基于新型量子逻辑门库的最优NCV三量子电路快速综合算法

李志强[1],陈汉武[2],刘文杰[2],薛希玲[2],肖芳英[2]
(1.扬州大学信息工程学院,江苏扬州 225009;2.东南大学计算机科学与工程学院,江苏南京 210096)

摘 要: 许多量子电路综合算法由于指数级时间与空间复杂度,只能用可逆逻辑门综合3量子逻辑电路,仅有少数算法实现用量子非门,控制非门,控制V门与控制V+门(NCV)综合3量子逻辑电路,主要方法是将电路综合问题简化为四值逻辑综合问题.本文提出用NCV门构造新型量子逻辑门库,该库与NCV门库在综合最优3量子逻辑电路上等价,因此又可将四值逻辑综合问题进一步简化为更易求解的二值逻辑综合问题,使用基于完备Hash函数的3量子电路快速综合算法,快速生成全部最优的3量子逻辑电路,以最小代价综合电路的平均速度是目前最好结果Maslov 2007的近127倍.

关键词: 可逆逻辑; NCV门库; 多值逻辑; 完备Hash函数; 量子代价
中图分类号: TN911.23 **文献标识码:** A **文章编号:** 0372-2112 (2013)04-0690-08
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.04.011

Efficient Algorithm for Synthesis of Optimal NCV 3-Qubit Reversible Circuits Using New Quantum Logic Gate Library

LI Zhi-qiang[1], CHEN Han-wu[2], LIU Wen-jie[2], XUE Xi-ling[2], XIAO Fang-ying[2]
(1. *College of Information Engineering, Yangzhou University, Yangzhou, Jiangsu* 225009, *China*;
2. *School of Computer Science and Engineering, Southeast University, Nanjing, Jiangsu* 210096, *China*)

Abstract: Owing to the exponential nature of the memory or run-time complexity, many existing methods can only synthesize 3-qubit logic circuits using quantum logic gate library, however, a few can optimally synthesize 3-qubit logic circuits for quantum NOT, CNOT, Controlled-V and Controlled-V + (NCV) gates, the key approach reduces the NCV quantum circuit synthesis problem to four-valued logic synthesis. This paper proposes using NCV gates to create a new quantum logic gate library, which is exactly the same as NCV gate library in the synthesis of all optimal 3-qubit circuits, thus it also reduces the four-valued logic synthesis to easily solved two-valued logic synthesis. We present a 3-qubit efficient synthesis algorithms based on perfect hash function, which can quickly construct all optimal 3-qubit circuits--the average speed that synthesizes circuits with minimum cost is nearly 127 times faster than that of the best result of Maslov 2007.

Key words: reversible logic; NCV gate library; multiple-valued logic; perfect hash function; quantum cost

1 引言

量子计算机可等效一个量子图灵机,量子图灵机可等价一个量子逻辑电路.量子逻辑门的组合与级联是组成量子计算机的基本元素.30年来,人们已经提出了多种量子门,如控制非门[1]、Toffoli门、Fredkin门[2]、Peres门等量子逻辑门,每条量子线的输入与输出值均为二元基态.还有如控制V门、控制V+门等量子非逻辑门[2],当每条量子线的输入均为二元基态时,输出却可能是叠加态.如何用指定量子门,自动生成代价最小的量子电路,其本质是可逆逻辑综合问题.为此人们做了大量研究,并提出许多基于量子逻辑门的3量子综合算法[3~7],而基于量子非逻辑门的综合算法并不多,目前有几种基于NCV的综合算法[8~11],尽管已提出多种4量子综合算法[12~14],但还是基于量子逻辑门的.综合NCV的主要方法是根据控制V门与控制V+门的特点,将量子电路综合问题简化为四值逻辑综合问题,而基于可逆逻辑门的综合算法可简化为二值逻辑综合问题,对

收稿日期:2011-04-06;修回日期:2012-11-07
基金项目:国家自然科学基金(No.61070240,No.60572071,No.61170321);江苏省高校自然科学基金(No.10KJB520021)

于 n 量子电路而言,前者生成量子电路的功能共有 $4^n!$ 种,而后者却仅有 $2^n!$ 种,如当 $n=3$ 时,$4^n|_{n=3}=1.269\times10^{89}$,$2^n!\ |_{n=3}=40320$,显然前者的解空间远大于后者,但所求全部 n 量子逻辑电路共有 $2^n!$ 种,前者还需从 $4^n!$ 种量子电路中筛选出 $2^n!$ 种所求的量子逻辑电路,因此前者算法效率远低于后者,若能将四值逻辑综合问题简化为更易求解的二值逻辑综合问题,必然会大幅度提高算法效率.经研究发现,先用 NCV 门库生成 Peres 门和三种类似 Peres 门的新型量子逻辑门,与非门、控制非门一起构成新型量子逻辑门库(NCP4),令人惊喜的是 NCP4 门库与 NCV 门库可构造出完全等价的全部最优 3 量子逻辑电路,即由两方法生成的功能相同的电路的代价相同,但构造方法不尽相同,可称这两个量子门库在综合 3 量子逻辑电路时等价.基于置换群理论与逻辑计算技术,采用位运算构造完备的 Hash 函数[5],提出了基于 Hash 表的量子可逆逻辑电路综合算法,可使用与量子门库 NCV 等价的 NCP4 门库,采用多种量子代价标准,以高效生成基于 NCV 的全部最优的 3 量子逻辑电路.实验结果表明,该算法在同等计算环境下,按各种量子代价标准综合电路的平均速度是目前最好结果[10]的近 127 倍.

2　量子逻辑电路的基本概念

利用微观粒子状态表示的信息称为量子信息,量子信息的基本单位是量子比特(qubit),与经典信息不同,量子比特能以叠加态的形式存在.任何量子比特均可由一个二元向量形式表示,形式为 $|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle$,用向量可写为 $|\Psi\rangle=\alpha\begin{pmatrix}0\\1\end{pmatrix}+\beta\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}\alpha\\\beta\end{pmatrix}$,其中 $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$,$|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$,$\alpha$ 和 β 为复数,满足归一化条件:$|\alpha|^2+|\beta|^2=1$.

量子门是处理量子信息的基本单元,它的级联构成量子电路,量子电路是可逆的.量子计算中,一个量子门对应一个幺正变换,根据输入输出的对数,量子门可分为单量子比特门与多量子比特门.

