

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, CA 90089-2562

This paper presents a quantum circuit design with linear depth to implement an n -qubit Toffoli gate. The proposed design, which uses no ancilla qubit, is a quadratic-size circuit comprising elementary 2-qubit controlled-rotation gates around the x axis. The circuit depth remains linear even in quantum circuit architectures with only adjacent neighbor interactions among the qubits. This design is related to the long-standing construction by Barenco et al. (Phys. Rev. A, 52: 3457-3467, 1995), which uses a quadratic-size, quadratic-depth quantum circuit for an n -qubit Toffoli gate.

PACS numbers: 03.67.Lx, 07.05.Bx, 89.20.Ff

I. INTRODUCTION

Efficient implementation of multi-qubit quantum gates is critical in the quest for building a scalable quantum computing system. In particular, the n -qubit Toffoli gate plays a key role in realizing many of the archetypal quantum algorithms. Example uses of this gate include circuits compiled 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’, by itself forms a universal gate set for reversible Boolean logic, see [5]. Additionally, the 3-qubit Toffoli gate with an additional appropriate single-qubit gate constitute a universal gate set for quantum computing [6]. In the recent years, several protocols have been proposed to realize the 3-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 for implementing a highly conditional gate is to apply *decomposition*, which breakdowns the gate into ‘elementary’ gates with at most one control signal [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 3-qubit Toffoli gate, the simplest known decomposition requires five 2-qubit gates [17, Lemma 6.1], or exactly six CNOTs [18] and several one-qubit gates. To avoid applying a long, at least quadratic-length sequence of single- and 2-qubit gates, several methods have been proposed to directly realize multi-qubit 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 needed. In this paper, we present a theoretical approach to decompose n -qubit Toffoli gates into 2-qubit gates in quadratic size, but lin-

ear depth, without using any ancilla qubits. For this purpose, we change the usual computational basis states $|0\rangle$ and $|1\rangle$ and propose a design that exploits quantum rotation gates conditioned on one qubit. The proposed design is related to the synthesis framework suggested in [23, 24]. In this manuscript, we focus on quantum algorithms implemented without quantum error correction, which is useful for short-term physical experimentation with quantum circuit elements.

The rest of this paper is organized as follows. The proposed circuit structure is introduced in Section II. The resulting circuit depth is analyzed in Section III for quantum computing systems with arbitrary-length and finite-length interaction distance between qubits. We compare the proposed design with prior constructions in Section 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 2-particle quantum computing system to serve as the computational basis states. Working with rotation gates $R_x(\pi)$ around the x axis, we keep $\hat{0} = |0\rangle$, but change the other vector to $\hat{1} = R_x(\pi)|0\rangle = [0 \ -i]^T$. Accordingly, $R_x(\pi)$ works as a NOT gate, which transforms $\hat{0}$ to $\hat{1}$ and vice versa. Adding one and two conditionals for $R_x(\pi)$ constructs analogous versions of the conventional 2-qubit CNOT and 3-qubit Toffoli gates. Accordingly, an n -qubit Toffoli gate is a π -rotation gate around the x axis with $n - 1$ conditionals. Note that, in circuit diagrams shown throughout the paper, k consecutive gates with the same control lines are depicted as a single gate with one control and k targets.

Figure 1 shows a possible decomposition of a 3-qubit Toffoli gate. In this figure, if at least one of the first two qubits is $\hat{0}$, 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

* Corresponding author: msaeedi@usc.edu

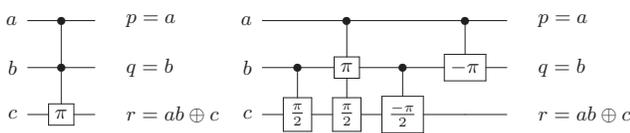


Figure 1. The 3-qubit Toffoli gate and its decomposition into 2-qubit controlled-rotation gates. Two consecutive gates with controls on a are depicted as a single gate with one control and two targets on b and c .

a network of the form given in Figure 2 where all gates are conditional θ -rotation gates around the x axis.

Proof. To prove, we restructure the circuit shown in Figure 2 as illustrated in Figure 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 3 qubit constructs a 3-qubit Toffoli, and finally gate in the first 2 qubits is a CNOT. We ignore conditional rotation gates with $\theta = -\pi$ in Figure 3 since these gates are applied to restore values of control qubits.

