Int J Theor Phys (2017) 56:2350–2361
DOI 10.1007/s10773-017-3389-4

Decompositions of n-qubit Toffoli Gates with Linear Circuit Complexity

Yong He[1] · Ming-Xing Luo[2,3] · E. Zhang[1] · Hong-Ke Wang[1] · Xiao-Feng Wang[1]

Received: 24 January 2017 / Accepted: 13 April 2017 / Published online: 26 April 2017

Abstract Toffoli gates are natural elements for the circuit model based quantum computation. We investigate general resource requirements for arbitrary n-qubit Toffoli gate. These resources consist of the nontrivial Clifford gate (CNOT), non-Clifford gate (T gate), ancillary qubits, and circuit depth. To implement n-qubit Toffoli gates, we consider two cases: only one auxiliary qubit and unlimited auxiliary qubits. The key of the first case is to decompose an n-qubit Toffoli gate into the reduced Toffoli gate modulo phase shift using the Clifford gates and one ancillary qubit. With this construction, it only requires $O(n)$ number of general resources for an n-qubit Toffoli gate. For the second case, an approximate Toffoli gate is constructed to obtain efficient decomposition of a Toffoli gate. The new decomposition can further reduce general resources except auxiliary qubits.

Keywords Toffoli gate · Quantum circuit · Clifford gates · circuit complexity

1 Introduction

Quantum computation has been proved to be efficient for solving many difficult problems [1–8]. Most of these quantum algorithms are based on the Deutsch's quantum computational network model [9, 10]. It means that quantum task may be characterized by initial

✉ Yong He
heyongmath@163.com

[1] Department of Mathematics and Physics, Chongqing University of Science and Technology, Chongqing 401331, China

[2] Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu 610031, China

[3] Department of Physics, University of Michigan, Ann Arbor, MI 48109, USA

system, special quantum evolution and proper quantum measurement. As an important component of quantum speedup, the joint system's evolution should be implemented efficiently. However, this may be difficult for the most quantum algorithms with large systems in experiment. Fortunately, using the traditional matrix decompositions such as the cosine-sine decomposition or Shannon decomposition [11], complicated evolutions of n-qubit system may be synthesized by a series of special operations such as single-qubit rotations and n-qubit controlled-NOT gates (n-qubit Toffoli gates) [12–15]. For $n = 2$, multi-qubit Toffoli gate is reduced to special CNOT gate. When $n = 3$, three-qubit Toffoli gate (Toffoli gate in common) is used to flip target qubit conditional on two controlling qubits. Toffoli gate plays a key role in some well-known quantum algorithms such as quantum error correcting [16–19]. Different from the CNOT gate and qubit rotations [12–15], Toffoli gate and a proper single-qubit gate form another universal gate set for the quantum computation [20]. Several experiments [21–26] have been proposed to realize Toffoli gate with different systems.

For an n-qubit Toffoli gate, the traditional decomposition is using elementary gates of CNOT gate and qubit rotations [14, 25, 26], which is justified by the Solovay-Kitaev Theorem [27]. Unfortunately, these implementations always require quadratic number of logic gates and quadratic depth of quantum circuits without ancillary qubits. For the Toffoli gate, the simplest decomposition costs five two-qubit gates [14, 20], or six CNOTs [28] and several one-qubit gates. Recently, a new efficient algorithm is introduced by using $O(\log(1/\epsilon))$ gates consisting of these gates in the Clifford group and the non-Clifford gate $T = \mathrm{diag}(1, e^{i\pi/4})$ [29–31]. Here, the non-Clifford gate (T) is expensive in time and space resources to realize in experiment [29–37].

In this paper, motivated by expensive costs of CNOT (non-trivial Clifford gate) and T (non Clifford gate) in quantum simulation [24–34], we consider general circuit complexity of n-qubit Toffoli gates. The complexity examined consists of the number of the CNOT gate, T gate and auxiliary qubit, and logic depth of implementation circuit. Our goal is to provide options in simulations up to different physical conditions. We firstly propose an approach to decompose n-qubit Toffoli gates into blocked multiple-qubit Toffoli gates with efficient circuit by using only one ancillary qubit. Combining with the decomposition network in Ref. [12], these reduced multiple-qubit Toffoli gates may be further realized with $O(n)$ CNOT gates and T gates. Our circuit complexity is lower than previous scheme [12, 35, 36]. Note that our decomposition holds for one auxiliary qubit without initialization requirement. Hence, our setup is reasonable for quantum computation because any one of inactive quantum registers or quantum encoders may act as an ancillary qubit. Our circuit complexity is only a half of previous scheme [12], a quarter of previous scheme [35] or a quadric-speedup of previous scheme [36]. And then, using an efficient decomposition of an approximate Toffoli on the special target qubit, a Toffoli gate may be exactly synthesized by 5 CNOT gates and 4 T gates. Based on this subroutine, the circuit complexity of n-qubit Toffoli gates may be reduced, especially the circuit depth from $O(n)$ to $O(\log_2 n)$. All the examined resources of this decomposition are lower than the decomposition [37–40] except the number of ancillary qubits. Generally, all of these decompositions of n-qubit Toffoli gates have their own superiorities up to special in requirements. Our results may speed up the progress towards scalable quantum computation.

