SCIENTIFIC REPORTS

OPEN

Efficient decomposition methods for controlled-R_n using a single ancillary qubit

Received: 3 October 2017
Accepted: 20 March 2018
Published online: 03 April 2018

Taewan Kim & Byung-Soo Choi

We consider decomposition for a controlled-R_n gate with a standard set of universal gates. For this problem, a method exists that uses a single ancillary qubit to reduce the number of gates. In this work, we extend this method to three ends. First, we find a method that can decompose into fewer gates than the best known results in decomposition of controlled-R_n. We also confirm that the proposed method reduces the total number of gates of the quantum Fourier transform. Second, we propose another efficient decomposition that can be mapped to a nearest-neighbor architecture with only local CNOT gates. Finally, we find a method that can minimize the depth to 5 gate steps in a nearest-neighbor architecture with only local CNOT gates.

Due to the recent advances in quantum device technology, an arbitrary single-qubit gate or a Z-rotation gate can be implemented with fairly high accuracy, and a small quantum algorithm can be tested. However, even with the gate of a small error rate currently being realized, it is difficult to directly perform scalable quantum computation since it requires that arbitrarily large computations is implemented. In order to overcome this problem, fault-tolerable computation is still needed[1]. Therefore, for reliable quantum computation, all quantum operations of a quantum algorithm should be represented by a universal gate set that arises from a fault-tolerant protocol such as Clifford + T gates[2].

We consider a standard set of universal gates consisting of Hadamard (denoted H), phase (S), $\pi/8$ (T), and controlled-NOT (CNOT) gates. Although it is known that quantum algorithms have much lower computational complexities than classical algorithms for problem such as factoring large integers[3], when such quantum algorithm are decomposed into CNOT, H, S, and T gates, the result includes a huge number of gates. Thus, the advantages of quantum computing might be nullified. To enhance the benefits of quantum computation, it is important to use an efficient decomposition of quantum algorithms into universal gates. Here, we first consider the decomposition of single-qubit gates and two-qubit gates. Any single-qubit gate can be decomposed in terms of Hadamard gates and Z-rotation gates $R_z(\theta)$[4,5], and there are well-known methods to approximate $R_z(\theta)$ efficiently[6–9]. Next, we consider a controlled-R_n gate as the simplest 2-qubit gate to be decomposed into a universal set of gates. Controlled-R_n gates represent the fundamental part of the quantum Fourier transform (QFT) and many other quantum algorithms. Thus, controlled-R_n decomposition has a significant impact on the overall decomposition of a quantum algorithm. In this work, we propose efficient controlled-R_n decomposition methods as a technique to help enhance the benefits of quantum computation.

Background

Approximation of R_n gate.

An R_n gate is defined as follows:

$$R_n = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/2^{n-1}} \end{bmatrix}. \tag{1}$$

The R_2 gate is an S gate (or P gate), and the R_3 gate is a T gate. The R_2 and R_3 gates are included in the universal set. However, R_n for $n \geq 4$ cannot be exactly decomposed with only a standard set of universal gates[8]. Thus, we should approximate R_n for $n \geq 4$ to express it with the standard set.

To approximate the R_n gate, we use the gridsynth method[9]. Given a precision $\varepsilon > 0$, the approximation of an R_n gate is to find an operator U expressible as H, S, T and Pauli operators such that

Electronics and Telecommunications Research Institute, Daejeon, 34129, Korea. Correspondence and requests for materials should be addressed to B.-S.C. (email: bschoi3@etri.re.kr)

Angle	Precision 10^{-5}	Precision 10^{-10}	Precision 10^{-15}
$\pi/2^3$	126.9226	253.3806	379.3563
$\pi/2^4$	126.7122	253.3352	379.4713
$\pi/2^5$	126.8313	253.2603	379.0883
$\pi/2^6$	126.8625	253.3316	379.3822
$\pi/2^7$	126.8923	253.4391	379.0980
$\pi/2^8$	126.9019	253.1520	379.9702
$\pi/2^9$	126.9230	253.2793	379.0183
$\pi/2^{10}$	126.9107	253.2635	379.2323
$\pi/2^{11}$	126.9982	253.5258	379.3016
$\pi/2^{12}$	126.7677	253.4237	379.1009
$\pi/2^{13}$	126.8485	253.4133	379.3630
$\pi/2^{14}$	126.8366	253.1778	379.3084
$\pi/2^{15}$	126.9337	253.5174	379.2136
Average number of gates	127	253	379

Table 1. Average numbers of gates over 10,000 runs for an approximation of R_n with angle $\pi/2^{n-1}$.