Consider the subcircuit Δ shown in Figure 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 Figure 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, whereas other applied gates cancel out 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 its 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 . \square

Figure 4 and Figure 5(a) show the proposed design for 4-qubit and 5-qubit Toffoli gates. In Figure 5(b), the construction used in the proof of Theorem 1 is illustrated for a 5-qubit Toffoli gate. To count the number of 2-qubit gates in the proposed design, 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 2-qubit gates in the proposed design 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 n . To do the depth analysis, we restructure the construction shown in Figure 2. In particular, we change the structure to have gates with common targets (vs. common controls in Figure 2) in sequence. Additionally, we divide the circuit in Figure 2 into 6 parts, namely $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_6$ as shown in the figure. To calculate the circuit depth, we focus on \mathcal{C}_1 . The result can be extended to the whole circuit. Figure 6 illustrates \mathcal{C}_1 in Figure 5(a) with time steps for each gate.

Theorem 2. The proposed design of an n -qubit Toffoli gate can be realized by a linear-depth circuit.

Proof. Restructuring the circuit structure in Figure 2 to have gates with common targets in sequence, one can verify that in $\mathcal{C}_1 + \mathcal{C}_2$ there are $n - 1$ gates with targets on qubit n , $n - 2$ gates with targets on qubit $n - 1$, \dots , one gate with target 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 $5, 6, \dots, n + 1$. This analysis shows that $2n - 3$ time steps are needed for $\mathcal{C}_1 + \mathcal{C}_2$. Likewise, \mathcal{C}_3 can be parallelized to depth $2n - 5$, $\mathcal{C}_4 + \mathcal{C}_5$ can be parallelized to depth $2n - 5$, and \mathcal{C}_6 can be parallelized to depth $2n - 7$. Altogether, circuit depth for an n -qubit Toffoli gate in the proposed design is $8n - 20$. \square

While the circuit depth of the proposed design is linear, our design of n -qubit Toffoli gate includes many long-distance 2-qubit gates. In general, restricting interactions to only nearest neighbor interactions can result in $O(n)$ overhead. Indeed, the circuit depth for the proposed design for an n -qubit Toffoli gate remains linear in n even in quantum circuit architectures nearest neighbor interactions as shown below. Obviously, one can realize the n -qubit Toffoli gate on quantum circuit architectures with other finite-distance interactions (e.g., qubit distance of $k > 1$) at the same or even lower logic depth.

Assume a SWAP gate between qubits a_1 and a_2 is represented by $\mathcal{S}(a_1, a_2)$. We use the term ‘local’ for gates that use *neighboring* qubits in a given architecture.

Theorem 3. Circuit depth for an n -qubit Toffoli gate realized by the proposed design remains linear even in quantum circuit architectures with nearest neighbor interactions among qubits.

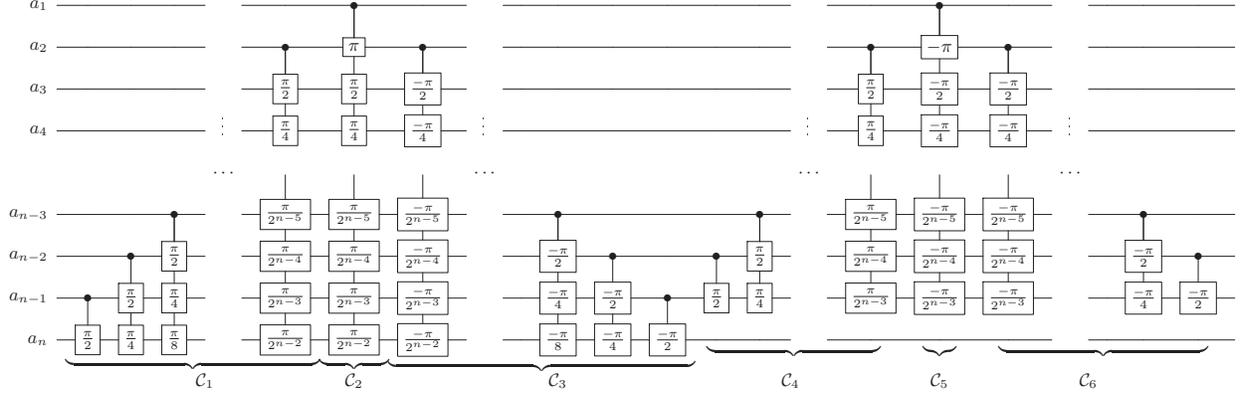


Figure 2. Circuit structure for an n -qubit Toffoli gate. The proposed design is divided into six parts C_1, C_2, \dots, C_6 .