定义 1　单量子通用门,记为 $\boldsymbol{U}$.见图 1,其单量子酉操作可用矩阵表示为 $\boldsymbol{U}=\begin{pmatrix}u_{00}&u_{01}\\u_{10}&u_{11}\end{pmatrix}$,该复矩阵有如下性质:$\boldsymbol{U}\times\boldsymbol{U}^{\dagger}=\boldsymbol{U}^{\dagger}\times\boldsymbol{U}=\boldsymbol{I}$,其中 $\boldsymbol{I}$ 为单位矩阵,$\boldsymbol{U}^{\dagger}$ 为矩阵 $\boldsymbol{U}$ 的共轭转置,即 $\boldsymbol{U}^{\dagger}=(\boldsymbol{U}^{\mathrm{T}})^{*}$,即对 $\boldsymbol{U}$ 先转置再取复共轭.如量子非门,见图 1,可用矩阵定义为 $\boldsymbol{U}=\boldsymbol{N}=\begin{pmatrix}0&1\\1&0\end{pmatrix}$.当该门输入 $|\Psi\rangle$ 后,输出为 $\boldsymbol{N}_{\Psi}=\boldsymbol{N}\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\begin{pmatrix}\beta\\\alpha\end{pmatrix}$.量子 $\boldsymbol{V}$ 门、$\boldsymbol{V}^{+}$ 门用矩阵分别定义为 $\boldsymbol{U}=\boldsymbol{V}=\frac{1+i}{2}\cdot\begin{pmatrix}1&-i\\-i&1\end{pmatrix}$,$\boldsymbol{U}=\boldsymbol{V}^{+}=\frac{1-i}{2}\begin{pmatrix}1&i\\i&1\end{pmatrix}$,可得 $\boldsymbol{V}\boldsymbol{V}^{+}=\boldsymbol{V}^{+}\boldsymbol{V}=\boldsymbol{I}$,$\boldsymbol{V}\boldsymbol{V}=\boldsymbol{V}^{+}\boldsymbol{V}^{+}=\boldsymbol{N}$,因此 $\boldsymbol{V}$ 门与 $\boldsymbol{V}^{+}$ 门也称为平方根非门.显然 $\boldsymbol{N}$ 门与 $\boldsymbol{CN}$ 门为量子逻辑门,$\boldsymbol{CV}$ 门与 $\boldsymbol{CV}^{+}$ 门为量子非逻辑门.

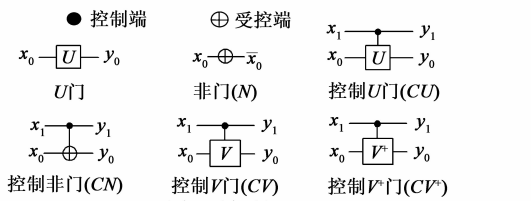

图1　量子门

引理 1　二量子通用控制 $\boldsymbol{U}$ 门,记为 $\boldsymbol{CU}$.见图 1,其输入的控制端、受控端分别为 x^1、x^0,输出的控制端、受控端分别为 y^1、y^0,设 $x^1\in\{|0\rangle,|1\rangle\}$,得 $y^1\equiv x^1$,若 $x^1=|1\rangle$,$y^0=\boldsymbol{U}x^0$,否则 $y^0=x^0$.因此 $\boldsymbol{CU}$ 门的功能可用 $|c\rangle|t\rangle\rightarrow|c\rangle\boldsymbol{U}^{c}|t\rangle$ 表示,其中 $\boldsymbol{U}^0=\boldsymbol{I}$,$\boldsymbol{U}^1=\boldsymbol{U}$.

证明　已知 $\boldsymbol{CU}$ 门可用矩阵定义为 $\boldsymbol{CU}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&u_{00}&u_{01}\\0&0&u_{10}&u_{11}\end{pmatrix}$.当输入端 $x_1=|1\rangle$,$x_0=|\Psi\rangle$ 时,输入值可用向量的张量积表示为 $|1\rangle|\Psi\rangle=\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}\alpha\\\beta\end{pmatrix}=(0\quad0\quad\alpha\quad\beta)^{-1}$,则输出值为:$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&u_{00}&u_{01}\\0&0&u_{10}&u_{11}\end{pmatrix}\begin{pmatrix}0\\0\\\alpha\\\beta\end{pmatrix}=\begin{pmatrix}0\\0\\u_{00}\alpha+u_{01}\beta\\u_{10}\alpha+u_{11}\beta\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}\otimes\left(\begin{pmatrix}u_{00}&u_{01}\\u_{10}&u_{11}\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix}\right)=|1\rangle\boldsymbol{U}|\Psi\rangle=|1\rangle\boldsymbol{U}^{1}|\Psi\rangle$.

同理,当 $x_1=|0\rangle$,$x_0=|\Psi\rangle$ 时,输出值为:$|1\rangle|\Psi\rangle=|1\rangle\boldsymbol{U}^{0}|\Psi\rangle$,显然以上命题成立.

当 $\boldsymbol{CU}$ 门中 $\boldsymbol{U}=\boldsymbol{V}$ 或 $\boldsymbol{U}=\boldsymbol{V}^{+}$ 时,则为控制 $\boldsymbol{V}$ 门($\boldsymbol{CV}$)与控制 $\boldsymbol{V}^{+}$ 门($\boldsymbol{CV}^{+}$),见图 1,也称为控制平方根非门.

命题 1　设 $\boldsymbol{CU}$ 门的任意输入值不发生纠缠,惟有当控制端的输入值为 $|0\rangle$ 或 $|1\rangle$ 时,输出值也不发生纠缠.其中,量子纠缠是一种量子力学现象,其定义上描述复合系统(具有两个以上成员系统)特殊的量子态,此量子态无法分解为成员系统各自量子态的张量积.如 $(|01\rangle+|10\rangle)/\sqrt{2}$ 无法写成两个量子比特的张量积.

证明　设任意控制量子门 $\boldsymbol{CU}$,见图 1,当 $x_1=|\Psi_1\rangle$,$x_0=|\Psi_0\rangle$ 时,输入 $\boldsymbol{P}_{\mathrm{in}}=|\Psi_1\rangle|\Psi_0\rangle=\begin{pmatrix}\alpha_1\\\beta_1\end{pmatrix}\otimes\begin{pmatrix}\alpha_0\\\beta_0\end{pmatrix}=$

$\begin{pmatrix}\alpha_1\alpha_0\\ \alpha_1\beta_0\\ \beta_1\alpha_0\\ \beta_1\beta_0\end{pmatrix}$，则输出 $\boldsymbol{P}_{\text{out}}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&u_{00}&u_{01}\\0&0&u_{10}&u_{11}\end{pmatrix}\begin{pmatrix}\alpha_1\alpha_0\\ \alpha_1\beta_0\\ \beta_1\alpha_0\\ \beta_1\beta_0\end{pmatrix}=\begin{pmatrix}\alpha_1\alpha_0\\ \alpha_1\beta_0\\ \beta_1\alpha_0u_{00}+\beta_1\beta_0u_{01}\\ \beta_1\alpha_0u_{10}+\beta_1\beta_0u_{11}\end{pmatrix}=\begin{pmatrix}\alpha_1\begin{pmatrix}\alpha_0\\ \beta_0\end{pmatrix}\\ \beta_1\begin{pmatrix}\alpha_0u_{00}+\beta_0u_{01}\\ \alpha_0u_{10}+\beta_0u_{11}\end{pmatrix}\end{pmatrix}$.