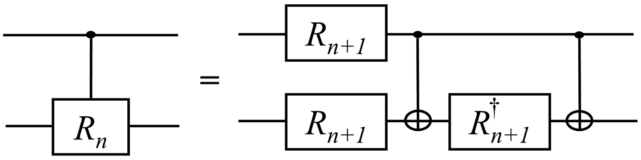

Figure 1. Circuit implementing a controlled-R_n gate with CNOT, R_{n+1} and $R^{\dagger}_{n+1}$ gates[10].

$$||R_n - U|| \le \varepsilon, \tag{2}$$

where the norm is the operator norm.

The gridsynth algorithm[9] gives the result of the efficient approximation of an R_n gate in a probabilistic manner. Thus, we estimate the average number of gates for it. From Table 1, we can assume the average numbers of gates for an approximation of an R_n gate as 127, 253 and 379 with $\varepsilon = 10^{-5}$, 10^{-10}, and 10^{-15}, respectively. Note that the average number of gates is independent of the rotation angle.

Zero ancillary qubit method (Method 1). A controlled-R_n gate is defined as follows:

$$\text{Controlled-}R_n = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^{n-1}} \end{bmatrix}. \tag{3}$$

Figure 1 shows the circuit of the controlled-R_n gate with 2 CNOTs, 2 R_{n+1}s and 1 $R^{\dagger}_{n+1}$ gate. This method is a well-known and fundamental method for the decomposition of a controlled-R_n[10]. When we approximate the controlled-R_n with precision 10^{-10}, the total number of gates is 761 on average from Table 1. Thus, the approximation of one controlled-R_n requires an excessive number of gates.

One ancillary qubit method (Method 2). Figure 2 shows the circuit of the controlled-R_n gate using a single ancillary qubit. The circuit consists of 1 R_n, 16 CNOTs, 4 Hs, 8 Ts and 6 $T^{\dagger}$s.

As noted in ref.[8], one advantage of such a circuit is that it reduces the depth with only a small constant overhead. As mentioned earlier, R_n and R_{n+1} require many gates according to the precision. In the case of the precision 10^{-10}, R_n and R_{n+1} both require approximately 253 gates. Therefore, the approach where a single ancillary qubit is employed appears to be beneficial.

We note that the ref.[11] offers an approach to implementing a controlled-U operation using an ancillary qubit containing an eigenstate of U. However, in this paper, we only focus on an approach using $|0\rangle$ state as an ancillary qubit. Thus, we have considered decomposition of controlled-R_n gate in an approach of the ref.[11]. As future work, we will analyze the decomposition of a controlled-U operation.

Controlled-T decomposition based method (Method 3). The previously known efficient decomposition of a controlled-T is shown in ref.[12]. We can observe that the middle T gate in ref.[12] can be replaced with the R_n. In this case, controlled-R_n gate can be decomposed into 4 Hadamard gates, 2 Phase gates, 12 CNOT gates, 8 T gates, and 1 R_n gate. This result is the best known to date and is the same as in ref.[13]. If we use two ancillary qubits,

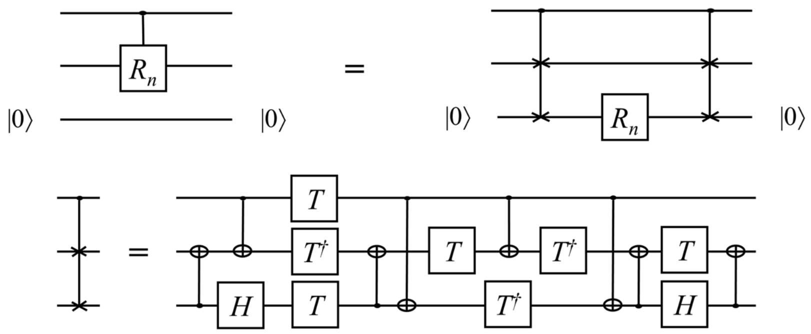

Figure 2. Circuit implementing a controlled-R_n gate with a single ancillary qubit $|0\rangle$[11,12,18]. The ancillary qubit is initialized in and returned to state $|0\rangle$.