This paper is organized as follows. In Section 2, an n-qubit Toffoli gate is decomposed with only one ancillary qubit. And then, the derived controlled gates may be further synthesized using CNOT gate and T gate. In Section 3, we present a gate-synthesis approach for the approximate Toffoli gate and general n-qubit Toffoli gates with linear auxiliary qubits while the last section concludes this paper.

2 Resource Requirements for an n-qubit Toffoli Gate with One Ancillary Qubit

In this section, the general circuit complexity of an n-qubit Toffoli gate will be analyzed. Here, an n-qubit Toffoli gate is a flip gate σ_x with the first $n-1$ qubits as the controlling qubits, which may be defined by

$$C^{n-1}[\sigma_x] : \otimes_{i=1}^{n}|x_i\rangle \rightarrow \otimes_{i=1}^{n-1}|x_i\rangle|x_n \oplus x_1x_2\cdots x_{n-1}\rangle \tag{1}$$

By using an arbitrary ancillary qubit, the following basic decomposition may be proved for the main result.

Lemma 1 *An n-qubit Toffoli gate $C^{n-1}[\sigma_x]$ can be implemented as is shown in* Fig. 1 *with one auxiliary qubit, where $n \geq 3$.*

Proof To obtain this lemma, it is sufficient to prove that the right circuit (except two Hs) of Fig. 1 has realized the $n+1$-qubit controlled phase gate $C^n[-I]$ in the first n qubits. It may be completed from the following four cases.

(1) If some of the first k_1 bits and the second k_2 bits are 0, the transformation applied to the auxiliary qubit is $S^\dagger \cdot S \cdot S^\dagger \cdot S = I$.

(2) If some of the first k_1 bits are 0 and all the second k_2+1 bits are 1, the transformation applied to the auxiliary qubit is

$$S^\dagger \cdot \sigma_x \cdot S \cdot S^\dagger \cdot \sigma_x \cdot S = I \tag{2}$$

(3) If all the first k_1 bits are 1 and some of the second k_2+1 bits are 0, the transformation applied to the auxiliary qubit is

$$S^\dagger \cdot S \cdot \sigma_x \cdot S^\dagger \cdot S \cdot \sigma_x = I \tag{3}$$

(4) If all the first n bits are 1, the transformation applied to the auxiliary qubit is

$$S^\dagger \cdot \sigma_x \cdot S \cdot \sigma_x \cdot S^\dagger \cdot \sigma_x \cdot S \cdot \sigma_x = -I \tag{4}$$

It means that the circuit except two Hadamard gate Hs has realized the $n+1$-qubit controlled phase transformation $C^n[-I]$. Furthermore, this $n+1$-qubit controlled phase transformation is equivalent to an n-qubit controlled phase gate $C^{n-1}[\sigma_z]$ on the first n qubits in the Fig. 1. Hence, it is easy to get this lemma from the fact $H \cdot \sigma_z \cdot H = \sigma_x$. □

Lemma 2 *An m-qubit Toffoli gate $C^m[\sigma_x]$ on n-qubit system with $2m \leq n$ can be implemented by a network consisting of $4(m-2)$ Toffoli gates.*

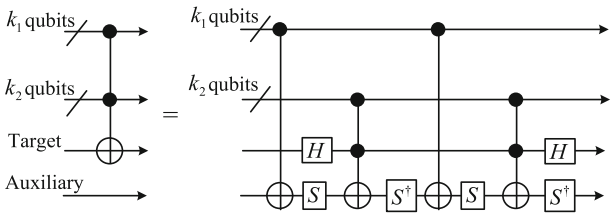

Fig. 1 Efficient decomposition of n-qubit Toffoli gate $C^n[\sigma_x]$. $k_1 + k_2 = n-1$. An auxiliary qubit is used. $S = |0\rangle\langle 0| + i|1\rangle\langle 1|$ is a Clifford gate

The proof is easy to follow from the Lemma 7.2 [12] and the symmetric properties of the decomposed network (each Toffoli gate from $C^m[\sigma_x]$ has performed two times, the phase -1 of $|101\rangle$ may be canceled).

Corollary 1 *An n-qubit Toffoli gate $C^{n-1}[\sigma_x]$ can be simulated by $8n-24$ approximate Toffoli gates assisted by an auxiliary qubit.*

Proof For an n-qubit Toffoli gate $C^{n-1}[\sigma_x]$, from the Fig. 1 of the Lemma 1, it can be decomposed into 2 number of k_1+1-qubit Toffoli gate $C^{k_1}[\sigma_x]$ and 2 number of k_2+2-qubit Toffoli gate $C^{k_2+1}[\sigma_x]$, where $k_1=\lceil\frac{n}{2}\rceil$ denotes the smallest integer no less than $\frac{n}{2}$ and $k_2+1=\lfloor\frac{n}{2}\rfloor$ denotes the largest integer no more than $\frac{n}{2}$. Now, by using the Lemma 2, each $C^{k_1}[\sigma_x]$ gate can be realized by using $4(k_1-2)$ approximate Toffoli gates and each $C^{k_2+1}[\sigma_x]$ gate can be realized by using $4(k_2-1)$ approximate Toffoli gates. Totally, an n-qubit Toffoli gate $C^{n-1}[\sigma_x]$ requires $2\times(4(k_1-2)+4(k_2-1))=8n-24$ approximate $C^2[\sigma_x]$ gates (Fig. 2).