若该门输出不发生纠缠，则 $\boldsymbol{P}_{\text{out}}$可写成两个量子比特张量积的形式. 由于 $\begin{pmatrix}u_{00}&u_{01}\\u_{10}&u_{11}\end{pmatrix}\begin{pmatrix}\alpha_0\\ \beta_0\end{pmatrix}=\begin{pmatrix}\alpha_0u_{00}+\beta_0u_{01}\\ \alpha_0u_{10}+\beta_0u_{11}\end{pmatrix}$，根据归一化条件，得 $|\alpha_0|^2+|\beta_0|^2=1$，$|\alpha_0u_{00}+\beta_0u_{01}|^2+|\alpha_0u_{10}+\beta_0u_{11}|^2=1$，因此，$\alpha_0$ 与 β_0 不可能同时为 0，同样 $\alpha_0u_{00}+\beta_0u_{01}$与 $\alpha_0u_{10}+\beta_0u_{11}$也不可能同时为 0，因此 $\boldsymbol{P}_{\text{out}}$写成两个量子比特张量积的形式只可能有三种情况.

(1) 当 $\alpha_1=0$，则 $\beta_1=1$，得 $\boldsymbol{P}_{\text{out}}=\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}\alpha_0u_{00}+\beta_0u_{01}\\ \alpha_0u_{10}+\beta_0u_{11}\end{pmatrix}$.

(2) 当 $\beta_1=0$，则 $\alpha_1=1$，得 $\boldsymbol{P}_{\text{out}}=\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}\alpha_0\\ \beta_0\end{pmatrix}$.

(3) 当$\begin{pmatrix}\alpha_0\\ \beta_0\end{pmatrix}$与$\begin{pmatrix}\alpha_0u_{00}+\beta_0u_{01}\\ \alpha_0u_{10}+\beta_0u_{11}\end{pmatrix}$对应成比例，即 $\exists k\neq 0$，$\alpha_0k=\alpha_0u_{00}+\beta_0u_{01}$，$\beta_0k=\alpha_0u_{10}+\beta_0u_{11}$，则 $\boldsymbol{P}_{\text{out}}=\begin{pmatrix}\alpha_1\\ k\beta_1\end{pmatrix}\begin{pmatrix}\alpha_0\\ \beta_0\end{pmatrix}$，又因为 $\alpha_1^2+\beta_1^2=1$ 且 $\alpha_1^2+k^2\beta_1^2=1$，得 $k=1$，因此 $\alpha_0=\alpha_0u_{00}+\beta_0u_{01}$，$\beta_0=\alpha_0u_{10}+\beta_0u_{11}$，则 $\boldsymbol{P}_{\text{out}}=\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}\begin{pmatrix}\alpha_0\\ \beta_0\end{pmatrix}=|\Psi_1\rangle|\Psi_0\rangle=\boldsymbol{P}_{\text{in}}$，得 $\boldsymbol{CU}$ 为单位矩阵，即为恒等电路，与量子门定义不符，因此该情况不可能. 所以只有当 $\alpha_1=0$ 或 $\beta_1=0$ 时，即控制端的输入值为$|0\rangle$或$|1\rangle$时，输出信息才不发生量子纠缠.

量子逻辑电路要求输入与输出均为逻辑值，即每条量子线的输入与输出为$|1\rangle$或$|0\rangle$，显然输入与输出值不发生纠缠，当量子逻辑电路内部发生纠缠时，电路中的信息变得复杂，即有从非纠缠变为纠缠，最终变为非纠缠的过程，在综合电路的过程中，只要满足命题 1 的要求，就能完全避免发生纠缠，从而简化了综合过程，通过大量实验发现，最优的量子逻辑电路中都不发生纠缠，但该命题尚未能到理论上的严格证明.

命题 2 在最优的 NCV 量子逻辑电路中，若电路的每条量子线上的输入是$|0\rangle$或$|1\rangle$，即输入为逻辑值，则电路中任意量子线上的值只可能有 4 种.

证明 当 $\boldsymbol{V}$ 门输入分别为$|0\rangle$、$|1\rangle$，输出分别为 $\boldsymbol{V}_0=\frac{1+i}{2}\begin{pmatrix}1&-i\\-i&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\frac{1+i}{2}\begin{pmatrix}1\\-i\end{pmatrix}$、$\boldsymbol{V}_1=\frac{1+i}{2}\cdot\begin{pmatrix}-i\\1\end{pmatrix}$，当 $\boldsymbol{V}^+$门输入分别为$|0\rangle$、$|1\rangle$，输出分别为 $\boldsymbol{V}_0^+=\frac{1-i}{2}\begin{pmatrix}1&i\\i&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\boldsymbol{V}_1$、$\boldsymbol{V}_1^+=\boldsymbol{V}_0$；当 $\boldsymbol{V}_0$ 分别经过非门、$\boldsymbol{V}$ 门或 $\boldsymbol{V}^+$门时，其输出分别为 $\boldsymbol{N}_{V0}=\frac{1+i}{2}\begin{pmatrix}-i\\1\end{pmatrix}=\boldsymbol{V}_1$、$|1\rangle$和$|0\rangle$，同理，当 $\boldsymbol{V}_1$ 分别经过非门、$\boldsymbol{V}$ 门或 $\boldsymbol{V}^+$门时，其输出分别为 $\boldsymbol{V}_0$、$|0\rangle$和$|1\rangle$. 根据命题 1 得，最优量子逻辑电路中，量子门的控制端只能是$|0\rangle$或$|1\rangle$，因此可构造如表 1 的真值表.

从表 1 与表 2 可得，当电路输入逻辑值时，电路中任意一点的值 $d\in\{|0\rangle,|1\rangle,\boldsymbol{V}_0,\boldsymbol{V}_1\}$.

关于 n 变量可逆逻辑对应真值表和由 $2^n!$ 个元素组成的 2^n 次置换群的相关定义见文献[13]的定义 4.

