LETTER

IEICE Electronics Express, Vol.13, No.5, 1–9

Synthesis of quantum circuits by multiplex rotation gates

Hu Jiang[1,2], Wang Pengjun[1a), and Zhang Qiaowen[1,2]

[1] *Institute of Circuits and Systems, Ningbo University, 818, Fenghua Road, Ningbo 315211, China*

[2] *Ningbo Key Laboratory of EDA, Zhejiang Wanli University, 8, Qianhu Road (South), Ningbo 315100, China*

a) *wangpengjun@nbu.edu.cn*

Abstract: As a model for quantum computation, quantum circuits have found their wide applications in communications, cryptography and information processing. In order to synthesize arbitrary quantum circuits, we present a new type of gate called quantum multiplex rotation gate, which is implemented by simply elementary gates. A method based on QR decomposition and two optimization rules are proposed to decompose general quantum circuit acting on n-qubits into quantum multiplex rotation gates. In comparison with other synthesis algorithms by QR decomposition, our methods achieve better performance in terms of elementary gate counts, 1.2×4^n approximately.

Keywords: quantum circuits, synthesis, rotation gates

Classification: Integrated circuits

References

[1] D. S. Simon, C. A. Fitzpatrick and A. V. Sergienko: Phys. Rev. A **91** (2015) 043806. DOI:10.1103/PhysRevA.91.043806
[2] D. Deutsch: Proc. R. Soc. London Ser. A **425** (1989) 73. DOI:10.1098/rspa.1989.0099
[3] A. Abdollahi, M. Saeedi and M. Pedram: Quant. Inf. Comput. **13** (2013) 771.
[4] G. Duclos-Cianci G and K. M. Svore: Phys. Rev. A **88** (2013) 042325. DOI:10.1103/PhysRevA.88.042325
[5] A. Barenco, C. H. Bennett and R. Cleve: Phys. Rev. A **52** (1995) 3457. DOI:10.1103/PhysRevA.52.3457
[6] E. Knill: eprint arXiv:quant-ph/9508006. 8 (1995) 5.
[7] M. Mottonen and J. J. Vartiainen: Ch.7 in Trends in Quantum Computing Research (NOVA Publishers, 2006).
[8] V. V. Shende, S. S. Bullock and I. L. Markov: IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. **25** (2006) 1000. DOI:10.1109/TCAD.2005.855930
[9] V. V. Shende, S. S. Bullock and I. L. Markov: Phys. Rev. A **69** (2004) 062321. DOI:10.1103/PhysRevA.69.062321
[10] M. A. Nielsen and I. L. Chuang: *Quantum Computation and Quantum Information* (Cambridge University Press, 2010) 10th Anniversary Edition.
[11] D. Maslov and G. W. Dueck: Electron. Lett. **39** (2003) 1790. DOI:10.1049/el:20031202

DOI: 10.1587/elex.13.20151089
Received December 20, 2015
Accepted February 2, 2016
Publicized February 19, 2016
Copyedited March 10, 2016

IEICE Electronics Express, Vol.13, No.5, 1–9

1 Introduction

As the feature size of transistors approaches atomic proportions, we cannot build transistors in atom level, because the Heisenberg uncertainty principle of quantum mechanics indicates that atom's position is uncertain [1]. Therefore, a new computational model should be proposed to replace the digital one. Among various proposed ones, quantum computation according to the law of quantum mechanics has superior performance than their classical counterparts to solve certain discrete problems. In quantum computing, algorithms are commonly described by the quantum circuit model [2]. As a result, working on synthesis methods for quantum circuit design has received significant attentions [3].

The superposition principle of quantum mechanics reveals that quantum system must be discussed in terms of vectors, matrices, and other linear algebraic constructions. A quantum bit (*qubit*) can have any linear combination of its basic states ($|0\rangle, |1\rangle$), as $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers and $\alpha||^2 + \beta||^2 = 1$. A n-qubits quantum gate performs a special $2^n \times 2^n$ unitary operation on selected n qubits [1]. Therefore, the n-qubit quantum circuit can be represented by a unitary matrix. It is reasonable to assume that the gate decomposition may correspond to some known matrix decompositions. However, the more important issue is how these circuits are decomposed into elementary gates sequences, called the gate library, which is universal and consist of all one-qubit gates and the controlled-NOT gate (CNOT). Since the physically realization of the 2-qubits gate is a much slower process than that of a one-qubit gate [4], the cost of a quantum circuit can be realistically calculated by counting 2-qubits gates.

