

Five Two-Qubit Gates Are Necessary for Implementing 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, NSW 2007, Australia*

In this paper, we settle the long-standing open problem of the minimum cost of two-qubit gates for simulating a Toffoli gate. More precisely, we show that five two-qubit gates are necessary. Before our work, it is known that five gates are sufficient and only numerical evidences have been gathered, indicating that the five-gate implementation is necessary. The idea introduced here can also be used to solve the problem of optimal simulation of three-qubit control phase introduced by Deutsch in 1989.

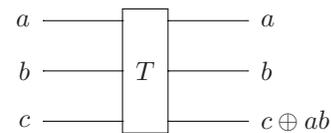
Since quantum computation provides the possibility of solving certain problems which are believed to be infeasible with a classical computer [1–4], a huge amount of effort has been devoted to building functional and scalable quantum computers over the last two decades. Quantum logical circuit is the most popular model of quantum computer hardwares. In order to be a general purpose computational device, a quantum computer must implement a small set of quantum logical gates [5], which can universally serve as the basic building blocks of quantum circuits, in the same way as classical logical gates did 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 [6]. 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 qubits have been presented with fidelities higher than 90% [7]. 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 multi-qubit gates with the least number of possible basic gates. Thus an important problem is how to implement more-than-two-qubit gates using only two-qubit gates. Indeed, studying the minimum cost of two-qubit gates for simulating a multi-qubit gate is not only of theoretical importance, but also an experimental requirement: to accomplish a quantum algorithm, even in a small size, one has to implement a relatively high level of control over the multi-qubit quantum system. A lot of experimental effort has been devoted to demonstrating multi-qubit controlled-NOT gates in ion traps [8], linear optics [9], superconductors [10] and atoms [11].

The Toffoli gate is perhaps one of the most important quantum logical gates as it can universally realize

classical reversible computation [12], as well as universal quantum computation [13] with little extra help. It also plays a central role in quantum error-correction [11, 14–17]. Recently, experimental implementation of the Toffoli gate has received considerable attention [8–10, 19, 20]. However, it remains still unknown what is the optimal simulation of the Toffoli gate by using bipartite quantum logical gates, which has been an important open problem explicitly listed in the influential textbook on quantum computation [5]. Here, we settle this problem by showing that five two-qubit gates are necessary and sufficient for implementing the Toffoli gate. A five two-qubit gates decomposition of the Toffoli gate was known long time ago, but before this work numerical evidences showing that the five-gate implementation is optimal have been found [21–24]. Our result gives, for the first time, a theoretical proof for the optimality beyond numerical evidences.

The function of 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, namely A, B , and C . Here A and B are 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 system C only if both the states of A and B are 1. The Toffoli gate can be depicted by the following diagram,



It can also be written as the following version by considering the output over the computational basis:

$$T_{ABC} = I - |110\rangle\langle 110| - |111\rangle\langle 111| + |110\rangle\langle 111| + |111\rangle\langle 110|.$$

It is well known that the Toffoli gate is universal for the classical computation in the sense that all conventional boolean circuits can be built upon it in a reversible way. It was also proved to be universal for quantum computation if the one-qubit Hadamard gate is provided as free

resource [13]. Furthermore, a series of works showed that the Toffoli gate is an indispensable ingredient in realizing fault-tolerant quantum computation [11, 14–18]. Recently, a rapid progress has been made on implementing the Toffoli gate experimentally. The first experimental realization of the quantum Toffoli gate is presented in an ion trap quantum computer, in January 2009 at the University of Innsbruck, Austria [8]. A new approach using higher-dimensional Hilbert spaces was proposed [25] that enables us to simplify the implementation of the Toffoli gate in linear optics [9] and superconducting circuits [10, 19, 20].

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 quite long history. It was well known that six CNOT gates are optimal when single-qubit unitary is provided as free resources [21, 26–28]. Then an interesting question naturally arises: how many general two-qubit gates rather than the CNOT are required to implement the Toffoli gate? This question has attracted many different researchers in the last two decades. In particular, Nielsen and Chuang explicitly listed it as an unsolved problem in their standard textbook on quantum computation [5] (see page 213, Problem 4.4). What we know until now is that the Toffoli gate can be decomposed as a circuit consisting of five two-qubit gates, and numerical evidences have been gathered, indicating that the five-gate implementation is optimal [21–23]. Here, we finally settle this problem and present a theoretical proof of the optimality.

