

Linear-depth quantum circuits for n -qubit Toffoli gates with no ancilla

Mehdi Saeedi* and Massoud Pedram

Department of Electrical Engineering, University of Southern California, Los Angeles, California 90089-2562, USA

(Received 8 March 2013; published 17 June 2013)

We design a circuit structure with linear depth to implement an n -qubit Toffoli gate. The proposed construction uses a quadratic-size circuit that consists of elementary two-qubit controlled-rotation gates around the x axis and uses no ancilla qubit. Circuit depth remains linear in quantum technologies with finite-distance interactions between qubits. The suggested construction is related to the long-standing construction by A. Barenco *et al.* [*Phys. Rev. A* **52**, 3457 (1995)], which uses a quadratic-size, quadratic-depth quantum circuit for an n -qubit Toffoli gate.

DOI: 10.1103/PhysRevA.87.062318

PACS number(s): 03.67.Lx, 07.05.Bx, 89.20.Ff

I. INTRODUCTION

Practical implementation of multiqubit quantum gates in quest of a scalable quantum computing system is essential. In particular, an n -qubit Toffoli gate plays a key role in established quantum algorithms. Examples include compiled circuits for modular multiplication and exponentiation in Shor's number-factoring algorithm [1–3] and quantum error-correction codes [4]. For $n = 3$, the entangling Toffoli gate, which flips the “target” state conditioned on its two “controls,” is universal in reversible Boolean logic (see [5]). Additionally, with an appropriate single-qubit gate, the three-qubit Toffoli gate constructs a universal gate set for quantum computing [6]. In recent years, several protocols have been proposed to realize the three-qubit Toffoli gate and its variants in different physical quantum technologies, e.g., with superconducting qubits [7,8], trapped ions [9,10], optical elements [11,12], and cavity quantum electrodynamics [13].

A common approach to implement a highly conditional gate is to apply *decomposition*, which breaks down the gate into “elementary” gates with at most one control [14–16]. For an n -qubit Toffoli gate, this path results in quadratic-size, quadratic-depth quantum circuits with no ancilla [17], Corollary 7.6]. For the three-qubit Toffoli gate, the simplest known decomposition requires five two-qubit gates [17], Lemma 6.1], or exactly six controlled NOT (CNOT) [18] and several one-qubit gates. To avoid applying a long, at least quadratic-length sequence of single- and two-qubit gates, several methods have been proposed to directly realize multiqubit gates with trapped ions [19,20], neutral atoms [21], or superconducting qubits [22].

To streamline the realization of Toffoli gates conditioned on many qubits, which can speed up the progress towards scalable quantum computation, both theoretical and experimental attempts are extremely important. In this paper, we propose a theoretical approach to decompose n -qubit Toffoli gates into two-qubit gates of quadratic size but linear depth without using additional ancilla qubits. For this purpose, we change the usual computational basis states $|0\rangle$ and $|1\rangle$ and propose a construction which exploits quantum rotation gates conditioned on one qubit. The proposed construction is related to the synthesis framework we suggested in [23]. In this paper, we focus on quantum algorithms implemented

without quantum error correction, which is useful for near-term physical experiments.

The rest of this paper is organized as follows. The proposed circuit structure is introduced in Sec. II. Circuit depth is analyzed in Sec. III for quantum computing systems with arbitrary-length and finite-length interaction distances between qubits. We compare the proposed structure with prior constructions in Sec. IV. Section V concludes the paper with further discussion.