表 1 非门的真值表

输入 x_0	输出 y_0
0	1
1	0
$\boldsymbol{V}_0$	$\boldsymbol{V}_1$
$\boldsymbol{V}_1$	$\boldsymbol{V}_0$

表 2 控制量子门的真值表

各门输入		CN 门输出		CV 门输出		CV$^+$门输出	
x_1	x_0	y_1	y_0	y_1	y_0	y_1	y_0
0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	1
0	$\boldsymbol{V}_0$	0	$\boldsymbol{V}_0$	0	$\boldsymbol{V}_0$	0	$\boldsymbol{V}_0$
0	$\boldsymbol{V}_1$	0	$\boldsymbol{V}_1$	0	$\boldsymbol{V}_1$	0	$\boldsymbol{V}_1$
1	0	1	1	1	$\boldsymbol{V}_0$	1	$\boldsymbol{V}_1$
1	1	1	0	1	$\boldsymbol{V}_1$	1	$\boldsymbol{V}_0$
1	$\boldsymbol{V}_0$	1	$\boldsymbol{V}_1$	1	1	1	0
1	$\boldsymbol{V}_1$	1	$\boldsymbol{V}_0$	1	0	1	1

定义 2 定义 L_n 为量子门库，是 n 变量的量子门的集合，可用于综合 n 变量的量子电路，简写为 L. 用 $T(L)$为库 L 能综合的所有 n 变量的量子电路的集合. $|L|$为库 L 中量子门的总数量，$|T(L)|$为 $T(L)$中电路的总数量.

定义 3 线置换[12]是指量子电路中各量子门与量子线的交点不变，量子线之间的顺序发生变化，即量子线发生置换，显然它属于拓扑变换，设量子门 g 经过线置换σ后，生成新量子门记为 $P_\sigma(g)$. 设电路 G 为量子门 g_1, g_2 级联，经线置换 σ 后，电路变为 $P_\sigma(G)=P_\sigma(g_1g_2)=P_\sigma(g_1)P_\sigma(g_2)$，令 $\sigma=\begin{pmatrix}0&1&2\\2&0&1\end{pmatrix}=(0\ 2\ 1)=(0\ 2)(0\ 1)$，电路线置换过程见图 2.

设 n 变量的量子门库 L 中有 m 个基本的量子门，分别为 $g_1,g_2,\cdots,g_m$，显然有 $L=\bigcup_{j\in SNF,i\in SM}P_{\sigma_j}(g_i)$，$L$ 中所有量子门的置换的集合为 $\bigcup_{j\in SNF,i\in SM}P_{\sigma_j}(\pi(g_i))$，其中

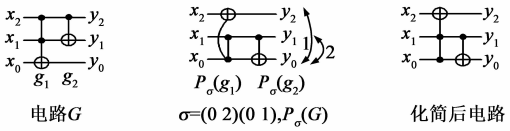

图2　电路G经线置换后所得电路$P_\sigma(g)$

$SNF=\{1,2,\cdots,n!\}$, $SM=\{1,2,\cdots,m\}$, 置换 $\sigma=(0,1,\cdots,n-1)$共有 $n!$ 种,分别为 $\sigma_1,\sigma_2,\cdots,\sigma_{n!}$, $\pi(g)$表示门 g 的置换.

定义 4　量子电路 G 的最小置换电路[12]定义为:G 经过全部线置换后生成的新电路中置换值最小的电路,简称为 G 的最小置换电路,用 $\mathrm{Min}(G)$表示量子电路 G 经过全部线置换生成电路构成的集合为 $S=\bigcup_{j\in SNF}P_{\sigma_j}(G)$,则 $\mathrm{Min}(\pi(G))=\min\{P_{\sigma_j}(\pi(G))\mid j\in SNF\}$, $\exists\, k\in SNF$, $P_{\sigma_k}(\tau)=\mathrm{Min}(\pi(G))$,则 $\mathrm{Min}(G)=P_{\sigma_k}(G)$, $\mathrm{Min}(S)=\{\mathrm{Min}(G)\mid G\in S\}$.

定义 5　定义 $C(a)$和 $C_{\min}(a)$分别为 $T(L)$中任意量子电路 a 的量子代价和最小量子代价;电路的量子代价等于该电路中各个量子门的量子代价之和;简言之,用量子门库 L 中的量子门制造量子电路 a 的最小成本为 $C_{\min}(a)$. $C_{\max}(T(L))$是 $T(L)$中量子电路的最小量子代价的最大值.量子门或量子电路的量子代价是指制造量子门或量子电路的成本,或表示其它物理含义.量子代价标准 NCV-abc 表示量子门 $\boldsymbol{N}$、$\boldsymbol{CN}$、$\boldsymbol{CV}$ 与 $\boldsymbol{CV}^+$的量子代价分别为 a、b、c.常见的 NCV 量子代价标准有四种,分别为 NCV-111、NCV-012、NCV-155[10] 和 NCV-011[7].结合定义 2, $T(L,CM)$表示库 L 以量子代价标准 CM 综合的所有最优的 n 量子电路的集合.

定义 6　定义 $M(L_n,CM)$为量子逻辑门库,记 LCM,以量子代价标准 CM 综合所有最优的 n 量子逻辑电路时,使用该库与使用量子门库 L_n 等价,它具有三个性质.

(1)最优性. LCM 中全部是用 L_n 构造的最优量子逻辑电路,显然 $LCM\subseteq T(L_n,CM)$;

(2)最简性. LCM 中不存在一量子电路可用 LCM 中的两个或以上电路以相同量子代价综合而成,当然量子代价不可能变得更小,因为 LCM 中全是最优电路;

(3)等价性.可用 LCM 门库以相同量子代价综合全部 $T(L_n,CM)$中的量子逻辑电路.

命题 3　一定存与 L_n 等价的量子逻辑门库 LCM.

证明　已知 L_n 为通用量子门库,可综合任意 n 量子逻辑电路,假设 $T(L_n,CM)$中存在一个电路 R 不可用 LCM 综合,则在满足定义 6 的基础上,如果在 $T(L_n,CM)$中存在若干非 R 电路加入 LCM 后,化简而成的新 LCM 能综合电路 R,结论成立,否则,可直接将电路 R 加入 LCM 中,并进行化简,显然新库中的门 R 可最优综合电路 R,结论仍成立.

3　新型量子可逆逻辑电路综合算法

量子门的功能本质上是实现数据的某种置换.量子电路由若干个量子门的级联组成,其本质就是若干置换的叠加,即置换的乘积.这在基于量子逻辑门的综合中容易实现,而在使用量子非逻辑门时,要通过对量子电路中可能出现的全部值进行编码,并间接描述量子门的置换,这是用置换法解决 NCV 量子逻辑电路综合问题的前提. 3.1 ~ 3.3 节实现用四值逻辑综合基于 NCV 库的量子逻辑电路.而 3.4 节给出了本文核心算法,即构造新型量子逻辑门库的算法,生成新型量子逻辑门库 NCP4,然后使用库 NCP4,调用文献[5]的 3 量子逻辑电路综合算法,综合全部最优 3 量子逻辑电路.

