ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.9, September 2009, pp.2332−2343
doi: 10.3724/SP.J.1001.2009.03407

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

量子可逆逻辑综合的关键技术及其算法*

李志强[1,2], 李文骞[3], 陈汉武[1+]

[1](东南大学 计算机科学与工程学院,江苏 南京 210096)

[2](扬州大学 信息工程学院,江苏 扬州 225009)

[3](南京森林公安高等专科学校 信息技术系,江苏 南京 210046)

Algorithm of Optimizing Quantum Reversible Logic Synthesis

LI Zhi-Qiang[1,2], LI Wen-Qian[3], CHEN Han-Wu[1+]

[1](School of Computer Science and Engineering, Southeast University, Nanjing 210096, China)

[2](College of Information Engineering, Yangzhou University, Nanjing 225009, China)

[3](Department of Information Technology, Nanjing Forestry Police College, Nanjing 210046, China)

+ Corresponding author: E-mail: hw_chen@seu.edu.cn

Li ZQ, Li WQ, Chen HW. Algorithm of optimizing quantum reversible logic synthesis. *Journal of Software*, 2009,20(9):2332−2343. http://www.jos.org.cn/1000-9825/3407.htm

Abstract: The key of optimizing quantum reversible logic lies in automatically constructing quantum reversible logic circuits with the minimal quantum cost. In order to improve the efficiency of an automatic synthesis and optimization of the reversible logic, a semi-template technique and a fast algorithm was proposed. Template is an efficient optimizing tool, and the semi-template technique can significantly improve the matching efficiency in optimization. R-M synthesis arithmetic is a good iterative method in reversible logic synthesis. Based on the original idea of R-M arithmetic, by constructing an optimal and collision-free Hash function, a new fast algorithm for synthesizing the quantum reversible logic circuits was proposed. This algorithm can construct optimal quantum reversible logic circuits with various types of gates and quantum cost. The experimental results show that to the best of the knowledge in the same testing environment, the results are much better than others.

Key words: quantum reversible logic; reversible logic optimization; automatic born and optimization; reversible logic synthesis; Hash function table

摘 要: 最优化量子可逆逻辑的关键在于用最小的量子代价自动构造量子可逆逻辑.为了提高可逆逻辑自动生成与优化的效率,提出了类模板技术和一种快速算法.模板技术是一个有效的优化工具,类模板技术可以显著提高模板技术的匹配效率;R-M 算法是可逆逻辑综合的一种较好的迭代方法,基于 R-M 算法的原始思想,构造了一个 Hash 函数,并在此基础上提出了一种可逆逻辑综合的快速算法.实验结果表明,在同等实验环境下使用类模板技术与快速算法,其优化的效果与效率远远优于已知的其他算法.

关键词: 量子可逆逻辑;可逆逻辑优化;自动生成与优化;可逆逻辑综合;Hash 函数关键词

* Supported by the National Natural Science Foundation of China under Grant Nos.60572071, 60873101 (国家自然科学基金); the Jiangsu Provincial Natural Science Foundation of China under Grant Nos.BK2007104, BK2008209 (江苏省自然科学基金)

Received 2007-01-11; Revised 2007-11-12, 2008-03-12; Accepted 2008-06-11

中图法分类号: TP301 文献标识码: A

一个 n 位输入、n 位输出的量子可逆电路称为 $n\times n$ 规模的量子可逆电路.量子可逆电路的合成不同于经典电路的合成,若干经典电路中的特有概念——回路、扇入、扇出,在量子可逆电路合成中通常不能出现.因此,在量子可逆电路合成时通常采用量子可逆逻辑门级联的综合方式.

量子可逆电路综合方法有若干种,关键是如何使用指定的可逆门(如 CNOT 门,Toffoli 门和 Fredkin 门等),以较高的效率自动生成量子代价较小的可逆逻辑电路.实践指出,应用不同的实现技术,通常量子可逆门的代价是不相同的.为此,人们提出了若干可逆逻辑综合的算法.Shende 等人[1]与 Song 等人[2]提出的一种 3 变量的综合方法,利用经典型穷举算法可以穷举所有 $n\times n$ 的可逆电路,结果具有理论意义,但算法比较耗时.Iwama 等人[3]提出了使用 CNOT 门的电路综合方法,该方法描述了 CNOT 门序列顺序变化的规律,采用消除实现相同变换的相邻门的规则,最终实现可逆电路的化简.该方法给出了一种综合的思想,但变换规则较为烦琐,且对电路有特别要求; Miller[4]应用谱函数实现近似最优的可逆电路化简.Miller 等人[5]和 Maslov 等人[6]在可逆电路自动构造的前提下,利用电路的可逆性和模板电路的恒等性提出了可逆电路模板优化的思想,利用该技术确实可以实现电路的自动优化,由于模板匹配技术本身具有重复和递归性,因此算法的速度较慢.在可逆电路综合领域,Mishchenko 等人[7]首先提出使用 Reed_Muller 技术综合的思想并给出相应算法.随后,Gupta 等人[8]给出了基于 Reed_Muller 技术的启发式算法,新算法在性能上有所改善,但通用性不强.Shende 等人[9]将群论思想引入可逆逻辑综合领域,他们将综合抽象成置换问题,算法运用了置换群的思想,较好的递归描述使算法性能有本质性的提高;Yang 等人[10]在此基础上将可逆逻辑综合进一步抽象成群论问题,使得构建于 GAP 软件上的算法在性能上很大程度地超越了其他算法,由于算法的核心是 GAP 软件,体大且个性不足,性能也没有达到理想.将以上的这些算法归纳起来大致可以分成两类:使用 Toffoli 门执行一个异或和操作的乘积法[7]、穷举法[1]、探索法(即通过测量汉明距离[11]或变换谱均数[12]来简化函数的迭代次数,穷举法的改进)和基于置换法的合成法[3,6,8,9,13,14]等.目前,综合算法中效率较高的还是基于置换法的合成算法,这些算法能够以较快的速度用最小量子代价来合成电路.

本文介绍了本研究小组在量子可逆逻辑综合与优化课题的研究中总结出的两个新想法:一是类模板思想及其优化技术,二是基于置换群理论的一种 Hash 函数的构造方法,以及基于线置换的量子可逆逻辑门库的构造思想.利用类模板技术可以在可逆逻辑优化中提供更多一些的模板,增加待优化电路的匹配率,进一步提高优化效率;利用计算性能良好的 Hash 函数和模板库技术可以更加快速地设计出性能良好的最小长度或最小代价的量子可逆逻辑电路.

