Analytic Constructions of General $n$-Qubit Controlled Gates

Yang Liu, Gui Lu Long and Yang Sun

1 Key Laboratory of Atomic and Molecular NanoScience and Department of Physics, Tsinghua University, Beijing 100084, P. R. China
2 Department of Physics and Astronomy, University of Notre Dame, Indiana 46556, USA

(Dated: February 1, 2008)

PACS numbers: 03.67.Lx

I. Introduction—The study of quantum computers has been developing very rapidly over the past years. It provides exponential speedup in factoring [1], or square-root speedup in unsorted database search [2]. In the circuit model of universal quantum computer [3], the unitary operation that completes a computation task is a series of gates on a fixed number of qubits. Any unitary gate can be constructed from a set of universal gates [3, 4].

Using the smallest number of basic gates to construct an arbitrary unitary transformation is very important, not only for using less executing time, but also for resulting less errors.

Complexity of circuit is measured in terms of the number of basic gates, namely the one-bit gate and the two-bit CNOT gate. For a general $2^n \times 2^n$ unitary matrix $U$ with $4^n$ degrees of freedom, $O(4^n n^2)$ elementary operations are needed in principle [5]. Later on, efficient schemes implementing arbitrary quantum gates have reduced the circuit complexity to $O(4^n)$ [6, 7, 8].

$I^n(U)$ gates are typical $n$-qubit fully controlled-$U$ gates that apply a unitary $U$ to the target qubit if and only if all the first $n-1$ control qubits are 1. Circuits for $I^2(U)$, $I^3(U)$ and $I^4(U)$ gates have been constructed [10, 11, 12, 13]. But for the general case with $n \geq 5$, the explicit construction is absent. In this Letter, we present two different construction schemes for an arbitrary $I^n(U)$ gate, one uses an exponential and the other uses polynomial number of CNOT and one-qubit gates. The polynomial complexity scheme is good for large scale quantum computing. The exponential complexity scheme prevails for a circuit with a small qubit number. In particular, they are analytic. These results are very appealing in designing quantum computer programming language, because it not only saves computing time for its construction, but also avoids errors in numerical construction because of error accumulation.

II. Exponential Construction Scheme—First we introduce some notation. For a generic n-qubit circuit, its qubits are numbered from the top from 1 to $n$. $\Lambda^k(V)$ stands for a controlled-V gate with $k$ control qubits and one target qubit, so $C^n(U)$ gate is equally represented by $\Lambda^{n-1}(U)$ whose $(n-1)$ control qubits positioned at the top and the target qubit at the bottom. Order of operations in an expression as well as in circuits are performed from left to right.

Previous investigations gave explicit networks of $C^n(U)$ gates for $n = 2, 3, 4$. In this Letter, we present a general analytic scheme implementing $C^n(U)$ gates for arbitrary values of $n$ and any unitary operator $U$. Firstly, we define two kinds of quantum gate-array blocks, the A-block and the B-block as shown in Fig. 1.

FIG. 1: $A$ and $B$ blocks in repair section. The left part is a $A$-block, the right one is a $B$-block.

The A-block is indicated as $A^m$, where $m = 1, \ldots, n-3$. Its qubit nodes involve qubits $m$, $m+1$, $m+2$ and $n$. The B-block is labeled as $B^j_i$, where $1 \leq i < j < n$. Its qubit nodes involve qubits $i$, $j$ and $n$. First we suppose the explicit gate-array components of $C^{n-1}(U)$ network has been known, then we give a general analytic expression. Our strategy for $C^n(U)$ network is a two-step procedure: basic section constructing in the left part and repair section constructing in the right part of the circuit. Basic section is obtained by combining $C^{n-1}(U)$ network with a control input that is the $(n-1)$-th line without any performance. The basic section of $C^n(U)$ network is indicated as $C_{n-1}^n$. $C_{n-1}^n$ contains $2^{n-2} - 2$ CNOT gates, $(2^{n-2} - 1)$ number of $\Lambda^1(V)$ and $\Lambda^1(V')$ gates,
where $V^{2n-2} = U$. Repair section is yielded by placing $A^n$ and $B^n_j$ gate-array blocks in an alternating sequence with respective number of $2n-4$.