3.1　量子门 CV 的真值表构造

据命题 2 知,在 NCV 最优量子逻辑电路中,只有 $|0\rangle$、$|1\rangle$、$\boldsymbol{V}_0$ 与 $\boldsymbol{V}_1$ 这 4 个值,分别用 00、01、10 与 11 编码,并构造完整的真值表,表中 $ID'_x=(x_{11}x_{10}x_{01}x_{00})_2$, $ID'_y=\begin{cases}(y_{11}y_{10}y_{01}y_{00})_2, x_{11}=0\\ 16(\text{无效情形}), x_{11}=1\end{cases}$,其中 $x_{11}=1$ 表示控制端为 $\boldsymbol{V}_0$ 或 $\boldsymbol{V}_1$,根据命题 1 得,此为无效情形,这样在综合时可将一些无效的电路快速去除.设用该门综合 2 量子逻辑电路,$\boldsymbol{CV}$ 完整的真值表见表 3.为判断当前电路的每位输出是否为逻辑值,则要判断输出值是否属于{0,1,4,5},这些数据没有规律,只能依次比较,效率较低,为提高算法性能,将二制数中 x_{10}与 x_{01}以及 y_{10}与 y_{01}同时交换,可得 $ID_x=(x_{11}\ x_{01}\ x_{10}\ x_{00})_2$, $ID_y=\begin{cases}(y_{11}y_{01}y_{10}y_{00})_2, x_{11}=0\\ 16(\text{无效情形}), x_{11}=1\end{cases}$,分别取代 ID'_x, ID'_y,此时判断输出值是否属于{0,1,2,3},则判断条件可简化为:电路输出值是否都小于 4.

为综合 3 量子电路,需将表 3 真值表拓展为 3 个输入与输出变量的真值表,方法是令 $ID_x=(b_1x_{11}x_{01}b_0x_{10}x_{00})_2$, $ID_y=\begin{cases}(b_1y_{11}y_{01}b_0y_{10}y_{00})_2, x_{11}=0\\ 64(\text{无效情形}), x_{11}=1\end{cases}$,其中 $b_1b_0\in\{00,01,10,11\}$,为此可用算法自动生成 $4^n|_{n=3}=64$ 个输入与输入的真值表,判断逻辑电路的条件为:电路输出值是否都小于 $2^n|_{n=3}=8$,因该真值表太大,现从文中略去.

使用 NCV 库综合 n 量子逻辑电路时,输入值分别为$\{0,1,2,\cdots,2^n-1\}$,各量子门功能是实现$\{0,1,2,\cdots,4^n-1\}$ 的置换,则每层电路输出值是$\{0,1,2,\cdots,4^n-1\}$中 2^n 个不同的数,但不一定是$\{0,1,2,\cdots,2^n-1\}$的置换,因所求为逻辑电路,则电路最终输出一定是$\{0,1,2,\cdots,2^n-1\}$的置换.

表 3 控制 V 量子门真值表

输入					输出				
x_1	x_0	$x_{11}x_{10}x_{01}x_{00}$	ID_x'	ID_x	y_1	y_0	$y_{11}y_{10}y_{01}y_{00}$	ID_y'	ID_y
0	0	0 0 0 0	0	0	0	0	0 0 0 0	0	0
0	1	0 0 0 1	1	1	0	1	0 0 0 1	1	1
0	V_0	0 0 1 0	2	4	0	V_0	0 0 1 0	2	4
0	V_1	0 0 1 1	3	5	0	V_1	0 0 1 1	3	5
1	0	0 1 0 0	4	2	1	V_0	0 1 1 0	6	6
1	1	0 1 0 1	5	3	1	V_1	0 1 1 1	7	7
1	V_0	0 1 1 0	6	6	1	1	0 1 0 1	5	3
1	V_1	0 1 1 1	7	7	1	0	0 1 0 0	4	2
V_0	0	1 0 0 0	8	8	-	-	-	16	16
V_0	1	1 0 0 1	9	9	-	-	-	16	16
V_0	V_0	1 0 1 0	10	12	-	-	-	16	16
V_0	V_1	1 0 1 1	11	13	-	-	-	16	16
V_1	0	1 1 0 0	12	10	-	-	-	16	16
V_1	1	1 1 0 1	13	11	-	-	-	16	16
V_1	V_0	1 1 1 0	14	14	-	-	-	16	16
V_1	V_1	1 1 1 1	15	15	-	-	-	16	16

3.2 基于量子门库 L_n 以最小代价整体综合算法

设量子电路有 n 条量子线,量子门库中有 m 个不同量子门,即 m 个不同置换规则,可重复取若干量子门级联,构成的电路分别实现不同的置换,要求得到的每个电路总代价最少.将综合过程生成的量子电路存入红黑树,以方便查找与删除,该树节点的数据类型为:

```
struct rbtnode
{  gate;//本电路最后量子门名称及其所处位置.
   cp; //本电路的置换值.
   pcp;//指向上一层电路的置换值.
   len; //本电路的长度.
   cost;} //本电路的量子代价.
```

根据广度优先方法,从仅需 0 个量子门的恒等电路开始,构建红黑树 $S[0]$,仅有一个节点,其内容为$(cp:\pi_e,\cos t:0)$,显然 0 个量子门的量子代价为 0,为最优,设已有所有长度为 $j-1$ 的准最优电路,这里准最优电路是指当电路长度从 0 到 $j-1$ 时,量子代价最小的电路,因此准最优电路是指目前是最优电路,但最终不一定是最优电路;则所有长度为 j 的最优电路的生成方法是将长度为$j-1$ 的准最优电路 B 的后面分别试探m 个不同的量子门 A,即 B 的置换分别乘以 m 个 A 的置换,得到新的置换 C,判断 $S[0..j]$是否存在置换 C,若不存在,或树中存在节点的量子代价大于 B 与 A 的量子代价之和,则写入数据,否则说明此前一定存在功能相同即置换相同,且量子代价不大于当前电路的量子代价,因此要去除,依次类推,直至电路试探生成的全部量子电路都要去除,即没有生成量子代价更优的电路.

算法 1 最小代价量子电路整体综合算法 QMC4

输入: 量子门库 L_n,量子代价标准 $costs$.