第 1 节简介可逆逻辑综合的置换法,包括真值表变化法和 R-M 变化法.第 2 节介绍了可逆电路的模板优化方法以及类模板的思想,定义及其优化可逆电路的方法,在表 2 中给出了在同等硬件环境下标准结果(F)与各种有代表性方法结果的比较.第 3 节中首先给出了基于置换群理论的 Hash 函数的构造方法和基于线置换的量子门库的构造方法,随后给出求最小长度的 QML 算法以及求最小代价的 QMC 算法,最后在 QML 和 QMC 的基础上,给出了求可逆逻辑电路综合的通用算法 QGA.表 3 和表 4 分别给出了利用不同量子门集合的 QML 和 QMC 的运行结果以及与相关论文结果的比较.

1 基于置换法的综合方法

基于置换法的综合方法主要是通过一些变换规则,将输出值逆向逐次变换成输入值,在每一次的变换过程中选取相应的 Toffoli 门,最终构成所需要的量子电路.这类方法中较为常用的是真值表变换法[6,14]和 R-M 变换法[8,13].

① 真值表变换法:通过真值表的变换,选取相应的 Toffoli 门级联,将输出的值逐次变换,直至输出的值等于输入值.

例如,在一个 n=3 的线路上实现以下的变换 f,其对应的逻辑电路与真值表见表 1:

$f(0)=2$, $f(1)=6$, $f(2)=0$, $f(3)=1$, $f(4)=7$, $f(5)=3$, $f(6)=5$, $f(7)=4$,

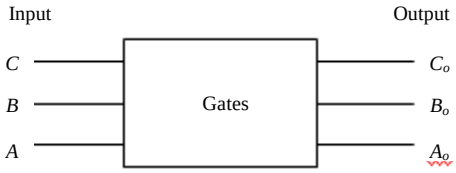
算法将根据变换规则,把CoBoAo的值一步步地变换成CBA的值,真值表的每一步变换都由一个Toffoli门实现,重复此过程,直至将输出值全部变换成输入值.根据级联的位置不同,合成方法有3种:前向合成、后向合成和双向合成.

Table 1 Logic function truth table of permutation σ

表 1 置换σ的逻辑函数真值表

$$\sigma\begin{pmatrix}0&1&2&3&4&5&6&7\\2&6&0&1&7&3&5&4\end{pmatrix}$$

σ quantum circuit diagram



Input				Output			
i	C	B	A	j	C_o	B_o	A_o
0	0	0	0	2	0	1	0
1	0	0	1	6	1	1	0
2	0	1	0	0	0	0	0
3	0	1	1	1	0	0	1
4	1	0	0	7	1	1	1
5	1	0	1	3	0	1	1
6	1	4	0	5	1	0	1
7	1	1	1	4	1	0	0

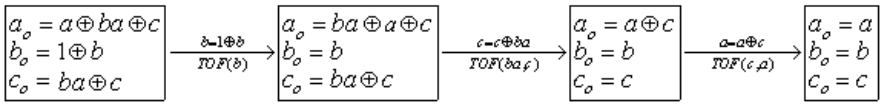
② R-M 变换法:通过 Reed-Muller 展开式,利用矩阵的初等变换及其性质,可以生成较为优化的可逆电路.Reed-Muller 展开式如下:其中 $a_i\in\{0,1\}$.

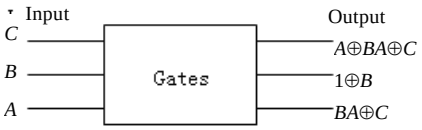
$$f(x_1,x_2...,x_n)=a_0\oplus a_1x_1\oplus a_2x_2\oplus...\oplus a_nx_n\oplus a_{12}x_1x_2\oplus a_{13}x_1x_3\oplus...\oplus a_{n-1,n}x_{n-1}x_n \\ \oplus a_{123}x_1x_2x_3...\oplus a_{n-2,n-1,n}x_{n-2}x_{n-1}x_n...\oplus a_{12\cdots n}x_1x_2...x_n.$$

例如,n=3 的 Reed-Muller 展开式为

$$f(A,B,C)=a_0\oplus a_1A\oplus a_2B\oplus a_3AB\oplus a_4C\oplus a_5AC\oplus a_6BC\oplus a_7ABC \\ =(a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)(1,A,B,AB,C,AC,BC,ABC)^T=\vec{a}\cdot\vec{P}.$$

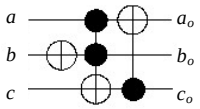
就上面的例子来说,将每一根输出线通过Reed-Muller展开后,其输出如图1(a)所示的表达式.同真值表的方法一样,从输出端开始,通过如下所示的变换规则,将输出端的表达式变换为输入端的表达式,同时,在变换的每一步选取相应的 Toffoli 门,从输入端开始排列,当变换完成时,量子线路也就成功地合成了.由此可见,基于 R-M 的方法综合的本质是对 Reed-Muller 展开式进行化简.图 1(b)给出了以上例子的实际量子可逆逻辑.





(a) Expression after using R-M expansion

(a) R-M 展开后的表达式



(b) Quantum circuit implementation of logic function in Table 1

(b) 实现表 1 逻辑函数功能的量子电路

Fig.1

图 1

我们的研究表明,无论采取上述何种变换方法,所得到的量子电路往往并不是最优的电路,即门的数量并不是最少的电路.因此文献[15−18]提出了运用模板技术的等价性替换电路中的某一部分逻辑门,从而达到减少逻辑门数量的目的,即量子可逆逻辑的(规模或代价)模板优化技术.

2 类模板及其优化方法

2.1 传统的模板技术

一个长度为 m 的模板是指由 m 个 Toffoli 门组成的最优电路,即长度为 m 的模板不能被长度为 $n(n<m)$的模板所化简.模板电路实现的是一个恒等的逻辑函数功能,长度为 m 的模板记为 $T=G_0G_1G_2...G_m=Id$ (ld 表示恒等).

定义 1. 对于量子电路的一条输入/输出线段,如果这条线路上没有受控端(XOR 门),则称这条输入/输出线为控制线,记为 $C_i(i>0)$.反之则称为受控线,记为 $t_i(i>0)$.特别地,在模板电路中,C_i 和 t_i 分别表示一组相同的控制线的集合和受控线的集合.

