Optimal simulation of Deutsch gates and the Fredkin gate

Nengkun Yu[1,2] and Mingsheng Ying[3,4]
[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada*
[2]*Department of Mathematics & Statistics, University of Guelph, Guelph, Ontario, Canada*
[3]*Center for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering and Information Technology, University of Technology, Sydney, NSW 2007, Australia*
[4]*State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China*
(Received 16 November 2014; published 6 March 2015)

In this paper, we study the optimal simulation of the three-qubit unitary using two-qubit gates. First, we completely characterize the two-qubit gate cost of simulating the Deutsch gate (controlled-controlled gate) by generalizing our result on the two-qubit cost of the Toffoli gate. The function of any Deutsch gate is simply a three-qubit controlled-unitary gate and can be intuitively explained as follows: The gate outputs the states of the two control qubits directly, and applies the given one-qubit unitary u on the target qubit only if both the states of the control qubits are $|1\rangle$. Previously, it was only known that five two-qubit gates are sufficient for implementing such a gate [Sleator and Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995)]. We show that if the determinant of u is 1, four two-qubit gates are optimal. Otherwise, five two-qubit gates are required. For the Fredkin gate (the controlled-SWAP gate), we prove that five two-qubit gates are necessary and sufficient, which settles the open problem introduced in Smolin and DiVincenzo [Phys. Rev. A **53**, 2855 (1996)].

DOI: 10.1103/PhysRevA.91.032302 PACS number(s): 03.67.−a, 03.65.Ud, 07.05.Bx

I. INTRODUCTION

A fundamental issue of several interacting systems is to quantify the strength of this interaction, in other words, to compare interactions of different types of systems or particles and different physical manifestations of the interaction. In order to provide an intellectual background of comparing the interaction strength of different physical systems, a robust characterization is highly desirable. Quantum information theory has provided new insights into this question. In particular, there has been considerable progress in quantifying the strength of Hamiltonian and unitary interactions [1–9] for bipartite systems. The starting point was the theory of entanglement of quantum states which quantifies how much nonclassical correlation the state embodies. The most intriguing approach might be to study how much bipartite correlation is needed to implement a multipartite correlation. In other words, how many two-qubit unitaries are needed to simulate a given multiqubit gate? One difficulty that the characterization of multipartite entanglement is clear. A possible approach is to consider those symmetric gates.

A great challenge in the contemporary science and engineering is building a full-fledged quantum computer, which is essentially a large quantum circuit consisting of basic quantum logical gates. In order to implement a quantum algorithm, even in a small size, one has to simulate a relatively high level of control over the multiqubit quantum system. It has also been experimentally demonstrated that two-qubit gates can be realized with high fidelity using the current technology, for example, two-qubit gate with superconducting quibts have been presented with fidelities higher than 90% [10]. Finding more efficient ways to implement quantum gates may allow small-scale quantum computing tasks to be demonstrated on a shorter time scale.

Due to its significance in quantum computing, lots of efforts have been devoted to study the two-qubit gate cost of controlled unitary; see [11–15] as an incomplete list. The answer to the optimal implementation of the Toffoli gate was found recently [16]. It would be of interest to understand the two-qubit gate cost of the Deutsch gate, the generalization of the Toffoli gate. Another gate that has received particular attention is the three-qubit conditional SWAP gate—the Fredkin gate. The Fredkin gate is of interest because it is a universal gate for classical reversible computation [17], which means that any logical or arithmetic operation can be constructed entirely of Fredkin gates. Ekert and Macchiavello [18] use the quantum version of the Fredkin gate to design quantum circuits for error-correcting quantum computations with the symmetric subspace method [19]. The experimental and theoretical pursuit of efficient implementation of the Fredkin gate using a sequence of single- and two-qubit gates has a long history. A simple optical model to realize a reversible, potentially error-free logic Fredkin gate is proposed in [20]. Chau and Wilczek give a specific six-gate construction of the Fredkin gate in 1995 [21]. An analytic five-gate construction is presented and numerical tests suggest that this construction is minimal [22].

In this paper, the two-qubit gate cost on simulating any Deutsch gate and Fredkin gate is completely characterized. More precisely, it is shown that any Deutsch gate (controlled-controlled u) requires at least four two-qubit gates to simulate. If the determinant of the unitary u is one, we provide a four-gate construction. Otherwise, five-gate implementation is optimal. Later, we present a theoretical proof that five two-qubit gates are indeed the optimal implementation for the Fredkin gate.

Each three-qubit gate is regarded as a unitary transformation performed on a tripartite system ABC; all the two-qubit gates employed to implement the three-qubit gate can be simply classified into three classes: class $\mathcal{K}_{AB}$, the gates acting on the subsystem AB; class $\mathcal{K}_{BC}$, the gates on BC; and class $\mathcal{K}_{AC}$, the gates on AC.

Bipartite unitary U_{AR} acting on a qubit system A and a general system R is said to be a controlled gate with control on A if it can be decomposed into the form of

$$U_{AR} = |0_A\rangle\langle 0_A| \otimes u_0 + |1_A\rangle\langle 1_A| \otimes u_1.$$

A controlled-controlled-u gate—the Deutsch gate, acting on three qubits, namely A, B, and C. Here A and B are control qubits, and C is the target qubit with computational basis $\{|0\rangle,|1\rangle\}$ for each qubit. Upon input $|abc\rangle$, the gate will output the states of A and B directly, and apply u on the system C only if both the states of A and B are $|1\rangle$.

The validity of the following propositions is showed in [16].

Proposition 1. Any two-dimensional $2 \otimes 2$ state subspace contains some product state.

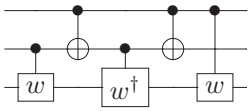
Proposition 2. If $U_{AB}U_{AC}$ is a three-qubit controlled unitary with control on A, where $U_{AB} \in \mathcal{K}_{AB}$ and $U_{AC} \in \mathcal{K}_{AC}$, then there exist v_{B0}, v_{B1} and w_{C0}, w_{C1} being one-qubit unitaries on $\mathcal{H}_B$ and $\mathcal{H}_C$ such that

$$U_{AB}U_{AC} = |0\rangle\langle 0| \otimes v_{B0} \otimes w_{C0} + |1\rangle\langle 1| \otimes v_{B1} \otimes w_{C1}.$$

II. OPTIMAL SIMULATION OF DEUTSCH GATES

The particular "controlled-controlled" gates—Deutsch gates—were introduced by Deutsch in [23] where the universality of such gates was proved for the first time. They are adequate for constructing networks with any possible quantum computational property.