输出: $maxl, maxc, N[0..MAXC], S[0..MAXL]$.

```
1.  S[0] = {(cp:π_e, cost:0)}, j = 0, N[0] = 1, N[1..MAXC] = 0
2.  while S[j] ≠ ∅ do {
3.    j = j + 1, S[j] = ∅
4.    for all Nodex in S[j − 1] do {
5.      b = Nodex.cp; icost_prev = Nodex.cost
6.      for all a in L_n do {
7.        p = b°a.cp; icost = icost_prev + costs[a]
8.        if 4^n ∈ p then continue
9.        else if p ∉ ∪_{i=0}^{j} {g.cp | g ∈ S[i]} then {
10.         S[j] = S[j] ∪ {(gate: a.gate, cp: p, cp: b, len: j, cost: icost)}
11.       if ∀ x ∈ p, x < 2^n then {
12.         N[icost] = N[icost] + 1 }}
13.     else if ∃ l ∈ {0,1,…,j} ∃ g ∈ S[l], g.cp = p ∧ g.cost > icost then {
14.       S[l] = S[l] − {g}
15.     S[j] = S[j] ∪ {(gate: a.gate, cp: p, cp: b, len: j, cost: icost)}
16.         if ∀ x ∈ p, x < 2^n then {
17.         N[icost] = N[icost] + 1;
18.         N[g.cost] = N[g.cost] − 1 }}}}
19.   maxl = j − 1; maxc = MAXC
20.   while N[maxc] = 0 do {
21.     maxc = maxc − 1 }
```

算法 QMC4 将生成全部量子代价最小的 n 变量最优量子电路,统计出各个量子代价的电路总数,存入数组 N 中,$MAXC$ 是指全部最优量子电路的最大量子代价.第 1 步,$S[0]$中只包含一个恒等电路,实现恒等置换 π_e,$j=0$ 表示电路中没有门,$N[j]=1$ 表示长度为 0 的电路总数为 1,并对数组 N 的其他元素清零;第 2 步,若还存在长度为 j 的最优电路,则试求长度为 $j+1$ 的最优电路;第 3 步,长度 j 增加 1,最优电路的置换构成的集合 $S[j]$置为空;第 4 步,依次取出长度为 $j-1$ 的最优电路对应节点 $Nodex$;第 5 步,b 与 $icost\_prev$ 分别为节点 $Nodex$ 的置换与量子代价;第 6 ~ 18 步,在长度为 $j-1$ 的准最优电路 b 后面追加量子门库 L 中的每个量子门 a;第 7 步,将置换 b 依次与置换 $a.cp$ 乘积,生成新的置换 p,所得电路的量子代价为 $icost$;第 8 步,当置换中存在非法值时,表示当前电路不可能为最优电路,应去除;第 9 ~ 10 步,若置换 p 不存在于已生成的准最优电路中,将当前所得电路的相关值存入 $S[j]$;第 11 ~ 12 步,若 p 为逻辑电路的置换,将量子代价为 $icost$ 的准最优逻辑电路个数加一;第 13 ~ 18 步,如果置换 p 存在于 $S[l]$中,且新电路比已有的电路 g 更优,则将电路 g 从$S[l]$中去除,并将新电路存入 $S[j]$,若 p 为逻辑电路的置换,将量子代价为 $icost$ 与 $g.cost$ 的准最优逻辑电路个数分别加一与减一;转至第 6 步、第 4 步、第 2 步,

如此反复,直至运行至第 19 步,全部最优量子电路生成完毕;第 19 ~ 21 步,分别求出最优电路中的最大长度 $maxl$ 与最大量子代价 $maxc$,显然 $T(L_n, CM) = \bigcup_{i=0}^{maxl} S[i]$.

为何在第 14 步中可直接从 $S[l]$中去除电路 g?显然 $S[l+1], S[l+2], \cdots, S[j]$中必然存在电路的最前面子电路为 g,因此这样操作必然会影响以 g 为子电路的全部电路,事实不然,因为所求为最优量子电路,既然已发现当前电路比 g 优化,因此所有包含电路 g 的电路一定不为最优,最终一定都会被删除,对最终结果没有影响.

为何使用库 L_{ncv}和库 L_{nct}综合量子逻辑电路时,前者算法复杂度比后者高出许多,原因有:(1)L_{ncv}和 L_{nct}的量子门数分别为 21 和 12,因此前者每次级联门的次数更多;(2)L_{nct}为二值逻辑综合,L_{ncv}为四值逻辑综合,后者的电路置换数更多,综合规则更复杂;(3)库 L_{nct}中只有量子逻辑门,所以只能综合量子逻辑电路,而库 L_{ncv}综合逻辑电路的过程中,还会伴随生成量子非逻辑电路,因为最优电路中可能包含若干最优非逻辑电路,已知 3 量子逻辑电路共 $2^3! = 40320$ 个,因此库 L_{nct}只会生成 40320 个最优 3 量子逻辑电路,而库 L_{nct}使用算法 QMC4,共生成 887039 个最优量子电路,含大量非逻辑电路,因此需从中筛选出所求的 40320 个最优逻辑电路.

3.3　基于算法 QMC4 综合具体量子电路算法

算法 2　具体量子电路序列生成算法 QMR4

输入:量子门库 L_n,量子代价标准 $costs$,所求量子电路的置换 p.

输出:所求长度最小的量子电路序列 G.

1. 运行 $QMC4(L_n, costs)$,生成 $S[0..maxl], G = \{\}$.
2. if $\exists l \in \{maxl, maxl-1, \cdots, 0\}\ \exists g \in S[l], g.cp = p$ then {
3.　$i = l, mynode[i] = g$
4.　while $i > 1$ do {
5.　　$i = i - 1, \exists g \in S[i], g.cp = mynode[i+1].pcp$
6.　　$mynode[i] = g$ }
7. for $i = 1$ to l do {
8.　$G = G\&mynode[i].gate$ }

第 1 步,算法 QMC4 生成全部基于 L_n 的量子逻辑电路,存于 S 中;第 2 步顺序查找电路长度为 l,并在 $S[l]$中查询电路的置换为 p 的节点.第 3 步得到当前节点对应量子门的前面相连量子门的置换;第 4 ~ 6 步不断向前找出电路中全部节点;第 7 ~ 8 步生成所求最优量子电路序列.

3.4　构造新型量子逻辑门库算法

由命题 3 知,与量子门库 L_n 等价的新型量子逻辑门库一定存在,如能得到最简且等价的量子逻辑门库,则在综合电路时就可以不用算法 QMC4,而可用更为简捷高效的基于量子逻辑门库的综合算法,现给出自动构造新型量子逻辑门库的算法.

算法 3　构造新型量子逻辑门库算法 QLL

输入:量子门库 L_n,量子代价标准 $costs$.

输出:L_{new}.