A $\beta$-bit Gray code $[14]$ strings $\{g_n\}$, where $\alpha = 1, \ldots, 2^\beta$ is a palindromically ordering with special property that the adjacent bit strings differ only by a single bit. We define a function $\gamma(\alpha, \beta)$ to represent the numerical value of the position where $g_n$ and $g_{n+1}$ differ. In the repair section of $C^n(U)$, the index $m$ of $A^n$ block is definite as $n - 3$, the index $j$ of $B_j^1$ blocks is definite as $n - 1$, whereas index $i$ varies complying with a $(n-4)$-bit binary Gray code strings sequence. Denote $C^k$ as a network obtained from $C^k(U)$ gate combined with $n - k$ extra qubits positioned between its last two qubits. Carrying out the recursion, the following results are obtained:

$$C^n(U) = \tilde{C}^nA^nB^n_1A^nB^n_1,$$

$$C^n(U) = \tilde{C}^nA^nB^n_1A^nB^n_1A^nB^n_1,$$

$$C^n(U) = \tilde{C}^nA^nB^n_1A^nB^n_1A^nB^n_1A^nB^n_1,$$

$$C^n(U) = \tilde{C}^nA^nB^n_1A^nB^n_1A^nB^n_1A^nB^n_1,$$

$$C^n(U) = \tilde{C}^nA^nB^n_1A^nB^n_1A^nB^n_1A^nB^n_1.$$

So a generic $C^n(U)$ circuit where $n \geq 5$ can be expressed:

$$C^n(U) = \tilde{C}^{n-4}A^{2n-4}B^{n-1}_1B^{n-1}_2.$$

Given a unitary operator $V$, there must exist one-qubit unitary operations $D$, $E$, $F$ and real number $a$ such that $DEF = I$ and $e^{ia}D\sigma_xE\sigma_xF = V$. $\sigma_x$ and $G$ are unitary one-qubit operations corresponding to matrices $\sigma_x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $G = \begin{bmatrix} 1 & 0 \\ 0 & e^{ia} \end{bmatrix}$. Let $C^k_{k'}(U)$ denote a $\Lambda^k(U)$ gate where qubit $k$ controls the qubit $k'$. We rewrite Eq. (2) in terms of CNOT and one-qubit gates after certain gate counting:

$$C^n(U) = \tilde{C}^{n-4}A^{2n-4}F^n_{\beta+3}C^{\beta+3}_{\gamma_{\beta+3}^n}(\sigma_x)C^{\beta+3}_{\gamma_{\beta+3}^n}(\sigma_x)G^{\beta+3}_{\gamma_{\beta+3}^n}E^n_{\beta+3}C^{\beta+3}_{\gamma_{\beta+3}^n}(\sigma_x)$$

$$\sigma_x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } G = \begin{bmatrix} 1 & 0 \\ 0 & e^{ia} \end{bmatrix}.$$
with period $d = 2\lceil n/2 \rceil - 4$, then use a formula to describe the regulation of Toffoli gates

\[
\wedge^{m_1}(\sigma_x) = \prod_{i=1}^{4\lceil n/2 \rceil - 8} T_{n-\lceil n/2 \rceil+2+f(n)}^{1+\lfloor \delta_i, \delta_{i+n} \rfloor(n-\lceil n/2 \rceil+f(n))},
\]

where $f(n) = \lceil d/2 \rceil + \frac{1}{2} \arctan(\tan(\frac{\pi i}{n} - \frac{\pi}{2})) - \lfloor \frac{n}{2} \rfloor + 1$. It denotes the deviation of $i$ to $\frac{n}{2} - 1$ when $1 \leq i \leq d$ or to $\frac{n}{2} - 1 + d$ when $d + 1 \leq i \leq 2d$. The absolute value function expresses symmetric property, the arctan function fixes periodic regulations, and the $\delta$ functions correspond to certain singular points at $i = \lceil n/2 \rceil - 1$ and $3\lceil n/2 \rceil - 5$ referred in above formalism.

Similarly, for $n \geq 7$, $\wedge^{m_2}(\sigma_x)$ gates can be simulated by the network in Fig. 5. We find that there are $4n - 4\lceil n/2 \rceil - 12$ Toffoli gates in $\wedge^{m_2}(\sigma_x)$ network. Inspecting the mathematic property of indices, it is periodic with period $d' = 2n - 2\lceil n/2 \rceil - 6$, symmetric around $j_0 = n - \lceil n/2 \rceil - 2$ and $j_0 + d' = 3n - 3\lceil n/2 \rceil - 8$, we obtain the following formula

\[
\wedge^{m_2}(\sigma_x) = \prod_{j=1}^{4n-4\lceil n/2 \rceil-12} T_{n-2-d(n)}^{n+1+\lfloor \delta_j, \delta_{j+n} \rfloor(1-\delta_j, \delta_{j+n} \rceil(2\lceil n/2 \rceil-2n+3+g(n))}
\]