Let $V_{ABC} = I_{ABC} - 2|111\rangle\langle 111|$ with I_{ABC} the identity operator on 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 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 to realize. Thus in the following discussions, we will focus 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.

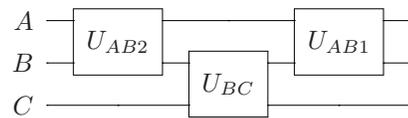
Since V_{ABC} is regarded as a three-qubit gate acting on ABC , any two-qubit gate used to implement V_{ABC}

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 only two two-qubit gates are not sufficient for the simulation of V_{ABC} . To see this, one only 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 contradiction by a routine calculation.

Three observations are quite helpful during our proof: 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 v_{B1}, v_{B2} and w_{C1}, w_{C2} being one-qubit gates on \mathcal{H}_B and \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 will achieve this goal by analysing all possible circuits consisting of three two-qubit gates. Due to the highly symmetric properties of V_{ABC} , we only need to consider the following two cases: Case 1: These three gates belong to just two types. Without any 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 there is no solution of the following equation

$$U_{AB1}U_{BC}U_{AB2} = V_{ABC},$$

where U_{AB1} and U_{AB2} 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 $U_{BC} = U_{AB1}^\dagger V_{ABC} U_{AB2}^\dagger$, where \dagger stands for the Hermitian conjugate. We can 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.

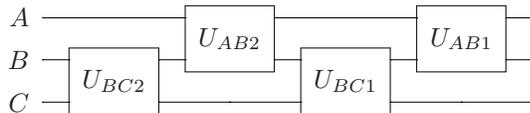
Case 2: Three gates belong to different types. Wlog, we can assume the circuit is

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

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

We can generalize this technique to show that the gate 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 only need to show the following circuit cannot be V_{ABC} ,



that is to show the following equation has no solution:

$$U_{AB1}U_{BC1}U_{AB2}U_{BC2} = V_{ABC}.$$

The proof detail of this case is given in appendix.

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

Case 2.1: The circuit is represented by $U_{AC}U_{AB1}U_{BC}U_{AB2} = V_{ABC}$. We can reduce this circuit to the circuit considered in Case 1 by observing that $S_{AB}V_{ABC}S_{AB} = V_{ABC}$ and

$$(S_{AB}U_{AC}S_{AB})(S_{AB}U_{AB1})U_{BC}(U_{AB2}S_{AB}) = V_{ABC},$$

where S_{AB} is the swap gate on system $\mathcal{H}_A \otimes \mathcal{H}_B$ given by $S|x_A\rangle|y_B\rangle = |y_A\rangle|x_B\rangle$ for any two states $|x\rangle$ and $|y\rangle$. Here we have employed the fact that $S_{AB}U_{AC}S_{AB}$ a two-qubit gate acting on BC , $S_{AB}U_{AB1}$ and $U_{AB2}S_{AB}$ are two-qubit gates acting on AB .

Case 2.2: The circuit is represented by $U_{AB1}U_{BC}U_{AC}U_{AB2} = V_{ABC}$. We know that $U_{BC}U_{AC}$ is a controlled gate with control system C . Directly, we can obtain U_{BC} and U_{AC} are controlled-gates with 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 to the product of the other two. Impossible.

We have shown that four two-qubit gates are not sufficient for simulating the Toffoli gate, which further implies that any circuit consisting of less 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 form a compact set; in other words, the Toffoli gate cannot be well approximated by such circuits.

This above argument can also be used to show that the following two-qubit controlled phase gate (three-qubit quantum gates with two control systems and one target qubit) introduced by Deutsch [29] can not 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 [23], we conclude that five two-qubit gates are optimal for simulating the the two-qubit controlled phase gate.

In this paper, we study the problem of implementing multi-qubit gate using two-qubit unitaries. It is demonstrated that four two-qubit unitaries is not enough for constructing a three-qubit Toffoli gate, thus, five two-qubit gates is optimal. More precisely, our idea can be directly used to prove that in order to implement a three-qubit control phase gate, five two-qubit gates is also needed. We hope this work will be helpful for further determining minimal cost of implementing larger quantum logical gates, e.g. the multi-qubit controlled gate, and for studying optimization of quantum logical circuits, a crucial issue in the design and implementation of quantum computer hardware and architecture.