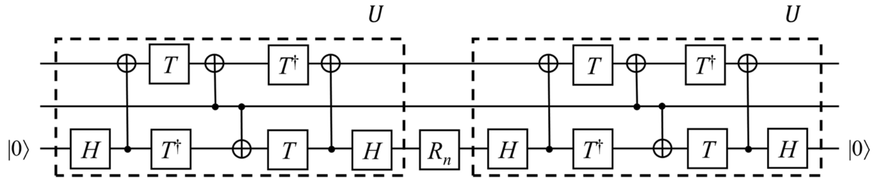

Figure 3. Circuit for the controlled-R_n decomposition for a smaller number of gates.

Controlled-R_n	Controlled-T			
Resource analysis	**Method 1**	**Method 2**	**Method 3**	**Improvement 1**
Number of qubits (K)	2	3	3	3
Total number of gates	790	35	27	21
Critical path (Q)	528	21	19	17
Reduction rate of total number of gates	1	22.57	29.26	37.62
Reduction rate of KQ	1	16.76	18.53	20.71

Table 2. Decomposition of controlled-T gate by four methods. Here, the precision for the approximation is 10^{-10}, and the reduction rate means the reduction rate for Method 1.

T depth of decompsition of controlled-T can be reduced from 5 to 3[13]. However, if we consider only one ancillary qubit, T-depth 5 and T-count 9 are the best results in decomposition of controlled-T gate.

Results

In this work, we improve the previous method to three ends: to reduce the total number of gates, achieve an efficient layout and achieve a smaller depth.

Smaller number of total gates (Improvement 1).

We propose an improvement whereby the controlled-R_n consists of a lower total number of gates keeping one R_n gate.

Theorem 1. *The controlled-R_n gate can be decomposed with at most one ancillary state* $|0\rangle$ into one R_n, eight CNOTs, four Hs, four Ts and four $T^\dagger$s.

The proof is given in Section Proofs. The corresponding decomposition is shown in Fig. 3.

The advantage of the proposed method is shown in Table 2. The data were estimated by the ScaffCC program[14]. In particular, in the case of a controlled-T, using ancillary qubits results in an exact decomposition of the controlled-R_n and not an approximation. Thus, the gap between Method 1 and Improvement 1 is more larger. The Method 3 is more efficient than the Method 2 in decomposition of controlled-T. However, it consist of 12 CNOTs, 4 Hs, 1 P, 1 $P^\dagger$, 5 Ts and 4 $T^\dagger$s. The decomposition includes 27 gates, whereas our decomposition includes only 21 gates. In more detail, T-count is the same for ref.[12] and our method. However, the advantage of our method is reduction by 4 CNOT gates and 2 Phase gates. The reduction of CNOT gates is important since implementation of CNOT gates is physically not easy and controlled-R_n is not the final algorithm[15,16]. Thus, its impact in quantum algorithms will be large. For example, according to module count analysis of ScaffCC Program[14] for Shor's algorithm, the controlled-T gate is used 641,990,656 times in total. This means that reducing 6 gates in decomposition of the controlled-T gate reduces 3,851,943,936 gates in computing of Shor's algorithm.

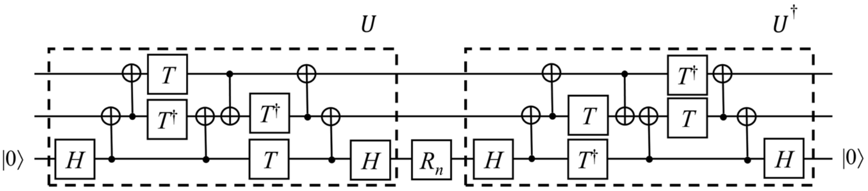

Figure 4. Circuit implementing a controlled-R_n gate for an architecture with only nearest-neighbor interactions.