II. CIRCUIT STRUCTURE

The choice of basis states in quantum computing is not unique, and any two orthogonal unit vectors can be used in a two-particle quantum computing system to serve as the computational basis states. Working with rotation gates $R_x(\pi)$ around the x axis, we keep $\hat{O} = |0\rangle$ but change the other vector to $\hat{I} = R_x(\pi)|0\rangle = |0 - i\rangle^T$. Accordingly, $R_x(\pi)$ works as a NOT gate which transforms \hat{O} to \hat{I} and vice versa. Adding one and two conditions for $R_x(\pi)$ leads to analogous versions of the conventional two-qubit CNOT and three-qubit Toffoli gates. Accordingly, an n -qubit Toffoli gate is a π -rotation gate around the x axis with $n - 1$ conditionals. In circuit diagrams throughout the paper, k consecutive gates with the same control lines are shown as a single gate with one control and k targets.

Figure 1 shows a possible decomposition for a three-qubit Toffoli gate. In Fig. 1, if at least one of the first two qubits is \hat{O} , then the circuit applies either an identity I gate or $R_x(\frac{\pi}{2} - \frac{\pi}{2}) = I$ gate to the target qubit. Otherwise, $R_x(\frac{\pi}{2} + \frac{\pi}{2})$ is applied, which is a NOT gate.

Theorem 1. An n -qubit Toffoli gate with controls a_1, a_2, \dots, a_{n-1} and target a_n can be implemented by a network of the form given in Fig. 2 where all gates are conditional θ -rotation gates around the x axis.

Proof. To prove this theorem, we restructure the circuit shown in Fig. 2 as illustrated in Fig. 3. To verify, note that gates in the first (top) $n - 1$ lines construct an $(n - 1)$ -qubit Toffoli gate, gates in the first $n - 2$ lines construct an $(n - 2)$ -qubit Toffoli gate, \dots , gates in the first three qubits construct a three-qubit Toffoli, and, finally, the gate in the first two qubits is a CNOT. We ignore conditional rotation gates with $\theta = -\pi$ in Fig. 3 as these gates are applied to restore values of control qubits.

*Corresponding author: msaeedi@usc.edu

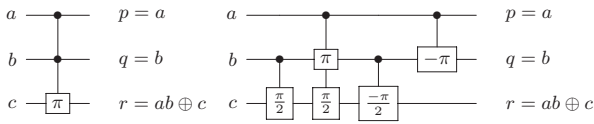


FIG. 1. The three-qubit Toffoli gate and its decomposition into two-qubit controlled-rotation gates. Two consecutive gates with controls on a are shown as a single gate with one control and two targets on b and c .

Consider the subcircuit Δ shown in Fig. 3. Focusing on Δ , assume Δ input qubits are a_i and Δ output qubits are b_i for $1 \leq i \leq n - 1$. Assume that a_k is the first qubit (starting from $k = 1$) with value $\hat{0}$. After applying Δ , we have $b_1 = a_1, b_i = 0$ for $2 \leq i \leq k - 1, b_k = 1$, and $b_i = a_i$ for $k + 1 \leq i \leq n$.

Now, consider the complete circuit in Fig. 3. The case $a_1 = \hat{0}$ is trivial because gates in Δ are disabled, the gate with control qubit a_1 and target qubit a_n is deactivated, and other applied gates cancel out the effects of each other. Therefore, we assume $a_1 = \hat{1}$. Note that before applying Δ , each controlled-rotation gate with control qubit a_i for $2 \leq i \leq n - 1$ applies $\pi/2^{n-i}$ to qubit a_n . Similarly, after applying Δ , each controlled-rotation gate with control qubit a_i for $2 \leq i \leq n - 1$ applies $-\pi/2^{n-i}$ to qubit a_n .

If a_k (starting from $k = 1$) is the first qubit with value $\hat{0}$, then conditional rotation gates with controls a_1, a_2, \dots, a_{k-1} are activated, and a θ_1 -rotation gate with $\theta_1 = \frac{\pi}{2^{n-2}} + \frac{\pi}{2^{n-2}} + \frac{\pi}{2^{n-3}} + \dots + \frac{\pi}{2^{n-k+1}}$ is applied to the target qubit. However, after applying Δ a θ_2 -rotation gate with $\theta_2 = \frac{-\pi}{2^{n-k}}$ is applied, which removes the effect of θ_1 given $\theta_1 = -\theta_2$. Additionally, each gate with control qubit a_i for $k + 1 \leq i < n - 1$ after Δ removes the effect of the corresponding gate before Δ .