An example of $n=6$ is shown in Fig. 3. Here, $k_1=4$ and $k_2=2$. An $C^6[\sigma_x]$ gate is decomposed into two $C^4[\sigma_x]$ and two $C^3[\sigma_x]$. And then, each $C^4[\sigma_x]$ and $C^3[\sigma_x]$ are decomposed by the network in the Lemma 2. □

Theorem 1 *An n-qubit Toffoli gate $C^{n-1}[\sigma_x]$ can be implemented by a circuit depth of $216n-648$ assisted by a recyclable auxiliary qubit. Moreover, $C^{n-1}[\sigma_x]$ requires $24n-72$ CNOT gates and $32n-96$ T or $T^\dagger$.*

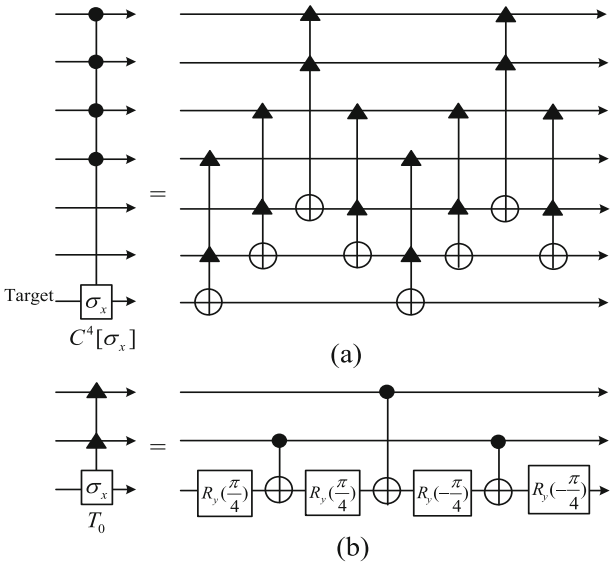

Fig. 2 Efficient decomposition of an approximate Toffoli gate $C^4[\sigma_x]$ without auxiliary qubit. This approximate Toffoli gate is different from the Toffoli gate with the phase -1 at the $|101\rangle$

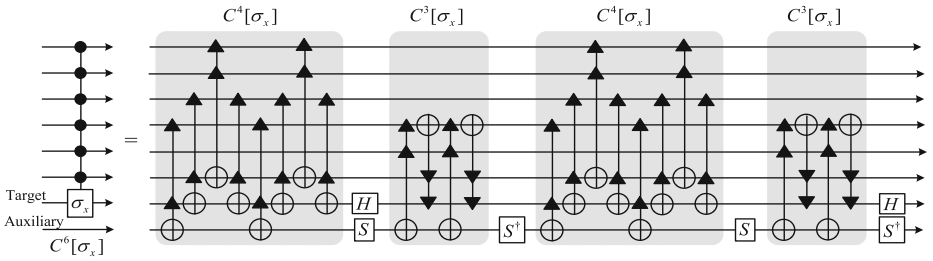

Fig. 3 Efficient decomposition of a 7-qubit Toffoli gate $C^6[\sigma_x]$ using an 8-qubit system. Here, one qubit is used as auxiliary qubit

Proof Note that

$$R_y(\frac{\pi}{4}) = e^{-i\pi/8} SHTHSZ \tag{5}$$

From the Fig. 2b, a Toffoli gate can be realized with 3 CNOT gates and 4 T or $T^\dagger$ gates, in the depth of 27. Note that from the Corollary 1, all the single qubit gates S and $S^\dagger$ may be implemented in parallel with the Toffoli gate before them. The first H gate may be implemented in parallel with the Toffoli gate after it. Thus an n-qubit Toffoli gate $C^{n-1}[\sigma_x]$ can be implemented by a depth of $27 \times (8n-24)+1 = 216n-648$ assisted by a recyclable auxiliary qubit. Moreover, $C^{n-1}[\sigma_x]$ gate can be implemented with $3\times(8n-24) = 24n-72$ CNOT gates and $4 \times (8n-24) = 32n-96$ non-Clifford gate T or $T^\dagger$.

The circuit complexity of n-qubit Toffoli gates are compared with these in Refs. [12, 35, 36], as shown in Table 1. Their complexity is evaluated by using the decomposition in the Sec.V [35] and the Lemma 2. Note that they have to perform 2 number of n-qubit gate $C^{n-1}[i\sigma_x]$, each $C^{n-1}[i\sigma_x]$ requires 2 number of k_1+1-qubit Toffoli gate $C^{k_1}[\sigma_x]$, 2 number of k_2+2-qubit Toffoli gate $C^{k_2+1}[\sigma_x]$ and 4 number of T or $T^\dagger$. The number of their CNOT gate is $12 \times (8n-24)+1 = 96n-287$; the number of their T gate is $14 \times (8n-24)+4 = 112n-332$; and the logic depth is $2 \times (10 \times (8n-24)+6)+1 = 160n-467$. Saeedi & Pedram [36] have realized an n-qubit gate $C^{n-1}[i\sigma_x]$ with $O(n^2)$ controlled rotations. Each decomposed controlled rotation may be realized with $O(1)$ CNOT gate and T gate. To complete a $C^{n-1}[\sigma_x]$ gate, an auxiliary qubit in the state $|0\rangle$ should be used as its in Ref.