定义 2. 对于一个门序列 $G_0G_1G_2...G_{m-1}$,它的一条控制线可以用特征向量 $(a_0,a_1,a_2,...,a_{m-1})$ 来表示,其中 $a_i\in\{0,1\}, 0\le i\le m-1$,$a_i=1$ 当且仅当 G_i 在这条控制线上有控制点,否则,$a_i=0$.

例如,$n=5$ 的模板如图 2 所示.

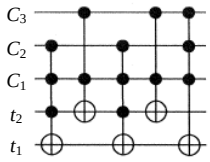


Fig.2 A template of length 5

图 2 长度为 5 的模板

其中,$C_{i\{1\le i\le 3\}}$ 和 $t_{i\{1\le i\le 2\}}$ 分别表示控制线和受控线,对于控制线 C_2,它的特征向量为(1,0,1,0,1).而在模板的实际应用中,C_2 也可以代表需要化简的电路中数条这样的控制线.

命题 1[11]. 如果一个门序列 $G_0G_1G_2...G_{m-1}$ 实现的是恒等函数功能,那么它的 k 阶轮换 $G_kG_{(k+1)\bmod m}...G_{(k-1)\bmod m}$ 实现的也是恒等函数功能.

命题 2[23]. 模板有以下属性:

(1) 如果长度为 m 的模板中有一条特征向量为 $(a_0,a_1,a_2,...,a_{m-1})$ 的控制线,那么任何具有相同特征向量控制线的集合是一个模板控制线的集合.

(2) 对于任何模板,特征向量为(0,0,0,0,0)和(1,1,1,1,1)的控制线是模板控制线.

(3) 如果特征向量为 $(a_0,a_1,a_2,...,a_{m-1})$ 和 $(b_0,b_1,b_2,...,b_{m-1})$ 是模板的控制线,那么特征向量$(a_0\cup b_0,a_1\cup b_1,a_2\cup b_2,...,a_{m-1}\cup b_{m-1})$ 也是这个模板的控制线.

(4) 如果一条线段上有且仅有两个 XOR 门(受控点),记为门 G_i 和 G_j,那么对于每一条模板的控制线,都有 $a_i=a_j$.

命题 3. 模板是一个衡等变换,因此判断一条控制线是否有效的充要条件是,考察当它取值为 0 时,该控制线是否还能保持该模板的恒等函数功能.

证明:

首先考虑控制线的取值对模板 $G_0G_1G_2...G_{m-1}$ 的影响.对于一条特征向量为 $(a_0,a_1,a_2,...,a_{m-1})$ 的控制线,它的取值有两种情况:$x=0$ 或 $x=1$.当 $x=0$ 时,则对应于特征向量中所有 $a_i=1$ 的门都是无效的.这容易理解,$a_i=1$ 表示门 G_i 在这个控制线上有控制点,当控制线为 0 时,门 G_i 在这条控制线上的控制点的值为 0,根据 Toffoli 门的定义,门 G_i 是无效的,那么模板就等价于移除特征向量中所有 $a_i=1$ 的门的电路.当 $x=0$ 时,这条控制线可以被忽略,因为控制线取值为 1 时,无论控制向量中 a_i 为何值,都不会使任何门无效,也就是说,当 $x=1$ 时,控制线不会对任何门起任何作用,也就不会改变这个模板的函数功能,所以可以将这条控制线忽略.因此,判断一个控制线是否为有效的控制线,只需考虑它取值为 0 时,是否还能保持原有的模板恒等的函数功能. □

文献[11,23]中,Maslov 等人找到了如图 3 所示的 $m=2,4,5,6,7,9$ 的模板.

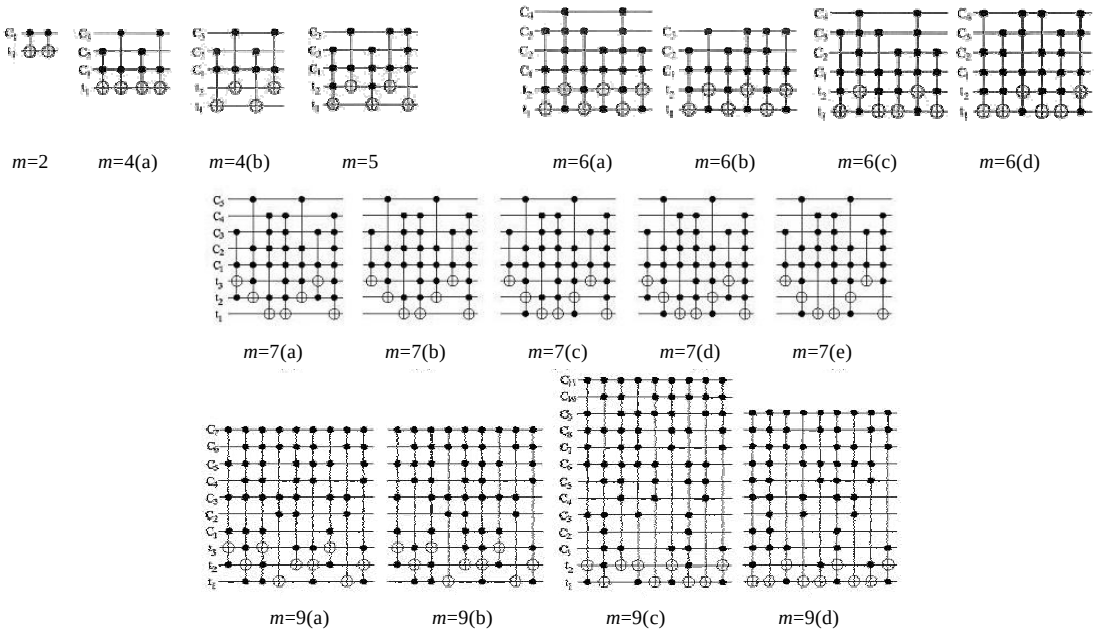


Fig.3 A template with $m=i$ (i=2,4,5,6,7,9)

图 3 $m=i$(i=2,4,5,6,7,9)的模板

利用模板技术优化可逆电路的方法十分简单.例如,对于长度为 m 的模板,取任意的 k(0<k<n),令 $f=G_0...G_k$,则根据酉算子性质,有 $G_{k+1}...G_n=f^{-1}$(每一个量子门对应一个酉算子),也就是说,$G_0...G_k=(G_{k+1}...G_n)^{-1}$.对于一个 Toffoli 门电路,当电路中的一个门序列与 $G_0...G_k$ 相匹配,并且 $k>\lfloor m/2 \rfloor$,则可以用 $(G_{k+1}...G_n)^{-1}=G_n...G_{k+1}$(Toffoli 门的逆就是它本身 $G^{-1}=G$)的门序列等价替换当前电路中的门序列,在减少门个数的同时,模板性质可以确保函数功能不变.