The QR decomposition is the first numerical matrix computation used for quantum logic synthesis which returns a circuit containing $O(n^3 4^n)$ CNOT gates to decompose an arbitrary n-qubit gate [5]. The work in [6] shows that the circuit complexity could be reduced down to $O(n4^n)$. Improvements on this method have used Gray codes to lower this gate counts to $8.7 \cdot 4^n$ CNOT gates approximately [7]. A more optimized QR decomposition has led to circuit with CNOT-counts of $2 \times 4^n - (2n + 3) \times 2^n + 2n)$ [8]. The theoretical lower bound for the number of CNOT gates needed to realize a general unstructured n-qubits gate is $|(4^n - 3n - 1)/4|$ [9], but no circuit construction has been presented to our best knowledge.

In this paper, we establish our library of elementary gates by choosing the one-qubit rotation gates, CNOT, the controlled-V gate and a phase gate adjusting the unobservable global phase. An efficient method is presented to synthesize and optimize quantum circuits by utilizing QR decomposition. We decompose the unitary matrix into a product of matrices, identified by a new type of gate which we call a quantum multiplex rotation gate. In order to implement these gates, their efficient decomposition into elementary gates is given.

2 Quantum multiplex rotation gate

The term "quantum multiplexor" was first used to refer to the circuit block implementing a quantum conditional in Ref. [8]. The concept of uniformly controlled rotation gate with efficient gates implementation was introduced in Ref. [7].

DOI: 10.1587/elex.13.20151089
Received December 20, 2015
Accepted February 2, 2016
Publicized February 19, 2016
Copyedited March 10, 2016

IEICE Electronics Express, Vol.13, No.5, 1–9

Both works have been used in decomposition of arbitrary n-qubits gates and initialization quantum registers. The uniformly controlled rotation gate $F_m^k(R_a)$ is a sequence of 2^k rotation gates, each having a different sequence of k control nodes and the same rotation axis. Combining the two concepts, we propose a quantum multiplex rotation gate where the rotation axes may be different.

Definition 1: We use $G_m^k(R)$ to define a quantum multiplex rotation gate. The gate consists of k-fold controller and some rotations about three-dimension vectors $a_s, s = 1, 2, \cdots, 2^k$ acted on qubit m. For n-qubits gate, the region of m is $1, \cdots, n$, k is $1, \cdots, n-1$, and s is $1, \ldots, 2^k$.

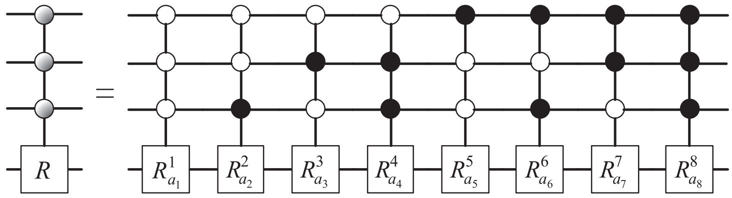

Fig. 1. Definition of quantum multiplex rotation gate $G_4^3(R)$. Here white dots represent 0, black 1.

Fig. 1 shows an example of $G_m^k(R)$, where $m = 4$, $k = 3$. It has a sequence of 8 rotation gates which commute, each having a different sequence of 3 control nodes. The matrix representation is

$$G_4^3(R) = \begin{pmatrix} R_{a_1}(\alpha_1) & & \\ & \ddots & \\ & & R_{a_8}(\alpha_8) \end{pmatrix} \tag{1}$$

where $R_{a_s}(\alpha_s), s = 1, \cdots, 2^k$ is a two-level rotation matrix, α_s and a_s denote rotation angle and rotation vector respectively.

Definition 2: Let $G_m^k(R)|_{l=0,p=1}$ denote a quantum multiplex rotation with fixed controllers (qubit $l = 0$, $p = 1$). The range of values allowed for fixed controller is $1, \ldots, n-1$.

Lemma 1: For any rotation matrix $R_a(\alpha)$, there is $\sigma_x R_a(\alpha)\sigma_x = R_a(-\alpha)$. The parameter σ_x is one of Pauli matrices, also it is the representation matrix of NOT gate.

