

Optimal Design of Two-Qubit Quantum Circuits

Farrokh Vatan and Colin Williams

Jet Propulsion Laboratory, California Institute of Technology

4800 Oak Grove Drive, Pasadena, CA 91109-809, USA

Abstract

Current quantum computing hardware is unable to sustain quantum coherent operations for more than a handful of gate operations. Consequently, if near-term experimental milestones, such as synthesizing arbitrary entangled states, or performing fault-tolerant operations, are to be met, it will be necessary to minimize the number of elementary quantum gates used.

In order to demonstrate non-trivial 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 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 requires at most 2 CNOTs 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.

1 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 [13, 2]. However, even for two-qubit gates, finding the *optimal* circuit with respect to a particular family of gates is not easy [9]. 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 [5]. 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 [1]. Although it is known, in principle, how to synthesize any such state [17], the resulting quantum circuits can be sub-optimal, requiring excessive numbers of CNOT gates, if done injudiciously [8]. 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 3 CNOTs are sufficient to implement a general $U \in \text{SU}(4)$ and that two-qubit controlled- V operations require at most 2 CNOTs [16]. Vatan and Williams proved that any $U \in \text{SU}(4)$ requires at most 3 CNOTs, and 16 elementary one-qubit $\{R_y, R_z\}$ gates, that any $U \in \text{SO}(4)$ (i.e., real gate) requires at most 2 CNOTs and 12 one-qubit $\{R_y, R_z\}$ gates, and that these constructions are optimal [15]. Later, Shende, Markov, and Bullock reported similar results on circuit complexity for $U \in \text{SU}(4)$, and specialized the complexity bounds depending on which families of one-qubit gates were being used [14]. Fundamentally, all these results rest upon the decomposition of a general $U \in \text{SU}(4)$ given in [11, 12] and used in the GQC quantum circuit compiler [6].

The remainder of the paper is organized as follows. After introducing some notation, we discuss the *magic* basis [11], and prove (in Theorems 1 and 2) its most important

property, namely, that real entangling two-qubit operations become non-entangling in the magic basis. We also prove (via the circuit shown in Figure 2, first introduced in [15]) that the magic basis transformations require at most *one* CNOT to implement them explicitly. This is in contrast to Figure 3 in [7], which required three CNOTs. 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. Next, in Theorem 3, we present the first such construction, which proves that any two-qubit gate in $\text{SO}(4)$ can be implemented in 12 elementary (i.e., R_y , R_z) gates and 2 CNOTs. Theorem 4 extends this results to any two-qubit gate in $\text{O}(4)$ with determinant equal to -1 , and proves that any such gate requires 12 elementary gates and 3 CNOTs. Theorem 5 then generalizes these results to generic two-qubit gates in $\text{U}(4)$, and provides an explicit construction that requires 15 elementary gates and 3 CNOTs. Finally, we prove that our construction for generic two-qubit gates is optimal by showing that there is at least one gate in $\text{U}(4)$, namely the two-qubit SWAP gate, which cannot be implemented in fewer than 3 CNOTs.

Notation

Throughout this paper we identify a quantum gate with the unitary matrix that defines its operation.

Throughout this paper we identify a quantum gate with the unitary matrix that defines its operation. We use the usual rotations about the y and z -axis as one-qubit elementary gates:

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

We also use the following standard notation for one-qubit Hadamard and phase gates:

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

We denote the identity matrix of order 2 by \mathbb{I}_2 .

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

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



Figure 1: The SWAP gate.

The two-qubit gate $\text{SWAP} = \text{CNOT1} \cdot \text{CNOT2} \cdot \text{CNOT1}$ gate, is defined by the matrix

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and is denoted by the symbol of Figure 1 in the figures.

We use the notation the $\Lambda_1(V)$ for the controlled- V gate, where $V \in \text{U}(2)$. Throughout this paper we assume that for the $\Lambda_1(V)$ gate the control qubit is the first (top) qubit. Therefore,

$$\Lambda_1(V) = \begin{pmatrix} \mathbb{I}_2 & & \\ & & V \end{pmatrix}.$$

In the special case of the $\Lambda_1(\sigma_z)$ gate, we use the notation CZ. For any unitary matrix U , we denote its inverse, i.e., the conjugate-transpose of U , by U^* .

