文章编号:1004-9037(2014)06-0975-06

基于控制 K 次平方根非门的类 Toffoli 门构造方法

李志强[1] 冯小霞[1] 陈汉武[2]

(1.扬州大学信息工程学院,扬州,225009;2.东南大学计算机科学与工程学院,南京,210096)

摘要:在量子电路综合算法中,由于非置换量子门比置换量子门具有更复杂的规则,直接使用非置换量子门会大幅度提高综合算法的复杂性,因此可先使用非置换量子门生成相应的置换量子门,然后再用这些置换量子门综合所求量子可逆逻辑电路,从而提高算法性能。本文重点研究如何用非置换量子门构造新的置换量子门,为此吸收了格雷码的思想,提出了一种高效的递归构造方法,实现使用控制非门和控制 K 次平方根非门(非置换量子门),快速生成最优的类 Toffoli 门(置换量子门)。

关键词:量子门;量子电路;可逆逻辑;格雷码

中图分类号:TN91 **文献标志码**:A

Realization of Toffoli-Like Gates Using Controlled-*K*th-Root-of-NOT Quantum Gates

Li Zhiqiang[1], *Feng Xiaoxia*[1], *Chen Hanwu*[2]

(1. College of Information Engineering, Yangzhou University, Yangzhou, 225009, China;
2. School of Computer Science and Engineering, Southeast University, Nanjing, 210096, China)

Abstract: Since non-permutative quantum gates have more complex rules than permutative quantum gates, direct use of non-permutative quantum gates can greatly increase the complexity of the synthesis algorithm, so given quantum gates should be used to create new permutative quantum gates, and then these permutative gates are used to synthesize the desired quantum reversible logic circuit, thus improving the algorithm performance. This paper focuse on how to use non-permutative quantum gates to construct new permutative gates, therefore, we absorb the idea of Gray code and present an efficient recursive construction which can use controlled-NOT gates and controlled-Kth-root-of-NOT gates (non-permutative quantum gates) to construct the optimal Toffoli-like gates (permutative quantum gates).

Key words: quantum gate; quantum circuit; reversible logic; Gray code

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,(1)量子逻辑门(即置换的量子门),如控制非门[1](Controlled-NOT,CNOT)、Toffoli 门、Fredkin 门[2]、Peres 门等,每条量子线的输入与输出值均为二元基态;(2)量子非逻辑门(即非置换的量子门),如控制 V 门(CV)、控制 V^+ 门(CV^+)等[2]。

自动构造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,并提出许多量子电路综合算法。如何用指定量子门,自动生成基于量子逻辑门的 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

基金项目:国家自然科学基金(61070240,60572071,61170321)资助项目;江苏省高校自然科学基金(10KJB520021)资助项目。

收稿日期:2014-09-03;**修订日期**:2014-10-14

特点，将量子电路综合问题简化为四值逻辑综合问题[15]，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，$4^n|_{n=3}=1.269\times10^{89}$，$2^n!\ |_{n=3}=40\ 320$，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。文献[9]研究发现，先用 NCV 门库生成 4 种类 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。因此，关键问题是如何使用 CNOT，CV 和 CV+门生成 4 种类 Peres 门的新型量子逻辑门。

在没有使用辅助位的情况下，直接使用 CV、CV^+ 门和 CNOT 是无法构造 3 个或 3 个以上控制端的类 Toffoli 门，因此本文提出使用文献[6]中提出的控制 K 次平方根非门(Controlled-Kth-Root-of-NOT)综合任意类 Toffoli 门，其中 $K=2,4,8\cdots$，而用通常的综合算法无法实现，这也为解决类似电路综合问题提供了一种新颖高效的方法。

1 量子逻辑电路基本概念

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。

每个有 n 条线可逆或量子电路的操作可用 2^n 维度的方阵表示。因此，当 $n=1$ 时，其维度为 2，如非门矩阵是 $\boldsymbol{N}=\begin{pmatrix}0&1\\1&0\end{pmatrix}$。

由文献[6]可得

$$\boldsymbol{N}^{1/k}=\frac{1}{2}\begin{pmatrix}1+\mathrm{i}^{2/k}&1-\mathrm{i}^{2/k}\\1-\mathrm{i}^{2/k}&1+\mathrm{i}^{2/k}\end{pmatrix}\tag{1}$$

式中：k 为 2 的幂；$\boldsymbol{N}^{1/k}$ 为 $\boldsymbol{N}$ 的 K 次方根，有 $(\boldsymbol{N}^{1/k})^k=\boldsymbol{N}$。