2.2 类模板技术

在图 3 的模板表示中,我们发现 Maslov 等人对于模板控制线的表示还不完全.例如,对于图 3 中 6(a)和 6(c)的模板,若选特征向量为(0,0,1,0,0,1)的控制线 C_5,对于 6(a)模板,C_5,C_1,t_1,t_2,可以构成一个新模板,但是如果将 C_5 加入原有的 6(a)和 6(c)模板,则原先的模板控制线就不满足命题 2 的性质 3 了.显然对于模板来说,少一条控制线就可能少一块模板.受上例启发,我们引入了模板控制线库及类模板的概念,其目的就是利用控制线构建一个模板控制线库,使其在实际应用中能够动态生成相应的模板,以提高模板匹配的成功率.

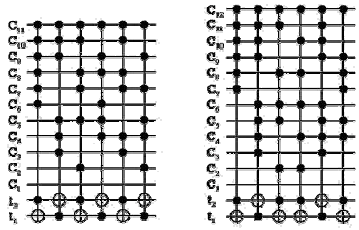
定义 4(模板控制线库). 一个模板的控制线库是指门数为 m 模板的所有有效控制线所组成的集合,所谓模板的有效控制线是指这条控制线和模板的所有受控线组成的量子电路都能够实现模板的恒等函数功能.

定义 5(类模板). 一个模板的控制线库就是一个类模板.类模板满足命题 2 中除了性质 3 以外的性质.类模板利用命题 2 中的性质 3 可以自由组织控制线动态生成模板.

引入模板控制线库的概念有两点好处:一是控制线库包含了模板的所有有效控制线,在模板匹配的应用中增加了控制线的选择范围,提高了匹配成功率;二是可以将 Maslov 的模板进行合并.例如,图 3 中的 m=6(a)和 m=6(c),以及 m=6(b)和 m=6(d)((d)的 1 阶轮换后受控线等价于(b)的受控线)即可合并.

通过模板控制线库的概念重构门数为 m=6 的类模板如图 4 所示.显然,类模板的规模比 Maslov 模板的规模大许多,之所以称之为类模板,是因为此时类模板的控制线之间已不满足命题 2 的性质 3,所以重构后的类模板本身不能实现恒等的函数功能.实际上,Maslov 的模板是根据命题 2 的性质 3 进行分类的,而类模板正好相反,是将模板合并.

类模板在计算机内分两部分存储,一是模板所有的受控线集合$\{t_i\}$,我们要求受控线组成的电路能够实现恒等的函数功能,另一部分就是模板的控制线库$\{C_i\}$.这样的分类在模板应用的算法实现上是很有用的,有助于提高算法的时空效率.



m=L6(a) *m*=L6(b)

Fig.4 A semi-template of length 6 after reconstruction

图 4 重构后的长度为 6 的类模板

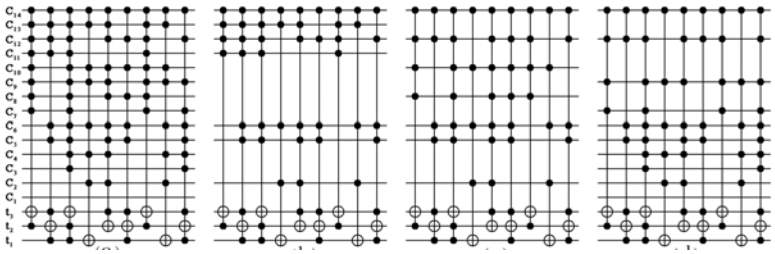
命题 4. 一个具有 K 条有效控制线的模板是有效的(实现恒等函数功能),当且仅当它的任意 $i(1\le i\le K)$条控制线的特征向量的并所表示的控制线也是这个模板的有效控制线.

证明:对于长度为 m 的模板,其所有的受控线组成的电路实现的是恒等函数功能,我们只要证明对于这个模板的所有控制线的任意取值,模板所有受控线组成的电路实现的还是恒等函数功能即可.

假设模板电路有 K 条有效控制线.对这 K 条控制线进行任意取值,设有 $n(1\le n\le K)$条取值为 1,$j(1\le j\le K)$条取值为 0,根据引理 2 的证明,取值为 1 的控制线可以忽略不计,对于 j 条取值为 0 的有效控制线,它们的作用等效于将所有与这 j 条控制线上有控制点的门从电路中移除,也就等价于一条特征向量为$(a_{0,0}\vee a_{1,0}\ldots\vee a_{j-1,0},a_{0,1}\vee\vee a_{1,1}\ldots\vee a_{j-1,1},a_{0,2}\vee a_{1,2}\ldots\vee a_{j-1,2},\ldots,a_{0,m-1}\vee a_{1,m-1}\ldots\vee a_{j-1,m-1})$ 的控制线,其中 $a_{x,y}$ 中的 x 表示第 x 条取值为 0 的控制线,y 表示控制线特征向量的第 y 个分量.若这条控制线也是模板的有效控制线,则对于 j 条取值为 0 的控制线,模板的受控线组成的电路实现的还是恒等函数功能,即这 K 控制线的取值不影响模板的恒等函数功能. □

根据命题 4,可以从类模板的控制线库中选取合适的控制线,同模板的受控线动态组合成模板,这时类模板控制线库的优势就体现出来.由于控制线库包含了模板所有的有效控制线,根据命题 1,在相同的模板规模下,类模板技术可以生成比 Maslov 更多的模板,这样就增加了模板匹配的几率,提高了匹配的成功率.

图 5 中的(a)是重构后的类模板 L9(a);(b)和(c)分别是 Maslov 的模板 9(a)和 9(b),它们是 10×10 的电路,(d)是通过我们的类模板技术生成的另一个新的模板,它是 13×13 的规模.显然这个新的模板可以简化多个 10×10 的电路(去掉其中的任意 3 根控制线),也就是说,相同规模下,重构后的模板可以生成多个新的模板,增加了模板匹配成功的概率.