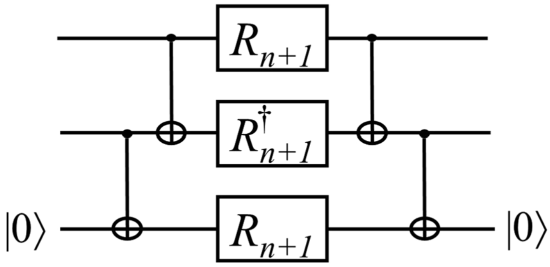

Figure 5. Circuit for the controlled-R_n gate for a smaller depth.

Efficient layout (Improvement 2). For practical quantum computing, we should consider the layout of quantum circuits. Since nonlocal two-qubit-gate operation is not allowed in general, a long-range CNOT gate is implemented with several adjacent SWAP gates. In the following theorem, we present an efficient decomposition of a controlled-R_n gate without using nonlocal CNOT gates.

Theorem 2. *A controlled-R_n gate can be implemented under the nearest-neighbor-interaction-only architecture with at most one ancillary state* $|0\rangle$ using one R_n, twelve adjacent CNOTs, four Hs, four Ts and four $T^{\dagger}$s.

The proof is given in Section Proofs. The corresponding circuit is shown in Fig. 4. Let us consider one long-range CNOT gate, where the control qubit is the first qubit and the target qubit is the third qubit. Naively, we can decompose such a CNOT gate into one adjacent CNOT gate and two swap gates. The swap gates can be decomposed into three CNOT gates. Thus, the long-range CNOT can be implemented with 7 CNOT gates. More efficiently, the long-range CNOT can be implemented with only 4 CNOT gates[17]. Thus, Method 2 consists of 1 R_n, 28 adjacent CNOTs, 4 Hs, 8 Ts and 6 $T^{\dagger}$s, while Improvement 2 consists of 1 R_n, 12 adjacent CNOTs, 4 Hs, 4 Ts and 4 $T^{\dagger}$. Therefore, using our method, we use 16 fewer CNOT gates, 4 fewer T gates and 2 fewer $T^{\dagger}$ gates.

Smaller depth (Improvement 3). The depth of a circuit means the length of the critical path of the circuit. To ensure an efficient run time of a practical quantum computer, the depth of a circuit should be minimized. For this purpose, we propose a circuit with a smaller depth for a controlled-R_n.

Theorem 3. *While maintaining the R_n-type gate depth 1, the controlled-R_n* can be implemented with at most one ancillary state $|0\rangle$ with a depth of 5 gates in $\{adjacent\ CNOT,\ R_{n+1},\ R^{\dagger}_{n+1}\}$.

The proof is given in Section Proofs. The corresponding circuit is shown in Fig. 5. Method 2 for the controlled-R_n has a depth of 25, while this circuit only has a depth of 5. Although Method 1 only has a depth of 4, the depth after the approximation of the R_n-type gates is nearly twice that of Improvement 3.

We note that from Fig. 8.(a) in ref.[12], controlled-S gate can be decomposed in a depth of 5. However, in the decomposition, two long-range CNOTs is used. Thus, in order to represent controlled-S gate only with adjacent CNOTs and R_n-type gates, the long-range CNOTs should be transformed into several adjacent CNOTs or layout of qubits should be changed. That is, more resources than in the method of in Fig. 5 are required. According to module count analysis of ScaffCC Program[14] for Shor algorithm, the controlled-S gate is used 641,013,760 times in total. This means that reducing one depth in decomposition of the controlled-S gate affects 641,013,760 computing in Shor's algorithm.

Efficient decomposition of the quantum Fourier transform

The quantum Fourier transform (QFT) is the key ingredient for quantum factoring and many other quantum algorithms[2]. The total number of gates of the QFT for n qubits (denoted $QFT(n)$) is obtained as

$$QFT(n) = \frac{n(n+1)}{2} + 3\left\lfloor \frac{n}{2} \right\rfloor. \tag{4}$$

n-qubit QFT	$n=3$			
Precision	**Method 1**	**Method 2**	**Method 3**	**Improvement 1**
10^{-5} ($c=127$)	399	51	43	37
10^{-10} ($c=253$)	777	51	43	37
10^{-15} ($c=379$)	1155	51	43	37

Table 3. Total numbers of gates induced in the approximation for the 3-qubit QFT with precision 10^{-5}, 10^{-10} and 10^{-15}. Note that c denotes the expected number of gates obtained in the approximation of the R_n gate.

