PHYSICAL REVIEW A **88**, 010304(R) (2013)

Five two-qubit gates are necessary for implementing the Toffoli gate

Nengkun Yu,* Runyao Duan, and Mingsheng Ying

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 and Center for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering and Information Technology, University of Technology, Sydney, New South Wales 2007, Australia

(Received 22 January 2013; published 30 July 2013)

In this Rapid Communication, we consider the open problem of the minimum cost of two-qubit gates for simulating the Toffoli gate and show that five two-qubit gates are necessary. Before our work, it was known that five two-qubit gates are sufficient to implement the Toffoli gate, and numerical evidence indicates that five two-qubit gates are also necessary. The idea introduced here can also be used to solve the problem of optimal simulation of Deutsch three-qubit gates.

DOI: 10.1103/PhysRevA.88.010304 PACS number(s): 03.67.Ac, 03.65.Ud, 89.70.Eg

Since quantum computation provides the possibility of solving certain problems much faster than any classical computer using the best currently known algorithms [1–5], a huge amount of effort has been devoted to building functional and scalable quantum computers over the last two decades. The quantum circuit model is one popular model of quantum computer hardware [6–18]. In order to be a general purpose computational device, a quantum computer must implement a small set of quantum logical gates [14], which are universal, that is, can serve as the basic building blocks of quantum circuits, in the same way as do classical logical gates for conventional digital circuits. It is quite natural to choose certain gates operating on a small number of qubits as the basic gates.

Theoretically, any two-qubit gate that can create entanglement, like the controlled-NOT (CNOT) gate, together with all single-qubit gates, is universal [18]. It has also been experimentally demonstrated that two-qubit gates can be realized with high fidelity using the current technology, for example, two-qubit gates with superconducting qubits have been presented with fidelities higher than 90% [19]. Finding more efficient ways to implement quantum gates may allow small-scale quantum computing tasks to be demonstrated on a shorter time scale. More precisely, it would be quite helpful for defeating quantum decoherence to realize multiqubit gates with the least number of possible basic gates. Thus an important problem is how to implement multiqubit gates using only two-qubit gates. Indeed, a study of the minimum cost of two-qubit gates for simulating a multiqubit gate is not only of theoretical importance, but also an experimental requirement: to accomplish a quantum algorithm, even at a small size, one has to implement a relatively high level of control over the multiqubit quantum system. A lot of experiments demonstrate multiqubit controlled-NOT gates in ion traps [20], linear optics [21], superconductors [22], and atoms [23].

Making controlled unitaries is an essential task for many algorithms in quantum computing [1]. Among all quantum controlled gates, those highly controlled unitaries (i.e., unitaries controlled on more than one other qubit) are useful in numerous quantum algorithms including the oracle in the binary welded tree algorithm [5] and quantum simulation [24]. The Toffoli gate is perhaps one of the most important highly controlled unitaries for three reasons: (1) The Toffoli gate is universal for classical reversible computation in the sense that all conventional Boolean circuits can be built upon it in a reversible way [25]; (2) it is also universal for quantum computation with little extra help in the sense that the one-qubit Hadamard gate is provided as a free resource [26]; (3) it is the simplest highly controlled unitary. Furthermore, a series of works showed that the Toffoli gate is an indispensable ingredient in realizing fault-tolerant quantum computation [23,27–30]. Recently, experimental implementation of the Toffoli gate has received considerable attention. The first experimental realization of the quantum Toffoli gate was presented in an ion-trap quantum computer, in 2009 at the University of Innsbruck, Austria [20]. Then, the Toffoli gate was realized in linear optics [21] and superconducting circuits [22,31,32].