令 $\boldsymbol{G}_k=\boldsymbol{N}^{1/k}$，$k=2^n$，其中 $n\in\{0,1,2,3,\cdots\}$，则 $\boldsymbol{G}_{2^n}=\boldsymbol{N}^{2^{-n}}$，此外 $\boldsymbol{G}^{\dagger}\dagger_{2^n}$ 为 $\boldsymbol{G}_{2^n}$ 的伴随矩阵。

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 $\boldsymbol{I}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ 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 $|\phi>$ 后，输出为 $\boldsymbol{N}_{\phi}=\boldsymbol{N}\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\begin{pmatrix}\beta\\\alpha\end{pmatrix}$。恒等电路矩阵是 $\boldsymbol{I}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$，当该门输入 $|\phi>$ 后，输出为 $\boldsymbol{N}_{\psi}=\boldsymbol{I}\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\boldsymbol{N}_{\phi}$。

定义 2 当式(1)中 $k=2$ 时，$\boldsymbol{N}^{1/2}=\frac{1}{2}\cdot\begin{pmatrix}1+\mathrm{i}&1-\mathrm{i}\\1-\mathrm{i}&1+\mathrm{i}\end{pmatrix}$，为平方根非门的矩阵，即可定义量子 $\boldsymbol{V}$ 门、$\boldsymbol{V}^+$ 门用矩阵分别为 $\boldsymbol{V}=\frac{1+\mathrm{i}}{2}\begin{pmatrix}1&-\mathrm{i}\\-\mathrm{i}&1\end{pmatrix}$，$\boldsymbol{V}^+=\frac{1-\mathrm{i}}{2}\begin{pmatrix}1&\mathrm{i}\\\mathrm{i}&1\end{pmatrix}$，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。

定义 3 设 $\boldsymbol{G}_k$ 门为 K 次平方根非门，则 $\boldsymbol{G}_k$ 门矩阵可为式(1)$\boldsymbol{N}^{1/k}$，而 $\boldsymbol{G}_k^+$ 门矩阵为 $\boldsymbol{N}^{1/k}$ 的共轭

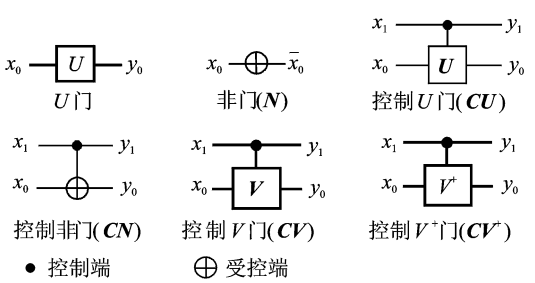

图 1 量子门

Fig. 1 Quantum gates

转置。可得 $\boldsymbol{G}_k\boldsymbol{G}_k^+ = \boldsymbol{G}_k^+\boldsymbol{G}_k = \boldsymbol{I}$，$\underbrace{\boldsymbol{G}_k\boldsymbol{G}_k\cdots\boldsymbol{G}_k}_{K} = \underbrace{\boldsymbol{G}_k^+\boldsymbol{G}_k^+\cdots\boldsymbol{G}_k^+}_{K} = \boldsymbol{N}$，即 K 个 $\boldsymbol{G}_k$ 门或 K 个 $\boldsymbol{G}_k^+$ 门级联的功能相当于一个非门，因此 $\boldsymbol{G}_k$ 门与 $\boldsymbol{G}_k^+$ 门也称为 K 次平方根非门。$C\boldsymbol{G}_k$ 门与 $C\boldsymbol{G}_k^+$ 门为控制 K 次平方根非门。

2　量子电路自动综合算法

2.1　基于格雷码的综合算法

在一组二进制数的编码中，若任意两个相邻的代码只有 1 位二进制数不同，则称这种编码为格雷码，另外由于最大数与最小数之间也仅 1 位数不同，即“首尾相连”，因此又称循环码或反射码。而这些特点恰好可用于新型量子逻辑门的控制端电路的构造，可设格雷码的每一位对应于量子电路的每一根量子线，因为格雷码是相连的两个编码相差一位，这个正好可用一个 CNOT 门实现。格雷码又是循环码，因此电路的输出值与输入值相等，满足类 Toffoli 门对控制端电路的要求，而类 Peres 门就没有这个要求，即该门控制端电路的输出值与输入值不完全相等[16]。