where $g(n) = \lceil d'/2 \rceil + \frac{1}{2} \arctan(\tan(\frac{\pi j}{n} - \frac{\pi}{2})) - n + \lfloor \frac{n}{2} \rfloor + 2$. Then we propose a cascade decomposition of $C^n(U)(n \geq 7)$ gate by a recursive method shown in Fig. 6, where unitary $V_i$ is defined by $V_i^2 = U$.
for $C^6(U)$ and we have proven that the Toffoli gates labeled as 4, 6, 8, 10, 15, 20, 25, 30 as shown in Fig. 7 for $C^6(V_{n-6})$ part, and all the Toffoli gates other than $C^6(V_{n-6})$ in Eq. (7) can be replaced by the modulo phase shift of Toffoli gates.

![Diagram](image)

FIG. 7: The explicit structure of $C^6(U)$ (congruent to $C^6(V_{n-6})$) in terms of Toffoli and two-qubit controlled gates.

Given a unitary operator $V_{n-k+1}$, $L$, $P$, $R$ and $S$ are one-qubit unitary gates such that $e^{ibL}σ_xPσ_xQ = V_{n-k+1}$, $LPQ = I$ and $S = \begin{bmatrix} 1 & 0 \\ 0 & e^{ib} \end{bmatrix}$, their subscripts represent which qubit they are performed on. Now we obtain the $C^9(U)$ in terms of CNOT and one-qubit gates:

$$C^9(U) = C^9(V_{n-6}) \prod_{k=7}^n W_{k-1} W_{k-1}^{-1} \sigma_n^{-1} (σ) P_n C_n^{-1} (σ) S_n \sigma_n,$$

where

$$W_{k-1} = \prod_{i=1}^{4[k/2]-8} R_{k-1}^{-1}(1-\delta_{i,1})(1-\delta_{i,2}+a)(k-[k/2]+f(k))(σ_x)$$

$$+ \prod_{i=1}^{4k-[k/2]-12} R_{k-1}^{-1}(1-\delta_{j,1})(1-\delta_{j,2}+a)(2[k/2]-2k+5+g(k))$$

Taking account of the merges of CNOT gates and one-qubit gates, we obtain the total number of basic operations in $C^9(U)$ construction are $24n^2 - 212n + 340$ CNOT gates and $32n^2 - 288n + 739$ one bit gates ultimately.

**IV. Conclusions**— In conclusion, we have given two analytic schemes for constructing a $C^9(U)$ gate for arbitrary value of $n$ and any unitary $U$ operator, one with exponential complexity and the other with polynomial complexity. General expression for decomposition of $C^9(U)$ gates with basic one-qubit gates and CNOT gates has been derived explicitly. We have compared the exact numbers of basic operations required in these two methods for $n = 1 - 20$. It shows that the exponential construction is advantageous for the value of $n = 1 - 8$, whereas the polynomial simulation is efficient for larger values of $n > 8$.

This work is supported by the National Fundamental Research Program Grant No. 2006CB921106, China National Natural Science Foundation Grant Nos. 10325521, 60433050.

---

1 Electronic address: gllong@mail.tsinghua.edu.cn

[1] P. W. Shor, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, 1994), pp. 124.

[2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[3] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).

[4] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, England, 2000, Chapter 4.

[6] J. J. Vartiainen, M. Motto, M. M. Saloma, Phys. Rev. Lett. **92**, 177902 (2004).

[7] M. Motto, J. J. Vartiainen, V. Bergholm, M. M. Saloma, Phys. Rev. Lett. **93**, 130502 (2004).

[8] R. R. Tucci, [quant-ph/9902062](http://arxiv.org/abs/quant-ph/9902062) (2001, 2nd version).

[9] G. L. Long and Y. Sun, Phys. Rev. A **64**, 014303 (2001).

[10] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).

[11] V. V. Shende, I. L. Markov, S. S. Bullock, Phys. Rev. A **69**, 062321 (2004).

[12] F. Vatan and C. P. Williams, Phys. Rev. A **69**, 032315 (2004).

[13] A. Barenco *et al*., Phys. Rev. A **52**, 3457 (1995).

[14] W. H. Press *et al*., *Numerical Recipes in FORTRAN: The Art of Scientific Computing* (Cambridge University Press Cambridge, United Kingdom, 1992), 2nd ed., pp.886-888.

[15] D. P. DiVincenzo and J. Smolin, *Proceedings of the Workshop on Physics and Computation, PhysComp’94* (IEEE, Los Alamitos, 1994), pp.14.