It is proved in [14] that any Deutsch gate can be implemented using only five two-qubit gates,



where W is a unitary satisfying $w^2 = u$.

To study the two-qubit gate cost for implementing the general "controlled-controlled-u" gate, we only need to deal with the diagonal unitary as follows,

$$V(\theta_1,\theta_2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & e^{i\theta_1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & e^{i\theta_2} \end{pmatrix}.$$

$V(\theta_1,\theta_2)_{ABC}$ is regarded as a tripartite unitary with control on A and B. It can be considered as a controlled unitary with control on A, B or C,

$$V(\theta_1,\theta_2)_{ABC} = |0\rangle\langle 0| \otimes I_{BC} + |1\rangle\langle 1| \otimes R_{BC},$$

where $R = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\theta_1}|10\rangle\langle 10| + e^{i\theta_2}|11\rangle\langle 11|$.

Also, we can verify that $V(\theta_1,\theta_2)_{ABC}$ is invariant under the permutation of A and B, that is,

$$V(\theta_1,\theta_2)_{ABC} = S_{AB}V(\theta_1,\theta_2)_{ABC}S_{AB},$$

with S_{AB} denoting the SWAP gate on A and B.

The following result from [16] is useful for our discussion.

Theorem 1. $V(0,\theta) = I - (1 - e^{i\theta})|111\rangle\langle 111|$ requires five two-qubit gates to simulate, provided that $e^{i\theta} \neq 1$.

One can easily verify the following equation:

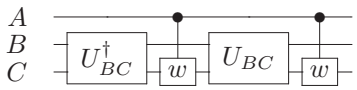
$$\begin{aligned} V(0,\theta_2 - \theta_1)_{ABC} &= V(\theta_1,\theta_2)_{ABC}W(-\theta_1)_{AB} \\ &= W(-\theta_1)_{AB}V(\theta_1,\theta_2)_{ABC}, \end{aligned}$$

where $W(\theta) = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11|$. Therefore, we can conclude the following.

Lemma II.1. Any three-qubit controlled-controlled gate $V(\theta_1,\theta_2)$ with $e^{i\theta_1} \neq e^{i\theta_2}$ requires at least four two-qubit gates to simulate.

If such $V(\theta_1,\theta_2)$ can be implemented by three or less two-qubit gates, then four two-qubit gates or less can simulate some $V(0,\theta) = I - (1 - e^{i\theta})|111\rangle\langle 111|$ with $e^{i\theta} \neq 1$, which conflicts with Theorem 1.

Interestingly, for $V(-\theta,\theta)$, we can find the following simulation circuit consisting of four two-qubit gates, therefore, it is optimal for $e^{i\theta} \neq 1$.



where

$$w = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix},$$

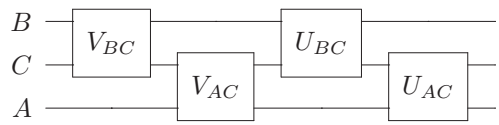
and U_{BC} satisfies that

$$U_{BC}(w_C \otimes I_B)U_{BC}^\dagger = \mathrm{diag}\{e^{i\theta/2},e^{-i\theta/2},e^{-i\theta/2},e^{i\theta/2}\}.$$

Such U_{BC} does exist since the eigenvalues of $w_C \otimes I_B$ are $\{e^{i\theta/2},e^{-i\theta/2},e^{-i\theta/2},e^{i\theta/2}\}$.

In order to study the case $e^{i\theta_1} \neq e^{-i\theta_2}$, we show the following.

Lemma II.2. There exists no $U_{AC},V_{AC} \in \mathcal{K}_{AC}, U_{BC},V_{BC} \in \mathcal{K}_{BC}$ such that $V(\theta_1,\theta_2)$ can be implemented in the following circuit with $e^{i(\theta_1+\theta_2)} \neq 1$ and $e^{i\theta_1} \neq e^{i\theta_2}$,



Proof. We only need to study the case that all the two-qubit gates are nonlocal. The circuit is

$$U_{AC}U_{BC}V_{AC}V_{BC} = V(\theta_1,\theta_2)_{ABC},$$

then $U_{AC}U_{BC}V_{AC} = V(\theta_1,\theta_2)_{ABC}V_{BC}^\dagger$ is a controlled unitary with control on A by noticing that $V(\theta_1,\theta_2)_{ABC}$ is a controlled unitary with control on A. Moreover, for any input state $|i\rangle_A|y\rangle_B|z\rangle_C$, the A part's state of the following state is $|i\rangle_A$,

$$U_{AC}U_{BC}V_{AC}|i\rangle_A|y\rangle_B|z\rangle_C.$$

Invoking Proposition 1, there is $|z_0\rangle_C$ such that $V_{AC}|0\rangle_A|z_0\rangle_C$ is the product; after moving the local unitaries, we assume

$$V_{AC}|0\rangle_A|0\rangle_C = |0\rangle_A|0\rangle_C.$$

Thus, the A part's state of the following state is $|0\rangle_A$,

$$U_{AC}U_{BC}V_{AC}|0\rangle_A|y\rangle_B|0\rangle_C = U_{AC}U_{BC}|0\rangle_A|y\rangle_B|0\rangle_C.$$

There are three cases about the state $U_{BC}|y\rangle_B|0\rangle_C$.

Case 1. There exists some $|y_0\rangle_B$ such that $U_{BC}|y_0\rangle_B|0\rangle_C$ is entangled; we can assume there is $0 < \lambda < 1$ such that

$$U_{BC}|y_0\rangle_B|0\rangle_C = \sqrt{\lambda}|\alpha\rangle_B|0\rangle_C + \sqrt{1-\lambda}|\alpha^\perp\rangle_B|1\rangle_C.$$

Define $|\chi\rangle_{ABC} = U_{AC}U_{BC}|0\rangle_A|0\rangle_B|z_0\rangle_C$, then $\chi_A = |0\rangle\langle 0|$. We know that

$$|\chi\rangle_{ABC} = \sqrt{\lambda}|\Phi\rangle_{AC}|\alpha\rangle_B + \sqrt{1-\lambda}|\Psi\rangle_{AC}|\alpha^\perp\rangle_B,$$
$$\Rightarrow \chi_A = \lambda\Phi_A + (1-\lambda)\Psi_A \Rightarrow \Phi_A = \Psi_A = |0\rangle\langle 0|,$$

where $|\Phi\rangle = U_{AC}|00\rangle_{AC}$ and $|\Psi\rangle = U_{AC}|01\rangle_{AC}$.