(a) (b) (c) (d)

Fig.5 A schematic diagram of generating template (b),(c),(d) from (a)

图 5 由类模板(a)可以生成模板(b),(c),(d)的示意图

2.3 实验及其结果与标准数据的比较

采用国际流行的生成所有 3×3 量子可逆电路的实验(共计 $2^3!$=40,320 个函数)验证类模板的性能.实验进行两次,分别采用类模板技术和 Maslov 的模板进行量子电路匹配,其结果见表 2.其中,k 表示生成的可逆逻辑电路

中门的个数.A 表示采用 RM 合成法的迭代算法得到的结果;B 表示 A+采用类模板得到的结果;C 表示 A+采用 Maslov 等人的模板得到的结果;D:Pallav[13]的实验结果;E 表示 Agrawal[13]的实验结果;F 表示理想的结果[9].F 栏是标准数据.比较算法的优劣,除了时间因素外考察表格的每一行,应该是对应算法实验结果与标准数据差的绝对值越小越好.显然,类模板技术是有效的,其结果略好于模板技术,其关键在于类模板可以生成更多的模板用于简化电路.实验环境是 P4 3.0G+512MB 内存.其中,A 用了 3 小时,B 用了 9 小时,C 用了 5 小时.实验的同时也用迭代穷举算法(即穷举所有的因子)生成了 F 的结果,用了 40 小时.

Table 2 Experimental data

表 2 实验数据

k	A	B	C	D	E	F
9				36	30	
8	3 988	3 137	3 290	3 351	3 297	577
7	12 679	11 941	12 210	12 476	12 488	10 253
6	13 080	14 013	13 828	13 596	13 620	17 049
5	7 236	7 813	7 618	7 479	7 503	8 921
4	2 597	2 676	2 634	2 642	2 642	2 780
3	625	625	625	625	625	625
2	102	102	102	102	102	102
1	12	12	12	12	12	12
0	1	1	1	1	1	1
AVG	6.15	6.07	6.09	6.10	6.10	5.87

3 一种基于 Hash 表的算法

3.1 问题及解决的方案

从以上的讨论可以看出,量子可逆电路的自动生成和优化是一个较复杂的问题,关键在于一个 $n\times n$ 的可逆逻辑有 $2^n!$变换,若一个变换对应一个置换,则一切 2^n 次置换的集合就组成一个置换群.例如当 n=3 时,其置换群就有 $2^3!$=20430 个元素.一个最优的可逆逻辑设计系统,通常情况下需要考虑所有可能的情况,即在到达客户要求的条件下,使电路代价(规模与功耗)最小.

为了构建实用的经典量子信息仿真平台,提高各元素算法的效率是关键.在可逆逻辑综合上,我们提出了一种基于 Hash 表的算法.算法的内核是求给定 n 位量子比特全部置换的集合,结果生成一个量子门库;其次是基于量子门库求全部置换的优化逻辑门序列,结果构建出求最小长度用和求最小代价用的两棵多叉树;最后是基于两棵多叉树给出经典量子信息仿真平台中可逆逻辑优化设计模块.其中,为了提高量子门库的查询效率,我们研究了具有 $2^n!$个元素的置换群与整数集合{0,1,…,$2^n!$−1}之间的映射关系,给出了一个带有普遍性的构造简单的 1−1 的 Hash 函数;为了快速生成量子比特的全部置换(门库),我们提出了量子线拓扑变换的思想;构建了一个全新的高效量子可逆逻辑自动生成系统.

3.2 基于置换群上的Hash函数

从置换群元素 $X(a_0a_1...a_{2^n-1})$ 到整数 $Z\in\{0,1,...,2^n!-1\}$ 的映射函数描述如下:

$$H(X)::f\left(\underbrace{a_0a_1...a_{2^n-1}}_{X\text{的二进制表示}}\right)=bn(a_0)\cdot 0!+bn(a_1)\cdot 1!+...+bn(a_{2^n-1})\cdot(2^n-1)!=\sum_{i=1}^{2^n-1}\left(\sum_{j=0}^{i-1}\mathrm{sgn}(a_j-a_i)\right)\cdot i!,$$

其中,$bn(a_i)$为 a_i 的逆序数,即比 a_i 大且排在 a_i 前面的元素 $a_j\{0\le j<i\}$的个数,则

$$bn(a_i)=\sum_{j=0}^{i-1}\mathrm{sgn}(a_j-a_i),\text{其中}\mathrm{sgn}(x)=\begin{cases}1,x>0\\0,x<0\end{cases}.$$

因为

$$\min\{H(X)\}=\min\left(\sum_{i=1}^{2^n-1}\left(\sum_{j=0}^{i-1}\mathrm{sgn}(a_j-a_i)\right)i!\right)\geq\sum_{i=1}^{2n-1}\min\left(\sum_{j=0}^{i-1}\mathrm{sgn}(a_j-a_i)\right)i!=\sum_{i=1}^{2^n-1}0*i!=0,$$

$$\max\{H(X)\}=\max\left(\sum_{i=1}^{2^n-1}\left(\sum_{j=0}^{i-1}\mathrm{sgn}(a_j-a_i)\right)i!\right)\leq\sum_{i=1}^{2^n-1}\max\left(\sum_{j=0}^{i-1}\mathrm{sgn}(a_j-a_i)\right)i!=\sum_{i=1}^{2^n-1}i*i!=2^n!-1.$$

所以 $0\leq H(x)\leq 2^n!-1$.显然若 $X_i(a_{i0}a_{i1}...a_{i2^n-1})\neq X_j(a_{j0}a_{j1}...a_{j2^n-1})f$ 时,一定有 $H(X_i)\neq H(X_j)$,因为它们的逆序数一定不相等,所以置换与整数在此 Hash 函数下是 1 对 1 的.即如果一个 n=3,元素个数为 2^3=8 的置换为 $\sigma\begin{pmatrix}0&1&2&3&4&5&6&7\\7&6&5&4&3&2&1&0\end{pmatrix}$,则 Hash 函数值为

$$H(X)::f\left(\underbrace{76543210}_{X\text{的二进制表示}}\right)=bn(7)\cdot 0!+bn(6)\cdot 1!+...+bn(0)\cdot 7!$$

$$=0\cdot 0!+1\cdot 1!+2\cdot 2!+...+7\cdot 7!=1+4+18+...+35280=40320-1=2^3!-1.$$

因此,该函数将 $2^n!$个元素映射到 $0\sim 2^n!-1$ 连续的整数上.