Finally, if $a_i = \hat{1}$ for all $1 \leq i \leq n - 1$, then all gates before Δ are enabled and all gates after Δ are disabled, and a θ -rotation gate with $\theta = \frac{\pi}{2^{n-2}} + \frac{\pi}{2^{n-2}} + \frac{\pi}{2^{n-3}} + \dots + \frac{\pi}{2^2} + \frac{\pi}{2} = \pi$ is applied to the target qubit a_n . ■

Figures 4 and 5(a) show the proposed construction for four-qubit and five-qubit Toffoli gates. In Fig. 5(b), the construction used in the proof of Theorem 1 is illustrated for a five-qubit Toffoli gate. To count the number of two-qubit gates in the proposed construction, note that there are $2\sum_{i=1}^{n-2} i + n - 1$ gates to construct the transformation on the target line, and

$2\sum_{i=1}^{n-3} i + n - 2$ gates to restore control lines to their original values. Therefore, the total number of two-qubit gates in the proposed construction is $2n^2 - 6n + 5$ or $2n^2 + O(n)$.

III. DEPTH ANALYSIS

In this section, we show that in spite of the quadratic size of the proposed structure for an n -qubit Toffoli gate (no ancilla), the circuit depth is linear. In order to consider depth, we restructure the construction shown in Fig. 2. In particular, we change the structure to have gates with common targets (vs common controls in Fig. 2) in sequence. Additionally, we divide the circuit in Fig. 2 into six parts, namely, C_1, C_2, \dots, C_6 , as shown in Fig. 2. To evaluate circuit depth, we focus on C_1 . The result can be extended to the whole circuit. Figure 6 illustrates C_1 in Fig. 5(a) with time steps for each gate.

Theorem 2. The proposed structure for an n -qubit Toffoli gate can be implemented by a linear-depth circuit.

Proof. Restructuring the circuit structure in Fig. 2 to have gates with common targets in sequence, one can verify that in $C_1 + C_2$ there are $n - 1$ gates with targets on qubit $n, n - 2$ gates with targets on qubit $n - 1, \dots$, one gate with targets on qubit 2. Assign time steps $1, 2, \dots, n - 1$ to $n - 1$ gates with targets on qubit n . Next, consider the $n - 2$ gates with targets on qubit $n - 1$. Among these gates, $n - 3$ gates can be executed in parallel with the gates with targets on qubit n . Precisely, gates with targets on qubit $n - 2$ can be executed in time steps $3, 4, \dots, n - 1, n$. Similarly, the next $n - 4$ gates can be executed in time steps $5, 6, \dots, n + 1$. Following this path results in $2n - 3$ time steps for $C_1 + C_2$. Likewise, C_3 can be parallelized to depth $2n - 5$, $C_4 + C_5$ can be parallelized to depth $2n - 5$, and, finally, C_6 can be parallelized to depth $2n - 7$. Altogether, the circuit depth for an n -qubit Toffoli gate in the proposed construction is $8n - 20$. ■

While circuit depth in the proposed construction is linear, our construction includes many long-distance two-qubit gates. In general, restricting interactions to only linear dimension (one dimension) results in $O(n)$ overhead. However, circuit depth in the proposed construction remains linear even in very restrictive quantum architectures with possible interactions in a line. Assume a SWAP gate between qubits a_1 and a_2 is