Proof: From Ref. [10], the equalities $R_a(\alpha) = R_z(\phi)R_y(\beta)R_z(\gamma)$, $\sigma_x\sigma_x = I$, $\sigma_x R_z(\phi)\sigma_x = R_z(-\phi)$, $\sigma_x R_y(\beta)\sigma_x = R_y(-\beta)$ hold. Then

$$\begin{aligned} \sigma_x R_a(\alpha)\sigma_x &= \sigma_x R_z(\phi)\sigma_x\sigma_x R_y(\beta)\sigma_x\sigma_x R_z(\gamma)\sigma_x \\ &= R_z(-\phi)R_y(-\beta)R_z(-\gamma) = R_a(-\alpha). \end{aligned} \tag{2}$$

Theorem 1: Arbitrary quantum multiplex rotation gate $G_m^k(R_a)$ can be decomposed using a convertible sequence of 2^k CNOTs and 2^k one-qubit rotation R_a which act on qubit m.

Proof: From definition 1, quantum multiplex rotation gate is a rotation gate with full condition. Therefore, it can be described with *if* − *elseif* − *else* conditional statement by the k control qubits. Consider the one-to-one correspondence between

DOI: 10.1587/elex.13.20151089
Received December 20, 2015
Accepted February 2, 2016
Publicized February 19, 2016
Copyedited March 10, 2016

ELectronics EXpress

if − elseif − else and *if − else* nested statement, we can use conditional nesting sentence to express quantum multiplex rotation gate. Fig. 2 is an example of the decomposition of $G_4^3(R_a)$.

If using the exponential form to represent rotation gates, then

$$R_{b_1}(\beta_1)R_{b_2}(\beta_2) = e^{b_1\beta_1}e^{b_2\beta_2} = e^{b_1\beta_1+b_2\beta_2} = e^{a_1\alpha_1} \tag{3}$$

$$\sigma_x R_{b_1}(\beta_1)\sigma_x R_{b_2}(\beta_2) = R_{b_1}(-\beta_1)R_{b_2}(\beta_2) = e^{-b_1\beta_1}e^{b_2\beta_2} = e^{-b_1\beta_1+b_2\beta_2} = e^{a_2\alpha_2} \tag{4}$$

a_1, a_2, b_1, b_2 denote rotation vectors, α_1, α_2, β_1, β_2 angles.

According to the *if − elseif − else* form and the *if − else* nested form of $G_m^k(R_a)$, we can give the expression below.

$$N^k \begin{pmatrix} b_1 \cdot \beta_1 \\ \vdots \\ b_{2^k} \cdot \beta_{2^k} \end{pmatrix} = \begin{pmatrix} a_1 \cdot \alpha_1 \\ \vdots \\ a_{2^k} \cdot \alpha_{2^k} \end{pmatrix} \tag{5}$$

The elements of $2^k \times 2^k$ matrix N^k can be determined by Eq. (6).

$$N_{ij}^k = (-1)^{(i_1 \cdot j_1 \oplus i_2 \cdot j_2 \oplus \cdots \oplus i_{2^k} \cdot j_{2^k})} \tag{6}$$

From Eq. (6) the matrix N^k is a k-bit Walsh-Hadamard matrix whose rows are mutually orthogonal. Therefore, we acquire the invers matrix $(N^k)^{-1} = 2^{-k}(N^k)^T$ and the objective rotation of b_s, β_s for any known rotation a_s, α_s is settled.

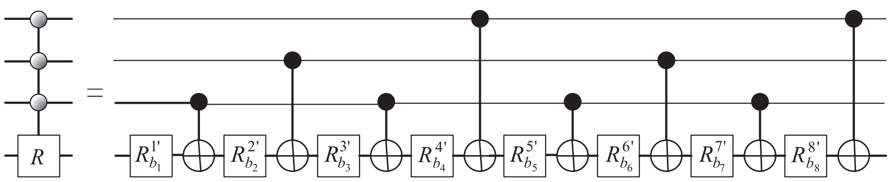

Fig. 2. The efficient implementation of quantum multiplex rotation gate $G_4^3(R_a)$

Corollary 1: Quantum multiplex rotation $G_m^k(R)$ with l-qubits fixed controllers can be decomposed using a convertible sequence of 2 l-bit Toffoli gates and 2 quantum multiplex rotation gates $G_m^{k-l}(R)$.