3.3 量子门库的构造

一般论著在求解量子门的全部置换时,通常采用固定量子线、移动量子门的处理方法,此类方法计算冗余且复杂.构造量子门库时必须求解全部置换,我们采用量子线拓扑思想,将量子门移动变成量子线变换,即计算量子线之间不同顺序的置换.此方法可以高效地求解量子门的全部置换,从而高效地构造完整的量子门库.以 n=3 为例,图 6 给出了任意给定的量子门,求解其全部置换,构造量子门库算法过程的图解,实际算法如下:

任一量子门拓扑结构图到输入/输出的真值表.

真值表输入/输出对应列全排序(即量子线顺序全排序)得 $n!$真值表.

将 $n!$真值表按输入值从小到大排序,得到最终的 $n!$真值表,从而生成 $n!$个置换,去除重复置换,就得到当前量子门的全部置换.

所有量子门的全部置换即构成量子门库.

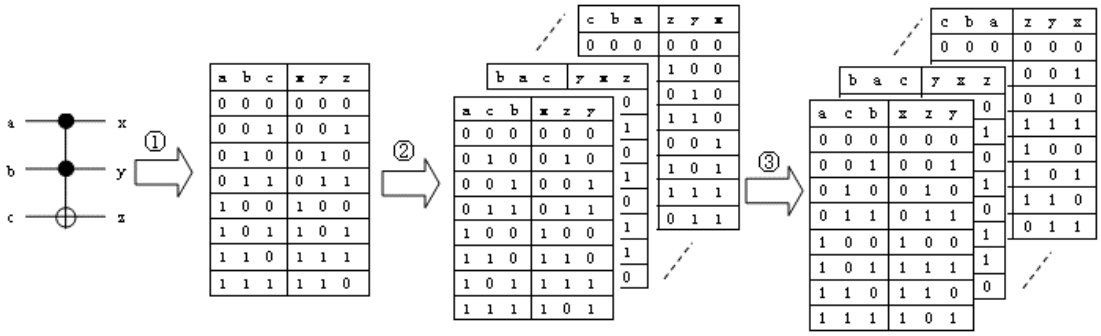


Fig.6 Sorting quantum line to get all the permutations of an arbitrary quantum gate

图 6 采用量子线排序求解任意量子门全部置换的图解

输入:任意给定基本量子门的某种置换构成的集合 L'.

输出:所有量子门的全部置换的集合 L,即所求的量子门库.

$L=\varnothing$

设量子电路有 n 条量子线,即有 n 个输入变量与 n 个输出变量,每个向量共有 n 种全排列.

for all p' in L' do

for $i=1$ to $n!$ do

置换 p'执行①,②,③步骤即可得到新置换 p;

$L=L\cup p$;

end for

end for

3.4 求最小长度可逆电路的算法QML(quantum circuits with minimum length)

算法设可逆电路有 n 条量子线;量子门库有 m 个不同量子门 $\{G_1,G_2,...,G_m\}$,即 m 个不同的置换规则;算法要求可重复地任选若干个量子门进行级联,构成的电路分别实现全部不同的置换;算法的输出要求得到的每个可逆电路的量子门数量最少(即长度最短).

设每个电路的置换为 σ,其 Hash 值为 $H(\sigma)$.构造值为 $\{0,1,2,...,2^n!-1\}$ 的 Hash 表,分别存放 $2^n!$个不同的 Hash 值.算法从仅需 1 个量子门的电路开始,依次试探 m 个不同的量子门,即 m 个不同的置换规则,将电路的输出值对应的置换生成 Hash 值,并写入到 Hash 表中.显然,1 个量子门一定是最优的.设 D^L 表示所有长度为 L 的电路集合: $D^L=\{d_1^L,d_2^L,...,d_k^L\}$, $\forall d_j^L\in D^L$,$1\le j\le k$ 且 $d_j^L\equiv\sigma_j^L$;则长度为 L+1 的电路集合 $D^{L+1}=\{d_1^{L+1},d_2^{L+1},...,d_t^{L+1}\}$ 的生成方法是,在长度为 L 的电路的后面分别级联上 m 个不同量子门中的一个进行试探,即 $d_p^{L+1}=d_j^L\times G_i$,$1\le j\le k$,$1\le i\le m$,

$$\sigma_p^{L+1}=\sigma_j^L\times\sigma_i=\begin{pmatrix}0&1&...&7\\x_0^j&x_1^j&...&x_7^j\end{pmatrix}\times\begin{pmatrix}0&1&...&7\\y_0^i&y_1^i&...&y_7^i\end{pmatrix}=\begin{pmatrix}0&1&...&7\\z_0^p&z_1^p&...&z_7^p\end{pmatrix}.$$

再将得到的置换 σ_p^{L+1} 转变为 Hash 值,检测 Hash 表中项 $H\left(\sigma_p^{L+1}\right)$ 的“登录否”属性数据,如果为“F”,则写入数据,否则说明在此之前一定存在置换相同,且长度不大于当前长度的量子电路,因为算法是按电路长度从小到大依次生成,所以可以丢弃此结果.依此类推,直至电路试探全部量子门的 Hash 值都存在于 Hash 表中,其算法中 Hash 表变化示意图如图 7 所示(注:表栏目“节点指针”中的标记 *Zt* 表示指向图 9 的多叉树中的某一个叶节点).

Hash value	Login	Pointer
0	F	Null
1	F	Null
2	F	Null
…		
…		
40319	F	Null

⇒

Hash value	Login	Pointer
0	T	→
1	T	→
…		
i	T	→(Zt)
…		
40319	F	→

Fig.7 A schematic diagram of calculating Hash table of mini-length reversible logic circuit

图 7 求最小长度可逆逻辑电路 Hash 表的计算示意图

3.5 求最小代价可逆电路的算法QMC(quantum circuits with minimum cost)

实践已知采用不同技术实现的量子门其代价不相同;采用相同技术实现不同类型的量子门其代价也不相同.如在实验中广泛使用核磁共振技术制造的常用量子门 NOT,CNOT,Peres,Toffoli,Fredkin 的量子代价就分别为 0,1,4,5,5.显然,若假设每个量子门的代价均为 1 时,最小长度就成为最小代价的特殊情况.在算法 QML 基础上,基于任意给定的一组量子代价,我们给出了最小代价可逆电路的生成算法 QMC.QMC 先将 Hash 表中每个节点的“代价”数据项初始化为无穷大,利用 QML 方法依次试探量子门,同时计算当前量子电路的代价值,并与该电路在 Hash 表中对应节点的量子代价比较,若是严格小于,则将当前电路最后试探的量子门覆盖 Hash 表中对应节点的量子门数据项,否则放弃.不断试探量子门,直至试探的每个量子门全部被放弃为止,从而生成了全部最小代价的量子电路,并按量子代价统计量子电路数量,其结果如图 8 所示.与文献[12]提出的直接求出最小代价量子电路的算法相比,QMC 在时空效率上都有很大的提高.