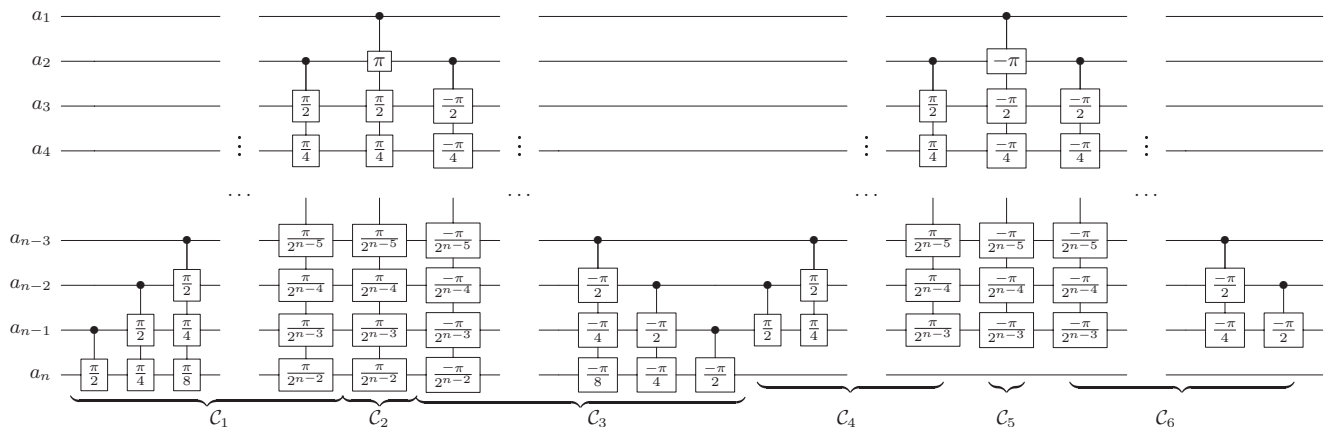


FIG. 2. Circuit structure for an n -qubit Toffoli gate. The proposed construction is divided into six parts, C_1, C_2, \dots, C_6 .

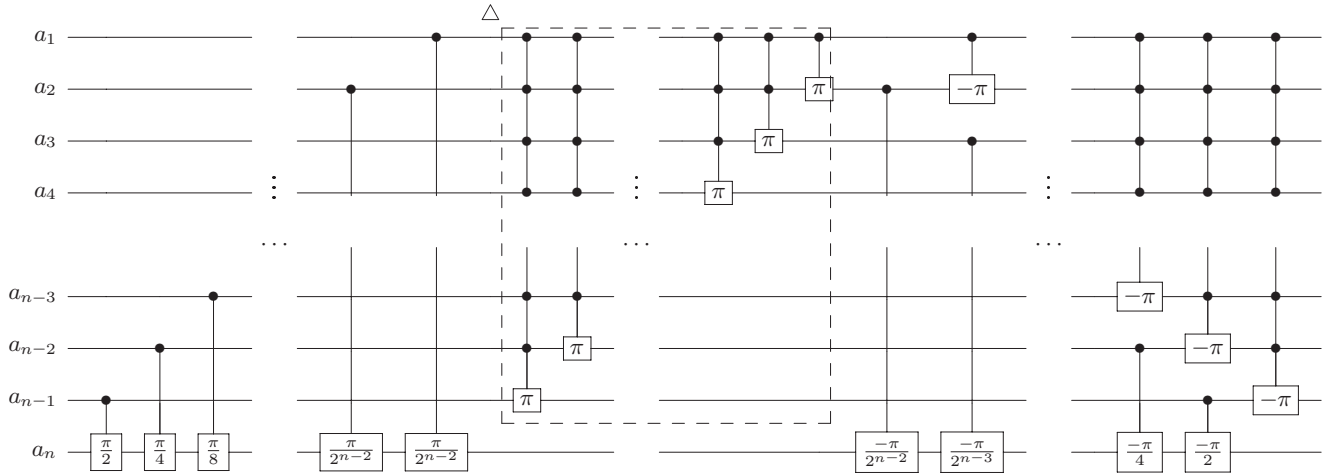


FIG. 3. The circuit in Fig. 2 is restructured to use 2-, 3-, ..., $(n - 1)$ -qubit Toffoli gates to construct an n -qubit Toffoli gate.

represented by $S(a_1, a_2)$. We use the term “local” for gates that use neighbor qubits in a given architecture.