Now, we compare the total number of gates for the QFT by applying each decomposition method. $QFT_{\mathrm{M1}}(n)$, $QFT_{\mathrm{M2}}(n)$, $QFT_{\mathrm{M3}}(n)$ and $QFT_{\mathrm{I1}}(n)$ denote the total number of gates by Method 1, Method 2, Method 3 and Improvement 1, respectively, as follows:

$$QFT_{\mathrm{M1}}(n) = 6n - 5 + \frac{(n-1)(n-2)(2+3c)}{2} + 3\left\lfloor \frac{n}{2} \right\rfloor \tag{5}$$

$$QFT_{\mathrm{M2}}(n) = 41n - 75 + \frac{(n-2)(n-3)(34+c)}{2} + 3\left\lfloor \frac{n}{2} \right\rfloor, \tag{6}$$

$$QFT_{\mathrm{M3}}(n) = 33n - 59 + \frac{(n-2)(n-3)(26+c)}{2} + 3\left\lfloor \frac{n}{2} \right\rfloor, \tag{7}$$

$$QFT_{\mathrm{I1}}(n) = 27n - 47 + \frac{(n-2)(n-3)(20+c)}{2} + 3\left\lfloor \frac{n}{2} \right\rfloor, \tag{8}$$

where c means average number of gates over 10,000 runs for an approximation of R_n with angle $\pi/2^{n-1}$ corresponding to the precision of Table 1. For example, if a precision $\varepsilon = 10^{-10}$ then $c = 253$. Thus, the benefit of Improvement 1 for Method 3 is obtained as

$$QFT_{\mathrm{M3}}(n) - QFT_{\mathrm{I1}}(n) = 6n - 12 + 3(n-2)(n-3) = 3(n-1)(n-2) \tag{9}$$

for n. In this paper, we only consider the error rate in approximation of R_n gate not the overall error rate in approximation of QFT. However, we can notice that Method 3 and Improvement 1 have the same number of R_n gate, and Improvement 1 has smaller number of gates than Method 3. Thus, the overall error rate in approximation of QFT for Improvement 1 might be not greater than that for Method 3. From Table 3 and the above Equations (5–8), it is shown that Improvement 1 is more efficient than Method 1, Method 2 and Method 3.

Discussion

We have investigated the decomposition problem for the controlled-R_n gate since it is an important two-qubit gate. One method has been proposed that utilized a single ancillary qubit to reduce the number of gates. In this work, we have extended this method for three purposes: to reduce the number of gates, to find a good mapping for an architecture with only nearest-neighbor interactions, and to minimize the critical path. Specifically, we have realized that the proposed method reduces the number of gates for the quantum Fourier transform.

As future work, we will consider three issues. First, we need to check whether the proposed methods are optimal. In addition, it would be interesting to investigate how much performance gain is possible for quantum algorithms such as Shor's factoring algorithm since it heavily uses the quantum Fourier transform. For more general situations, we need to develop a decomposition method for controlled multi-qubit unitary transforms.

Proofs

Proof of Theorem 1.

Proof. Let $|\psi\rangle$ be an arbitrary two-qubit state. Then, $|\psi\rangle$ can be represented as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \tag{10}$$

where α_i are complex numbers and $\sum_{i=00}^{11}|\alpha_i|^2 = 1$. Thus,

$$\text{Controlled-}R_n|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + e^{i\pi/2^{n-1}}\alpha_{11}|11\rangle. \tag{11}$$

Let an unitary operator U be an operator denoted by

$$U = (I \otimes I \otimes H)C_{31}(T^{\dagger} \otimes I \otimes T)C_{23}C_{21}(T \otimes I \otimes T^{\dagger})C_{31}(I \otimes I \otimes H), \tag{12}$$

where C_{ij} denotes a CNOT gate with control qubit i and target qubit j. Then,

$$\begin{aligned} U = {} & |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| - |011\rangle\langle 011| \\ & + |100\rangle\langle 100| + |101\rangle\langle 101| + i|110\rangle\langle 111| - i|111\rangle\langle 110|. \end{aligned} \tag{13}$$