This work was partly supported by the Australian Research Council (Grant No: DP110103473) and the Overseas Team Program of Academy of Mathematics and Systems Science, Chinese Academy of Sciences.

* Electronic address: nengkunyu@gmail.com

- [1] Shor, P. SIAM J. Comp. **26**, 1484 (1997).
- [2] Feynman, R. P. Inter. J. Theo. Phys. **21**, 467 (1982).
- [3] Hallgren, S. Journal of the ACM, Volume 54 Issue 1, March 2007.
- [4] Freedman, M. H., Kitaev, A. and Wang, Z. Comm. Math. Phys. **227**, 587 (2002).
- [5] Nielsen, M. A. and Chuang, I. L. Quantum Computation and Quantum Information, First Edition (2000).
- [6] Bremner, M. J., Dawson, C. M., Dodd, J. L., Gilchrist, A., Harrow, A. W., Mortimer, D., Nielsen, M. A. and Osborne, T. J. Phys. Rev. Lett. **89**, 247902 (2002).
- [7] DiCarlo, L., Chow, J. M., Gambetta, J. M., Bishop, L. S., Johnson, B. R., Schuster, D. I., Majer, J., Blais, A., Frunzio, L., Girvin, S. M. and Schoelkopf, R. J. Nature **460**, 240 (2009).
- [8] Monz, T., Kim, K., Hansel, W., Riebe, M., Villar, A. S., Schindler, P., Chwalla, M., Hennrich, M. and Blatt, R. Phys. Rev. Lett. **102**, 040501 (2009).
- [9] Lanyon, B. P., Barbieri, M., Almeida, M. P., Jennewein, T., Ralph, T. C., Resch, K. J., Pryde, G. J., O'Brien,

- J. L., Gilchrist, A. and White, A. G. *Nature Phys.* **5**, 134-140 (2009).
- [10] Fedorov, A., Steffen, L., Baur, M., da Silva, M. P. and Wallraff, A. *Nature* **481**, 170 (2012).
- [11] Cory, D. G., Mass, W., Price, M., Knill, E., Laflamme, R., Zurek, W. H., Havel, T. F. and Somaroo, S. S. *Phys. Rev. Lett.* **81**, 2152-2155 (1998).
- [12] Toffoli, T. in *Automata, Languages and Programming*, 7th Colloq. (eds de Bakker, J. W. van and Leeuwen, J.) 632-644 (Springer, 1980).
- [13] Shi, Y. *Quantum Inf. Comput.* **3**, 84-92 (2003).
- [14] Knill, E., Laflamme, R., Martinez, R. and Negrevergne, C. *Phys. Rev. Lett.* **86**, 5811-5814 (2001).
- [15] Chiaverini, J., Leibfried, D., Schaetz, T., Barrett, M. D., Blakestad, R. B., Britton, J., Itano, W. M., Jost, J. D., Knill, E., Langer, C., Ozeri, R. and Wineland, D. J. *Nature* **432**, 602-605 (2004).
- [16] Pittman, T. B., Jacobs, B. C. and Franson, J. D. *Phys. Rev. A* **71**, 052332 (2005).
- [17] Aoki, T., Takahashi, G., Kajiyama, T., Yoshikawa, J., Braunstein, S., Loock, P. and Furusawa, A. *Nature Phys.* **5**, 541-546 (2009).
- [18] Dennis, E. *Phys. Rev. A* **63**, 052314 (2001).
- [19] Marantoni, M., Wang, H., Yamamoto, T., Neeley, M., Bialczak, R. C., Chen, Y., Lenander, M., Lucero, E., OConnell, A. D., Sank, D., Weides, M., Wenner, J., Yin, Y., Zhao, J., Korotkov, A. N., Cleland, A. N. and Martinis, J. M. *Science* **334**, 61 (2011).
- [20] Reed, M. D., DiCarlo, L., Nigg, S. E., Sun, L., Frunzio, L., Girvin, S. M. and Schoelkopf, R. J. *Nature* **482**, 382-385 (2012).
- [21] DiVincenzo, D.P. *Proc. R. Soc. Lond. A*, **454**:261-276, (1998).
- [22] DiVincenzo, D.P. and Smolin, J. A. *Proc. of the Workshop on Physics and Computation* (1994).
- [23] Sleator, T. and Weinfurter, H. *Phys. Rev. Lett.* **74**, 4087 (1995).
- [24] Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P., Sleator, T., Smolin, J. A., and Weinfurter, H. *Phys. Rev. A* **52**, 3457 (1995).
- [25] Ralph, T. C., Resch, K. J., and Gilchrist, A. *Phys. Rev. A* **75**, 022313 (2007).
- [26] Margolus, N. Unpublished manuscript (circa 1994).
- [27] Song, G. and Klappenecker, A. *Quantum Inf. Comp.* **4**, 361-372 (2004).
- [28] Shende, V. V. and Markov, I. L. *Quantum Inf. Comp.* **9**, 461 (2009).
- [29] Deutsch, D. *Proc. Roy. Soc. Lond. A*. 425 (1989).