2 Magic basis

There are different ways to define the magic basis [3, 10, 12]. Here we use the definition used in [3, 10]:

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

The circuit of Figure 2 implements this transformation.

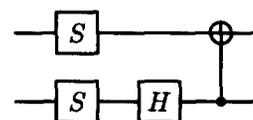


Figure 2: A circuit for implementing the magic gate \mathcal{M} .

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

Proof. We prove the theorem by showing that for every $A \otimes B \in \text{SU}(2) \otimes \text{SU}(2)$, we have $\mathcal{M}^* (A \otimes B) \mathcal{M} \in \text{SO}(4)$. It is well-known that every matrix $A \in \text{SU}(2)$ can be written as the product $R_z(\alpha) R_y(\theta) R_z(\beta)$, for some α, β , and θ . Therefore any matrix $A \otimes B \in \text{SU}(2) \otimes \text{SU}(2)$ 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 $\text{SO}(4)$. We have

$$\begin{aligned} & \mathcal{M}^{-1} (R_y(\theta) \otimes \mathbb{1}_2) \mathcal{M} \\ &= \begin{pmatrix} \cos \theta/2 & 0 & 0 & -\sin \theta/2 \\ 0 & \cos \theta/2 & \sin \theta/2 & 0 \\ 0 & -\sin \theta/2 & \cos \theta/2 & 0 \\ \sin \theta/2 & 0 & 0 & \cos \theta/2 \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} & \mathcal{M}^{-1} (R_z(\alpha) \otimes \mathbb{1}_2) \mathcal{M} \\ &= \begin{pmatrix} \cos \alpha/2 & \sin \alpha/2 & 0 & 0 \\ -\sin \alpha/2 & \cos \alpha/2 & 0 & 0 \\ 0 & 0 & \cos \alpha/2 & -\sin \alpha/2 \\ 0 & 0 & \sin \alpha/2 & \cos \alpha/2 \end{pmatrix}. \end{aligned}$$

We have similar results for the cases of $\mathbb{1}_2 \otimes R_y(\theta)$ and $\mathbb{1}_2 \otimes R_z(\alpha)$.

Since the mapping $A \otimes B \mapsto \mathcal{M}^* (A \otimes B) \mathcal{M}$ is one-to-one and the spaces $\text{SU}(2) \otimes \text{SU}(2)$ and $\text{SO}(4)$ 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 $\text{O}(4)$. In fact, for every matrix $U \in \text{O}(4)$, 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 $U \in \text{O}(4)$ with $\det(U) = -1$, the matrix $\mathcal{M} U \mathcal{M}^*$ is a tensor product of 2-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 $A, B \in \text{U}(2)$.

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 $\mathcal{M} U \mathcal{M}^* = (\mathcal{M} (U \cdot \text{CNOT1}) \mathcal{M}^*) \cdot (\mathcal{M} (\text{CNOT1}) \mathcal{M}^*)$, the theorem follows from Theorem 1. ■

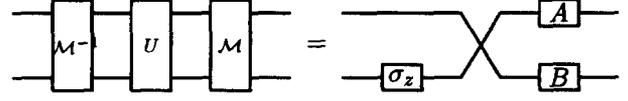


Figure 3: The action of the magic basis on $U \in \text{O}(4)$ with $\det(U) = -1$.

3 Realizing two-qubit gates from $\text{O}(4)$

Let $U \in \text{SO}(4)$. Then Theorem 1 shows that $\mathcal{M} U \mathcal{M}^* = A \otimes B$, where $A, B \in \text{SU}(2)$. Therefore, $U = \mathcal{M}^* (A \otimes B) \mathcal{M}$. We use the circuit of Figure 2 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 Figure 4 for computing a general two-qubit gate from $\text{SO}(4)$. Thus

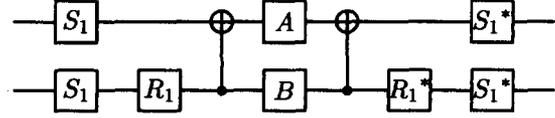


Figure 4: A circuit for implementing a general transform in $\text{SO}(4)$, where $A, B \in \text{SU}(2)$, $S_1 = R_z(\pi/2)$ and $R_1 = R_y(\pi/2)$.

we have proved the following theorem.