Proof: We select two quantum multiplex rotation matrices R_1, R_2, which meet two conditions, $R_1R_2 = I$ and $R_1\sigma_xR_2\sigma_x = R$. If the l-qubits fixed controllers get the fixed values, the operation acting on the target qubits is rotation R. Otherwise, there is no operation. Therefore, the function of the decomposition is the same as the quantum multiplex rotation matrix with l-qubits fixed controllers. Fig. 3(a) shows how to decompose the $G_4^3(R)|_{1=1,2=0}$ gate.

Corollary 2: (Absorbing rules) The quantum multiplex rotation gate with fixed controllers $G_m^k(R)|_{fixed\ controller}$ is absorbed by the quantum multiplex rotation gate $G_m^k(R)$.

Proof: From the definitions, the quantum multiplex rotation gate with fixed controllers $G_m^k(R)|_{fixed\ controller}$ is a special condition of the quantum multiplex rotation gate $G_m^k(R)$. Therefore, it can be absorbed. An example of absorbing rules is shown in Fig. 3(b).

DOI: 10.1587/elex.13.20151089
Received December 20, 2015
Accepted February 2, 2016
Publicized February 19, 2016
Copyedited March 10, 2016

IEICE Electronics Express, Vol.13, No.5, 1–9

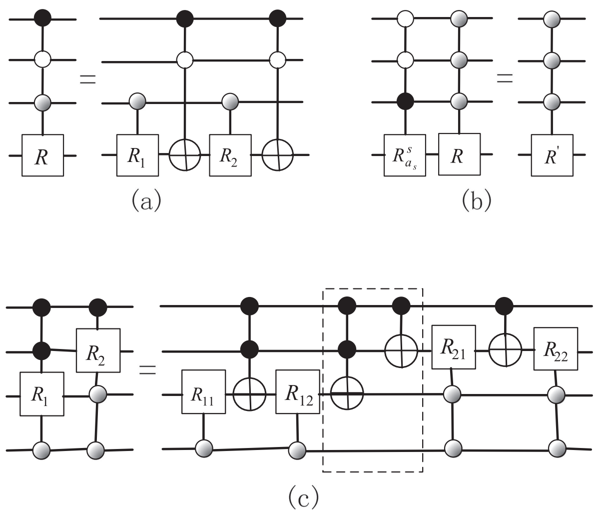

Fig. 3. (a) The implementation of gate $G_4^3(R)|_{1=1,2=0}$. (b) An example of absorbing rules. (c) An example of using of combining rules, where the two gates in the dotted box can reduce as a Peres gate

Corollary 3: (Combining rules) When two gates $G_m^k(R)|_{l\ fixed\ controllers}$ and $G_{m+1}^k(R)|_{l-1\ fixed\ controllers}$, having the same $l-1$ fixed controllers, operate on qubits in order, there is an optimum combination between two multiple-controlled Toffoli gates.

Proof: According to corollary 1, we decompose $G_m^k(R)|_{l\ fixed\ controllers}$ and $G_{m+1}^k(R)|_{l-1\ fixed\ controllers}$. There appear two adjacent multiple-controlled Toffoli gates with the same $l-1$ fixed controllers. With the result in Ref. [11], there is an optimum combing the two gates. From the dotted box in Fig. 3(c), a Toffoli gate followed by a CNOT gate is equivalent to a Peres gate, whose cost is only 4.

3 Synthesis algorithms

Matrix decomposition is useful to synthesizing the quantum gates. The theorem of QR factorization indicates that for each complex matrix A the equation $A = QR$ holds, where Q is unitary matrix, R is invertible and upper triangular matrix. If A is unitary matrix, R is diagonal matrix, and Q is a product of two-level matrices called Givens rotation.

Theorem 2: Let $x = (\xi_1, \xi_2, \cdots, \xi_{2^k})^T \neq 0, x \in C^{2^k}$ denote a unit vector. The equalities $Gx = e_s, s = 1, 2, \cdots, 2^k$ hold, where matrix G is a product of k quantum multiplex rotation matrices and quantum multiplex rotation matrices with fixed controllers.

Proof: Consider the case of $s = 1$, that is, $Gx = e_1$. The dimension of x is 2^k, so we use k-bits binary to represent the position of vector elements. e_1 is a standard basis vector, that the value of the first element is 1, others are 0. Therefore, our target position is $\overbrace{00\cdots0}^{k}$.