下面以 3 位格雷码为例，如表 1 所示。

表 1　3 位格雷码与对应控制比特

Table 1　3-bit Gray codes and corresponding control bits

$x_2x_1x_0$	控制比特
000	
100	x_2
110	$x_2\oplus x_1$
010	x_1
011	$x_1\oplus x_0$
111	$x_2\oplus x_1\oplus x_0$
101	$x_2\oplus x_0$
001	x_0

在表 1 中，不难验证，当 $x_2x_1x_0$ 取任意值时，表中所有控制比特的数值和一定为 0 或 4，即 $x_2+x_2\oplus x_1+x_1+x_1\oplus x_0+x_2\oplus x_1\oplus x_0+x_2\oplus x_0+x_0=0$ 或 4。而每个控制比特为 0 或 1，可得有 0 个或 4 个控制比特为 1，其他控制比特为 0，即全部控制比特为 1 的个数为 0 或 4，因此电路图中的 U 门为 $\boldsymbol{G}_4$ 门。

根据表 1 中的控制比特，可得到图 2 所示的类 Toffoli 门的控制端电路，即 $x_2x_1x_0$ 控制线构成的电路，由于格雷码又是循环码，因此图中控制端电路的输入与输出值恒等。

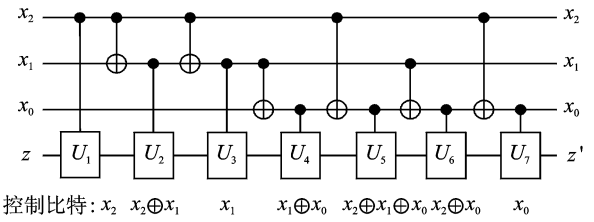

图 2　表 1 对应的 3 位控制线的类 Toffoli 门

Fig. 2　Toffoli-like gate with three control lines for Table 1

由于格雷码的不唯一性，表 2 给出另一种格雷码。

表 2　另一种 3 位格雷码与对应控制比特

Table 2　Another 3-bit Gray codes and corresponding control bits

$x_2x_1x_0$ 格雷码	控制比特
000	
001	x_0
011	$x_1\oplus x_0$
010	x_1
110	$x_2\oplus x_1$
111	$x_2\oplus x_1\oplus x_0$
101	$x_2\oplus x_0$
100	x_2

根据表 2 中的控制比特生成图 3 所示的类 Toffoli 门的控制电路，即 $x_2x_1x_0$ 控制线构成的电路。

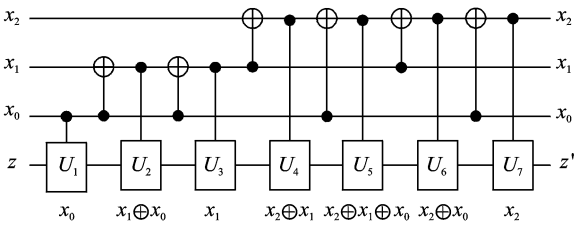

图 3　表 2 对应的 3 位控制线的类 Toffoli 门

Fig. 3　Toffoli-like gate with three control lines for Table 2

图 2，3 构建的是同一个门，因为将图 2 电路执行线置换 $\begin{bmatrix} x_0 & x_1 & x_2 \\ x_2 & x_1 & x_0 \end{bmatrix}$ 后，即第一根线与第三根线对换，并得到图 3 电路。4 位的格雷码与相应类 Toffoli 门和上述相似，如表 3 所示。

表 3 4 位格雷码与对应控制比特

Table 4 4-bit Gray codes and corresponding control bits

$x_3x_2x_1x_0$	控制比特
0000	
1000	x_3
1100	$x_3\oplus x_2$
0100	x_2
0110	$x_2\oplus x_1$
1110	$x_3\oplus x_2\oplus x_1$
1010	$x_3\oplus x_1$
0010	x_2
0011	$x_1\oplus x_0$
1011	$x_3\oplus x_1\oplus x_0$
1111	$x_3\oplus x_2\oplus x_1\oplus x_0$
0111	$x_2\oplus x_1\oplus x_0$
0101	$x_2\oplus x_0$
1101	$x_3\oplus x_2\oplus x_0$
1001	$x_3\oplus x_0$
0001	x_0

可以验证，对于 $x_3x_2x_1x_0$ 的任意输入值，表 3 的全部控制比特为 1 的个数为 0 或 8，因此电路图中的 $\boldsymbol{U}$ 门为 $\boldsymbol{G}_8$ 门。同样，可根据表 3 中的控制比特，可得到图 4 所示的类 Toffoli 门的控制端电路，即 $x_3x_2x_1x_0$ 控制线构成的电路。