Table 1 The cost of exact synthesis of n-qubit Toffoli gates with only one ancillary qubit

n-qubit Toffoli gate	N_T	N_{CNOT}	N_d	N_a
Barenco et al. [12]	$56n-280$	$48n-204$	$O(n)$	1
Giles & Selinger [35]	$112n-332$	$96n-287$	$160n-467$	1
Saeedi & Pedram [36]	$O(n^2)$	$O(n^2)$	$O(n)$	1
Our scheme	$32n-96$	$24n-72$	$216n-648$	1

N_{CNOT}, N_T and N_a denote the number of CNOT gate, T gate and auxiliary qubit, respectively. N_d denotes the logic depth of circuit. The auxiliary qubit should be initialized as $|0\rangle$ [35] while our scheme has no requirement

[35]. From this table, the present circuit complexity is lower more than previous complexity [12, 35, 36]. □

3 Resource Requirements for an n-qubit Toffoli Gate with Ancillae

Different from the decomposition in the Section 2 with only one auxiliary qubit, in this section, we consider decompositions of n-qubit Toffoli gates with ancillae. It will show that the total numbers of T gate and CNOT gate, and circuit depth may be greatly reduced by increasing the number of ancillae.

3.1 Toffoli Gate

Let us denote a Toffoli$*$ gate as the operation in Fig. 4a, which requires four non-Clifford T gates. Here, Toffoli$*$ gate has the following matrix representation

$$Toffoli* = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -i \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{6}$$

It is easy to prove that Toffoli gate and Toffoli$*$ gate are different in the phases of terms $|001\rangle$, $|011\rangle$, $|101\rangle$, $|111\rangle$. However, both of them have the same operation on the joint system

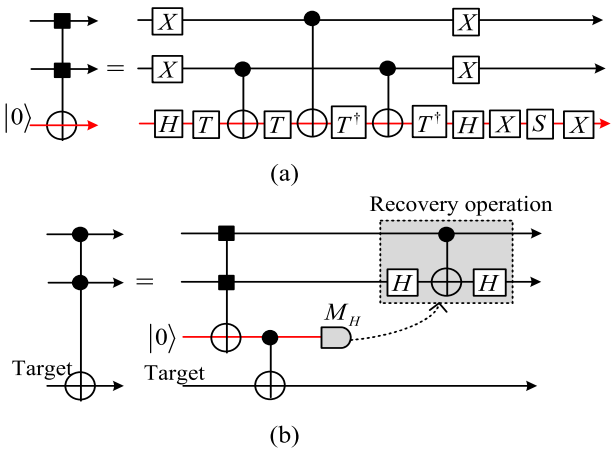

Fig. 4 (Color online)Exact gate synthesis of a Toffoli gate with ancillary qubit. **a** The Toffoli$*$ gate defined in (6). It has the same operation to the desired Toffoli gate if the target qubit in the state $|0\rangle$. **b** The decomposition of the desired Toffoli gate by combining the Toffoli$*$ circuit with teleportation and phase correction. The measurement is performed under the basis $\{|\pm\rangle\}$, and the recovery operation controlled-σ_z is conditional on the measurement result $|-\rangle$

Table 2 The cost of a Toffoli gate with ancillary qubits

N_{CNOT} denotes the number of CNOT gate. N_T denotes the number of T gate. N_d denotes the circuit depth. N_a denotes the number of auxiliary qubit

Toffoli gate	N_T	N_{CNOT}	N_d	N_a
Selinger [37]	7	16	25	4
Jones [38]	4	10	22	2
Scheme in Fig. 4	4	5	17	1

where the target qubit is in the state $|0\rangle$. It means that Toffoli$*$ gate has realized a Toffoli gate on the target qubit in the state $|0\rangle$. With this Toffoli$*$ gate, an ancillary qubit and teleportation are used to implement a Toffoli gate on arbitrary three-qubit system, as shown in Fig. 4b. In detail, a Toffoli* gate is firstly performed on the three-qubit system, where the controlling qubits are same to the desired Toffoli gate while the target qubit is an ancillary qubit in the state $|0\rangle$. And then, the followed CNOT gate, measurement and feed-forward corrections may complete a Toffoli gate on the desired system. Here, the correction operation, i.e., a controlled-σ_z, is performed for the measurement result $|-\rangle$. From the Table 2, our results have reduced the required resources for a Toffoli gate [37, 38].

3.2 *n*-qubit Toffoli Gates

By using the Toffoli gate shown in Fig. 4b, we can get another linear complexity decomposition of n-qubit Toffoli gate $C^{n-1}[\sigma_x]$, shown in Fig. 5. Figure 5a shows a nontrivial example of 5-qubit Toffoli gate. The general linear complexity decomposition of an n-qubit Toffoli gate is represented iteratively in Fig. 5b. In fact, we can get the following theorem. An example is shown in Fig. 6.