Technical appendix: In this appendix, we show that there is no unitaries U_{AB1}, U_{AB2} and U_{BC1}, U_{BC2} such that

$$U_{AB1}U_{BC1}U_{AB2}U_{BC2} = V_{ABC}.$$

Notice that $U_{AB1}U_{BC1}U_{AB2}$ is a controlled gate on the bipartition $A-BC$ with control on A . Moreover, the A 's part state of the output state $U_{AB1}U_{BC1}U_{AB2} |i\rangle_A |\psi\rangle_{BC}$ is still $|i\rangle_A$ for any input state $|i\rangle_A |\psi\rangle_{BC}$ with $i = 0, 1$. Since U_{AB2} maps some state $|0\rangle_A |\xi\rangle_B$ to product state, we can assume that $U_{AB2} |0\rangle_A |0\rangle_B = |0\rangle_A |0\rangle_B$ by absorbing one-qubit gates into U_{BC1} and U_{AB1} . Then the state of A 's part of $U_{AB1}U_{BC1}U_{AB2} |0\rangle_A |0\rangle_B |z\rangle_C = U_{AB1}U_{BC1} |0\rangle_A |0\rangle_B |z\rangle_C$ is still $|0\rangle_A$. We now need to

consider three subcases according to different forms of the state $U_{BC1}|0\rangle_B|y\rangle_C$:

Case 1.1: There is some $|z_0\rangle_C$ such that $U_{BC1}|0\rangle_B|z_0\rangle_C$ is entangled. Assume that there is $0 < \lambda < 1$ such that

$$U_{BC1}|0\rangle_B|z_0\rangle_C = \sqrt{\lambda}|0\rangle_B|\alpha\rangle_C + \sqrt{1-\lambda}|1\rangle_B|\alpha^\perp\rangle_C,$$

where we have absorbed a local unitary acting on B into U_{AB1} . Let $|\Phi\rangle = U_{AB1}|00\rangle$ and $|\Psi\rangle = U_{AB1}|01\rangle$, we know that

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

we can readily obtain

$$\chi_A = |0\rangle\langle 0| = \lambda\Phi_A + (1-\lambda)\Psi_A \Rightarrow \Phi_A = \Psi_A = |0\rangle\langle 0|.$$

Therefore, U_{AB1} is a controlled gate with control system A , then one know that $U_{AB2} = U_{BC1}^\dagger U_{AB1}^\dagger V_{ABC} U_{BC2}^\dagger$ is a controlled gate with control A . Assume that $U_{AB1} = |0\rangle\langle 0| \otimes I_B + |1\rangle\langle 1| \otimes u_B$ and $U_{AB2} = |0\rangle\langle 0| \otimes I_B + |1\rangle\langle 1| \otimes v_B$. We conclude that $U_{BC1}v_B U_{BC1}^\dagger = u_B^\dagger \otimes |0\rangle\langle 0| + u_B^\dagger Z_B \otimes |1\rangle\langle 1|$, where Z is the Pauli matrix given by $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$.

The set of eigenvalues of $U_{BC1}v_B U_{BC1}^\dagger$ counting multiplicity is $\{e^{i\theta_1}, e^{i\theta_1}, e^{i\theta_2}, e^{i\theta_2}\}$, which is also the eigenvalues counting multiplicity of the right hand side of the above equality. Note that u_B^\dagger should not equal to 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 $U_{BC1}|0\rangle_B|z\rangle_C$ is always product for any $|z\rangle_C$. This leads us to consider the following two subcases.

Case 1.2: There is a $|\gamma\rangle_C$ and a local unitary w_B on system B such that $U_{BC1}|0\rangle_B|z\rangle_C = w_B|z\rangle_B|\gamma\rangle_C$. Then U_{AB1} maps $\{|0\rangle_A\} \otimes \mathcal{H}_B$ to itself, hence U_{AB1} is a controlled gate with control system A . Similarly U_{AB2} is also a controlled gate with the same control bit. The rest proof is the same as Case 1.1.