Theorem 3. Circuit depth for an n -qubit Toffoli in the proposed construction is linear in architectures with finite-distance interactions between qubits.

Proof. To prove this theorem, we consider one-dimensional (1D) architectures. One can execute a 1D quantum circuit on architectures with interactions in a higher dimension. Working with $C_1 + C_2$, consider a chain of $n - 1$ serial SWAP gates $S(a_n, a_{n-1}), S(a_{n-1}, a_{n-2}), S(a_{n-2}, a_{n-3}), \dots, S(a_2, a_1)$ in sequence. For an initial qubit ordering $1, 2, \dots, n$, the resulting ordering is $n, 1, 2, \dots, n - 1$ (i.e., a one-bit rotation). Immediately after each SWAP gate, one can apply a local controlled-rotation gate with the target on qubit n . Now, apply a chain of $n - 2$ SWAP gates $S(a_n, a_{n-1}), S(a_{n-1}, a_{n-2}), S(a_{n-2}, a_{n-3}), \dots, S(a_3, a_2)$ in sequence. Among these $n - 2$ gates, $n - 3$ gates can be executed in parallel with the previous gates. After the second SWAP chain, the resulting qubit ordering is $n, n - 1, 1, 2, \dots, n - 2$, i.e., a two-bit rotation. Accordingly, we can apply $n - 2$ local controlled-rotation gates with targets on $n - 1$. Following this path results in $2n - 3$ time steps for SWAP gates, and $2n - 3$ time steps for controlled-rotation gates, $4n - 6$ two-qubit time steps in total. Circuit size is increased by $2n - 3$ for SWAP gates. The final qubit ordering is $n, n - 1, n - 2, \dots, 2, 1$.

To construct a local circuit for C_3 starting from qubit ordering $n, n - 1, n - 2, \dots, 2, 1$, we can apply the same structure discussed. It leads to depth $4n - 10$ for C_3 . The resulting qubit ordering is $2, 3, \dots, n - 1, n, 1$. At this time, applying the next $C_4 + C_5$ circuit is tricky because qubit ordering has been changed from the initial one $1, 2, \dots, n - 1, n$. Actually,

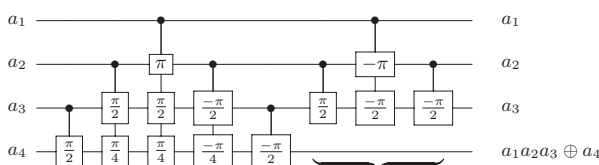


FIG. 4. Circuit structure for a four-qubit Toffoli gate. The last three gates are applied to restore values of the control lines.

the first qubit is far from other qubits $2, 3, \dots$. For this case, we apply a linear-depth circuit with depth $n + 5$ and size $4n - 6$ [24], Theorem 4.1] to restore the ordering $1, 2, \dots, n - 1, n$. Accordingly, $C_4 + C_5$ and C_6 can be implemented in depths $4n - 10$ and $4n - 14$, respectively. We recover the final qubit ordering to the initial ordering $1, 2, \dots, n - 1, n$ with another linear-depth circuit.

Altogether, circuit depth for an n -qubit Toffoli gate with only 1D interactions can be calculated as $18n - 31$. Circuit size remains $2n^2 + O(n)$. ■

In summary, circuit depth in the proposed structure is only increased by a constant factor, e.g., 2.25 in 1D architectures. Figure 7 illustrates the circuit in Fig. 6 with only local gates.