Theorem 2 *An n-qubit Toffoli gate can be synthesized by* $4n-7$ *CNOT gates,* $4n-8$ *T gates, depth of* $16n-32$*, and* $n-2$ *auxiliary qubits.*

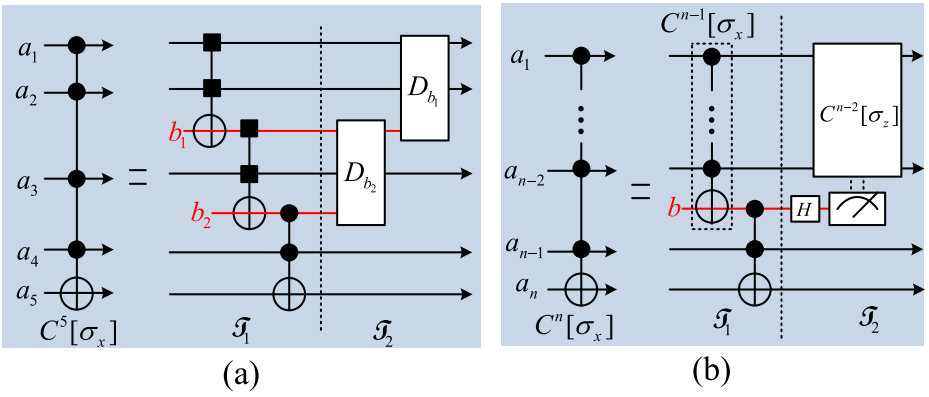

Fig. 5 (Color online)Exact gate synthesis of an n-qubit Toffoli gate with ancillary qubits. **a** A 5-qubit Toffoli gate using 3 Toffoli gates. b_i are auxiliary qubits in the state $|0\rangle$. D_x denotes disentangling operation (the measurement M_H and corresponding recovery operation) on the qubit x, as shown in the Fig. 4b. $\mathcal{T}_1$ denotes the first subcircuit to implement multiple controlling whereas $\mathcal{T}_2$ denotes disentangling operations. **b** An n-qubit Toffoli gate using $n-2$ Toffoli gates

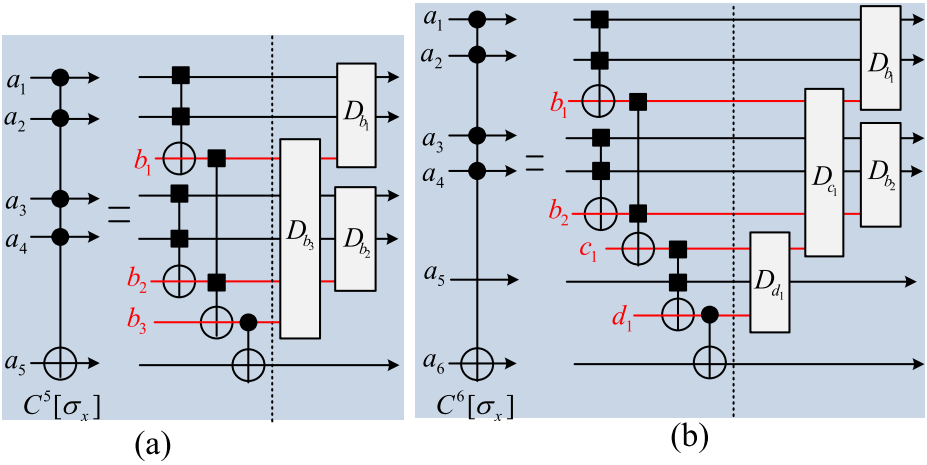

Fig. 6 (Color online)A parallel circuit construction for multiple-qubit Toffoli gate. b_i and c_i are auxiliary qubits in the state $|0\rangle$. D_x denotes disentangling operation on the ancillary qubit x, as shown in the Fig. 5b

The proof of this theorem is shown in Appendix A.

Corollary 2 *The proposed structure for an n-qubit Toffoli gate can be synthesized by a depth of no more than* $16\lceil\log_2(n-1)\rceil + 12$*, with* $4n-7$ *CNOT gates,* $4n-8$ T *gates, and* $n-1$ *auxiliary qubits.*

The proof of this corollary is shown in Appendix B.

The comparisons of resources are shown in Table 3. Here, from the Jones's implementation [37] of a Toffoli gate, we can obtain that their costs of n-qubit Toffoli gates are $n-2$ Toffoli gates, $n-3$ disentangling operations, $4n-8$ T gates and $2n-4$ auxiliary qubits. This scheme will cost $8(n-3)+10+n-3 = 9n-17$ CNOT gates and has the depth of $20n-43$. From this table, the numbers of the T gate and CNOT gate, and the circuit depth in our scheme are less than these in previous schemes [37–40]. Our schemes requires more auxiliary qubits than previous schemes [37, 38, 40].