Firstly, we can build a quantum multiplex rotation matrix G_k^{k-1} to make $G_k^{k-1}x = (^*, 0, ^*, 0, \cdots, ^*, 0)$. For $\xi_1\xi_2$, let $c_1 = \dfrac{|\xi_1|}{|\xi_1|^2 + |\xi_2|^2}$, $s_1 = \dfrac{|\xi_2|}{|\xi_1|^2 + |\xi_2|^2}$,

DOI: 10.1587/elex.13.20151089
Received December 20, 2015
Accepted February 2, 2016
Publicized February 19, 2016
Copyedited March 10, 2016

IEICE Electronics Express, Vol.13, No.5, 1–9

$\theta_1 = -\arg\xi_1$, $\theta_2 = -\arg\xi_2$ constitute complex Givens transformation $M_1 = \begin{pmatrix} c_1 e^{i\theta_1} & s_1 e^{i\theta_2} \\ -s_1 e^{i\theta_2} & c_1 e^{i\theta_1} \end{pmatrix}$. $\xi_3\xi_4, \ldots, \xi_{2^k-1}\xi_{2^k}$ can be used to generate the matrices $M_2, \ldots, M_{2^{k-1}}$ respectively by the same way as $\xi_1\xi_2$. The matrix G_k^{k-1} can be determined by Eq. (7).

$$G_k^{k-1} = \begin{pmatrix} M_1 & & & \\ & M_2 & & \\ & & \ddots & \\ & & & M_{2^{k-1}} \end{pmatrix} \tag{7}$$

$$G_k^{k-1}x = \left(\sqrt{|\xi_1|^2 + |\xi_2|^2}, 0, \sqrt{|\xi_3|^2 + |\xi_4|^2}, 0, \cdots, \sqrt{|\xi_{2^k-1}|^2 + |\xi_{2^k}|^2}, 0\right) \tag{8}$$

Secondly, we can build a quantum multiplex rotation matrix with fixed controller $G_{k-1}^{k-2}|_{k=0}$ to make $G_{k-1}^{k-2}|_{k=0}(G_k^{k-1}x) = ({}^*, 0, 0, 0, {}^*, 0, 0, 0, \cdots, {}^*, 0, 0, 0)$. For $\sqrt{|\xi_1|^2 + |\xi_2|^2}\sqrt{|\xi_3|^2 + |\xi_4|^2}$, the Givens transformation $M_1 = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ can be given by the aforementioned method. In the meantime, we can generate matrices $M_2, \cdots M_{2^{k-2}}$ by other couples. Then matrix $G_{k-1}^{k-2}|_{k=0}$ is determined by Eq. (9).

$$G_{k-1}^{k-2}|_{k=0} = \begin{pmatrix} m_{11} & & m_{12} & & \\ & 1 & & & \\ m_{21} & & m_{22} & & \\ & & & 1 & \\ & & & & \ddots \end{pmatrix} \tag{9}$$

$$\begin{aligned} G_{k-1}^{k-2}|_{k=0}(G_k^{k-1}x) = \Big(&\sqrt{|\xi_1|^2 + |\xi_2|^2 + |\xi_3|^2 + |\xi_4|^2}, 0, 0, 0, \cdots, \\ &\sqrt{|\xi_{2^k-3}|^2 + |\xi_{2^k-2}|^2 + |\xi_{2^k-1}|^2 + |\xi_{2^k}|^2}, 0, 0, 0\Big) \end{aligned} \tag{10}$$

Keeping it on, in the last step we generate matrix $G_1^0|_{2=0,\cdots,k=0}$ to transform the value of the element to 0, whose position is $\overbrace{10\cdots0}^{k}$. Then, the matrix $G = G_1^0|_{2=0,\cdots,k=0} G_2^1|_{3=0,\cdots,k=0} \cdots G_{k-1}^{k-2}|_{k=0} G_k^{k-1}$ makes Eq. (11) hold.

$$Gx = G_1^0|_{2=0,\cdots,k=0} \cdots G_{k-1}^{k-2}|_{k=0} G_k^{k-1} x = \left(\sqrt{|\xi_1|^2 + |\xi_2|^2 + \cdots + |\xi_{2^k}|^2}, 0, \cdots, 0\right) = e_1 \tag{11}$$

For $s = 2, \cdots, 2^k$, the process of proof is the same as $s = 1$, except changing the target position.