1. $S_n = \{g \mid g \in T(L_n, costs) \wedge islogic(g)\}$
2. $L_{new} = \mathrm{Min}(\{g \mid g \in L_n \wedge islogic(g)\})$
3. $S_{new} = T(L_{new}, costs); S_n = S_n - S_{new}$
4. while $S_n \neq \varnothing$ do {
5.　$minc = \min\{g.cost \mid g \in S_n\}$
6.　$minl = \min\{g.len \mid g \in S_n \wedge g.cost = minc\}$
7.　$S_{tmp} = \{g \mid g \in S_n \wedge g.cost = minc \wedge g.len = minl\}$
8.　if $|S_{tmp}| > 0$ then {
9.　　$L_{new} = L_{new} \cup \mathrm{Min}(S_{tmp})$
10.　　$S_{new} = T(L_{new}, costs); S_n = S_n - S_{new}$ } }

所求新型量子逻辑门库 L_{new}为 $QLL(L_{ncv})$,该库中产生的新量子门为:$L_{new} - \mathrm{Min}(\{N, CN\})$,可得如下 4 个量子逻辑门,其中一个为 Peres 门.

第 1 步,算法 QMC4 以量子代价 $costs$ 为标准,使用库 L_n,生成全部的量子逻辑电路存入集合 S_n 中;第 2 步,将库 L_n 中逻辑门的最小置换电路存入 L_{new}中;第 3 步,使用新库 L_{new},以量子代价 $costs$ 为标准,综合全部逻辑电路,因这些电路可以用 L_{new}综合,所以将这些电路从 S_n 中去除;第 4 步,若 S_n 为空,则新库生成完毕;第 5 步,获取 S_n 中各电路的代价的最小值;第 6 步,获取这些最小代价电路的最短长度;第 7 步,将满足这两个条件的电路存入 S_{tmp};第 8 ~ 10 步,若 S_{tmp}不为空,则将该集合的电路的最小置换电路加入 L_{new}中,再次用新库 L_{new}综合量子逻辑电路,并将这些电路从 S_n 去除,返回第 4 步,如此反复,直至 S_n 为空为止,即新库 L_{new}可综合全部量子逻辑电路.

运行以上算法,可得新型量子门的构造图见图 3,其中门 g_1、g_2 和 g_3 处分别填入 $\boldsymbol{V}$ 或 $\boldsymbol{V}^+$ 门,当 $x_1 = x_2 = 0$ 时,不选择任何门;当 $x_1 = 0, x_2 = 1$ 时,选择门 g_2 和 g_3;当 $x_1 = 1, x_2 = 0$ 时,选择门 g_1 和 g_3;当 $x_1 = 1, x_2 = 1$ 时,选择门 g_1 和 g_2,新型量子门的功能见表 4.

表 4　新型量子逻辑门库的构造表

门的名称	$g_1\ g_2\ g_3$	$x_1=0$ $x_2=0$	$x_1=0$ $x_2=1$	$x_1=1$ $x_2=0$	$x_1=1$ $x_2=1$
Peres	$\boldsymbol{VV^+}$	$\boldsymbol{I}$	$\boldsymbol{VV^+ = I}$	$\boldsymbol{VV^+ = I}$	$\boldsymbol{VV = N}$
P1	$\boldsymbol{VV^+\ V^+}$	$\boldsymbol{I}$	$\boldsymbol{V^+\ V^+ = N}$	$\boldsymbol{VV^+ = I}$	$\boldsymbol{VV^+ = I}$
P2	$\boldsymbol{VV^+\ V}$	$\boldsymbol{I}$	$\boldsymbol{V^+\ V = I}$	$\boldsymbol{VV = N}$	$\boldsymbol{VV^+ = I}$
P3	$\boldsymbol{VVV}$	I	$\boldsymbol{VV = N}$	$\boldsymbol{VV = N}$	$\boldsymbol{VV = N}$

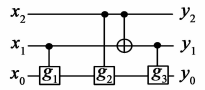

图3　基于NCV的新型量子逻辑门构造图

表 4 中描述了在量子门的各种组合情况下 y_0 上实现的功能,以上量子门的组合实现新型量子门的功能各不相同,且包含其它所有组合情况的功能,第一种是 Peres 门,我们还构造了三种类似 Peres 的新型量子门,加入 ***N*** 与 ***CN*** 门,形成新型量子逻辑门库,取名 NCP4.

使用 3 量子逻辑门库,基于位运算的 3 量子可逆逻辑电路综合算法见我们已发表论文[5].使用已构造的新型 3 量子逻辑门库 NCP4,调用文献[5]的 QMC 算法,快速生成全部最小代价的 3 量子逻辑电路,与前面 QMC4 的运行结果等价.可用文献[5]的 QMR 算法取出所求电路序列.

4 实验结果与分析

本文采用 3 变量可逆函数测试标准进行实验,共生成 40320 个可逆逻辑电路.实验的目的是用较短的时间生成全部量子代价尽可能小的电路.本实验采用多种量子门库,以多种量子代价标准,快速生成全部最优电路.在量子电路综合的许多算法中,基于量子非逻辑门库 NCV 的综合算法却不多,如本领域的权威 Maslov 教授的最新文献公布的情况[10],在 Sun Blade 1000 750MHz 电脑上,运用 4 值逻辑综合算法,并引入一些优化规则,提高了算法效率,用时约为 60s,而文献[8]仅综合一个 6 个门的 Miller 电路就用时 318.29s,文献[9]只能综合其中 10136 个电路;为公平比较,本实验的电脑为联想奔腾 III 667MHz 64M,电脑配置略低些,算法 QMC4(L_{ncv}, *costs*)生成全部电路,平均用时 24s,而算法 QLM(L_{ncp4}, *costs*)生成全部电路,平均用时 0.48s,比文献[10]快了近 127 倍.基于量子代价 NCV-111、NCV-012 综合的三量子逻辑电路的统计结果与文献[10]相同,但文献[10]并没有给出基于量子代价 NCV-155 与常用标准 NCV-011 的统计结果,且文献最后给出的基于 NCV-1 14 9 的新量子代价标准的统计结果有误,可能作者与 NCV-155 的统计值相混淆,详细的统计结果见表 5 和表 6.为检验本文算法,我们还采用 Maslov 提供的 3 量子标准测试电路进行实验.以基于 CNT 量子门的电路 3_17 为例,以多种量子代价标准,先调用 QMC 生成电路整体综合数据,再运行 QMR,仅运行几步就生成基于 NCV 量子门电路序列,可以验证,这些电路的置换都为 $P=(7,1,4,3,0,2,6,5)$,因 Toffoli 门可以用 Peres 门与 CN 门级联而得,得第一个门的代价是后两个门的代价之和.将电路 3_17 以多种量子代价标准综合,生成各种 NCV 最优量子逻辑电路,此电路的代价与 3_17 按此代价换算后的电路代价参见表 7.生成电路见图 4,各标准综合最优 NCV 量子电路图相同,显然,这是巧合,没有必然性.