Due to its significance in quantum computing, the theoretical pursuit of efficient implementation of the Toffoli gate using a sequence of single- and two-qubit gates has a quite long history [7,8,11,12,33–37]. It was explicitly stated as an open problem by Nielsen and Chuang in their influential textbook on quantum computation [14]: How many general two-qubit gates (or CNOT gates) are required to implement the Toffoli gate (see [14], p. 213, Problem 4.4)? What is known already is that the Toffoli gate can be decomposed as a circuit consisting of five two-qubit gates (or six CNOT gates), and numerical evidence has been gathered indicating that the five-gate implementation is optimal [8,11,12]. The cost of using a CNOT gate was first solved by Shende and Markov; they showed that six CNOT gates are optimal when single-qubit unitaries are free [36], a situation which was studied in [11,35,38]. However, the optimal simulation of the Toffoli gate by using general bipartite quantum logical gates remains unknown. This problem has attracted attention from many researchers in the last two decades [8,11,12,34–37]. In this Rapid Communication, we address this problem by showing that five two-qubit gates are necessary for implementing the Toffoli gate. The main difficulty of analyzing a circuit consisting of general two-qubit gates is that it contains more degrees of freedom. We would like to point out that the main

*nengkunyu@gmail.com

tool used in [36], the Cartan decomposition does not fit the implementation of using general two-qubit gates very well.

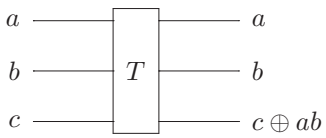
By counting the degrees of freedom (DOFs), in [7], it was shown that almost any n-qubit gate requires at least $\lceil \frac{4^n-3n-1}{9} \rceil$ two-qubit gates to implement without ancilla. To see the validity of this statement, one needs to study quantum gates with unit determinant and notice that each two-qubit unitary operation U can be expressed in the form [39] $U = (u_A \otimes u_B)U_d(v_A \otimes v_B)$, where u_A, u_B, v_A, and v_B are one-qubit unitary gates with unit determinants, with

$$U_d = \exp[i(\alpha_x X \otimes X + \alpha_y Y \otimes Y + \alpha_z Z \otimes Z)]$$

with Pauli matrices X, Y, Z. Then the DOFs of the circuit with any structure are upper bounded by the summation of the DOFs of all U_d's and one-qubit unitaries.

Let $n = 3$; then the simulation of a general three-qubit gate would require at least $\lceil \frac{4^3-3\times3-1}{9} \rceil = 6$ two-qubit gates. The following natural question then arose [12]: *Are six two-qubit quantum gates sufficient to generate any three-bit quantum gate?*

The general answer to this question remains open. In the following, we demonstrate the optimal implementation of the Toffoli gate. The Toffoli gate is simply a three-qubit controlled-NOT gate and can be intuitively explained as follows. The Toffoli gate is acting on three quantum bits, say A, B, and C. Here A and B are the control qubits, and C is the target qubit. Let us fix a computational basis $\{|0\rangle, |1\rangle\}$ for each qubit. Upon an input $|abc\rangle$, the gate will output the states of A and B directly, and flip the qubit C only if both the states of A and B are $|1\rangle$. The Toffoli gate can be depicted by the following diagram:



The Toffoli gate T_{ABC} can also been written as the following operator by considering the output over the computational basis:

$$I - |110\rangle\langle 110| - |111\rangle\langle 111| + |110\rangle\langle 111| + |111\rangle\langle 110|.$$

Let $V_{ABC} = I_{ABC} - 2|111\rangle\langle 111|$ with I_{ABC} being the identity operator on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. It is evident that

$$V_{ABC} = (I_{AB} \otimes H_C)T_{ABC}(I_{AB} \otimes H_C),$$

where H is the Hadamard gate given by

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

In other words, V_{ABC} and the Toffoli gate T_{ABC} are equivalent up to the local unitary H_C. By absorbing H_C into any two-qubit gates acting on AC or BC, we can easily conclude that V_{ABC} and T_{ABC} require the same number of two-qubit gates for realization. Thus in the following discussion, we focus only on the minimal cost of simulating V_{ABC} using two-qubit gates.

The gate V_{ABC} is a real Hermitian matrix that is invariant under any permutation of subsystems A, B, and C. Thus it can be regarded as a controlled gate with control on each qubit. Note that any bipartite unitary U_{AB} acting on a qubit system A and a general system B is said to be a controlled gate with control on A if it can be decomposed into the form of $U_{AB} = |0_A\rangle\langle 0_A| \otimes U_0 + |1_A\rangle\langle 1_A| \otimes U_1$. This simple observation is helpful to reduce the number of cases we need to consider.