Theorem 3: Arbitrary unitary matrix U can be decomposed into a product of a finite number of multi-axis rotation matrices and one diagonal matrix.

Proof: Assuming $U = (u_1, u_2, \cdots, u_{2^k})$ is a $2^k \times 2^k$ unitary matrix. The index $u_s, s = 1, 2, \cdots, 2^k$ denotes column vectors. There is a product of multi-axis rotation matrices $G = G_{2^k-2} \cdots G_2 G_1$, which makes Eq. (12) tenable by theorem 2.

DOI: 10.1587/elex.13.20151089
Received December 20, 2015
Accepted February 2, 2016
Publicized February 19, 2016
Copyedited March 10, 2016

IEICE Electronics Express, Vol.13, No.5, 1–9

$$GU = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & u'_{(2^k-1)(2^k-1)} & u'_{(2^k-1)2^k} \\ & & & u'_{2^k(2^k-1)} & u'_{2^k 2^k} \end{pmatrix} \tag{12}$$

From the Eq. (12), the two-level matrix is a unitary matrix which can be expressed as $e^{i\beta}R_a(\phi)$. If we product GU by a rotation matrix G_{2^k-1}, an extra diagonal matrix Δ will be presented, that is $G_{2^k-1}(GU) = \Delta$. Finally, $U = G'_1G'_2\cdots G'_{2^k-2}G'_{2^k-1}\Delta$.

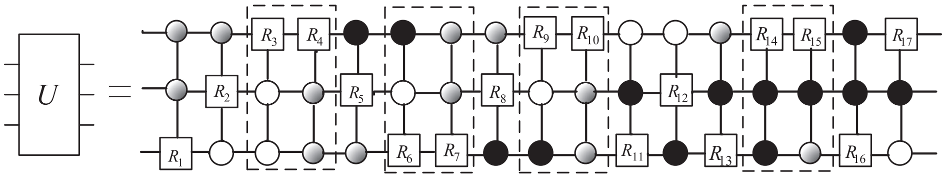

Fig. 4. Quantum circuit equivalent to an arbitrary 3-qubits unitary matrix U

As can be seen above, the quantum multiplex rotations operate non-trivially only to vectors with binary presentations differing only in one bit. Therefore, in order to acquiring optimum circuits, we label the column vectors of U using the binary reflected Gray code. The implement of the proposed synthesis algorithm is given as follows. Fig. 4 is an example to decompose an arbitrary 3-qubits quantum circuit using quantum multiplex rotation gates.

Step 1: Transforming $U = (u_1, u_2, \cdots, u_{2^k})$ to a diagonal matrix $\Delta = (e_1, e_2, \cdots, e_{2^{k-2}-1}, e^{i\beta}e_{2^{k-2}}, e_{2^{k-2}+1}, \cdots, e_{2^{k-1}+2^{k-2}-1}, e^{i\beta}e_{2^{k-1}+2^{k-2}}, e_{2^{k-1}+2^{k-2}+1}, \cdots e_{2^k})$ by using theorem 3. The transforming sequence is in the cycle of $0\times\cdots\times 0 \to 1\times\cdots\times 0 \to 1\times\cdots\times 1 \to 0\times\cdots\times 1$, where $\times\cdots\times$ remains unchanged in the cycle but is coded in binary reflected Gary code to keep the cycle until every vector changes to basis vector. Afterwards, there is $U = G_1G_2\cdots G_{2^k-2}G_{2^k-1}\Delta$, where G_s, $s = 1, 2, \cdots, 2^k$ is a product of quantum multiplex rotation matrices and quantum multiplex rotation matrices with fixed controllers. The number of both matrices is no more than k, that is, $G_s = G_1^0|_{2=0,\cdots,k=0}G_2^1|_{3=0,\cdots,k=0}\cdots G_{k-1}^{k-2}|_{k=0}G_k^{k-1}$.

Step 2: Optimizing the above circuit by absorbing rules (Corollary 2). The items in the dotted boxes in Fig. 4 are examples of these rules, where the first gate with fixed controllers can be assimilated by the second gate.

Step 3: Decomposing the quantum multiplex rotation gates and the quantum multiplex rotation gates with fixed controller in the circuit using theorem 1 and Corollary 1 respectively.

