computing SWAP and consists of less than three CNOT gates. We consider two possible cases.

*Case 1.* Suppose that SWAP is computed by a circuit consisting of two CNOT gates. We substitute each CNOT gate by a small subcircuit in terms of CZ (controlled-$\sigma_z$) gate; i.e.,

$$\mathrm{CNOT}=(\mathbb{1}_2\otimes H)\cdot\mathrm{CZ}\cdot(\mathbb{1}_2\otimes H).$$

Then by utilizing the following commutation rules,

$$\mathrm{CZ}\cdot[\mathbb{1}_2\otimes R_z(t)]=[\mathbb{1}_2\otimes R_z(t)]\cdot\mathrm{CZ},$$

$$\mathrm{CZ}\cdot[R_z(t)\otimes\mathbb{1}_2]=[R_z(t)\otimes\mathbb{1}_2]\cdot\mathrm{CZ},$$

we obtain the simplified circuit of Fig. 8 for computing the SWAP gate. Note that in this figure we choose the top (first) qubit as the control qubit for the CZ gates, but we could choose the other qubit as the control qubit as well, since the action of the CZ gate is not change by switching the control and target qubits. Now, let

$$U=\mathrm{CZ}\cdot[R_y(a)\otimes R_y(b)]\cdot\mathrm{CZ}.$$

Then

$$\mathrm{EP}(U)=\mathrm{EP}(\mathrm{SWAP})=\frac{1}{18}[3-\cos(2a)-\cos(2b)-\cos(2a)\cos(2b)]=0.$$

Therefore $a,b \in \{0,\pi\}$. Thus we have the following four possible cases for the unitary operation $U$:

(i) if $a=b=0$, then $U=\mathbb{1}_2$;
(ii) if $a=0, b=\pi$, then $U=\sigma_z \otimes R_y(\pi)$;
(iii) if $a=\pi, b=0$, then $U=R_y(\pi) \otimes \sigma_z$;
(iv) if $a=b=\pi$, then $U=-\sigma_x \otimes \sigma_x$.

In each case, we conclude that $\text{SWAP}=V_1 \otimes V_2$, for some $V_1, V_2 \in \mathbf{U}(2)$, which is a contradiction.

*Case 2.* Suppose that SWAP is computed by a circuit consisting of only one CNOT gate; for example,

$$\text{SWAP} = (A_1 \otimes A_2) \cdot \text{CNOT}1 \cdot (A_3 \otimes A_4),$$

where $A_j \in \mathbf{U}(2)$. Then $\text{EP}(\text{SWAP})=\text{EP}(\text{CNOT})$, which again is a contradiction. ■

## VII. CONCLUSION

In this paper we prove tight bounds on the numbers of one-qubit gates and CNOT gates needed to implement generic two-qubit quantum computations. In addition, we give a constructive procedure for finding such decompositions, which uses the Kraus–Cirac decomposition to find the core entangling operation underlying the two-qubit gate, i.e., $N(\alpha,\beta,\gamma)$, and then substitutes the discovered parameter values into an equivalent circuit template for $N(\alpha,\beta,\gamma)$ as shown in Fig. 6. The net result is an explicit circuit for any desired two-qubit unitary operation that uses at most 3 CNOT's and 15 elementary $y$- or $z$-single qubit rotations.

We point out that it is possible to decompose a desired unitary operation into many different families of quantum gates. For example, the basis of all one-qubit gates augmented with CNOT was first studied in Ref. [2], and was shown to be capable of implementing any $n$-qubit unitary operation *exactly*. This scheme has the advantage that only a single, fixed, type of two-qubit gate need be built. Similar schemes are known that use different fixed entangling operations such as $i$SWAP gates (in superconducting quantum computing) and $\sqrt{\text{SWAP}}$ gates (in spintronic quantum computing). In addition, other decompositions are possible that use parametrized two-qubit gates. These may lead to more efficient factorizations in special cases, but also make for a more complicated quantum computer architecture.

The motivation for our work comes from the fact that it is still very difficult, experimentally, to implement multiple quantum gates. Thus, in order to attain near term experimental milestones, it will be important to minimize the number of gates they require. Although our scheme yields minimal circuits for generic two qubit operations, further reductions are still possible in certain special cases. We therefore augment our procedure with rewrite rules, to find even simpler circuits if they exist. Hence our new construction brings certain state synthesis tasks within the grasp of experimentalists.

In addition, as quantum circuits for (arbitrary) $n$-qubit operations are always expressed in terms of a sequence of one-qubit and two-qubit gates, by designing component two-qubit operations minimally, we can sometimes improve the efficiency of implementing $n$-qubit computations.

## ACKNOWLEDGMENTS

The research described in this paper was performed at the Jet Propulsion Laboratory (JPL), California Institute of Technology, under contract with National Aeronautics and Space Administration (NASA). We would like to thank the sponsors, the National Security Agency (NSA), and the Advanced Research and Development Activity (ARDA), for their support.

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

[2] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. H. Margolus, P. W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[3] D. P. DiVincenzo and J. Smolin, in *Proceedings of the Workshop on Physics and Computation, PhysComp'94* (IEEE Computer Society, Los Alamitos, CA, 1994), p. 14.

[4] *Quantum Computing: Where Do We Want to Go Tomorrow?*, edited by S. L. Braunstein (Wiley-VCH, New York, 1999).

[5] ARDA Quantum Computing Roadmap available at http://qist.lanl.gov (2003).

[6] C. P. Williams and L. Song, in *Proceedings of SPIE Aerosense 2003* (International Society for Optical Engineering, Bellingham, WA, 2003).

[7] G. Cybenko, Comput. Sci. Eng. **3**, 27 (2001).

[8] G. Vidal and C. M. Dawson, e-print quant-ph/0307177.

[9] F. Vatan and C. P. Williams, e-print quant-ph/0308006.

[10] V. Shende, I. Markov, and S. Bullock, e-print quant-ph/0308033.

[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] 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).

[14] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

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

[16] S. Hill and W. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

[17] P. Zanardi, C. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301(R) (2000).

[18] J. Zhang, J. Vala, Sh. Sastry, and K. B. Whaley, Phys. Rev. A **67**, 042313 (2003).

[19] Y. Makhlin, Quantum Inf. Processing 1, 243 (2002).