Table 3 The cost of an exact synthesis of $C^{n-1}[\sigma_x]$ on n qubits with ancillae

$C^{n-1}[\sigma_x]$	N_T	N_{CNOT}	N_d	N_a
Selinger [37]	$8n-17$	$8n-18$	$4n-10$	$n-3$
Jones [38]	$4n-8$	$9n-17$	$20n-43$	$2n-4$
Maslov [39]	$8n-16$	$8n-20$	$4n-10$	$\lceil\frac{n-3}{2}\rceil$
Amy et al. [40]	$8n-17$	-	-	$n-3$
Our scheme	$4n-8$	$4n-7$	$16\lceil\log_2(n-1)\rceil+12$	$n-1$

N_{CNOT}, N_T, N_d and N_a are the same to these defined in the Table 1

4 Conclusion

We have investigated resource requirements for arbitrary n-qubit Toffoli gate. Our considerations of resources include typical Clifford gate (CNOT gate), non-Clifford gate (T gate), implementation "time" (depth of circuit) and auxiliary registers. Using an arbitrary ancillary qubit and Toffoli gate modulo phase shifts, an n-qubit Toffoli gate may be realized with linear circuit complexity. Our scheme has reduced the number of T gate by a factor of 4/7 in the leading constant and the CNOT by a factor 1/2 in the leading constant. If arbitrary ancillae are considered, we presented a parallel quantum circuit by using special approximate Toffoli gate. From this construction, the numbers of T gate and CNOT gate are saved one half while the circuit depth has been greatly reduced. Of course, this improvement is achieved by relaxing the number of ancillary qubits. Generally, each of two methods has its own superiorities. Hence, they should be traded-off if special requirements or restrictions are allowed in experiment.

Acknowledgments This work is supported by the Science and Technology Research Project of Chongqing Education Commission (No.KJ1713339), Sichuan Youth Science and Technique Foundation (No.2017JQ0048), National Natural Science Foundation of China (Nos.61303039), and CSC Scholarship.

Appendix A

Proof of Theorem 2 The proof is completed by induction. Firstly, when $n = 3$, the result is reduced to the Toffoli gate shown in Fig. 6b. And then, for a general n, assume that the result is right for $k \leq n-1$, it only needs to prove the decomposition for n. For convenience, the decomposition circuit is divided into two parts $\mathcal{T}_1$ and $\mathcal{T}_2$. For the first part $\mathcal{T}_1$, note that

$$
\begin{aligned}
&\sum_{i_1,\cdots,i_n=0}^{1} \alpha_{i_1\cdots i_n}(\otimes_{j=1}^{n}|i_j\rangle_{a_j})|0\rangle_b \\
\overset{C_b^{n-2}[\sigma_x]}{\rightarrow}\ &\sum_{i_{n-1},i_n=0}^{1} \beta_{i_{n-1}i_n}|i_{n-1}i_n\rangle_{a_{n-1}a_n} \\
&\cdot[\sum_{i_1+\cdots+i_{n-2}\neq n-2} \gamma_{i_1\cdots i_n}(\otimes_{j=1}^{n-2}|i_j\rangle_{a_j})|0\rangle_b \\
&\quad +\gamma_{1\cdots 1}|1\cdots 1\rangle_{a_1\cdots a_{n-2}})|1\rangle_b] \\
\overset{C_{a_n}^{2}[\sigma_x]}{\rightarrow}\ &\sum_{i_{n-1},i_n=0}^{1} \beta_{i_{n-1}i_n}|i_{n-1}i_n\rangle_{a_{n-1}a_n} \\
&\{\sum_{i_1+\cdots+i_{n-2}\neq n-2} \gamma_{i_1\cdots i_n}(\otimes_{j=1}^{n-2}|i_j\rangle_{a_j})|0\rangle_b \\
&+[\gamma_{1\cdots 1}(\beta_{00}|00\rangle+\beta_{01}|01\rangle+\beta_{10}|11\rangle \\
&+\beta_{11}|10\rangle)_{a_{n-1}a_n}|1\cdots 1\rangle_{a_1\cdots a_{n-2}}]|1\rangle_b\}
\end{aligned}
\tag{7}
$$

where $C_b^{n-2}[\sigma_x]$ denotes an $n-1$-qubit Toffoli gate on the qubits $a_1, a_2, \cdots, a_{n-2}$ and b, and $C_{a_n}^2[\sigma_x]$ denotes the Toffoli gate on the qubits b, a_{n-1} and a_n. Thus $\mathcal{T}_1$ has been used to complete an n-qubit Toffoli gate $C^{n-1}[\sigma_x]$ with an auxiliary state b in the state $|0\rangle$. □