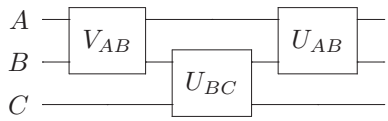
Since V_{ABC} is regarded as a three-qubit gate acting on ABC, any two-qubit gate used to implement V_{ABC} can be simply classified into three types: $\mathcal{K}_{AB}$, the gate acting on the systems A and B, and likewise $\mathcal{K}_{BC}$ and $\mathcal{K}_{AC}$. Clearly, it is impossible that all two-qubit gates used to simulate V_{ABC} belong to the same type. Furthermore, we can verify that two two-qubit gates are not sufficient for the simulation of V_{ABC}. To see this, one needs to notice that $U_{AB}U_{BC} = V_{ABC}$ implies that U_{BC} is also a controlled gate with control system C. This leads us to a contradiction by a routine calculation.

The following three observations will be very helpful for the remaining proof of the optimality: (i) Any two-dimensional two-qubit subspace contains some product state. (ii) A two-qubit unitary U_{AB} can be regarded as a controlled gate with control system A if the state of qubit A in $U_{AB}|0\rangle_A|y\rangle_B$ is always $|0\rangle_A$ for any state $|y\rangle_B$ of system B. (iii) Let $U_{AB}U_{AC}$ be a three-qubit unitary which can be regarded as a controlled gate between the bipartition A-BC with control system A. Then there exist one-qubit gates v_{B1}, v_{B2} on $\mathcal{H}_B$ and one-qubit gates w_{C1}, w_{C2} on $\mathcal{H}_C$ such that $U_{AB}U_{AC} = |0\rangle\langle 0| \otimes v_{B1} \otimes w_{C1} + |1\rangle\langle 1| \otimes v_{B2} \otimes w_{C2}$.

Observations (i) and (ii) are obvious. To see (iii), we can assume $U_{AC}|0\rangle_A|\gamma\rangle_C = |0\rangle_A|\psi\rangle_C$ by moving the local unitary to the left of U_{AB}. Then $U_{AB}U_{AC}|0\rangle_A|y\rangle_B|\gamma\rangle_C = U_{AB}|0\rangle_A|y\rangle_B|\psi\rangle_C$. Note that the state of A's part of $U_{AB}|0\rangle_A|y\rangle_B$ is always $|0\rangle$, which means that U_{AC} is a controlled gate with control on A. Similarly, U_{AB} is also a controlled gate with control on A. Hence the result follows.

Now we show that three two-qubit gates are not sufficient to implement V_{ABC}. We achieve this goal by analyzing all possible circuits consisting of three two-qubit gates. Due to the highly symmetric properties of V_{ABC}, we need to consider only the following two cases:

Case 1. These three gates belong to just two types. Without loss of generality (WLOG), we can assume that two gates are of the type $\mathcal{K}_{AB}$ and the third one is of the type $\mathcal{K}_{BC}$, and the circuit is (note that the time goes from left to right)



We only need to show that there is no solution of the equation

$$U_{AB}U_{BC}V_{AB} = V_{ABC},$$

where U_{AB} and V_{AB} are of type $\mathcal{K}_{AB}$, and U_{BC} of type $\mathcal{K}_{BC}$. Then U_{BC} must be a controlled gate with control on C by noticing that $U_{BC} = U_{AB}^{\dagger}V_{ABC}V_{AB}^{\dagger}$, where † stands for the Hermitian conjugate. We write $U_{BC} = |0\rangle\langle 0| \otimes I_B + |0\rangle\langle 0| \otimes w_B$. A direct calculation leads us to the conclusion that $I_A \otimes w_B$ and $I - 2|11\rangle\langle 11|$ share the same set of eigenvalues (counting multiplicity). That is impossible.

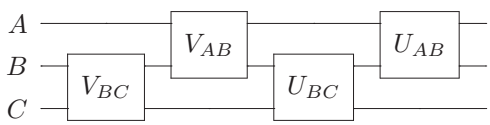
Case 2. Three gates belong to different types. WLOG, we assume the circuit is

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

Then $U_{BC}U_{AC}$ is a controlled gate with control bit C. As discussed in observation (iii), we can obtain that U_{BC} is a controlled gate with control system C, and so is U_{AC}. Consequently, we can assert that $I - 2|11\rangle\langle 11|$ is a local unitary by figuring out directly the form of the control unitary. That is again impossible.