IV. COMPARISON WITH PRIOR WORK

The current widely used decomposition [17], Corollary 7.6] for an n -qubit Toffoli gate uses a quadratic-size construction

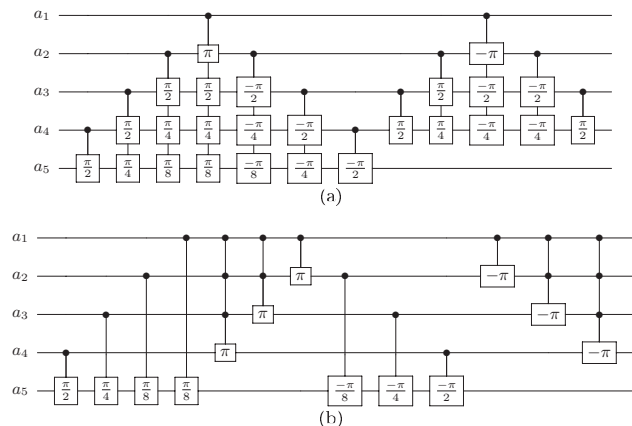


FIG. 5. Circuit structure for a five-qubit Toffoli gate. The circuit in (a) is the proposed structure. This circuit is restructured in (b) based on the circuits in Figs. 1 and 4. Note that direct decomposition of the gates in (b) does not result in the proposed construction in (a); such decomposition results in many redundant gates. In other words, the construction in (a) reuses gates of a k -qubit Toffoli gate to construct a $(k + 1)$ -qubit Toffoli gate.

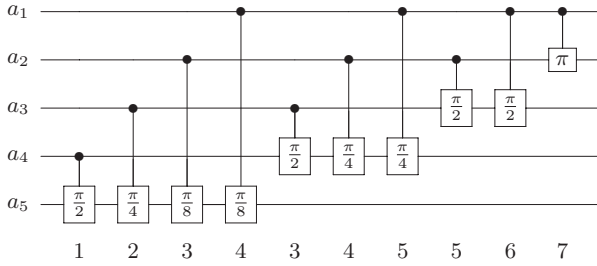


FIG. 6. A part of the circuit shown in Fig. 5(a) restructured to show parallel circuits. Numbers are the time slots that gates can be executed.

with staircase structure where the target of gate i depends on a control of gate $i - 1$. This results in a quadratic depth. The decomposition is illustrated in Fig. 8. In Fig. 8, U is a NOT gate which results in V and V^\dagger , where $V^2 = U$. The resulting multiple-control Toffoli gates have linear cost $48n + O(1)$ in [17] due to the availability of one ancilla qubit. The last gate can be decomposed by recursively applying the decomposition shown in Fig. 8 using $U = \sqrt{\text{NOT}}$. Following this path results in controlled- i -th-root-of-NOT gates for $i = 2^1, 2^2, \dots, 2^{n-1}$. Circuit size and depth are $48n^2 + O(n)$ two-qubit gates.

The optimizations in [25] improve the linear-cost implementation of multiple-control Toffoli gates with one ancilla from $48n + O(1)$ to $24n + O(1)$. The circuit depth remains quadratic, precisely $24n^2 + O(n)$. The method in [23], Sec. 6] benefits from a recursive construction with quadratic-depth $2n^2 + O(n)$. As discussed in Secs. II and III, our circuit size and circuit depth are quadratic and linear, respectively. All methods uses gates with similar complexity levels for physical realization.

In Theorem 1 we assumed no ancilla qubit is available to facilitate circuit construction. If at least one ancilla exists, prior circuit structures in [17], Lemmas 7.2, 7.3] and the extended versions [25] use linear-size circuits. When 1 and $n - 3$ ancillae are available, we can apply the same circuit structures in [17], Lemmas 7.2, 7.3]. Precisely, after applying various optimizations in [25], we can construct circuits with sizes $24n - 88$ and $12n - 34$ if one and $n - 3$ ancillae are available; note that Peres gate has a cost of 4 in the proposed construction, as in [25]. Reusing optimizations in [25] in the proposed circuit structure is straightforward.