Therefore, U_{AC} is a controlled unitary with control on system A, so $V_{AC} = U_{BC}^\dagger U_{AC}^\dagger V(\theta_1,\theta_2)_{ABC} V_{BC}^\dagger$. We can assume that

$$U_{AC} = |0\rangle\langle 0| \otimes I_C + |1\rangle\langle 1| \otimes w_{C_1},$$
$$V_{AC} = |0\rangle\langle 0| \otimes I_C + |1\rangle\langle 1| \otimes w_{C_2}.$$

We know that $U_{BC}V_{BC} = I_{BC}$ and

$$w_{C_1}U_{BC}w_{C_2}V_{BC} = R_{BC}$$
$$\Rightarrow U_{BC}w_{C_2}U_{BC}^\dagger = w_{C_1}^\dagger R_{BC} = w_{C_1}^\dagger \oplus w_{C_1}^\dagger D,$$

where $D = \mathrm{diag}\{e^{i\theta_1}, e^{i\theta_2}\}$ and

$$R = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\theta_1}|10\rangle\langle 10| + e^{i\theta_2}|11\rangle\langle 11|.$$

Notice that $\{e^{i\varphi_1}, e^{i\varphi_2}, e^{i\varphi_1}, e^{i\varphi_2}\}$ are the eigenvalues of $U_{BC}w_{C_2}U_{BC}^\dagger$, where $e^{i\varphi_1}, e^{i\varphi_2}$ are the eigenvalues of w_{C_2}. It is direct to see that $w_{C_1}^\dagger$ cannot have two identical eigenvalues ($w_{C_1}^\dagger$ is not identity), then $w_{C_1}^\dagger$ and $w_{C_1}^\dagger D$ enjoy the same eigenvalues, and then they have the same determinant.

$$\det\left(w_{C_1}^\dagger\right) = \det\left(w_{C_1}^\dagger D\right) = \det\left(w_{C_1}^\dagger\right)\det(D)$$
$$\Rightarrow \det(D) = 1 \Rightarrow e^{i(\theta_1+\theta_2)} = 1.$$

This is not possible.

Now, we only need to deal with the case that for any $|y\rangle_B$, $U_{BC}|y\rangle_B|0\rangle_C$ is the product. There are two cases.

Case 2. There exist some $|\beta\rangle_B$ and local unitary w_C on system C such that $U_{BC}|y\rangle_B|0\rangle_C = |\beta\rangle_B w_C|y\rangle_C$, U_{AC} maps $\{|0\rangle_A\} \otimes \mathcal{H}_C$ to itself. Therefore, U_{AC} is a controlled unitary with control on A, so V_{AC}. The rest of the argument is the same as case 1.

Case 3. There exists some state on system C, wlog, says $|0\rangle_C$, and local unitary v_B on system B such that

$$U_{BC}|y\rangle_B|0\rangle_C = v_B|y\rangle_B|0\rangle_C.$$

Therefore, U_{BC} is a controlled unitary with control on C. By moving this v_B to V_{BC}, we make the assumption that

$$U_{BC} = |0\rangle\langle 0| \otimes I_B + |1\rangle\langle 1| \otimes u_B.$$

Note that for any $|y\rangle_B$, we have

$$V(\theta_1,\theta_2)_{ABC}|0\rangle_A(V_{BC}^\dagger|y\rangle_B|0\rangle_C) = U_{AC}U_{BC}V_{AC}|0\rangle_A|y\rangle_B|0\rangle_C,$$
$$\Rightarrow |0\rangle_A(V_{BC}^\dagger|y\rangle_B|0\rangle_C) = U_{AC}|0\rangle_A|y\rangle_B|0\rangle_C.$$

Thus, part B's state of $V_{BC}^\dagger|y\rangle_B|0\rangle_C$ is $|y\rangle_B$ for all $|y\rangle_B \in \mathcal{H}_B$, which means that there exists some $|\gamma\rangle_C$ such that $V_{BC}|y\rangle_B|\gamma\rangle_C = |y\rangle_B|0\rangle_C$, for all $|y\rangle_B$.

Therefore, one can find a unitary w_C such that

$$V_{BC} = |0\rangle\langle\gamma| \otimes I_B + |1\rangle\langle\gamma^\perp| \otimes v_B.$$

In order to simplify the structure of the two-qubit gates, we observe that

$$V_{BC}^T V_{AC}^T U_{BC}^T U_{AC}^T = V(\theta_1,\theta_2)_{ABC}^T = V(\theta_1,\theta_2)_{ABC},$$

hence $V_{BC}^T V_{AC}^T U_{BC}^T U_{AC}^T$ also provides an implementation of $V(\theta_1,\theta_2)_{ABC}$.

Now we consider the state,

$$V_{BC}^T V_{AC}^T U_{BC}^T|x\rangle_A|0\rangle_B|0\rangle_C = V_{BC}^T V_{AC}^T|x\rangle_A|0\rangle_B|0\rangle_C.$$

The arguments of cases 1 and 2 exclude the following possibilities:

(i) $V_{AC}^T|x\rangle_A|0\rangle_C$ is entangled for some $|x\rangle_A$.

(ii) There exists some $|\delta\rangle_A$ and local unitary w_C on system C such that $V_{AC}^T|x\rangle_A|0\rangle_C = |\delta\rangle_A w_C|x\rangle_C$ for all $|x\rangle_A$.

The only case left is that there exists some state $|\phi\rangle_C$ on system C, and local unitary w_A on system A such that $V_{AC}^T|x\rangle_A|0\rangle_C = w_A|x\rangle_A|\phi\rangle_C$ for all $|x\rangle_A$.