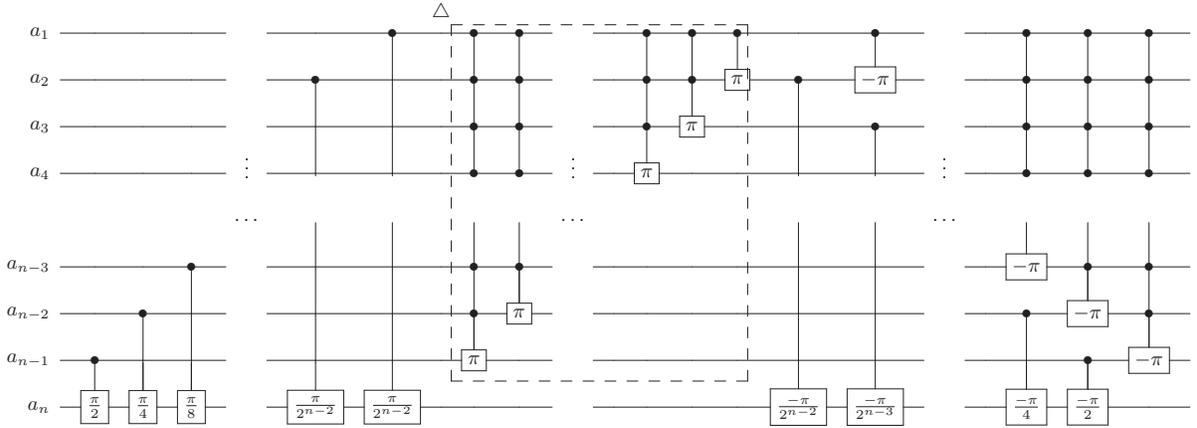


Figure 3. Circuit in Figure 2 is restructured to use 2-, 3-, \dots , $(n-1)$ -qubit Toffoli gates to construct an n -qubit Toffoli gate.

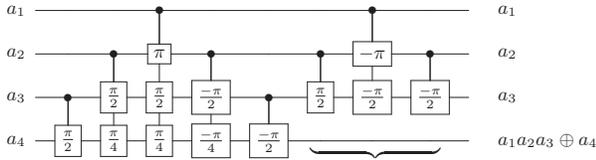


Figure 4. Circuit structure for a 4-qubit Toffoli gate. The last three gates are applied to restore values of control lines.

Proof. We consider quantum circuit architectures with adjacent neighbor interactions only. Working with $C_1 + C_2$, consider a chain of $n-1$ consecutive SWAP gates $\mathcal{S}(a_n, a_{n-1}), \mathcal{S}(a_{n-1}, a_{n-2}), \mathcal{S}(a_{n-2}, a_{n-3}), \dots, \mathcal{S}(a_2, a_1)$ in a sequence. For an initial qubit ordering of $1, 2, \dots, n$, the resulting qubit order will be $n, 1, 2, \dots, n-1$ (similar to the effect of a 1-bit rotation on the ordered sequence of qubits). Immediately after each SWAP gate, one can apply a local controlled-rotation gate with target on qubit n . Now, apply a chain of $n-2$ consecutive SWAP gates $\mathcal{S}(a_n, a_{n-1}), \mathcal{S}(a_{n-1}, a_{n-2}), \mathcal{S}(a_{n-2}, a_{n-3}), \dots, \mathcal{S}(a_3, a_2)$ 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 $n, n-1, 1, 2, \dots, n-2$. Accordingly, we can apply $n-2$ local controlled-rotation gates with targets on $n-1$. Proceeding in this manner, we incur $2n-3$ time steps for SWAP gates, and $2n-3$ time steps for controlled-rotation gates, $4n-6$ 2-qubit time steps in total. The circuit size is increased by $2n-3$ for SWAPs. 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, which 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, the first qubit is far from other qubits $2, 3, \dots$. Thus, we apply a linear-depth circuit with depth $n+5$, and size $4n-6$ [25, 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 depth $4n-10$ 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.