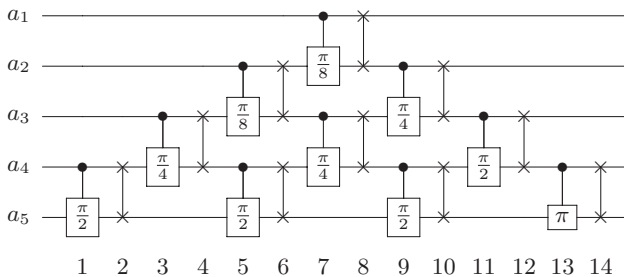


FIG. 7. Circuit in Fig. 6 with only local gates based on the proof of Theorem 3. Numbers are time slots that gates can be executed.

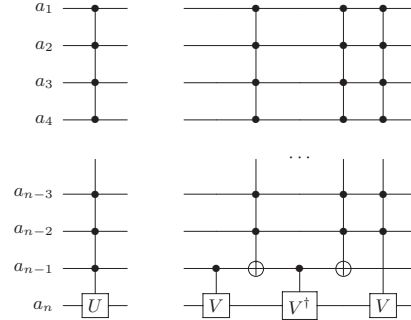


FIG. 8. Circuit structure for an n -qubit Toffoli gate in [17], Lemma 7.5] where $V^2 = U$. At the first step, U is a NOT gate. The resulting multiple-control Toffoli gates have linear cost due to the availability of one ancilla qubit. The last gate can be decomposed by recursively applying the current decomposition.

V. CONCLUSION AND DISCUSSION

We proposed a linear-depth quadratic-size quantum circuit with controlled-rotation gates around the x axis with no ancilla qubit to implement an n -qubit Toffoli gate. Restricting qubit interactions in finite length affects circuit depth and size by a constant factor.

The proposed structure may or may not be a physically realizable construction in a particular quantum computing technology. The physical implementations of quantum gates are imperfect due to various reasons, including decoherence and error in experimental setups. In the proposed circuit structure, we used θ -rotation gates around the x axis for $\theta = \frac{\pi}{2^k}$ and $1 \leq k \leq n - 2$. Obviously, $\frac{\pi}{2^{n-2}}$ can be very small for large n values, which makes its physical implementation complicated. Small rotation angles may be ignored in specific applications, as done for approximate quantum Fourier transform [26]. In particular, restricting $k \leq \lceil \log_2 n \rceil$ results in $\epsilon \approx \frac{\pi}{n}$ error.

For a scalable quantum physical implementation, quantum error correction should be applied. In this case, θ -rotation gates should be decomposed into several fault-tolerant gates [4] where decomposition of rotation gates with small angles is very complicated. The proposed approach is more interesting for near-term physical experiments where small quantum algorithms will be implemented without error correction.

Since conditional Toffoli gates are building blocks for various quantum algorithms, in-depth characterization of their operations and imperfections possibly based on quantum tomography [27] can be very useful. Recently, a multiqubit phase gate with one control qubit simultaneously controlling n target qubits was implemented using superconducting qubits [28]. Since we extensively benefit from such gates in the proposed construction, applying the method in [28] to physically realize conditional Toffoli gates based on the method presented in this paper, e.g., the small circuit in Fig. 4, may be useful.

Finally, while we use $\hat{0}$ and $\hat{1}$ for computational basis states, we can also use $|0\rangle$ and $|1\rangle$. To achieve this, one can transform $|0\rangle, |1\rangle$ to $\hat{0}, \hat{1}$ by applying n single-qubit gates with the same matrix M to all qubits. This should be followed by the proposed construction. The final quantum state can be restored from $\hat{0}, \hat{1}$

to $|0\rangle, |1\rangle$ by applying M^\dagger .

$$M = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad M^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}.$$

Restricting to have only one type of two-qubit gate can increase circuit depth and size by a constant given each two-qubit gate can be implemented by a constant-size circuit [17].