We can generalize this technique to show that V_{ABC} cannot be implemented by any circuit consisting of four nonlocal two-qubit gates. We do not count the number of one-qubit gates as they can be easily absorbed into relevant two-qubit gates. Again the symmetric property of V_{ABC} enables us to consider only the following two cases:

Case 1. Four gates belong to only two types, say $\mathcal{K}_{AB}$ and $\mathcal{K}_{BC}$. Due to the symmetry of V_{ABC}, we need to show only that the following circuit cannot simulate V_{ABC}:



This is necessary to show that the following equation has no solution:

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

For readability, we postpone the detailed proof of this conclusion to the Appendix.

Case 2. Each of three types contains at least one of the four two-qubit gates. Again due to the symmetry of V_{ABC}, we need to deal only with the following two subcases:

Case 2.1. The circuit is represented by $U_{AC}U_{AB}U_{BC}V_{AB} = V_{ABC}$. We can reduce this circuit to the circuit considered in Case 1 by observing that $S_{AB}V_{ABC}S_{AB} = V_{ABC}$ and

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

where S_{AB} is the SWAP gate on system $\mathcal{H}_A \otimes \mathcal{H}_B$ given by $S|x\rangle_A|y\rangle_B = |y\rangle_A|x\rangle_B$ for any two states $|x\rangle$ and $|y\rangle$. Here we have employed the fact that $S_{AB}U_{AC}S_{AB}$ is a two-qubit gate acting on BC, and $S_{AB}U_{AB}$ and $V_{AB}S_{AB}$ are two-qubit gates acting on AB.

Case 2.2. The circuit is represented by $U_{AB}U_{BC}U_{AC}V_{AB} = V_{ABC}$. We know that $U_{BC}U_{AC}$ is a controlled gate with control on system C. Directly, we observe that U_{BC} and U_{AC} are controlled gates with control on C. This leads us to the conclusion that $I - 2|11\rangle\langle 11|$ shares eigenvalues, counting multiplicity with a local unitary, which means that the product of two eigenvalues of $I - 2|11\rangle\langle 11|$ equals the product of the other two. This is impossible.

By summarizing the above arguments, we have shown that four two-qubit gates are not sufficient for simulating the Toffoli gate. This further implies that any circuit consisting of fewer than five two-qubit gates has a positive distance to the Toffoli gate since the set of three-qubit gates that can be implemented by using up to four two-qubit gates forms a compact set; in other words, the Toffoli gate cannot be well approximated by such circuits.

This proof technique above can also be used to show that the following three-qubit controlled phase gate (three-qubit quantum gates with two control systems and one target qubit) introduced by Deutsch [6] cannot be implemented by four two-qubit gates:

$$V_\theta = I - (1 - e^{i\theta})|111\rangle\langle 111|,$$

where $0 < \theta < 2\pi$. Note that V_{ABC} is the special case of $\theta = \pi$. Together with the result in [8], we conclude that five two-qubit gates are optimal for simulating the the two-qubit controlled phase gate.

More generally, by employing the proof technique here, we completely solve the optimal simulation for general three-qubit controlled gates [7,8] and Fredkin gates [10]:

Theorem 1. The three-qubit controlled unitary $C^2(U)$ is implementable by four two-qubit gates if and only if $\det(U) = 1$; otherwise, five is optimal. Five two-qubit gates is optimal for implementing the Fredkin gate.

A detailed proof of this theorem is presented in [40].

In this Rapid Communication, we study the problem of implementing a multiqubit gate using two-qubit unitaries. In particular, we demonstrate that four two-qubit unitaries are not sufficient for constructing the three-qubit Toffoli gate; thus, the implementation with five two-qubit gates is optimal. More generally, our idea can be used to characterize the two-qubit gate cost of implementing a three-qubit controlled gate. We hope this work will be helpful for further study of the minimal cost of implementing larger quantum logical gates, e.g., the multiqubit controlled gate, and for studying optimization of quantum logical circuits, a crucial issue in the design and implementation of quantum computer hardware and architecture.