2.2 基于递归的综合算法

现从图 4 电路中发现特定规律，并提出了高效的基于递归的综合算法，从而有效避免了构造格雷码的过程。其特定规律如下：

(1)第①块，$2^1=2$ 个门，$g_1\sim g_2$，受控点为 x_2；第②块，$2^2=4$ 个门，$g_3\sim g_6$，受控点为 x_1；第③块，$2^3=8$ 个门，$g_7\sim g_{14}$，受控点为 x_0。

(2)第①、②、③块的第一个门的控制端分别为 x_3，x_2，x_1，受控端分别为 x_2，x_1，x_0。

(3)每块的第 1 个门与该块后面的中间门的控制端与受控端的位置相同。如 g_1 与 g_2，g_3 与 g_5，g_7 与 g_{11}。

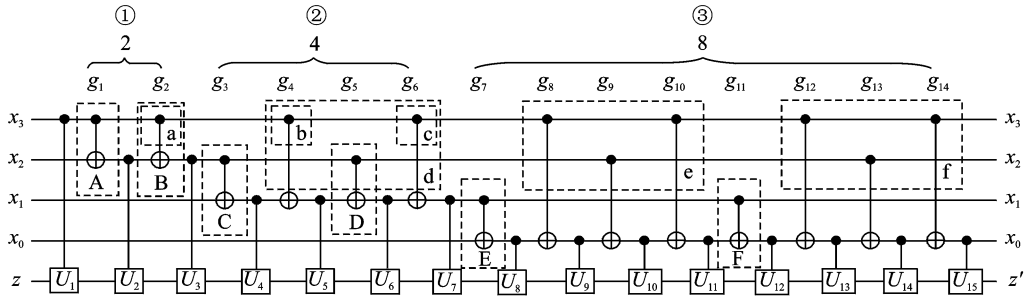

图 4 表 3 对应的 4 位控制线的类 Toffoli 门

Fig. 4 Toffoli-like gate with four control lines for Table 3

(4)控制端有如下递归关系，如第③块的左右两块：e 与 f 与第②块的 d 相同；如第②块的左右两块：b 与 c 与第①块的 a 相同。

下面给出基于该递归的类 Toffoli 门的控制端电路的综合算法。

```
Typedef struct Node
{control;   //CNOT 门的控制端位置
target;} TCNode   //CNOT 门的受控端位置
```

算法 1 类 Toffoli 门的控制端电路 TOFC

输入：控制端电路的量子线数 n

输出：控制端电路，TCNode $TC[2^n-2]$。

```
j=0
for i=1 to n-1 {
TC[j]={control:n-i+1,target:n-i}
Controls(TC,n-i+1,n-i,j+1,j+2^i-1);
j=j+2^i}
```

算法 2 类 Toffoli 门的控制端电路中的递归子电路 Controls

输入：控制端电路，TCNode $TC[2^n-2]$，子电路中间门的控制与受控端的序号分别为 iControl 与 iTarget，子电路第一个门的序号为 iStart，最后一个门的序号为 iEnd。

输出：控制端电路，TCNode $TC[2^n]$。

```
if(iStart<iEnd ) return
iMid=(iStart+iEnd)/2
Controls(TC, iControl + 1, iTarget, iStart, iMid-1)
TC[iMid]={control:iControl,target:iTarget}
```

Controls（TC，iControl＋1，Target，iMid＋1，iEnd）｝

原先是根据类 Toffoli 门的线数 n 生成相应的格雷码，再由该格雷码生成类 Toffoli 门的控制电路，最终生成 $n+1$ 位类 Toffoli 门。由于发现该电路存在规律，故可直接生成，见算法 1 与算法 2，该算法简练而高效。

当调用函数 TOFC(n)，可立即得到返回的数组 TC[2^n-2]，数组每个元素对应一个 CNOT 门，由这 2^n-2 个 CNOT 门级联可得到 $n+1$ 位类 Toffoli 门的控制电路，再像图 4 一样，依次加入 G_{2^n} 门，并可能到 $n+1$ 位类 Toffoli 门。这与传统的量子电路综合算法完全不一样，因为传统的方法并没有利用所求电路的规律，使用类似穷举方法依次搜索答案，效率很低，而本文方法是利用电路自身特殊的规律，快速直接构造而成，因此效率极大提高。且目前关于使用控制 K 次平方根非门的综合很少，因此常规的综合算法是无法使用该门综合电路的。