ACKNOWLEDGMENTS

The authors were supported by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center Contract No. D11PC20165. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of IARPA, DoI/NBC, or the US government.

-
- [1] R. Van Meter and K. M. Itoh, *Phys. Rev. A* **71**, 052320 (2005).
 [2] I. L. Markov and M. Saeedi, *Quantum Inf. Comput.* **12**, 361 (2012).
 [3] I. L. Markov and M. Saeedi, *Phys. Rev. A* **87**, 012310 (2013).
 [4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
 [5] M. Saeedi and I. L. Markov, *ACM Comput. Surv.* **45**, 21 (2013).
 [6] Y. Shi, *Quantum Inf. Comput.* **3**, 84 (2003).
 [7] A. Fedorov, L. Steffen, M. Baur, M. P. da Silva, and A. Wallraff, *Nature (London)* **481**, 170 (2012).
 [8] V. M. Stojanović, A. Fedorov, A. Wallraff, and C. Bruder, *Phys. Rev. B* **85**, 054504 (2012).
 [9] T. Monz, K. Kim, W. Hänsel, M. Riebe, A. S. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt, *Phys. Rev. Lett.* **102**, 040501 (2009).
 [10] M. Borrelli, L. Mazzola, M. Paternostro, and S. Maniscalco, *Phys. Rev. A* **84**, 012314 (2011).
 [11] T. C. Ralph, K. J. Resch, and A. Gilchrist, *Phys. Rev. A* **75**, 022313 (2007).
 [12] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White, *Nat. Phys.* **5**, 134 (2008).
 [13] X.-Q. Shao, A.-D. Zhu, S. Zhang, J.-S. Chung, and K.-H. Yeon, *Phys. Rev. A* **75**, 034307 (2007).
 [14] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, *Phys. Rev. Lett.* **92**, 177902 (2004).
 [15] V. V. Shende, S. S. Bullock, and I. L. Markov, *IEEE Trans. Comput. Aided Design* **25**, 1000 (2006).
 [16] M. Saeedi, M. Arabzadeh, M. Saheb Zamani, and M. Sedighi, *Quantum Inf. Comput.* **11**, 0262 (2011).
 [17] 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).
 [18] V. V. Shende and I. L. Markov, *Quantum Inf. Comput.* **9**, 461 (2009).
 [19] X. Wang, A. Sørensen, and K. Mølmer, *Phys. Rev. Lett.* **86**, 3907 (2001).
 [20] S. S. Ivanov and N. V. Vitanov, *Phys. Rev. A* **84**, 022319 (2011).
 [21] L.-M. Duan, B. Wang, and H. J. Kimble, *Phys. Rev. A* **72**, 032333 (2005).
 [22] C.-P. Yang and S. Han, *Phys. Rev. A* **72**, 032311 (2005).
 [23] A. Abdollahi, M. Saeedi, and M. Pedram, *Quantum Inf. Comput.* **13**, 0771 (2013).
 [24] S. Kutin, D. Moulton, and L. Smithline, *Chicago J. Theor. Comput. Sci.* (2007) 1.
 [25] D. Maslov, G. W. Dueck, D. M. Miller, and C. Negrevergne, *IEEE Trans. Comput. Aided Design Integr. Circuits Syst.* **27**, 436 (2008).
 [26] A. Barenco, A. Ekert, K.-A. Suominen, and P. Törmä, *Phys. Rev. A* **54**, 139 (1996).
 [27] M. Riebe, K. Kim, P. Schindler, T. Monz, P. O. Schmidt, T. K. Körber, W. Hänsel, H. Häffner, C. F. Roos, and R. Blatt, *Phys. Rev. Lett.* **97**, 220407 (2006).
 [28] C.-P. Yang, Y.-X. Liu, and F. Nori, *Phys. Rev. A* **81**, 062323 (2010).