Thus,

$$\begin{aligned} & U(I \otimes I \otimes R_n)U(|\psi\rangle \otimes |0\rangle) \\ & = U(I \otimes I \otimes R_n)U(\alpha_{00}|000\rangle + \alpha_{01}|010\rangle + \alpha_{10}|100\rangle + \alpha_{11}|110\rangle) \\ & = U(I \otimes I \otimes R_n)(\alpha_{00}|000\rangle + \alpha_{01}|010\rangle + \alpha_{10}|100\rangle - i\alpha_{11}|111\rangle) \\ & = U(\alpha_{00}|000\rangle + \alpha_{01}|010\rangle + \alpha_{10}|100\rangle - ie^{i\pi/2^{n-1}}\alpha_{11}|111\rangle) \\ & = \alpha_{00}|000\rangle + \alpha_{01}|010\rangle + \alpha_{10}|100\rangle + e^{i\pi/2^{n-1}}\alpha_{11}|110\rangle \\ & = (\text{Controlled-}R_n \otimes I)(|\psi\rangle \otimes |0\rangle). \end{aligned} \tag{14}$$

Proof of Theorem 2.

Proof. Let $|\psi\rangle$ be an arbitrary two-qubit state. Then, $|\psi\rangle$ can be represented as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \tag{15}$$

where α_i are complex numbers and $\sum_{i=00}^{11}|\alpha_i|^2 = 1$. Let an unitary operator U be the operator denoted by

$$U = (I \otimes I \otimes H)C_{32}C_{21}(I \otimes T^\dagger \otimes T)C_{12}C_{32}(T \otimes T^\dagger \otimes I)C_{21}C_{32}(I \otimes I \otimes H), \tag{16}$$

where C_{ij} denotes a CNOT gate with control qubit i and target qubit j. Then,

$$\begin{aligned} U = {} & |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 100| + |011\rangle\langle 101| \\ & + |100\rangle\langle 010| + |101\rangle\langle 011| - i|110\rangle\langle 111| - i|111\rangle\langle 110|. \end{aligned} \tag{17}$$

Thus,

$$\begin{aligned} & U^\dagger(I \otimes I \otimes R_n)U(|\psi\rangle \otimes |0\rangle) \\ & = U^\dagger(I \otimes I \otimes R_n)U(\alpha_{00}|000\rangle + \alpha_{01}|010\rangle + \alpha_{10}|100\rangle + \alpha_{11}|110\rangle) \\ & = U^\dagger(I \otimes I \otimes R_n)(\alpha_{00}|000\rangle + \alpha_{01}|100\rangle + \alpha_{10}|010\rangle - i\alpha_{11}|111\rangle) \\ & = U^\dagger(\alpha_{00}|000\rangle + \alpha_{01}|100\rangle + \alpha_{10}|010\rangle - ie^{i\pi/2^{n-1}}\alpha_{11}|111\rangle) \\ & = \alpha_{00}|000\rangle + \alpha_{01}|010\rangle + \alpha_{10}|100\rangle + e^{i\pi/2^{n-1}}\alpha_{11}|110\rangle \\ & = (\text{Controlled-}R_n \otimes I)(|\psi\rangle \otimes |0\rangle). \end{aligned} \tag{18}$$

Proof of Theorem 3.

Proof. Let $|\psi\rangle$ be an arbitrary two-qubit state. Then, $|\psi\rangle$ can be represented as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \tag{19}$$

where α_i are complex numbers and $\sum_{i=00}^{11}|\alpha_i|^2 = 1$. Then,

$$\begin{aligned} & C_{12}C_{23}(|\psi\rangle \otimes |0\rangle) \\ & = C_{12}C_{23}(\alpha_{00}|000\rangle + \alpha_{01}|010\rangle + \alpha_{10}|100\rangle + \alpha_{11}|110\rangle) \\ & = \alpha_{00}|000\rangle + \alpha_{01}|011\rangle + \alpha_{10}|110\rangle + \alpha_{11}|101\rangle, \end{aligned} \tag{20}$$

where C_{ij} denotes a CNOT gate with control qubit i and target qubit j.