Theorem 3 Every two-qubit quantum gate in $\text{SO}(4)$ 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 $\text{O}(4)$ with determinant equal to -1 .

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

The circuit that realizes this construction is shown in Figure 5.

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

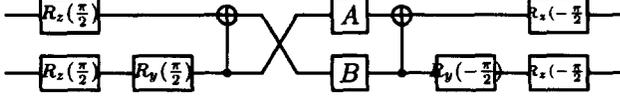


Figure 5: A circuit for implementing a transform in $O(4)$ determinant equal to -1 .

4 Realizing two-qubit gates from $U(4)$

It is known that every $U \in SU(4)$ can be written as $U = (A_1 \otimes A_2) \cdot N \cdot (A_3 \otimes A_4)$, where $A_j \in SU(2)$ and

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

for $\alpha, \beta, \gamma \in \mathbb{R}$ (see, e.g., [11, 12, 19]).

A simple calculation shows

$$N = \exp(i(\alpha \sigma_x \otimes \sigma_x + \beta \sigma_y \otimes \sigma_y + \gamma \sigma_z \otimes \sigma_z)) = e^{i\gamma} \begin{pmatrix} \cos(\alpha - \beta) & 0 & 0 & i \sin(\alpha - \beta) \\ 0 & e^{-2i\gamma} \cos(\alpha + \beta) & -i e^{-2i\gamma} \sin(\alpha + \beta) & 0 \\ 0 & -i e^{-2i\gamma} \sin(\alpha + \beta) & e^{-2i\gamma} \cos(\alpha + \beta) & 0 \\ i \sin(\alpha - \beta) & 0 & 0 & \cos(\alpha - \beta) \end{pmatrix}.$$

Then $D = \mathcal{M}^* \cdot N \cdot \mathcal{M}$ is a diagonal matrix of the form

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

Therefore, $N = \mathcal{M} \cdot D \cdot \mathcal{M}^*$. Utilizing the circuit of Figure 2 for \mathcal{M} , we get the circuit of Figure 6 for computing U , where $D_1 = (S \otimes S) \cdot D \cdot (S^* \otimes S^*)$. Then we substitute

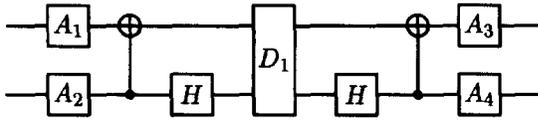


Figure 6: A circuit for implementing a transform in $SU(4)$.

the right hand-side Hadamard gate of Figure 6 by 3 gates, using the following identity: $\mathbb{1}_2 \otimes H = \text{CNOT1} \cdot (\mathbb{1}_2 \otimes H) \cdot \text{CZ}$. Now, the matrix $D_2 = \text{CZ} \cdot D_1$ is a diagonal matrix, and for some t we have $D_2 = \Lambda_1(V) \cdot (\mathbb{1}_2 \otimes R_z(t))$, where $V \in U(2)$. Note that $\det(D_2) = \det(V) = -1$. On the other hand, we have $(\mathbb{1}_2 \otimes H) \cdot \Lambda_1(V) \cdot (\mathbb{1}_2 \otimes H) = \Lambda_1(V_1)$, for some $V_1 \in U(2)$ with $\det(V_1) = -1$. Let $\Lambda_1(V_1) = e^{i\pi/4} \Lambda_1(V_2)$, where $V_2 \in SU(2)$. The result of [8] shows that

$$\Lambda_1(V_2) = (\mathbb{1}_2 \otimes R_z(\theta_1)) \cdot \text{CNOT1} \cdot (\mathbb{1}_2 \otimes V_3) \cdot \text{CNOT1} \cdot (\mathbb{1}_2 \otimes V_4),$$

where $V_3 = R_z(\beta_1) \cdot R_y(\alpha_1)$ and $V_4 = R_y(-\alpha_1) \cdot R_z(\beta_3)$. These substitutions lead to the circuit of Figure 7, where

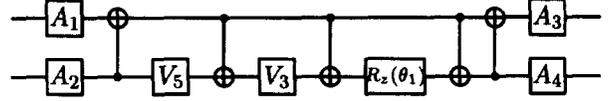


Figure 7: A circuit for implementing a transform in $SU(4)$.