We are grateful to Professor D. P. DiVincenzo for pointing out useful references. This work was partly supported by the Australian Research Council (ARC) (Grants No. DP110103473 and No. DP120103776) and the Overseas Team Program of the Academy of Mathematics and Systems Science, Chinese Academy of Sciences. R. Duan was also supported in part by the National Natural Science Foundation of China under Grant 61179030 and an ARC Future Fellowship under Grant FT120100449.

APPENDIX

In this Appendix, we show that there are no unitaries U_{AB}, V_{AB} and U_{BC}, V_{BC} such that

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

Notice that $U_{AB}U_{BC}V_{AB}$ is a controlled gate on the bipartition A-BC with control on A. Moreover, part A's state of the output state $U_{AB}U_{BC}V_{AB}|i\rangle_A|\psi\rangle_{BC}$ is still $|i\rangle_A$ for any input state $|i\rangle_A|\psi\rangle_{BC}$ with $i = 0,1$. Since V_{AB} maps some state $|0\rangle_A|\xi\rangle_B$ to a product state, we can assume that $V_{AB}|0\rangle_A|0\rangle_B = |0\rangle_A|0\rangle_B$ by absorbing one-qubit gates into U_{BC} and U_{AB}. Then the state of A's part of $U_{AB}U_{BC}V_{AB}|0\rangle_A|0\rangle_B|z\rangle_C = U_{AB}U_{BC}|0\rangle_A|0\rangle_B|z\rangle_C$ is still $|0\rangle_A$. We now need to consider three cases according to different forms of the state $U_{BC}|0\rangle_B|z\rangle_C$:

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

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

where we have absorbed a local unitary acting on B into U_{AB}.

Let $|\Phi\rangle = U_{AB}|00\rangle$ and $|\Psi\rangle = U_{AB}|01\rangle$. Then

$$\begin{aligned}|\chi\rangle_{ABC} &= U_{AB}U_{BC}|0\rangle_A|0\rangle_B|z_0\rangle_C \\ &= \sqrt{\lambda}|\Phi\rangle_{AB}|\alpha\rangle_C + \sqrt{1-\lambda}|\Psi\rangle_{AB}|\alpha^\perp\rangle_C.\end{aligned}$$

Thus, we obtain

$$\begin{aligned}\chi_A &= |0\rangle\langle 0| = \lambda\Phi_A + (1-\lambda)\Psi_A \\ &\Rightarrow \Phi_A = \Psi_A = |0\rangle\langle 0|.\end{aligned}$$

Consequently, U_{AB} is a controlled gate with control on system A, and one knows that $V_{AB} = U_{BC}^\dagger U_{AB}^\dagger V_{ABC} V_{BC}^\dagger$ is a controlled gate with control A. Assume that $U_{AB} = |0\rangle\langle 0| \otimes I_B + |1\rangle\langle 1| \otimes u_B$ and $V_{AB} = |0\rangle\langle 0| \otimes I_B + |1\rangle\langle 1| \otimes v_B$. We conclude that $U_{BC} v_B U_{BC}^\dagger = u_B^\dagger \otimes |0\rangle\langle 0| + u_B^\dagger Z_B \otimes |1\rangle\langle 1|$, where Z is the Pauli matrix given by $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$.

The set of eigenvalues of $U_{BC} v_B U_{BC}^\dagger$ counting multiplicity is $\{e^{i\theta_1}, e^{i\theta_1}, e^{i\theta_2}, e^{i\theta_2}\}$, which is also the set of eigenvalues counting the multiplicity of the right-hand side of the above equality. Note that $u_B^\dagger$ should not equal the identity up to a global phase. Then $u_B^\dagger$ and $u_B^\dagger Z_B$ have the same set of eigenvalues. Thus their determinants are equal, say,

$$\det(u_B^\dagger) = \det(u_B^\dagger Z_B) = \det(u_B^\dagger)\det(Z_B) = -\det(u_B^\dagger),$$

and $\det(u_B^\dagger) = 0$. This contradicts the fact that $u_B^\dagger$ is unitary. Thus $U_{BC}|0\rangle_B|z\rangle_C$ is always a product for any $|z\rangle_C$. This leads us to consider the following two cases.