3　结束语

量子电路综合算法研究发现，非置换量子门比置换量子门具有更复杂的规则，直接使用非置换量子门会大幅度提高综合算法的复杂性，因此可先使用非置换量子门生成相应的置换量子门，然后再用这些置换量子门综合所求量子可逆逻辑电路，从而提高算法性能，该方法在文献[9]得到了很好的验证。控制 K 次平方根非门（$K=2,4,8\cdots$）属于非置换量子门，为此本文使用该非置换量子门构造新的置换量子门，先给出了利用格雷码的思想，使用 CNOT 门与控制 K 次平方根非门巧妙生成置换量子门，即类 Toffoli 门，然后发现这些类 Toffoli 门内部存在递归，故又根据该规律，在不使用格雷码的情况下，提出了基于递归的综合算法，直接高效生成同样的类 Toffoli 门。今后，还会使用这些新型类 Toffoli 逻辑门，高效综合量子电路，不仅能减少一部分已有量子电路的量子代价，而且还能提高综合算法的效率。

参考文献：

[1] Li Z, Chen H, Song X. A novel hash-based algorithm for reversible logic circuits synthesis [J]. Journal of Computational Information Systems, 2012, 8(11): 4485-4493.

[2] Barenco A, Bennett C, Cleve R, et al. Elementary gates for quantum computation [J]. Physical Review A, 1995, 52(5): 3457-3467.

[3] Miller D M, Wille R, Sasanian Z. Elementary quantum gate realizations for multiple-control toffoli gates [C] // Proceedings of 41st IEEE International Symposium on Multiple-Valued Logic. Tuusula, Finland: IEEE, 2011: 288-293.

[4] Liu Y, Long G L, Sun Y. Analytic one-bit and CNOT gate constructions of general n-qubit controlled gates [J]. International Journal of Quantum Information, 2008, 6(3): 447-462.

[5] Tsai E, Perkowski M. Synthesis of permutative quantum circuits with toffoli and TISC gates[C]// Proceedings of IEEE 42nd International Symposium on Multiple-Valued Logic. Victoria, BC, Canada: IEEE, 2012: 50-56.

[6] Sasanian Z, Miller D M. Transforming MCT circuits to NCVW circuits [C] // Workshop on Reversible Computation 2011. Gent Belgium Berlin, Heidelberg: Springer, 2011: 163-174.

[7] Hung W N N, Song X, Yang G, et al. 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.

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

[9] 李志强，陈汉武，刘文杰，等. 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[J]. 电子学报，2013，41(4)：690-697.
Li Zhiqiang, Chen Hanwu, Liu Wenjie, Liu W, et al. Efficient algorithm for synthesis of optimal NCV 3-qubit reversible circuits using new quantum logic gate library[J]. Acta Electronica Sinica, 2013, 41(4): 690-697.

[10] Maslov D, Miller D M. 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] Yang G W, Song X, Perkowski M, et al. Four-level realization of 3-qubit reversible functions [J]. IET

Computers & Digital Techniques, 2007, 1(4): 382-388.

[12] Li Z, Chen H, Xu B, et al. Fast Algorithm for 4-Qubit Reversible Logic Circuits Synthesis [C] // Proceedings of WCCI 2008. Hong Kong: [s. n.], 2008: 2202-2207.

[13] Yang G, Xie F, Hung W N N, et al. Realization and synthesis of reversible circuits [J]. Theoretical Computer Science, 2011, 412(17): 1606-1613.

[14] Alhagi N, Lukac M, Tran L, et al. Two-stage approach to the minimization of quantum circuits based on ESOP minimization and addition of a single ancilla qubit [C]// Proceedings of 21st ULSI 2012. Columbia, Canada: [s. n.], 2012: 150-159.

[15] Yang G, Hung W N N, Song X, et al. Exact synthesis of three-qubit quantum circuits from non-binary quantum gates [J]. International Journal of Electronics, 2010, 97(4): 475-489.

[16] 陈庆芳,吴小俊. 基于分块互信息和量子粒子群算法的图像配准[J],数据采集与处理,2011,26(4):473-477.
Chen Qingfang, Wu Xiaojun. Image registration based on block mutunal information and quantum-behaved particle swarm optimization [J]. Journal of Data Acquisition and Processing, 2011, 26(4): 473-477.

作者简介:李志强(1974-),男,博士,副教授,研究方向:量子计算、可逆电路综合,E-mail: zqli@yzu.edu.cn;冯小霞(1990-),女,硕士研究生, 研究方向:可逆电路综合;陈汉武(1955-),男,博士,教授,研究方向:量子计算、信息论。