Step 4: Optimizing the above circuit by combining rules (Corollary 3), then decomposing all the multiple-control Toffoli gates by the methods which are given in Ref. [11].

Finally, we get a circuit which is equivalent to U and is constructed by CNOTs, Controlled-V gates and one-qubit rotation gates.

DOI: 10.1587/elex.13.20151089
Received December 20, 2015
Accepted February 2, 2016
Publicized February 19, 2016
Copyedited March 10, 2016

4 Algorithm analyses

In general, the performance of synthesis algorithm is always evaluated by the number of CNOTs needed to decompose an arbitrary quantum circuits. There are two steps needed to estimate the CNOT counts. First, we calculate the number of quantum multiplex rotation gates and such gates with fixed controller. For n-qubits circuits, the gate counts of the synthesis algorithm are given in Table I. Second, all the gates may be decomposed into CNOTs and one-qubit gates using Theorem 1 and Corollary 1.

Table I. The gate counts of the synthesis algorithm

Types of gate	Gate counts
$G_m^k(R_{a_s})$	2^{n-1}
$G_m^k(R_{a_s})\|_{1\ fixed\ controller}$	$2^{n-1}+2^{n-2}$
$G_m^k(R_{a_s})\|_{2\ fixed\ controller}$	$2^{n-1}+2^{n-2}+2^{n-3}$
$\cdots$	$\cdots$
$G_m^k(R_{a_s})\|_{n-2\ fixed\ controller}$	$2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^2+2^1$
$G_m^k(R_{a_s})\|_{n-1\ fixed\ controller}$	$\frac{2^{n-1}}{4}+\frac{2^{n-2}}{4}+\frac{2^{n-3}}{4}+\cdots+\frac{2^2}{4}+1$

According computation result, the CNOT counts which generated by the decomposition of the quantum multiplex rotation gates is no more than 1.2×4^n. For a n-bit Toffoli gate with one garbage bit, the quantum cost is $32(n-1)-96$, $n \geq 10$ in Ref. [11]. With the results, the number of elementary gates which come from the multiple-controlled Toffoli gates is no more than $k \times n^2 \times 2^n$, $k \leq 32$. We give a comparison of elementary gate counts for n-qubits quantum circuits generated by QR decomposition in Table II. With the value of n increasing gradually, it can be seen that our synthesis algorithm can reach a circuit with lower cost.

Table II. A comparison of elementary gates counts for n-qubits quantum circuits

Synthesis Algorithm	Number of qubits and elementary gates counts							
	1	2	3	4	5	6	7	n
Original QR [5]	–							$O(n^3 4^n)$
Improved QR [6]	–							$O(n4^n)$
QR [7]	0	4	64	536	4156	22618	108760	$\approx 8.7 \times 4^n$
QR [8]	0	8	62	344	1642	7244	30606	$\approx 2 \times 4^n$
QR	0	4	52	304	1520	8448	43072	$\approx 1.2 \times 4^n$

5 Conclusions

In this paper, quantum multiplex rotation gate and synthesis algorithm based QR decomposition are proposed to synthesize and optimize an arbitrary quantum

DOI: 10.1587/elex.13.20151089
Received December 20, 2015
Accepted February 2, 2016
Publicized February 19, 2016
Copyedited March 10, 2016

IEICE Electronics Express, Vol.13, No.5, 1–9

circuits. To evaluate the performance of the algorithm, we calculate the number of elementary gates needed to synthesize n-qubits circuits and compare with other algorithms based on QR. As see in Table II, our techniques achieve better known elementary gate counts, 1.2×4^n approximately. Our method has additional advantage that the generated circuit has small numbers of qubits and no garbage bits. To be closer to the lower bounds, $\lfloor(4^n - 3n - 1)/4\rfloor$, we need to find an efficient numerical matrix computation to improve the algorithm in the future.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (grant 61274132/61234002), the Natural Science Foundation of Zhejiang Province (grant LY14F040002), the Natural Science Foundation of Ningbo City (grant 2013A610006/2013A610008), and the K. C. Wong Magna Fund in Ningbo University, China.

DOI: 10.1587/elex.13.20151089
Received December 20, 2015
Accepted February 2, 2016
Publicized February 19, 2016
Copyedited March 10, 2016