Case 2. There is a $|\gamma\rangle_C$ and a local unitary w_B on system B such that $U_{BC}|0\rangle_B|z\rangle_C = w_B|z\rangle_B|\gamma\rangle_C$. Then U_{AB} maps $\{|0\rangle_A\} \otimes \mathcal{H}_B$ to itself; hence U_{AB} is a controlled gate with control system A. Similarly, V_{AB} is also a controlled gate with the same control bit. The rest of the proof is the same as in Case 1.

Case 3. There is a state on system B, say $|0\rangle_B$, and a local unitary w_C on system C such that $U_{BC}|0\rangle_B|z\rangle_C = |0\rangle_B w_C|z\rangle_C$. Then U_{BC} is a controlled gate with control system B. By moving this w_C into V_{BC}, we can assume that $U_{BC} = |0\rangle\langle 0| \otimes I_C + |1\rangle\langle 1| \otimes u_C$. Note that for any $|z\rangle_C$, part C's state of the output state $|\chi\rangle_{ABC} = U_{AB}U_{BC}V_{AB}|0\rangle_A|0\rangle_B|z\rangle_C = U_{AB}|0\rangle_A|0\rangle_B|z\rangle_C$ is still $|z\rangle_C$. By recalling that $|\chi\rangle_{ABC} = V_{ABC}|0\rangle_A(V_{BC}^\dagger|0\rangle_B|z\rangle_C) = |0\rangle_A(V_{BC}^\dagger|0\rangle_B|z\rangle_C)$. We know that 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 v_C such that $V_{BC} = |0\rangle\langle\beta| \otimes I_C + |1\rangle\langle\beta^\perp| \otimes v_C$. In order to simplify the structure of the two-qubit gates, we observe that $V_{BC}^\dagger V_{AB}^\dagger U_{BC}^\dagger U_{AB}^\dagger = V_{ABC}$. This also provides a simulation of V_{ABC}. Consider the state

$$V_{BC}^\dagger V_{AB}^\dagger U_{BC}^\dagger|0\rangle_C|0\rangle_B|x\rangle_A = V_{BC}^\dagger V_{AB}^\dagger|0\rangle_C|0\rangle_B|x\rangle_A$$

for any $|x\rangle_A$. The argument of Cases 1 and 2 excludes the following possibilities: (i) there is some $|x\rangle_A$ such that $V_{AB}^\dagger|0\rangle_B|x\rangle_A$ is entangled, or (ii) there are a $|\delta\rangle_A$ and a local unitary w_B on system B such that $V_{AB}^\dagger|0\rangle_B|x\rangle_A = w_B|x\rangle_B|\delta\rangle_A$. So the only possibility is that there is a state $|\phi\rangle_B$ on system B and a local unitary w_A on system A such that $V_{AB}^\dagger|0\rangle_B|x\rangle_A = |\phi\rangle_B w_A|x\rangle_A$. According to $V_{AB}^\dagger|0\rangle_A|0\rangle_B = |0\rangle_A|0\rangle_B$, we can choose $|\phi\rangle = |0\rangle$. Thus $V_{AB}^\dagger$ is a controlled gate with control system B, i.e., $V_{AB} = |0\rangle\langle 0| \otimes w_A + |1\rangle\langle 1| \otimes v_A$. By studying part C's state of $U_{AB}U_{BC}V_{AB}V_{BC}|0\rangle_A|0\rangle_B|z\rangle_C = |0\rangle_A|0\rangle_B|z\rangle_C$, we see that $|\beta\rangle_B$ defined in V_{BC} equals $|0\rangle_B$ or $|1\rangle_B$, up to some global phase. Otherwise, assume that $|0\rangle_B = a|\beta\rangle_B + b|\beta^\perp\rangle_B$ for $ab \neq 0$. Then the state of part C becomes a mixed state for general input $|0\rangle_A|0\rangle_B|z\rangle_C$ since u_C is not the identity up to some global phase and U_{BC} is nonlocal. For the case $|\beta\rangle_B = |0\rangle_B$, we know that all the four two-qubit gates are controlled gates with control system B, which implies that $I - 2|11\rangle\langle 11|$ is a local unitary, a contradiction. For the case $|\beta\rangle_B = |1\rangle_B$, let X_B be the NOT (flip) gate such that $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$, one can verify that