Moreover, to complete an n-qubit Toffoli gate $C^{n-1}[\sigma_z]$, the auxiliary qubit b should be disentangled. In detail, for the second part $\mathcal{T}_2$, note that by measuring the qubit b under the basis $\{|\pm\rangle\}$, the joint state in (7) may collapse into one of the following states

$$\begin{aligned}&\sum_{i_{n-1},i_n=0}^{1}\beta_{i_{n-1}i_n}|i_{n-1}i_n\rangle_{a_{n-1}a_n}\\&\{\sum_{i_1+\cdots+i_{n-2}\neq n-2}\gamma_{i_1\cdots i_n}(\otimes_{j=1}^{n-2}|i_j\rangle_{a_j})\\&\gamma_{1\cdots1}(\beta_{00}|00\rangle+\beta_{01}|01\rangle+\beta_{10}|11\rangle\\&+\beta_{11}|10\rangle)_{a_{n-1}a_n}|1\cdots1\rangle_{a_1\cdots a_{n-2}}\}\end{aligned}\tag{8}$$

which may be further transformed into

$$\begin{aligned}&\sum_{i_{n-1},i_n=0}^{1}\beta_{i_{n-1}i_n}|i_{n-1}i_n\rangle_{a_{n-1}a_n}\\&\{\sum_{i_1+\cdots+i_{n-2}\neq n-2}\gamma_{i_1\cdots i_n}(\otimes_{j=1}^{n-2}|i_j\rangle_{a_j})\\&+\gamma_{1\cdots1}(\beta_{00}|00\rangle+\beta_{01}|01\rangle+\beta_{10}|11\rangle\\&+\beta_{11}|10\rangle)_{a_{n-1}a_n}|1\cdots1\rangle_{a_1\cdots a_{n-2}}\}\end{aligned}\tag{9}$$

by performing the $n-2$-qubit controlled phase flip (correction operation) $C^{n-2}[\sigma_z]$ on the first $n-2$ qubits $a_1, a_2, \cdots$, and a_{n-2}. Thus we complete an n-qubit Toffoli gate.

By induction, one can get the Toffoli gate-based decomposition of an n-qubit Toffoli gate. For the subcircuit $\mathcal{T}_1$, this iteration is very simple by using $n-3$ auxiliary qubits and the Toffoli$*$ gate. For the subcircuit $\mathcal{T}_2$, it is tedious to prove that each auxiliary qubit may be disentangled using $C^2[\sigma_z]$ gate on its generation system (which has been used to complete a Toffoli$*$ gate) in the subcircuit $\mathcal{T}_1$, see Fig. 4b.

From the Fig. 4, each Toffoli$*$ gate may be implemented with the depth of 12. Moreover, from the Figs. 4 and 5b, each n-qubit Toffoli gate may be decomposed into $n-2$ Toffoli$*$ gates, and $n-2$ disentangling operations. Hence, the total depth is $12(n-2)+4(n-2)=16n-32$, the total number of CNOT gate is $3(n-2)+(n-2)+1=4n-7$, and the total number of T gate is $4(n-2)=4n-8$. The proof is completed.

Appendix B

Proof of the Corollary 2. Firstly, all control qubits $a_1, a_2, \cdots, a_{n-1}$ may be divided into $k_1 = \lceil (n-1)/2 \rceil$ pairs $(a_1, a_2), (a_3, a_4), \cdots, (a_{n-2}, a_{n-1})$ for an odd n or $(a_1, a_2), (a_3, a_4), \cdots, (a_{n-3}, a_{n-2}), a_{n-1}$ for an even n. Each of these pairs except a_{n-1} for the even n will be the controlling qubits of a Toffoli$*$ gate, whose target qubits are auxiliary qubits $b_1, \cdots, b_{k_1}$ in the state $|0\rangle$, respectively. These Toffoli$*$ gates may be implemented in parallel. Secondly, all auxiliary qubits $b_1, b_2, \cdots, b_{k_1}$ and the qubit a_{n-1} for even n may be divided into $k_2 = \lfloor k_1/2 \rfloor$ or $k_2 = \lfloor (k_1+1)/2 \rfloor$ pairs $(b_1, b_2), (b_3, b_4), (b_{k_1-1}, b_{k_1})$ for even k_1 or $(b_1, b_2), (b_3, b_4), \cdots, (b_{k_1-2}, b_{n_1-1}), (b_{k_1}, a_{n-2})$ for odd k_1. Here, $\lfloor x \rfloor$ denotes the maximal integer no more than x. Each of these pairs will be the controlling qubits of another Toffoli gate$*$, whose target qubits are auxiliary qubits c_j in the state $|0\rangle$. These Toffoli$*$ gates may be also implemented in parallel. Continue this procedure until one gets only two

auxiliary qubits e_1 and e_2 as target qubits. Now, these two auxiliary qubits as controlling qubits of one Toffoli gate while the qubit a_n is target qubit. This Toffoli gate may be also realized with one Toffoli$*$ gate and disentangling operations. This procedure costs at most $\lceil \log_2(n-1) \rceil$ parallel time steps. Finally, no more than $n-1$ auxiliary qubits may be disentangled by $\lceil \log_2(n-1) \rceil + 1$ parallel disentangling operations D, shown in Fig. 6b. Here, the measurement order is the inverse order of the parallel implementations of the Toffoli$*$ gate above. The corrections conditional on the measurement outcome are performed on its controlling qubits of the corresponding Toffoli$*$ gate (while the measured auxiliary qubit is its target qubit), see Fig. 6a for odd n and Fig. 6b for even n. The correctness of these corrections is derived from the proof of the Theorem 2. □

Moreover, from Fig. 4a, a Toffoli* gate has the same result to a Toffoli gate if the target qubit in the state $|0\rangle$. Hence, all the Toffoli$*$ gates cost $3(n-2)+1 = 3n-5$ CNOT gates and have the depth of $12\lceil \log_2(n-1) \rceil + 12$. The $n-2$ disentangling operations may be implemented with the depth of $4\lceil \log_2(n-2) \rceil$ with $n-2$ CNOT gates. Hence, the total circuit depth is no more than $16\lceil \log_2(n-1) \rceil + 12$ with $4n-7$ CNOT gates. The proof is completed.