According to $V_{AC}|0\rangle_A|0\rangle_C = |0\rangle_A|0\rangle_C$, we can choose $|\phi\rangle = |0\rangle$. Thus V_{AC} is a controlled gate with control system C, i.e.,

$$V_{AC} = |0\rangle\langle 0| \otimes w_A + |1\rangle\langle 1| \otimes v_A.$$

By studying part B's state of

$$U_{AC}U_{BC}V_{AC}V_{BC}|0\rangle_A|y\rangle_B|0\rangle_C = |0\rangle_A|y\rangle_B|0\rangle_C,$$

we see that $|\gamma\rangle_C$ defined in V_{BC} equals to $|0\rangle_B$ or $|1\rangle_B$, up to some global phase. To see this, we assume that $|0\rangle_C = a|\gamma\rangle_C + b|\gamma^\perp\rangle_C$ for $ab \neq 0$. Then the state of part B becomes a mixed state for general input $|0\rangle_A|y\rangle_B|0\rangle_C$ since u_B is not the identity up to some global phase and U_{BC} is nonlocal. For the case $|\gamma\rangle_C = |0\rangle_C$, we know that the four two-qubit gates are all controlled gate with control on system C, which implies that

$$R_{BC} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\theta_1}|10\rangle\langle 10| + e^{i\theta_2}|11\rangle\langle 11|$$

is a local unitary, then $e^{i\theta_1} = e^{i\theta_2}$. It is impossible.

For the case $|\gamma\rangle_C = |1\rangle_C$, let X_C be the NOT (flip) gate such that $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$, then one can verify that

$$V(\theta_1,\theta_2)_{ABC}(U_{AC}X_C)(X_C U_{BC}X_C)(X_C V_{AC}X_C)(X_C V_{BC}).$$

Now, we know that $U_{AC}X_C, X_C U_{BC}X_C, X_C V_{AC}X_C$ and $X_C V_{BC}$ are all controlled gate with control on system C. This also leads us to the impossible conclusion that $R_{BC} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\theta_1}|10\rangle\langle 10| + e^{i\theta_2}|11\rangle\langle 11|$ is local. ■

Now we are able to show the following.

Theorem 2. $V(\theta_1,\theta_2)$ requires five two-qubit gates to simulate, provided that $e^{i(\theta_1+\theta_2)} \neq 1$ and $e^{i\theta_1} \neq e^{i\theta_2}$.

Proof. We assume that $V(\theta_1,\theta_2)$ can be simulated by four two-qubit gates where $e^{i(\theta_1+\theta_2)} \neq 1$ and $e^{i\theta_1} \neq e^{i\theta_2}$. If the four gates belong to two of the classes $\mathcal{K}_{AB}, \mathcal{K}_{AC}, \mathcal{K}_{BC}$, the circuits that need to be considered are just $U_{AC}U_{BC}V_{AC}V_{BC} = V(\theta_1,\theta_2)_{ABC}$ and $U_{AB}U_{BC}V_{AB}V_{BC} = V(\theta_1,\theta_2)_{ABC}$. The previous one is shown to be impossible in Lemma 2. The latter one is impossible by noticing $W(-\theta_1)_{AB}U_{AB}$ is a two-qubit

unitary on AB system,

$$V(0,\theta_2-\theta_1)_{ABC} = W(-\theta_1)_{AB}V(\theta_1,\theta_2)_{ABC} = (W(-\theta_1)_{AB}U_{AB})U_{BC}V_{AB}V_{BC}.$$

Now, we can apply Theorem 1 directly.

Otherwise, the four gates belong to three of the classes $\mathcal{K}_{AB},\mathcal{K}_{AC},\mathcal{K}_{BC}$; then there exist two gates belonging to the same class. Due to the symmetric property of the $V(\theta_1,\theta_2)$, we only need to consider the following two cases.

Case 1. Two gates belong to $\mathcal{K}_{AB}$, then at least one of them lies in the front or the end of the circuit. Then we conclude that this is impossible by applying Theorem 1 and

$$V(0,\theta_2-\theta_1)_{ABC} = W(-\theta_1)_{AB}V(\theta_1,\theta_2)_{ABC} = V(\theta_1,\theta_2)_{ABC}W(-\theta_1)_{AB}.$$

Case 2. Two gates belong to $\mathcal{K}_{BC}$. The four gates are $U_{AB}\in\mathcal{K}_{AB}$, $U_{AC}\in\mathcal{K}_{AC}$ and $U_{BC},V_{BC}\in\mathcal{K}_{BC}$. According to symmetric properties of the $V(\theta_1,\theta_2)$, the three possible circuits are as follows.

Subcase 1. $U_{BC}U_{AC}V_{BC}U_{AB} = V(\theta_1,\theta_2)_{ABC}$; this is impossible by applying Theorem 1 and noticing

$$V(0,\theta_2-\theta_1)_{ABC} = V(\theta_1,\theta_2)_{ABC}W(-\theta_1)_{AB} = U_{BC}U_{AC}V_{BC}[U_{AB}W(-\theta_1)_{AB}].$$

Subcase 2. $U_{BC}U_{AB}V_{BC}U_{AC} = V(\theta_1,\theta_2)_{ABC}$. Let S_{BC} be the SWAP gate defined in subsystems B, C; then we can observe that this circuit can be reduced to Lemma 2 by noticing that $S_{BC}U_{BC},S_{BC}V_{BC}\in\mathcal{K}_{BC}$ and $S_{BC}U_{AC}S_{BC}\in\mathcal{K}_{AB}$ and $S_{BC}V(\theta_1,\theta_2)_{ABC}S_{BC}$ is the controlled-controlled gate with control on systems A and C, and

$$S_{BC}V(\theta_1,\theta_2)_{ABC}S_{BC} = (S_{BC}U_{BC})U_{AB}(S_{BC}V_{BC})(S_{BC}U_{AC}S_{BC}).$$

Subcase 3. $U_{BC}U_{AB}U_{AC}V_{BC} = V(\theta_1,\theta_2)_{ABC}$. Observe that $U_{AB}U_{AC} = U_{BC}^{\dagger}V(\theta_1,\theta_2)_{ABC}V_{BC}^{\dagger}$ is a controlled unitary with control on A. According to direct calculation, we can conclude that $R_{BC} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\theta_1}|10\rangle\langle 10| + e^{i\theta_2}|11\rangle\langle 11|$ shares eigenvalues with a local unitary by employing Proposition 2. That is impossible.