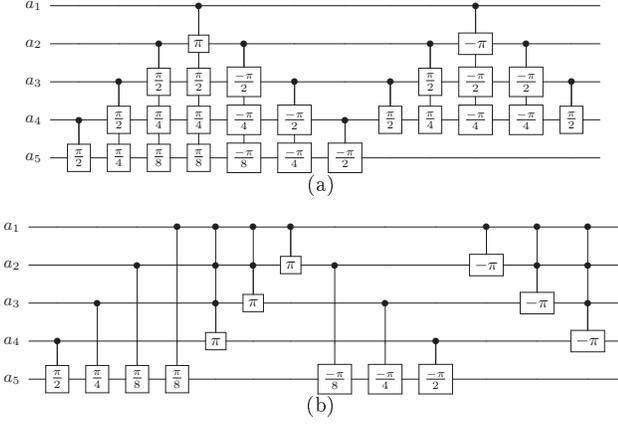


Figure 5. Circuit structure for a 5-qubit Toffoli gate. Circuit in (a) is the proposed structure. This circuit is restructured in (b) based on the circuits in Figure 1 and Figure 4. Note that direct decomposition of the gates in (b) does not result in the proposed construction in (a) — such decomposition 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.

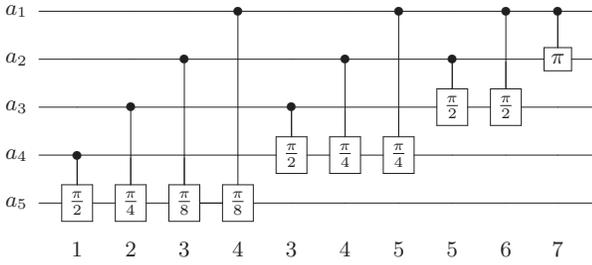


Figure 6. A part of the circuit shown in Figure 5(a) restructured to show parallel sub-circuits. Numbers denote time slots in which gates can be executed.

Altogether, the circuit depth for an n -qubit Toffoli gate with only adjacent qubit interactions is $18n - 31$. Circuit size remains $2n^2 + O(n)$. \square

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

IV. COMPARISON WITH PRIOR ART

The current widely-used decomposition [17, Corollary 7.6] for an n -qubit Toffoli gate uses a quadratic-size construction with a staircase structure where the target of gate i depends on a control of gate $i - 1$. This results in quadratic circuit depth. The decomposition is illustrated in Figure 8. In this figure, U is a NOT gate which results in V and V^\dagger where $V^2 = U$. The resulting multiple-

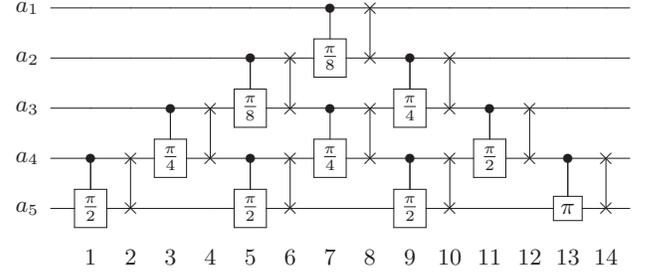


Figure 7. Circuit in Figure 6 with only local gates based on the proof of Theorem 3. Numbers are time slots that gates can be executed.

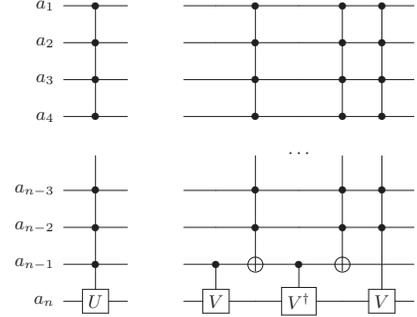


Figure 8. Circuit structure for an n -qubit Toffoli gate in [17, Lemma 7.5] where $V^2 = U$. At the first step, U is a NOT gate. The resulting multiple-control Toffoli gates have linear cost due to the availability of one ancilla qubit. The last gate can be decomposed by recursively applying the current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

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 Figure 8 using $U = \sqrt{\text{NOT}}$. Following this path results in controlled- i th-root-of-NOT gates for $i = 2^1, 2^2, \dots, 2^{n-1}$. The circuit size and depth are $48n^2 + O(n)$ 2-qubit gates.