$$(U_{AB}X_B)(X_B U_{BC} X_B)(X_B V_{AB} X_B)(X_B V_{BC}) = V_{ABC}.$$

$U_{AB}X_B$, $X_B U_{BC} X_B$, $X_B V_{AB} X_B$, and $X_B V_{BC}$ are controlled gates with control system B. This also leads us to a contradiction that $I - 2|11\rangle\langle 11|$ is local.

[1] P. Shor, SIAM J. Comput. **26**, 1484 (1997).
[2] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
[3] S. Hallgren, J. ACM **54**(1), 4 (2007).
[4] M. H. Freedman, A. Kitaev, and Z. Wang, Commun. Math. Phys. **227**, 587 (2002).
[5] A. M. Childs *et al*., in *Proceedings of the 35th ACM Symposium on the Theory of Computing (STOC 2003)* (ACM, New York, 2003), pp. 59–68.
[6] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1989).
[7] 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).
[8] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).
[9] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[10] H. F. Chau and F. Wilczek, Phys. Rev. Lett. **75**, 748 (1995).
[11] D. P. DiVincenzo, Proc. R. Soc. London, Ser. A **454**, 261 (1998).
[12] D. P. DiVincenzo and J. A. Smolin, in *Proceedings of the Workshop on Physics and Computation: Physcomp '94* (Dallas, Texas, 1994).
[13] G. Burkard, D. Loss, D. P. DiVincenzo, and J. A. Smolin, Phys. Rev. B **60**, 11404 (1999).
[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, First Edition (Cambridge University Press, 2003).
[15] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. Lett. **91**, 027903 (2003).
[16] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. Lett. **93**, 020502 (2004).

[17] M. A. Nielsen, M. R. Dowling, M. Gu, and A. C. Doherty, Science **311**, 1133 (2006).
[18] M. J. Bremner *et al*., Phys. Rev. Lett. **89**, 247902 (2002).
[19] L. DiCarlo *et al*., Nature (London) **460**, 240 (2009).
[20] T. Monz *et al*., Phys. Rev. Lett. **102**, 040501 (2009).
[21] B. P. Lanyon *et al*., Nat. Phys. **5**, 134 (2009).
[22] A. Fedorov *et al*., Nature (London) **481**, 170 (2012).
[23] D. G. Cory *et al*., Phys. Rev. Lett. **81**, 2152 (1998).
[24] A. Daskin and S. Kais, J. Chem. Phys. **134**, 144112 (2011).
[25] T. Toffoli, in *Automata, Languages and Programming, 7th Colloqium*, edited by J. W. van de Bakker and J. Leeuwen (Springer, Berlin, 1980), pp. 632–644.
[26] Y. Shi, Quantum Inf. Comput. **3**, 1 (2003).
[27] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne, Phys. Rev. Lett. **86**, 5811 (2001).
[28] J. Chiaverini *et al*., Nature (London) **432**, 602 (2004).
[29] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **71**, 052332 (2005).
[30] E. Dennis, Phys. Rev. A **63**, 052314 (2001).
[31] M. Mariantoni *et al*., Science **334**, 61 (2011).
[32] M. D. Reed *et al*., Nature (London) **482**, 382 (2012).
[33] T. C. Ralph, K. Resch, and A. Gilchrist, Phys. Rev. A **75**, 022313 (2007).
[34] D. Maslov and G. W. Dueck, IEE Electron. Lett. **39**, 1790 (2003).
[35] G. Song and A. Klappenecker, Quantum Inf. Comput. **4**, 5 (2004).
[36] V. V. Shende and I. L. Markov, Quantum Inf. Comput. **9**, 5 (2009).
[37] C. Moraga, Facta universitatis - series: Electronics and Energetics 2011, vol. 24, br. 3, str. 423–435.
[38] N. Margolus (unpublished).
[39] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[40] N. Yu and M. Ying, arXiv:1301.3727.