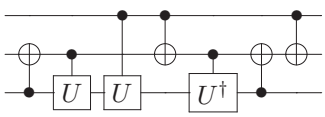
Therefore, one can conclude that $V(\theta_1,\theta_2)$ requires five two-qubit gates to simulate for $e^{i(\theta_1+\theta_2)}\neq 1$ and $e^{i\theta_1}\neq e^{i\theta_2}$. ■

III. OPTIMAL SIMULATION OF FREDKIN GATE

The Fredkin gate is the three-qubit gate that swaps the last two qubits if the first qubit is $|1\rangle$. The matrix form of the Fredkin gate is given as

$$F = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1 \end{pmatrix}.$$

It is shown that the Fredkin gate can be simulated by five two-qubit gates in the following circuit [22], where $U^2 = X$ with X being the Pauli flip matrix,



In this section, we show the following.

Theorem 3. Four two-qubit gates are not sufficient for implementing F_{ABC}.

The proof also heavily depends on the discussion of the possible circuit structures.

The following symmetric properties of the Fredkin gate are helpful to decrease the number of cases: The Fredkin gate is invariant under the permutation of B and C and it is symmetric, i.e., $F_{ABC} = F_{ACB}$ and $F_{ABC} = F_{ABC}^T$ with $F_{ACB} = S_{BC}F_{ABC}S_{BC}$, where S stands for the SWAP gate.

F_{ABC} can be regarded as a tripartite unitary of Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_C$. We can easily verify F_{ABC} is a controlled unitary with control on A by noticing

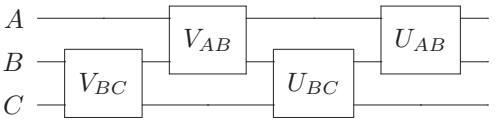
$$F_{ABC} = |0\rangle\langle 0|\otimes I_{BC} + |1\rangle\langle 1|\otimes S_{BC}.$$

In order to explain our idea and key technique of showing four gates are not enough, we first demonstrate that the Fredkin gate cannot be decomposed into two two-qubit gates by dividing the problem into two cases. Case 1: The two gates belong to classes $\mathcal{K}_{AB},\mathcal{K}_{BC}$, then U_{AB} must be a controlled unitary with control on A, direct calculation leads to the confliction; Case 2: The two gates belong to two of the classes $\mathcal{K}_{AB},\mathcal{K}_{AC}$; we assume the circuit is $U_{AB}U_{AC} = F_{ABC}$, invoking Proposition 2. We can assert that S_{BC} is a local unitary by figuring out directly the form of the controlled unitary. That is impossible. Therefore, we show the following.

Lemma III.1. Two two-qubit gates are not sufficient for implementing F_{ABC}.

In the rest, we show that four nonlocal two-qubit gates are not sufficient for implementing F_{ABC}. We first study two special circuits.

Lemma III.2. There is no $U_{AB},V_{AB}\in\mathcal{K}_{AB}$, $U_{BC},V_{BC}\in\mathcal{K}_{BC}$ such that the Fredkin gate can be implemented in the following circuit,



.

Proof. Assume that the circuit implements the Fredkin gate, that is,

$$U_{AB}U_{BC}V_{AB}V_{BC} = F_{ABC}.$$

Then, $U_{AB}U_{BC}V_{AB}$ is a controlled unitary with control on A. Moreover, for any input state $|0\rangle_A|\psi\rangle_{BC}$, the A part's state of $U_{AB}U_{BC}V_{AB}|0\rangle_A|\psi\rangle_{BC}$ is $|0\rangle_A$. We assume $V_{AB}|0\rangle_A|0\rangle_B = |0\rangle_A|0\rangle_B$ after moving the local unitaries by invoking Proposition 1. Thus, the A part's state of the following state is $|0\rangle_A$,

$$U_{AB}U_{BC}V_{AB}|0\rangle_A|0\rangle_B|z\rangle_C = U_{AB}U_{BC}|0\rangle_A|0\rangle_B|z\rangle_C.$$

There are three cases about the states $U_{BC}|0\rangle_B|z\rangle_C$.

Case 1. There exists some $|z_0\rangle_C$ such that $U_{BC}|0\rangle_B|z_0\rangle_C$ is entangled. There is $0 < \lambda < 1$ such that

$$U_{BC}|0\rangle_B|z_0\rangle_C = \sqrt{\lambda}|0\rangle_B|\alpha\rangle_C + \sqrt{1-\lambda}|1\rangle_B|\alpha^\perp\rangle_C.$$

Define $|\chi\rangle_{ABC} = U_{AB}U_{BC}|0\rangle_A|0\rangle_B|z_0\rangle_C$, and we know that

$$|\chi\rangle_{ABC} = \sqrt{\lambda}|\Phi\rangle_{AB}|\alpha\rangle_C + \sqrt{1-\lambda}|\Psi\rangle_{AB}|\alpha^\perp\rangle_C,$$
$$\Rightarrow \chi_A = \lambda\Phi_A + (1-\lambda)\Psi_A \Rightarrow \Phi_A = \Psi_A = |0\rangle\langle 0|,$$

where $|\Phi\rangle = U_{AB}|00\rangle$ and $|\Psi\rangle = U_{AB}|01\rangle$. Therefore, U_{AB} is a controlled unitary with control on system A, so is V_{AB}. We can assume that

$$U_{AB} = |0\rangle\langle 0| \otimes I_B + |1\rangle\langle 1| \otimes v_{B_1},$$
$$V_{AB} = |0\rangle\langle 0| \otimes I_B + |1\rangle\langle 1| \otimes v_{B_2}.$$

We know that $U_{BC}V_{BC} = I_{BC}$ and

$$v_{B_1}U_{BC}v_{B_2}V_{BC} = S_{BC} \Rightarrow U_{BC}v_{B_2}U_{BC}^\dagger = v_{B_1}^\dagger S_{BC},$$

therefore, $v_{B2} \otimes I_C$ shares eigenvalues with those of $v_{B_1}^\dagger S_{BC}$. By direct calculation, one can obtain that $\{e^{i\theta_1}, e^{i\theta_2}, e^{i(\theta_1+\theta_2)/2}, -e^{i(\theta_1+\theta_2)/2}\}$ are the eigenvalues of $v_{B_1}^\dagger S_{BC}$ with $e^{i\theta_1}, e^{i\theta_2}$ being the eigenvalues of $v_{B_1}^\dagger$. One can verify that these cannot be the eigenvalues of $v_{B_2} \otimes I_C$!