$V_5 = V_4 \cdot H \cdot R_z(t) \cdot H \in SU(2)$. Now we focus on the sequence $\text{CNOT1} \cdot (\mathbb{1}_2 \otimes R_z(\theta_1)) \cdot \text{CNOT1}$ of operations. We have the following identity

$$\text{CNOT1} \cdot (\mathbb{1}_2 \otimes R_z(\theta_1)) \cdot \text{CNOT1} = \text{CNOT2} \cdot (R_z(\theta_1) \otimes \mathbb{1}_2) \cdot \text{CNOT2}.$$

Then two consecutive CNOT2 gates on the right hand side of the circuit reduce to the identity, and the gate $R_z(\theta_1)$ will be “absorbed” by the gate A_3 . With these simplifications we get the circuit of Figure 8.

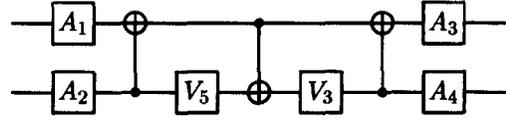


Figure 8: A circuit for implementing a transform in $SU(4)$.

Now let $V_5 = R_z(\bar{t}_3) \cdot R_y(\bar{t}_2) \cdot R_z(\bar{t}_1)$. The $R_z(\bar{t}_1)$ operation of V_5 commutes with the CNOT2 gate on its left, and will be “absorbed” by A_2 . The final result is the circuit of Figure 9.

Theorem 5 Every two-qubit quantum gate in $U(4)$ 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 [7] already shows that we need at least 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.

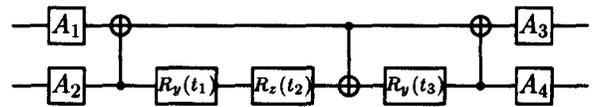


Figure 9: A circuit for implementing a transform in $SU(4)$.

5 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 $U(4)$, namely the two-qubit SWAP gate, a real unitary matrix having a determinant of -1 , which requires no less than 3 CNOT gates. Hence we prove the following statement.

Theorem 6 *To compute the SWAP gate at least 3 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 enumerate the possible cases.

Case 1. Suppose that

$$\text{SWAP} = (U_1 \otimes U_2) \cdot \text{CNOT1} \cdot (U_3 \otimes U_4) \cdot \text{CNOT1} \cdot (U_5 \otimes U_6), \quad (1)$$

where $U_j \in U(2)$. The above argument shows that we can assume, without loss of generality, that $U_3 = R_y(\alpha)$. Then

$$\begin{aligned} & \text{SWAP} \cdot (U_1 \otimes U_2)^* \cdot \text{SWAP} \cdot (U_5 \otimes U_6)^* \\ & = \text{SWAP} \cdot \text{CNOT1} \cdot (U_3 \otimes U_4) \cdot \text{CNOT1}. \end{aligned}$$

Since $\text{SWAP} \cdot (V_1 \otimes V_2) \cdot \text{SWAP} = V_2 \otimes V_1$, and $\text{SWAP} \cdot \text{CNOT1} = \text{CNOT1} \cdot \text{CNOT2}$, we have

$$\text{CNOT1} \cdot \text{CNOT2} \cdot (R_y(\alpha) \otimes U_4) \cdot \text{CNOT1} = A \otimes B, \quad (2)$$

for some $A, B \in U(2)$. Now suppose that $U_4 = R_z(\beta_1) \cdot R_y(\theta) \cdot R_z(\beta_2)$. Note that $\text{CNOT1} \cdot (\mathbb{1}_2 \otimes R_z(\alpha)) \cdot \text{CNOT1}$ is a diagonal matrix. Thus we can rewrite the above equation as follows:

$$\begin{aligned} & \text{CNOT1} \cdot \text{CNOT2} \cdot (R_y(\alpha) \otimes (R_y(\theta))) \cdot \text{CNOT1} \\ & = D_1 \cdot (A \otimes B) \cdot D_2, \quad (3) \end{aligned}$$

where $D_1, D_2 \in U(4)$ are *diagonal* matrices. Then we have $D_1 \cdot (A \otimes B) \cdot D_2 \in O(4)$, which implies that the only possible way that the identity (3) holds is that $D_1 \cdot (A \otimes B) \cdot D_2 = R_y(t_1) \otimes R_y(t_2)$, for some t_1, t_2 . Now we consider the *entangling power* of quantum gates (see, e.g., [18]). We have

$$\begin{aligned} & \text{entangling-power} [\text{CNOT1} \cdot \text{CNOT2} \cdot (R_y(\alpha) \otimes (R_y(\theta))) \cdot \text{CNOT1}] \\ & = \frac{1}{9} (3 - \cos(2\alpha) - 2 \cos(2\theta) \cos^2 \alpha), \quad (4) \end{aligned}$$

and $\text{entangling-power} [R_y(t_1) \otimes R_y(t_2)] = 0$. Therefore, the only way that (2) could be satisfied is by having $\alpha =$

$\theta = 0$. In this case, the identity (3) implies that $\text{SWAP} = R_y(t_1) \otimes R_y(t_2)$, which we know is not possible.

Case 2. Suppose that

$$\text{SWAP} = (U_1 \otimes U_2) \cdot \text{CNOT2} \cdot (U_3 \otimes U_4) \cdot \text{CNOT1} \cdot (U_5 \otimes U_6), \quad (5)$$

where $U_j \in U(2)$. We apply an argument similar the one we applied to the previous case. First we note that, without loss if generality, we can assume that $U_3 = R_z(\beta_1) R_y(\alpha)$ and $U_4 = R_y(\theta) R_z(\beta_2)$. Then, by argument similar to the previous case, we arrive to the following identities:

$$\begin{aligned} & \text{CNOT2} \cdot \text{CNOT1} \cdot (R_z(\beta_1) R_y(\alpha) \otimes \\ & R_y(\theta) R_z(\beta_2)) \cdot \text{CNOT1} = A \otimes B, \quad (6) \end{aligned}$$

$$\begin{aligned} & \text{CNOT2} \cdot \text{CNOT1} \cdot (R_y(\alpha) \otimes R_y(\theta)) \cdot \text{CNOT1} \\ & = R_y(t_1) \otimes R_y(t_2). \quad (7) \end{aligned}$$

As for the entangling power, (7) implies that

$$\begin{aligned} & \text{entangling-power} [\text{CNOT2} \cdot \text{CNOT1}] \cdot (R_y(\alpha) \otimes R_y(\theta)) \cdot \text{CNOT1} \\ & = \frac{1}{9} (3 + \cos(2\alpha) + 2 \cos(2\theta) \cos^2 \alpha). \quad (8) \end{aligned}$$

This implies that $\alpha = \theta = \frac{\pi}{2}$; and with assumption, (6) implies that

$$\begin{aligned} & \text{entangling-power} [\text{CNOT2} \cdot \text{CNOT1} \cdot \\ & (R_z(\beta_1) R_y(\frac{\pi}{2}) \otimes R_y(\frac{\pi}{2}) R_z(\beta_2))] \cdot \text{CNOT1}] \\ & = \frac{1}{9} (3 - \cos(2\beta_1) - 2 \cos(2\beta_2) \cos^2 \beta_1). \quad (9) \end{aligned}$$

The identity implies that $\beta_1 = \beta_2 = 0$. Then, since

$$\text{CNOT2} \cdot (R_y(\frac{\pi}{2}) \otimes R_y(\frac{\pi}{2})) \cdot \text{CNOT1} = R_y(\frac{\pi}{2}) \otimes H,$$

the identity (5) implies that $\text{SWAP} = U \otimes V$, which is impossible.