Case 1.3: There is a state on system B , wlog, says $|0\rangle_B$, and a local unitary w_C on system C such that $U_{BC1}|0\rangle_B|z\rangle_C = |0\rangle_B w_C|z\rangle_C$. Then U_{BC1} is a controlled gate with control system B . By moving this w_C into U_{BC2} , we can assume that $U_{BC1} = |0\rangle\langle 0| \otimes I_C + |1\rangle\langle 1| \otimes u_C$. Note that for any $|z\rangle_C$, part C 's state of the output state $|\chi\rangle_{ABC} = U_{AB1}U_{BC1}U_{AB2} |0\rangle_A |0\rangle_B |z\rangle_C = U_{AB1} |0\rangle_A |0\rangle_B |z\rangle_C$ is still $|z\rangle_C$. Recall that $|\chi\rangle_{ABC} = V_{ABC}|0\rangle_A(U_{BC2}^\dagger|0\rangle_B|z\rangle_C) = |0\rangle_A(U_{BC2}^\dagger|0\rangle_B|z\rangle_C)$. Thus part C 's state of $U_{BC2}^\dagger|0\rangle_B|z\rangle_C$ is $|z\rangle_C$ for all $|z\rangle_C \in \mathcal{H}_C$, which means that there is $|\beta\rangle_B$ such that

$U_{BC2}|\beta\rangle_B|z\rangle_C = |0\rangle_B|z\rangle_C$. Therefore, one can find a unitary v_C such that $U_{BC2} = |0\rangle\langle\beta| \otimes I_C + |1\rangle\langle\beta^\perp| \otimes v_C$. In order to simplify the structure of the two-qubit gates, we observe that $U_{BC2}^\dagger U_{AB2}^\dagger U_{BC1}^\dagger U_{AB1}^\dagger = V_{ABC}$, *i.e.*, hence also provides a simulation of V_{ABC} . Now we consider the state

$$U_{BC2}^\dagger U_{AB2}^\dagger U_{BC1}^\dagger |0\rangle_C |0\rangle_B |x\rangle_A = U_{BC2}^\dagger U_{AB2}^\dagger |0\rangle_C |0\rangle_B |x\rangle_A$$

for any $|x\rangle_A$. The argument of cases 1.1 and 1.2 excludes the following possibilities: (i) there is some $|x\rangle_A$ such that $U_{AB2}^\dagger |0\rangle_B |x\rangle_A$ is entangled, or (ii) there is a $|\delta\rangle_A$ and a local unitary w_B on system B such that $U_{AB2}^\dagger |0\rangle_B |x\rangle_A = w_B |x\rangle_B |\delta\rangle_A$. 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 $U_{AB2}^\dagger |0\rangle_B |x\rangle_A = |\phi\rangle_B w_A |x\rangle_A$. According to $U_{AB2} |0\rangle_A |0\rangle_B = |0\rangle_A |0\rangle_B$, we can choose $|\phi\rangle = |0\rangle$. Thus U_{AB2} is a controlled gate with control system B , *i.e.*, $U_{AB2} = |0\rangle\langle 0| \otimes w_A + |1\rangle\langle 1| \otimes v_A$. By studying

part C 's state of $U_{AB1}U_{BC1}U_{AB2}U_{BC2} |0\rangle_A |0\rangle_B |z\rangle_C = |0\rangle_A |0\rangle_B |z\rangle_C$, we see that $|\beta\rangle_B$ defined in U_{BC2} equals to $|0\rangle_B$ 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 identity up to some global phase and U_{BC1} is nonlocal. For the case $|\beta\rangle_B = |0\rangle_B$, we know that all the four two-qubit gates are controlled gate 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 $X|1\rangle = |0\rangle$, then one can verify that

$$(U_{AB1}X_B)(X_B U_{BC1}X_B)(X_B U_{AB2}X_B)(X_B U_{BC2}) = V_{ABC}.$$

Then $U_{AB1}X_B, X_B U_{BC1}X_B, X_B U_{AB2}X_B$ and $X_B U_{BC2}$ are all controlled gate with control system B . This also leads us to the impossible conclusion that $I - 2|11\rangle\langle 11|$ is local.