Therefore, we only need to deal with the case that $U_{BC}|0\rangle_B|z\rangle_C$ is the product for any $|z\rangle_C$.

Case 2. There exists some $|\gamma\rangle_C$ and a local unitary w_B on system B such that $U_{BC}|0\rangle_B|z\rangle_C = w_B|z\rangle_B|\gamma\rangle_C$, thus, U_{AB} maps $\{|0\rangle_A\} \otimes \mathcal{H}_B$ to itself. Therefore, U_{AB} is a controlled unitary with control on A, so is V_{AB}. The rest of the argument of this case is the same as case 1.

Case 3. There exists some state of system B, wlog, says $|0\rangle_B$, and local unitary w_C on system C such that $U_{BC}|0\rangle_B|z\rangle_C = |0\rangle_B w_C|z\rangle_C$. Therefore, U_{BC} is a control unitary with control on B. By moving this w_C to V_{BC}, we can make the assumption that $U_{BC} = |0\rangle\langle 0| \otimes I_C + |1\rangle\langle 1| \otimes u_C$. Note that for any $|z\rangle_C$, we have

$$F_{ABC}|0\rangle_A(V_{BC}^\dagger|0\rangle_B|z\rangle_C) = U_{AB}U_{BC}V_{AB}|0\rangle_A|0\rangle_B|z\rangle_C$$
$$\Rightarrow |0\rangle_A(V_{BC}^\dagger|0\rangle_B|z\rangle_C) = U_{AB}|0\rangle_A|0\rangle_B|z\rangle_C.$$

Thus part C's state of $V_{BC}^\dagger|0\rangle_B|z\rangle_C$ is $|z\rangle_C$ for all $|z\rangle_C \in \mathcal{H}_C$, which means that there is $|\beta\rangle_B$ such that $V_{BC}|\beta\rangle_B|z\rangle_C = |0\rangle_B|z\rangle_C$. Therefore, one can find a unitary w_C such that

$$V_{BC} = |0\rangle\langle\beta| \otimes I_C + |1\rangle\langle\beta^\perp| \otimes w_C.$$

The state of the C part of the following state is always $|\beta\rangle_B$,

$$U_{BC}V_{AB}|1\rangle_A|0\rangle_B|z\rangle_C = U_{BC}V_{AB}V_{BC}|1\rangle_A|\beta\rangle_B|z\rangle_C$$
$$= U_{AB}^\dagger F_{ABC}|1\rangle_A|\beta\rangle_B|z\rangle_C$$
$$= U_{AB}^\dagger|1\rangle_A|z\rangle_B|\beta\rangle_C.$$

On the other hand, assume $V_{AB}|1\rangle_A|0\rangle_B = |a\rangle_A|0\rangle_B + |b\rangle_A|1\rangle_B$, and direct calculation shows that

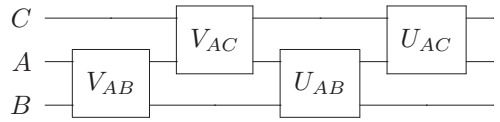
$$U_{BC}V_{AB}|1\rangle_A|0\rangle_B|z\rangle_C = |a\rangle_A|0\rangle_B|z\rangle_C + |b\rangle_A|1\rangle_B w_C|z\rangle_C.$$

The state of the C part of the above state is the mixture of $|z\rangle_C$ and $w_C|z\rangle_C$, which is not a constant state, of course not $|\beta\rangle_B$.

One can conclude that $U_{AB}U_{BC}V_{AB}V_{BC}$ can never be the Fredkin gate. ■

Another case we need to deal with is the following.

Lemma III.3. There is no $U_{AB}, V_{AB} \in \mathcal{K}_{AB}$, $U_{AC}, V_{AC} \in \mathcal{K}_{AC}$ such that $U_{AC}U_{AB}V_{AC}V_{AB} = F_{ABC}$. In other words, the Fredkin gate can never be implemented in the following circuit,



.

Proof. Assume that $U_{AC}U_{AB}V_{AC}V_{AB} = F_{ABC}$.

Wolg, we suppose that $V_{AB}|0\rangle_A|\beta\rangle_B = |0\rangle_A|0\rangle_B$ by invoking Proposition 1. Then we have the following equation:

$$|0\rangle_A|\beta\rangle_B|z\rangle_C = F_{ABC}|0\rangle_A|\beta\rangle_B|z\rangle_C$$
$$= U_{AC}U_{AB}V_{AC}V_{AB}|0\rangle_A|\beta\rangle_B|z\rangle_C$$
$$= U_{AC}U_{AB}V_{AC}|0\rangle_A|0\rangle_B|z\rangle_C.$$

Considering the state $V_{AC}|0\rangle_A|z\rangle_C$, we show the following.

Case 1. There is some $|z_0\rangle_C$ such that $V_{AC}|0\rangle_A|z_0\rangle_C$ becomes entangled. Define $|\chi\rangle_{ABC}$ as follows,

$$|\chi\rangle_{ABC} := U_{AC}U_{AB}V_{AC}|0\rangle_A|0\rangle_B|z_0\rangle_C.$$

By moving local unitaries, we can assume there is $0 < \lambda < 1$ such that

$$V_{AC}|0\rangle_A|z_0\rangle_C = \sqrt{\lambda}|0\rangle_A|0\rangle_C + \sqrt{1-\lambda}|1\rangle_A|1\rangle_C.$$

According to the fact that $\chi_B = \beta_B$, we know that

$$U_{AB} = I_A \otimes |\beta\rangle\langle 0| + u_A \otimes |\beta^\perp\rangle\langle 1|.$$

One can verify that $\omega_B = \beta^\perp$ by noticing that $U_{AC}|\omega\rangle_{ABC} = F_{ABC}|0\rangle_A|\beta^\perp\rangle_B|z\rangle_C = |0\rangle_A|\beta^\perp\rangle_B|z\rangle_C$, where $|\omega\rangle_{ABC} = U_{AB}V_{AC}V_{AB}|0\rangle_A|\beta^\perp\rangle_B|z\rangle_C$.

By employing the form of U_{AB} and $\omega_B = \beta^\perp$, we know that $V_{AB}|0\rangle_A|\beta^\perp\rangle_B = |\phi\rangle_A|1\rangle_B$ for some $|\phi\rangle_A \in \mathcal{H}_A$.