References

1. Feynman, R.: Int. J. Theor. Phys. **21**, 467–488 (1982)
2. Shor, P.W.: SIAM J. Comput. **26**, 1484–1509 (1997)
3. Grover, L.K.: Phys. Rev. Lett. **79**, 325–328 (1997)
4. Farhi, E., Goldstone, J., Gutmann, S., Lapan, J., Lundgren, A., Preda, D.: Science **292**, 472–475 (2001)
5. Harrow, A.W., Hassidim, A., Lloyd, S.: Phys. Rev. Lett. **103**, 150502 (2009)
6. Bacon, D., van Dam, W.: Commun. ACM **53**, 84–93 (2010)
7. Lin, J., Peng, X., Du, J., Suter, D.: Sci. Rep. **2**, 260 (2012)
8. Lloyd, S., Mohseni, M., Rebentrost, P.: Nature Phys. **10**, 631–633 (2014)
9. Deutsch, D.: Quantum computational networks. Proc. R. Soc. Lond. A **425**, 73–90 (1989)
10. Deutsch, D., Jozsa, R.: Proc. R. Soc. London, Ser. A **439**, 553–558 (1992)
11. Horn, R.A., Johnson, R.: Matrix Analysis, 2nd Edition. Cambridge University Press (2012)
12. Barenco, A., Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P.W., Sleator, T., Smolin, J.A., Weinfurter, H.: Phys. Rev. A **52**, 3457 (1995)
13. Zhang, J., Vala, J., Sastry, S., Whaley, K.B.: Phys. Rev. Lett. **91**, 027903 (2003)
14. Vartiainen, J.J., Möttönen, M., Salomaa, M.M.: Phys. Rev. Lett. **92**, 177902 (2004)
15. Shende, V., Bullock, S.S., Markov, I.L.: IEEE Tran. Comput. AID Design **26**, 1000–1010 (2006)
16. Shor, P.W.: Phys. Rev. A **52**, 2493 (1995)
17. Calderbank, A.R., Shor, P.W.: Phys. Rev. A **54**, 1098 (1996)
18. Steane, A.M.: Phys. Rev. A **54**, 4741 (1996)
19. Gottesman, D.: Phys. Rev. A **54**, 1862 (1996)
20. Shi, Y.: Quantum Info. & Comput. **3**, 84–92 (2003)
21. Fedorov, A., Steffen, L., Baur, M., da Silva, M.P., Wallraff, A.: Nature **481**, 170 (2012)
22. Stojanovic, V.M., Fedorov, A., Wallraff, A., Bruder, C.: Phys. Rev. B **85**, 054504 (2012)
23. Monz, T., Kim, K., Hänsel, W., Riebe, M., Villar, A.S., Schindler, P., Chwalla, M., Hennrich, M., Blatt, R.: Phys. Rev. Lett. **102**, 040501 (2009)
24. Borrelli, M., Mazzola, L., Paternostro, M., Maniscalco, S.: Phys. Rev. A **84**, 012314 (2011)
25. Ralph, T.C., Resch, K.J., Gilchrist, A.: Phys. Rev. A **75**, 022313 (2007)
26. 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., White, A.G.: Nature Phys. **5**, 134–140 (2008)
27. Dawson, C.M., Nielsen, M.A.: Quantum Info. & Comput. **6**, 81–95 (2006)
28. Yu, N., Duan, R., Ying, M.: Phys. Rev. A **88**, 010304 (2013)
29. Kliuchnikov, V., Maslov, D., Mosca, M.: Quantum Info. & Comput. **13**, 607–630 (2013)
30. Selinger, P.: Quantum Info. & Comput. **15**, 159–180 (2015)
31. Bravyi, S., Kitaev, A.: Phys. Rev. A **71**, 022316 (2005)

32. Jones, C.: Phys. Rev. A **87**, 042305 (2013)
33. Saeedi, M., Markov, I.L.: ACM Comput. Surv. **45**, 21 (2013)
34. Selinger, P.: Phys. Rev. A **87**, 042302 (2013)
35. Giles, B., Selinger, P.: Phys. Rev. A **87**, 032332 (2013)
36. Saeedi, M., Pedram, M.: Phys. Rev. A **87**, 062318 (2013)
37. Jones, C.: Phys. Rev. A **87**, 022328 (2013)
38. Saeedi, M., Arabzadeh, M., Saheb Zamani, M., Sedighi, M.: Quantum Inf. & Comput. **11**, 262–277 (2011)
39. Maslov, D.: Phys. Rev. A **93**, 022311 (2016)
40. Amy, M., Maslov, D., Mosca, M.: IEEE Trans. CAD **33**(10), 1476–1489 (2014)