$$\begin{aligned} & (R_{n+1} \otimes R_{n+1}^\dagger \otimes R_{n+1})C_{12}C_{23}(|\psi\rangle \otimes |0\rangle) \\ & = \alpha_{00}|000\rangle + \alpha_{01}|011\rangle + \alpha_{10}|110\rangle + e^{i\pi/2^{n-1}}\alpha_{11}|101\rangle. \end{aligned} \tag{21}$$

Thus,

$$\begin{aligned} & C_{23}C_{12}(R_{n+1} \otimes R_{n+1}^\dagger \otimes R_{n+1})C_{12}C_{23}(|\psi\rangle \otimes |0\rangle) \\ & = \alpha_{00}|000\rangle + \alpha_{01}|010\rangle + \alpha_{10}|100\rangle + e^{i\pi/2^{n-1}}\alpha_{11}|110\rangle \\ & = (\text{Controlled-}R_n \otimes I)(|\psi\rangle \otimes |0\rangle). \end{aligned} \tag{22}$$

References

1. Preskill, J. *Quantum Computing in the NISQ era and beyond*, arXiv:1801.00862, 2018.
2. Nielsen, M. and Chuang, I. *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
3. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).
4. Kliuchnikov, V., Maslov, D. & Mosca, M. Practical Approximation of Single-Qubit Unitaries by Single-Qubit Quantum Clifford and T Circuits. *IEEE Transactions on Computers* **65**, 161–172 (2016).
5. Kitaev, A. Y., Shen, A. H., and Vyalyi, M. N. *Classical and Quantum Computation*, ser. Graduate studies in mathematics, v. 47, Boston, MA, USA: American Mathematical Society, 2002.
6. Bocharov, A., Roetteler, M. & Svore, K. M. Efficient synthesis of probabilistic quantum circuits with fallback. *Physical Review A* **91**, 052317 (2015).
7. Bocharov, A., Roetteler, M. & Svore, K. M. Efficient synthesis of universal repeat-until-success quantum circuits. *Phys. Rev. Lett.* **114**, 080502 (2015).
8. Kliuchnikov, V., Maslov, D. & Mosca, M. Fast and efficient exact synthesis of single-qubit unitaries generated by clifford and T gates. *Quantum Information and Computation* **13**, 0607–0630 (2013).
9. Ross, N. J. & Selinger, P. Optimal ancilla-free clifford +T approximation of Z-rotations. *Quantum Information and Computation* **16**, 0901–0953 (2016).
10. Barenco, A. *et al*. Elementary gates for quantum computation. *Physical Review A* **52**, 3457 (1995).
11. Kitaev, A. Quantum measurements and the Abelian Stabilizer Problem. quantph/9511026 (1995).
12. Amy, M., Maslov, D., Mosca, M. & Roetteler, M. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* **32**, 818–830 (2013).
13. Selinger, P. Quantum circuits of T-depth one. *Physical Review A* **87**, 042302 (2013).
14. JavadiAbhari, A. *et al*. ScaffCC: A Framework for Compilation and Analysis of Quantum Computing Programs. ACM International Conference on Computing Frontiers (CF 2014), Cagliari, Italy, May 2014; https://github.com/epiqc/ScaffCC.
15. Shende, V., Bullock, S. & Markov, I. Synthesis of Quantum Logic Circuits. *IEEE Transactions on Computer-Aided Design* **25**, 1000 (2006).
16. Sedlák, M. & Plesch, M. Towards optimization of quantum circuits. *Central European Journal of Physics* **6**, 128 (2008).
17. Viamontes, G. F., Markov, I. L., and Hayes, J. P. *Quantum Circuit Simulation*, Springer, 2009.
18. Kliuchnikov, V. New methods for Quantum Compiling. *UWSpace*, http://hdl.handle.net/10012/8394 (2014).

Acknowledgements

We thank Ali JavadiAbhari for his support in the use of the ScaffCC software. This work was supported by a Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean government [17ZH1200, Research and Development of Quantum Computing Platform and its Cost-Effectiveness Improvement].

Author Contributions

T. Kim wrote the manuscript, and B.-S. Choi revised the manuscript. All authors reviewed the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.