Notice that $|1\rangle_A|0\rangle_B$ is orthogonal to $V_{AB}|0\rangle_A|\beta^\perp\rangle_B = |\phi\rangle_A|1\rangle_B$ and $V_{AB}|0\rangle_A|\beta\rangle_B = |0\rangle_A|0\rangle_B$, then there is a $|\xi\rangle_B \in \mathcal{H}_B$ such that $V_{AB}|1\rangle_A|\xi\rangle_B = |1\rangle_A|0\rangle_B$ since V_{AB} is a unitary.

Now we consider the state,

$$|\psi\rangle_{ABC} = U_{AB}V_{AC}|1\rangle_A|0\rangle_B|z\rangle_C.$$

Then we know that $\psi_B = |z\rangle\langle z|$ by noticing that

$$|\psi\rangle_{ABC} = U_{AC}^\dagger F_{ABC}|1\rangle_A|\xi\rangle_B|z\rangle_C = U_{AC}^\dagger|1\rangle_A|z\rangle_B|\xi\rangle_C.$$

We can observe that $\psi_B = |\beta\rangle\langle\beta|$ by employing the form of $U_{AB} = I_A \otimes |\beta\rangle\langle 0| + u_A \otimes |\beta^\perp\rangle\langle 1|$. Conflict!

Therefore, we only need to deal with the case that for any $|z\rangle_C$, $V_{AC}|0\rangle_A|z\rangle_C$ is product.

Case 2. There exist some $|\gamma\rangle_C$ and local unitary u_A on system A such that $V_{AC}|0\rangle_A|z\rangle_C = u_A|z\rangle_A|\gamma\rangle_C$, thus, U_{AB} maps $\mathcal{H}_A \otimes \{|0\rangle_B\}$ to $\mathcal{H}_A \otimes \{|\beta\rangle_B\}$. We can also obtain the form of U_{AB} as case 1. Repeating the argument of case 1, we are able to show the impossibility of this case.

Case 3. There exists some state $|\alpha\rangle_A$ on system A such that V_{AC} maps $\{|0\rangle_A \otimes \mathcal{H}_C\}$ to $\{|\alpha\rangle_A \otimes \mathcal{H}_C\}$. By moving the local unitary, we can make $|\alpha\rangle_A = |0\rangle_A$; that means V_{AC} is a controlled unitary with control on A. We can assume

that $V_{AC} = |0\rangle\langle 0| \otimes I_C + |1\rangle\langle 1| \otimes w_C$ by moving the local unitary, then

$$\begin{aligned} |0\rangle_A|\beta\rangle_B|z\rangle_C &= F_{ABC}|0\rangle_A|\beta\rangle_B|z\rangle_C \\ &= U_{AC}U_{AB}V_{AC}V_{AB}|0\rangle_A|\beta\rangle_B|z\rangle_C \\ &= U_{AC}U_{AB}|0\rangle_A|0\rangle_B|z\rangle_C. \end{aligned}$$

Notice that the B part's state of $U_{AB}|0\rangle_A|0\rangle_B$ is $|\beta\rangle$. Then, by moving the local unitary to the left of U_{AC}, we can make the assumption that $U_{AB}|0\rangle_A|0\rangle_B = |0\rangle_A|\beta\rangle_B$, and the above equation becomes

$$|0\rangle_A|z\rangle_C = U_{AC}|0\rangle_A|z\rangle_C,$$

therefore, U_{AC} is a controlled unitary with control on A.

Since F_{ABC} is symmetric, we observe that

$$V_{AB}^T V_{AC}^T U_{AB}^T U_{AC}^T = F_{ABC}^T = F_{ABC}.$$

If there is some $|y\rangle_B$ such that $U_{AB}^T|0\rangle_A|y\rangle_B$ is entangled or some $|\varphi\rangle_C$ and some local unitary u_{A1} on system A such that $U_{AB}^T|0\rangle_A|y\rangle_B = u_{A1}|y\rangle_A|\varphi\rangle_C$ is valid for any $|y\rangle_B$, we can conclude that it is impossible by repeating the argument above.

The rest of the case is that $U_{AB}^T|0\rangle_A|y\rangle_B = |\varphi\rangle_A u_{C1}|y\rangle_C$; we can reach the conclusion that V_{AB}^T and U_{AB}^T are both controlled unitary with control on A, so are V_{AB} and U_{AB}, and we can assert that S_{BC} is a local unitary by figuring directly out the form of controlled unitary. That is again impossible by direct calculation.

Therefore, $U_{AC}U_{AB}V_{AC}V_{AB} = F_{ABC}$ can never be satisfied. ■

Now we are ready to show the following.

Theorem 4. Four nonlocal two-qubit gates are not sufficient for implementing a Fredkin gate.

Proof. If the four gates belong to two of the classes $\mathcal{K}_{AB}$,$\mathcal{K}_{AC}$,$\mathcal{K}_{BC}$, the circuits that need to be considered are just $U_{AB}U_{BC}V_{AB}V_{BC} = F_{ABC}$ or $U_{AB}U_{AC}V_{AB}V_{AC} = F_{ABC}$, which have just been studied in Lemmas 4 and 5.

Otherwise, the four gates belong to three classes $\mathcal{K}_{AB}$,$\mathcal{K}_{AC}$,$\mathcal{K}_{BC}$, then there exist two gates belonging to the same class. Due to the symmetric property of the Fredkin gate, we need to consider the following two cases.

Case 1. Two gates belong to $\mathcal{K}_{AB}$. The four gates are $U_{AB}, V_{AB} \in \mathcal{K}_{AB}$, $U_{AC} \in \mathcal{K}_{AC}$ and $U_{BC} \in \mathcal{K}_{BC}$. According to symmetric properties of the Fredkin gate, the three possible circuits are as follows.

Subcase 1. $U_{AB}U_{BC}V_{AB}U_{AC} = F_{ABC}$. This circuit can be reduced to Lemma 4 by noticing that

$$(S_{AB}U_{AB})U_{BC}(V_{AB}S_{AB})(S_{AB}U_{AC}S_{AB}) = F_{BAC},$$

$S_{AB}U_{AB}, V_{AB}S_{AB} \in \mathcal{K}_{AB}$ and $S_{AB}U_{AC}S_{AB} \in \mathcal{K}_{BC}$, where $F_{BAC} = S_{AB}F_{ABC}S_{AB}$ is the Fredkin gate with control on B.