Case 3. Suppose that

$$\text{SWAP} = (U_1 \otimes U_2) \cdot \text{CNOT1} \cdot (U_3 \otimes U_4), \quad (10)$$

where $U_j \in U(2)$. Then the method of the previous cases implies that $\text{CNOT1} \cdot \text{CNOT2} = U \otimes V$. This is impossible, since, for example, $\text{entangling-power} [\text{CNOT1} \cdot \text{CNOT2}] = \frac{4}{9}$. ■

Acknowledgment. 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.

References

- [1] ARDA Quantum Computing Roadmap available at <http://qist.lanl.gov>, 2003.
- [2] A. Barenco and C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. H. Margolus, P. W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Physical Review A*, vol. 52, no. 5, pp. 3457–3467, 1995.
- [3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, *Physical Review A*, vol. 54, no. 5, pp. 3824–3851, 1996.
- [4] P. O. Boykin, T. Mor, M. Pulver, F. Vatan, and V. Roychowdhury, A new universal and fault-tolerant quantum basis, *Information Processing Letters*, vol. 75, pp. 101–107, 2000.
- [5] S. L. Braunstein (ed.), *Quantum Computing : Where Do We Want to Go Tomorrow?*, (Wiley-VCH, 1999).
- [6] M. J. Bremner, C. M. Dawson, J. L. Dodd, A. Gilchrist, A. W. Harrow, D. Mortimer, M. A. Nielsen, Practical scheme for quantum computation with any two-Qubit entangling gate, and T. J. Osborne, *Phys. Rev. Lett.*, vol. 89, 247902, 2002.
- [7] S. Bullock and I. Markov, Arbitrary two-qubit computation in 23 elementary gates, *Phys. Rev. A*, vol. 68, 012318, 2003.
- [8] G. Cybenko, Reducing quantum computations to elementary unitary operations, *Computing in Science & Engineering*, vol. 3, no. 2, pp. 27–32, March-April 2001.
- [9] D. P. DiVincenzo and J. Smolin, Results on two-bit gate design for quantum computers, *Proc. Workshop on Physics and Computation, PhysComp'94*, 14–23, 1994.
- [10] S. Hill and W. Wootters, Entanglement of a pair of quantum bits, *Physical Review Letters*, vol. 78, no. 26, pp. 5022–5025, 1997.
- [11] N. Khaneja, R. Brockett and S. J. Glaser, Time optimal control in spin systems, *Phys. Rev. A*, vol. 63, 032308, 2001.
- [12] B. Kraus and J. I. Cirac, Optimal creation of entanglement using a two-qubit gate, *Physical Review A*, vol. 63, no. 6, pp. 062309/1–8, June 2001.
- [13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, 2000).
- [14] V. Shende, I. Markov and S. Bullock, On universal gate libraries and generic minimal two-qubit quantum circuits, e-print quant-ph/0308033, 2003.
- [15] F. Vatan and C. P. Williams, Optimal realization of an arbitrary two-Qubit quantum gate, e-print quant-ph/0308006, 2003.
- [16] G. Vidal and C. M. Dawson, A universal quantum circuit for two-qubit transformations with three CNOT gates, e-print quant-ph/0307177, 2003.
- [17] C. P. Williams and L. Song, Quantum circuits for synthesizing any pure or mixed n -qubit state, *Proceedings 2003 International Symposium on Microelectronics, SPIE*, 2003.
- [18] P. Zanardi, C. Zalka, and L. Faoro, Entangling power of quantum evolutions, *Physical Review A*, vol. 62, R30301, 2000.
- [19] J. Zhang, J. Vala, Sh. Sastry, and K. B. Whaley, Geometric theory of nonlocal two-qubit operations, *Physical Review A*, vol. 67, no. 4, pp. 042313/1–18, 2003.
- [20] J. Zhang, J. Vala, Sh. Sastry, and K. B. Whaley, Exact Two-Qubit Universal Quantum Circuit, *Physical Review Letters*, vol. 91, no. 2, pp. 027903/1–4, 2003.