表 5 以多种量子代价标准综合最优 NCV 三量子逻辑电路的数量

Cost	NCV-111	NCV-012	NCV-011	NCV-155	NCV-1 14 9
0	1	8	8	1	1
1	9	48	48	3	3
2	51	192	192	3	3
3	187	408	408	1	1
4	417	480	672	0	0
5	714	192	1248	6	0
6	1373	16	3184	24	0
7	3176	192	4320	18	0
8	4470	1056	3552	0	0
9	4122	3168	11520	0	0
10	10008	4320	4416	24	0
11	5036	672	0	117	0
12	1236	0	9856	51	0
13	8340	0	896	0	0
14	1180	2880	0	0	6
15	0	11520	0	51	24
16	0	4416	0	282	18
17	0	0	0	75	0
20	0	0	0	84	0
21	0	9856	0	483	0
22	0	896	0	105	0
25-138	0	0	0	略	略

表 6 以多种量子代价标准综合最优 NCV 三量子逻辑电路的统计表

	NCV-111	NCV-012	NCV-155	NCV-1 14 9
$N(T(L))$	40320	40320	40320	40320
平均代价	10.03	14.98	46.35	75.17
$C_{\max}(T(L))$	14	22	66	138
$N(L)$	21	21	21	21
QMC4 时间(s)	24.22	24.28	24.39	24.40
QMC 时间(s)	0.45	0.45	0.45	0.56
文献[10]时间(s)	60	60	60	60
提高倍数	133.3	133.3	133.3	107.1

表 7 以多种量子代价标准综合最优 NCV 三量子逻辑电路的统计表

NCV 代价标准	NCV 最优电路代价	相应 NCT 代价标准	相应 NCT 电路代价
NCV-111	10	NCT-115	14
NCV-012	15	NCT-018	19
NCV-011	9	NCV-015	13
NCV-155	46	NCT-1 5 25	65
NCV-1 14 9	97	NCT-1 14 55	152

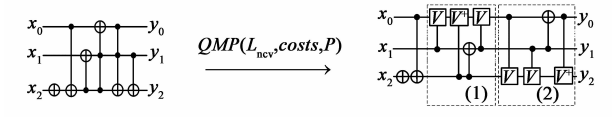

图4 实现3_17功能的最优NCV量子电路图,(1)是P2门,(2)是Peres门

5 结束语

量子非逻辑门的综合问题[8~11]一直是人们研究的重点,然而并没有取得突破性进展,本文通过构造新型

量子逻辑门,取代量子非逻辑门,从而将此难题简化为较易解决的量子逻辑门的综合问题,这是一个高效且通用的解决方法.并结合基于完备 Hash 函数的量子逻辑综合算法,实现使用多种量子逻辑门与非逻辑门,采用任意最小的上下无关的量子代价标准,高效生成全部最优的量子可逆逻辑电路.如何高效综合大规模量子电路,这是亟待解决的重要课题之一.

参考文献

[1] R Feynman. Quantum mechanical computers[J]. Optic News, 1986,16(6):1120.

[2] E Fredkin, T Toffoli. Conservative logic[J]. International Journal of Theoretical Physics, 1982,21(3):219 – 253.

[3] D Maslov, G W Dueck, et al. Toffoli network synthesis with templates[J]. IEEE Transactions on CAD, 2005,24(6):807 – 817.

[4] P Gupta, A Agrawa, N K Jha. An algorithm for synthesis of reversible logic circuits[J]. IEEE Transactions on CAD, 2006,25(11):807 – 817.

[5] 李志强,陈汉武.量子可逆逻辑电路最小代价综合算法[J].东南大学学报,2008,38(2):249 – 254.
Z Q Li, H W Chen. Synthetic algorithm for reversible logic circuits of quantum with minimal cost[J]. Journal of Southeast University, 2008,38(2):249 – 254. (in Chinese)

[6] V V Shende, A K Prasad, et al. Synthesis of reversible logic circuits[J]. IEEE Transactions on CAD, 2003,22(6):723 – 729.

[7] G W Yang, X Song, et al. Fast synthesis of exact minimal reversible circuits using group theory[A]. Proceedings of the 10th Asia and South Pacific Design Automation Conference[C]. Shanghai, China: IEEE Press, 2005. 18 – 21.

[8] W N N Hung, X Song, G W Yang, J Yang, M Perkowski. Optimal synthesis of multiple output boolean functions using a set of quantum gates by symbolic reach ability analysis[J]. IEEE Transactions on CAD, 2006,25(9):1652 – 1663.

[9] G W Yang, W N N Hung, X Song, M Perkowski. Exact synthesis of 3-qubit quantum circuits from non-binary quantum gates using multiple-valued logic and group theory[A]. Proceedings of DATE 2005[C]. Munich, Germany: IEEE Press, 2005. 434 – 435.

[10] D Maslov, D M Miller. Comparison of the cost metrics through investigation of the relation between optimal NCV and optimal NCT three-qubit reversible circuits[J]. IET Computers & Digital Techniques, 2007,1(2):98 – 104.

[11] G W Yang, X Song, M Perkowski, W N N Hung, J Biamonte, Z Tang. Four-level realization of 3-qubit reversible functions[J]. IET Computers & Digital Techniques, 2007,1(4):382 – 388.

[12] Z Q Li, H W Chen, B W Xu, et al. Fast algorithm for 4-qubit reversible logic circuits synthesis[A]. Proceedings of WCCI 2008[C]. Hong Kong: IEEE Press, 2008. 300 – 306.

[13] 李志强,陈汉武,等.四量子可逆逻辑电路快速综合算法[J].电子学报,2008,36(11):2081 – 2089.
LI Zhi-qiang, CHEN Han-wu, et al. Fast algorithms for 4-qubit reversible logic circuits synthesis[J]. Acta Electronica Sinica, 2008,36(11):2081 – 2089. (in Chinese)

[14] 杨忠明,陈汉武,等.基于二分法量子可逆逻辑电路综合[J].电子学报,2012,40(5):1045 – 1049.
YANG Zhong-ming, CHEN Han-wu, et al. Qubits reversible logic circuits synthesis based on bisection method[J]. Acta Electronica Sinica, 2012,40(5):1045 – 1049. (in Chinese)

作者简介

李志强　男.1974 年 5 月出生,江苏姜堰人.扬州大学副教授,硕士生导师,2011 年在东南大学计算机科学与工程学院获工学博士学位,主要从事量子计算、可逆电路综合等方面的研究工作.
E-mail:zqli@yzu.edu.cn

陈汉武　男.1955 年 11 月出生,南京人.东南大学教授、博士生导师.2000 年 3 月获日本国立山口大学大学院理工学研究科智能情报专业理工学博士学位.主要从事量子计算、信息论等方面的研究工作.
E-mail:hw_chen@seu.edu.cn