Hash value	Cost	Pointer
0	∞	Null
1	∞	Null
2	∞	Null
…		
…		
40319	∞	Null

⇨

Hash value	Cost	Pointer
0	J_0	→
1	J_1	→
…		
i	J_i	→(Zt)
…		
40319	J_{40319}	→

Fig.8 A schematic diagram of calculating Hash table of mini-cost reversible logic circuit

图 8 求最小代价可逆逻辑电路 Hash 表的计算示意图

3.6 求可逆逻辑电路综合的通用算法QGA(general algorithm of quantum circuits)

在 QML 与 QMC 基础上,可逆逻辑电路综合通用算法就显得非常简单.算法 QML 与 QMC 的运行结果已构建完一棵多叉树(如图 9 所示),其中包含了全部 n 变量的最优量子电路.通用算法将根据所求量子电路的置换σ,计算 $H(\sigma)$,通过“节点指针(Pointer)”项找到树中对应节点,该节点的 $G–k(1\le k\le m)$就是所求电路的最后一个量子门;再根据该节点的 *prev* 数据项找到其父节点,父节点的 $G–k$ 项是与该门级联的前一个量子门;依次计算直至达到根节点,将经过的全部量子门逆序级联,就是所求的量子可逆逻辑电路.基于 QML 的 QGA 算法可以描述如下:

输入:量子门库 L 和置换 p.

输出:满足置换 p 的最短长度可逆电路的量子门序列.

Call QML(L),生成Hash$\left[0..2^n-1\right]$

$iKey=H(p), j=0$

if $not 0\le iKey\le 2^n-1$ then return false

while $iKey\ne -1$ do

$Gate\left[j\right]=Hash\left[iKey\right].gate,\ \ iKey=Hash\left[iKey\right].prev$

endwhile

return $Gate\left[j-1\right],Gate\left[j-2\right],...,Gate\left[0\right]$

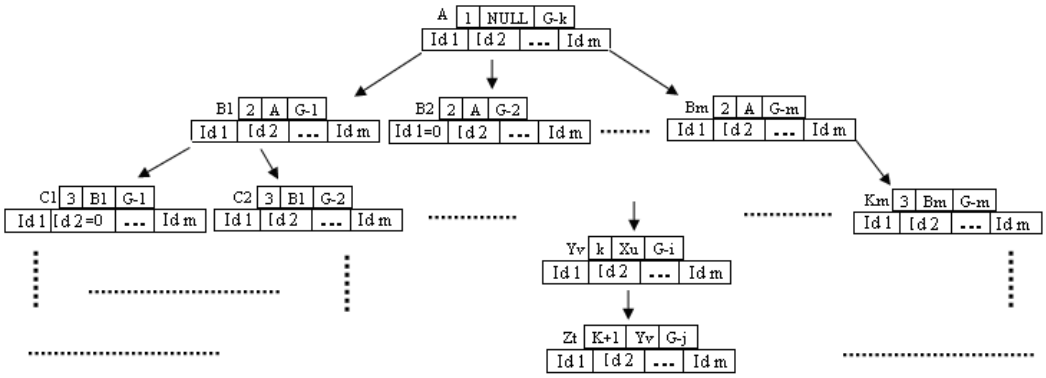


Fig.9 Structure diagram of the minimum length (cost) multi-tree created by OML (OML)

图 9 一棵由算法 QML(QMC)生成的最小长度(代价)多叉树的逻辑结构图

3.7 基于Hash函数综合算法的实验及其结果分析

在 Hash 函数和量子可逆逻辑门库技术及相关数据结构的支撑下,量子可逆逻辑综合算法的性能得以极大地提高.以国际同行认可的 3 变量可逆函数测试标准,在同等环境下,我们的算法按最小长度和最小代价标准测试,分别是目前最好结果[10,14]平均值的 25.06 倍和 186.14 倍(见表 3 和表 4.表 4 中,表中第 1 行的英文字母分别为 N:NOT 门;C:CNOT 门;T:Toffoli 门;P:Peres 门;F:Fredkin 门.表中倒数第 2 行的“文献时间”为文献[10,14]中的

实验在同等环境下的运行时间(s)).

Table 3 Number of quantum circuits with minimum length *K*

表 3 最小长度为 *K* 的量子电路的数量

k	NC	NCT	NCP	NCF	NCPT	NCTF	NCPF	NCTPF
0	1	1	1	1	1	1	1	1
1	9	12	15	12	18	15	18	21
2	51	102	174	101	228	143	248	281
3	187	625	1 528	676	1 993	1 006	2 356	2 551
4	393	2 780	8 968	3 413	10 503	5 021	12 797	13 181
5	474	8 921	23 534	11 378	23 204	15 083	22 794	22 323
6	215	17 049	6 100	17 970	4 373	17 261	2 106	1 962
7	14	10 253	0	6 739	0	1 790	0	0
8	0	577	0	30	0	0	0	0
Total	1 344	40 320	40 320	40 320	40 320	40 320	40 320	40 320
AVG len	4.47	5. 87	4.84	5.66	4.73	5.33	4.6	4.57
MAX len	7	8	6	8	6	7	6	6
Time (s)	0.011	0.378	0.47	0.384	0.557	0.466	0.556	0.634
Ref. [10] time	Null	12	10	13	10	12	11	Null
Ratio	Null	31.75	21.28	33.85	17.95	25.75	19.78	Null