The optimizations in [26] improve the linear-cost implementation of a 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, 24, Section 6] benefits from a recursive construction with quadratic-depth $2n^2 + O(n)$. As discussed in Section II and Section 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, Lemma 7.2] and [17, Lemma 7.3], and its improved versions [26], use linear-size circuits. When 1 and $n - 3$ ancillae are available, we can apply the same circuit structures in [17, Lemma 7.2] and [17, Lemma 7.3]. Precisely, after applying various

optimizations in [26], we can construct circuits with sizes $24n - 88$, and $12n - 34$ if one and $n - 3$ ancillae are available — note that Peres gate has cost 4 in the proposed construction as in [26]. Applying optimizations in [26] to the proposed circuit structure is straightforward.

V. CONCLUSION AND DISCUSSION

We presented 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 any finite length (including a distance of one only) affects the circuit depth and size by a constant factor.

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 [27]. 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 complex and costly. 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 key building blocks for many quantum algorithms, in-depth characterization of their operations and imperfections possibly based on quantum tomography [28] can be very useful. Recently, a multi-qubit phase gate with one control qubit simultaneously controlling n target qubits was implemented using superconducting qubits [29]. Since we extensively benefit from such gates in the proposed design of the n -qubit Toffoli gate, applying the method in [29] to physically realize conditional Toffoli gates based on the method presented in this paper, e.g. the small circuit in Figure 4, is promising.

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. Final quantum state can be restored from $\hat{0}, \hat{1}$ to $|0\rangle, |1\rangle$ by applying M^\dagger .

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

Restricting to have only one type of 2-qubit gate can increase the circuit depth/size by a constant factor given that each 2-qubit gate can be implemented by a constant-size circuit [17].

-
- [1] R. Van Meter and K. M. Itoh, Phys. Rev. A **71**, 052320 (2005).
- [2] I. L. Markov and M. Saeedi, Quant. Inf. Comput. **12**, 361 (2012), arXiv:1202.6614.
- [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, 2000).
- [5] M. Saeedi and I. L. Markov, ACM Computing Surveys **45** (2013), arXiv:1110.2574.
- [6] Y. Shi, Quant. Info. Comput. **3**, 84 (2003), arXiv:quant-ph/0205115.
- [7] A. Fedorov, L. Steffen, M. Baur, M. P. da Silva, and A. Wallraff, Nature **481**, 170 (2012), arXiv:1108.3966.
- [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, Nature Physics **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. on CAD **25**, 1000 (2006), arXiv:quant-ph/0406176.
- [16] M. Saeedi, M. Arabzadeh, M. Saheb Zamani, and M. Sedighi, Quant. Inf. Comput. **11**, 0262 (2011), arXiv:1011.2159.
- [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, Quant. Inf. Comput. **9**, 461 (2009), arXiv:0803.2316.
- [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 and M. Pedram, *Design, Automation and Test in Europe*, **1**, 317 (2006).
- [24] A. Abdollahi, M. Saeedi, and M. Pedram, Quant. Info. Comput. **13**, 0771 (2013).

- [25] S. Kutin, D. Moulton, and L. Smithline, Chicago J. of Theor. Comput. Sci. arXiv:quant-ph/0701194.
- [26] D. Maslov, G. W. Dueck, D. M. Miller, and C. Negrevergne, IEEE Trans. on CAD of Integrated Circuits and Systems **27**, 436 (2008), arXiv:quant-ph/0604001.
- [27] A. Barenco, A. Ekert, K.-A. Suominen, and P. Törmä, Phys. Rev. A **54**, 139 (1996).
- [28] 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).
- [29] C.-P. Yang, Y.-x. Liu, and F. Nori, Phys. Rev. A **81**, 062323 (2010).

ACKNOWLEDGMENTS

Authors were supported by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center contract number D11PC20165. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. 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 U.S. Government.