Subcase 2. $U_{AB}U_{AC}V_{AB}U_{BC} = F_{ABC}$. This circuit can be reduced to Lemma 5 by noticing that

$$(S_{AB}U_{AB})U_{AC}(V_{AB}S_{AB})(S_{AB}U_{BC}S_{AB}) = F_{BAC},$$

and $S_{AB}U_{BC}S_{AB} \in \mathcal{K}_{AC}$.

Subcase 3. $U_{AB}U_{BC}U_{AC}V_{AB} = F_{ABC}$. This circuit can be reduced to subcase 1 by noticing that

$$U_{AB}(U_{BC}S_{BC})(S_{BC}U_{AC}S_{BC})(S_{BC}V_{AB}S_{BC}) = F_{ABC}S_{BC}.$$

$S_{BC}U_{AC}S_{BC} \in \mathcal{K}_{AB}$ and $S_{BC}V_{AB}S_{BC} \in \mathcal{K}_{AC}$. Observe that $X_A F_{ABC} S_{BC} X_A = F_{ABC}$ where X_A denotes the Pauli flip unitary on system $\mathcal{H}_A$. This reduction is done.

Case 2. Two gates belong to $\mathcal{K}_{BC}$. The four gates are $U_{AB} \in \mathcal{K}_{AB}$, $U_{AC} \in \mathcal{K}_{AC}$ and $U_{BC}, V_{BC} \in \mathcal{K}_{BC}$. According to symmetric properties of the Fredkin gate, the three possible circuits are as follows.

Subcase 1. $U_{BC}U_{AC}V_{BC}U_{AB} = F_{ABC}$. This circuit can be reduced to Lemma 4 by noticing that

$$(S_{BC}U_{BC})U_{AC}(V_{BC}S_{BC})(S_{BC}U_{AB}S_{BC}) = F_{ABC}.$$

Subcase 2. $U_{BC}U_{AB}V_{BC}U_{AC} = F_{ABC}$. This circuit can be reduced to Lemma 4 by noticing that

$$(S_{BC}U_{BC})U_{AB}(S_{BC}V_{BC})(S_{BC}U_{AC}S_{BC}) = F_{ABC}.$$

Subcase 3. $U_{BC}U_{AB}U_{AC}V_{BC} = F_{ABC}$. Observe that $U_{AB}U_{AC}$ is a controlled unitary with control on A; we can conclude that S_{BC} share eigenvalues with a local unitary by invoking Proposition 2. That is impossible.

This completes the proof of this theorem. ■

Together with the previous known result, we can conclude that five two-qubit gates are optimal to implement a Fredkin gate.

By observing that the set of circuits consisting of four (or less) two-qubit gates forms a closed set, compact set indeed, a direct corollary of Theorem 4.2 is the following.

Corollary 1. There is $\epsilon > 0$ such that for any U_{ABC} which could be implemented by four two-qubit gates, the distance between U_{ABC} and F_{ABC} is greater than ϵ. In other words, the Fredkin gate cannot be well approximated by any circuit consisting of four two-qubit gates.

A similar statement can be made for Deutsch gates.

IV. CONCLUSION

In this paper, we study the problem of implementing Deutsch gates and the Fredkin gate using two-qubit unitaries. We first showed that any Deutsch gate requires at least four two-qubit gates to implement, and if the determinant is one then it can be simulated using four two-qubit gates; otherwise, five is optimal. We can construct a circuit consisting of four two-qubit gates which simulates the set of the universal Deutsch gate with the unit determinant.

Secondly, we proved that five two-qubit gates is optimal for constructing a three-qubit Fredkin gate. We hope this work will be helpful to study the problem of optimal simulation of the multiqubit gate using two-qubit gates.

ACKNOWLEDGMENTS

This work was partly supported by NSERC (Canada), NSERC DAS, CIFAR (Canada), National Natural Science Foundation of China (China) (Grants No. 61179030, and No. 60621062), Australian Research Council (Grants No. DP110103473, and No. DP120103776) and the Overseas Team Program of Academy of Mathematics and Systems Science, Chinese Academy of Sciences (China).

[1] W. Dür, G. Vidal, J. I. Cirac, N. Linden, and S. Popescu, Phys. Rev. Lett. **87**, 137901 (2001).
[2] D. Collins, N. Linden, and S. Popescu, Phys. Rev. A **64**, 032302 (2001).
[3] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000).
[4] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
[5] D. W. Berry and B. C. Sanders, Phys. Rev. A **67**, 040302(R) (2003).
[6] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin, IEEE Trans. Inf. Theor. **49**, 1895 (2003).
[7] N. Linden, J. A. Smolin, and A. Winter, Phys. Rev. Lett. **103**, 030501 (2009).
[8] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[9] N. Yu, R. Duan, and M. Ying, Phys. Rev. A **81**, 032328 (2010).
[10] L. DiCarlo *et al.*, Nature (London) **460**, 240 (2009).
[11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 1st ed. (Cambridge University Press, Cambridge, UK, 2000).
[12] D. P. DiVincenzo, Proc. R. Soc. London A **454**, 261 (1998).
[13] D. P. DiVincenzo and J. A. Smolin, *Proceedings of the Workshop on Physics and Computation: Physcomp '94* (Dallas, Texas, 1994).
[14] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).
[15] 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).
[16] N. Yu, R. Duan, and M. Ying, Phys. Rev. A **88**, 010304(R) (2013).
[17] Edward Fredkin and Tommaso Toffoli, Int. J. Theor. Phys. **21**, 219 (1982).
[18] A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
[19] A. Berthiaume, D. Deutsch, and R. Jozsa, in *IEEE Workshop on Physics and Computation* (IEEE, Washington, DC, 1994), pp. 60–62.
[20] G. J. Milburn, Phys. Rev. Lett. **62**, 2124 (1989).
[21] H. F. Chau and F. Wilczek, Phys. Rev. Lett. **75**, 748 (1995).
[22] J. A. Smolin and D. P. DiVincenzo, Phys. Rev. A **53**, 2855 (1996).
[23] D. Deutsch, Proc. R. Soc. London A **425**, 73 (1989).