Table 4 Number of quantum circuits with minimum cost *K*

表 4 最小代价为 *K* 的量子电路的数量

k	NC	NCT	NCP	NCF	NCPT	NCTF	NCPF	NCTPF
0	8	8	8	8	8	8	8	8
1	48	48	48	48	48	48	48	48
2	192	192	192	192	192	192	192	192
3	408	408	408	408	408	408	408	408
4	480	480	672	480	672	480	672	672
5	192	288	1 248	288	1 248	384	1 344	1 344
6	16	592	3 184	880	3 184	1 072	3 568	3 568
7	0	2 016	4 320	3 008	4 320	3 104	3 968	3 968
8	0	4 128	3 552	3 904	3 552	3 808	3 424	3 424
9	0	2 496	11 520	1 440	11 520	1 248	11 520	11 520
10	0	672	4 416	416	4 416	1 856	4 416	4 416
11	0	2 880	0	4 608	0	6 720	0	0
12	0	7 488	9 856	10 432	9 856	7 552	9 856	9 856
13	0	7 488	896	3 456	896	2 688	896	896
14	0	384	0	0	0	0	0	0
15	0	1 600	0	0	0	6 784	0	0
16	0	5 568	0	4 608	0	3 840	0	0
17	0	3 584	0	6 144	0	128	0	0
Total	1 344	40 320	40 320	40 320	40 320	40 320	40 320	40 320
AVG cost	3.45	11.98	9.08	11.87	9.08	11.38	9.06	9.06
MAX cost	6	17	13	17	13	17	13	13
Time (s)	0.015	0.511	0.762	0.497	0.97	0.639	1.002	1.168
Ref.[10] time	Null	112	111	123	126	159	126	Null
Ratio	Null	219.18	145.67	247.48	129.9	248.83	125.75	Null

4 结 论

本文针对可逆逻辑综合的关键技术及其实现方法进行了探讨,提出了类模板思想和基于 Hash 函数的一类快速算法.采用在相同的实验环境下,以国际认可的 3 变量可逆函数测试标准验证了这些方法.结果表明,基于 Hash 函数的一类快速算法按最小长度和最小代价标准测试,分别是目前最好结果[10,14]的 25.06 倍和 186.14 倍.类模板思想是一种方法、Hash 函数的构造具有一般性意义,基于上述思想,在改进 Hash 函数计算方法的基础之上,我们相信量子门库方法以及 QML 算法和 QMC 算法将会在量子可逆逻辑门综合中发挥更多的作用.显然,这些结论对我们下一步的研究有重要意义.

References:

[1] Shende VV, Prasad AK, Markov IL, Hayes JP. Reversible logic circuit synthesis. In: Proc. of the Int'l Conf. on Computer-Aided Design. 2002. 125−132. http://portal.acm.org/citation.cfm?id=774572.774625

[2] Song X, Yang G, Perkowski M, Wang Y. Algebraic characteristics of reversible gates. Theory of Computing Systems, 2006,39:311−319.
[3] Iwama K, Kambayashi Y, Yamashita S. Transformation rules for designing CNOT-based quantum circuits. Proc. of the Design Automation Conf., 2002,28(4):419−424.
[4] Miller D M. Spectral and two-place decomposition techniques in reversible logic. In: Proc. of the 45th IEEE Int'l Midwest Symp. on Circuits and Systems. 2002. 493−496. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.130.3502&rep= rep1&type=pdf
[5] Miller DM, Maslov D, Dueck GW. A transformation based algorithm for reversible logic synthesis. Proc. of the DAC, 2003,20(1): 318−323.
[6] Maslov D, Dueck GW, Miller DM. Toffoli network synthesis with templates. IEEE Trans. on Computer-Aided Design Integrated. Circuits Systems, 2005,24(6):807−817.
[7] Mishchenko A, Perkowski M. Logic synthesis of reversible wave cascades. In: Proc. of the 11th IEEE Int'l Workshop on Logic Synthesis. 2002. 197−202. http://www.eecs.berkeley.edu/~brayton/publications/2002/iwls02_casc.pdf
[8] Gupta P, Agrawal A, Jha NK. An algorithm for synthesis of reversible logic circuits. IEEE Trans. on Circuits and Systems-I, 2006,25(11):807−817.
[9] Shende VV, Prasad AK, Markov IL, Hayes JP. Synthesis of reversible logic circuits. IEEE Trans. on CAD, 2003,22(6):723−729.
[10] Yang GW, Song XY, Perkowski M, Hung WNN. Fast synthesis of exact minimal reversible circuits using group theory. In: Proc. of the IEEE ASP-DAC 2005, Vol.2. 2005. 18−21.
[11] Dueck GW, Maslov D. Reversible function synthesis with minimum garbage outputs. In: Proc. of the 6th Int'l Sym. on Representations and Methodology of Future Computing Technology. 2003. 154−161. http://www.cs.unb.ca/profs/gdueck/reversible/synthesis.pdf
[12] Miller DM, Dueck GW. Spectral techniques for reversible logic synthesis. In: Proc. of the 6th Int'l Symp. on Representations and Methodology of Future Computing Technology. 2003. 56−62. http://web.cecs.pdx.edu/~mperkows/temp/March17/spectral.pdf
[13] Agrawal A, Jha NK. Synthesis of reversible logic. In: Proc. of the Design, Automation and Test in Europe Conf. and Exhibition (DATE 2004). 2004. 1384−1385. http://portal.acm.org/citation.cfm?id=968879.969118
[14] Dueck GW, Maslov D, Miller DM. Transformation-Based synthesis of networks of Toffoli/Fredkin gates. In: Proc. of the IEEE Canadian Conf. on Electrical and Computer Engineering (IEEE CCECE 2003). 2003. 211−214. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1226380
[15] Maslov D, Dueck GW, Miller DM. Fredkin/Toffoli templates for reversible logic synthesis. In: Proc. of the 2003 IEEE/ACM Int'l Conf. on Computer-Aided Design. Washington: IEEE Computer Society 2003. 256−261. http://portal.acm.org/citation.cfm?id=996070.1009900
[16] Maslov D, Dueck GW, Miller DM. Simplification of Toffoli networks via templates. In: Proc. of the 16th Symp. on Integrated Circuits and Systems Design. Washington: IEEE Computer Society, 2003. 53−58. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1232806
[17] Maslov D, Young C, Miller DM, Dueck GW. Quantum circuit simplification using templates. In: Proc. of the Conf. on Design, Automation and Test in Europe (DATE 2005). Washington: IEEE Computer Society, 2005. 1208−1213. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1395758
[18] Maslov D, Miller DM, Dueck GW. Techniques for the synthesis of reversible Toffoli networks. http://www.cs.uvic.ca/~dmaslov/papers/tr1.pdf

李志强(1974－),男,江苏扬州人,博士生,讲师,主要研究领域为量子信息与计算,量子可逆逻辑综合.

陈汉武(1955－),男,博士,教授,博士生导师,主要研究领域为经典信息理论,量子信息与计算.

李文骞(1979－),男,助教,主要研究领域为量子信息与计算,量子可逆逻辑优化.