

基于矩阵初等变换的四量子比特 可逆电路综合算法

王 冬^{1,2}, 陈汉武¹, 安 博¹, 杨忠明¹

(1. 东南大学计算机科学与工程学院, 江苏南京 210096; 2. 河南大学计算中心, 河南开封 415002)

摘 要: 量子可逆电路实现信息变换的过程可用一个酉矩阵算子表示, 采用酉矩阵表示量子可逆电路能更好地反映量子系统的演化, 体现量子计算所特有的属性. 本文提出基于矩阵初等变换的 4 量子比特可逆电路综合算法. 该算法恰当地利用量子电路的矩阵表示及变换和邻接矩阵的电路转化规则, 总能以较小的量子代价综合出任意给定置换的 4 量子比特可逆逻辑电路.

关键词: 量子计算; 量子可逆逻辑电路; 酉矩阵

中图分类号: TP387; TN911.73 **文献标识码:** A **文章编号:** 0372-2112 (2010) 11-2561-05

Elementary Matrix Transformation Based Algorithm for 4-Qubit Reversible Circuits Synthesis

WANG Dong^{1,2}, CHEN Han-wu¹, AN Bo¹, YANG Zhong-ming¹

(1. School of Computer Science and Engineering, Southeast University, Nanjing, Jiangsu 210096, China;

2. Computer Center, Henan University, Kaifeng, Henan 475000, China)

Abstract: The process that the quantum reversible circuit realizes the information transformation can be demonstrated by unitary matrix. Matrix can better reflect the quantum state evolution and the physical properties of the quantum computation. Elementary Matrix transformation based algorithm for 4-qubit reversible circuits synthesis is proposed in this paper. The algorithm skillfully uses the matrix representation and transformation of the quantum circuit and the circuit rules of the adjacent matrix to construct any 4-qubit circuit given permutation with lower cost.

Key words: quantum computation; quantum reversible logic circuit; unitary matrix

1 引言

M A Nielsen 在其“Quantum Computation and Quantum Information”一书^[1]中指出: 利用量子力学理论进行信息加工处理的研究是未来最有前途的研究领域之一. 量子计算均可逆, Bennett 证明^[2]采用可逆逻辑门构建可逆电路可有效降低量子计算能耗. 近 30 年来, 人们已提出了多种量子可逆门, 如 Toffoli 门, Fredkin 门, Peres 门^[3]等. 如何使用指定量子门库自动生成量子代价较小的量子电路, 其本质就是量子可逆逻辑综合技巧问题. Maslov 等人提出利用真值表和模板技术构造优化量子电路的方法^[4,5]; Shende 将可逆电路综合转化为置换问题, 并提出了 3 量子可逆电路综合的最优算法^[6]; Yang 在此基础上利用 GAP 软件实现了 3 量子最小长度和最小代价可逆逻辑电路综合算法^[7]. 然而目前大多数算法只是在综

合 3 量子电路时效果很好, 随着综合量子比特数的增加, 综合可逆逻辑电路所需的内存空间远远超过经典计算机所能承受的范围. 在综合 4 量子比特电路时由于内存消耗太快, 所以综合出所有最优电路困难很大. Li 等人利用线置换和向变换进行无损压缩以及巧妙构造哈希函数可快速生成最多长度为 16 的最优 4 量子比特电路, 这是目前已知最好结果^[8].

本文提出基于矩阵初等变换的 4 量子比特可逆逻辑电路综合算法. 该算法利用量子电路的酉矩阵表示及变换和邻接矩阵的电路转化规则, 总能以较小的量子代价综合出任意给定置换的 4 量子比特可逆电路. 算法思想新颖, 基于酉矩阵演算, 理论基础可靠, 时空复杂度较小, 易于实现, 所使用量子门的数量比较为成熟的构造性算法^[9]更少.

2 置换的矩阵表示

定义 1 设 $\sum = \{a_1, a_2, \dots, a_n\}$ 是一个 n 元集合. 集合 \sum 到 \sum 的一一对应 σ 叫做 \sum 上的一个置换, 这个置换可以表示成:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{i_1} & a_{i_2} & \cdots & a_{i_n} \end{pmatrix}$$

\sum 上全部置换构成的集合叫做 \sum 上的对称群, 记作: S_n , 它的每个子群都叫做 \sum 上的置换群^[10].

量子可逆电路由量子门的组合与级联构成. n -qubit 电路实现的可逆操作作用函数表示为: $f(x_1, x_2, \dots, x_{2^n}) = (x_{i_1}, x_{i_2}, \dots, x_{i_{2^n}})$, $x_k \in (0 \cdots 2^n - 1)$. 其中, $x_{i_1}, x_{i_2}, \dots, x_{i_{2^n}}$ 为 x_1, x_2, \dots, x_{2^n} 的一个重新排列, 所以 f 是一个置换^[11], 记作: $f = \begin{pmatrix} x_1, x_2, \dots, x_{2^n} \\ x_{i_1}, x_{i_2}, \dots, x_{i_{2^n}} \end{pmatrix}$.

设 e_1, e_2, \dots, e_{2^n} 为 2^n 维 Hilbert 空间的一组标准正交基, $e_k (k \in (1 \cdots 2^n))$ 表示第 k 位为 1, 其余 $2^n - 1$ 位均为 0 的单位行向量, 即 $e_k = (0 \cdots \underset{k}{1} \cdots 0)$. n -qubit

可逆电路实现的置换 $f = \begin{pmatrix} x_1, x_2, \dots, x_{2^n} \\ x_{i_1}, x_{i_2}, \dots, x_{i_{2^n}} \end{pmatrix}$ 在映射 σ :

$$\sigma(x_{i_k}) = e_{x_{i_k}+1} \text{ 下被惟一表示成矩阵形式 } \begin{pmatrix} e_{x_{i_1}+1} \\ e_{x_{i_2}+1} \\ \vdots \\ e_{x_{i_{2^n}}+1} \end{pmatrix}. \text{ 因为}$$

在置换 $f = \begin{pmatrix} x_1, x_2, \dots, x_{2^n} \\ x_{i_1}, x_{i_2}, \dots, x_{i_{2^n}} \end{pmatrix}$ 中, $(x_{i_1}, x_{i_2}, \dots, x_{i_{2^n}})$ 是 $(x_1, x_2, \dots, x_{2^n})$ 的一个重新排列, 由 σ 的定义和矩阵乘法规则有:

$$\begin{pmatrix} e_{x_{i_1}+1} \\ e_{x_{i_2}+1} \\ \vdots \\ e_{x_{i_{2^n}}+1} \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2^n} \end{pmatrix} = \begin{pmatrix} x_{i_1} \\ x_{i_2} \\ \vdots \\ x_{i_{2^n}} \end{pmatrix}$$

则矩阵 $\begin{pmatrix} e_{x_{i_1}+1} \\ e_{x_{i_2}+1} \\ \vdots \\ e_{x_{i_{2^n}}+1} \end{pmatrix}$ 实现了置换 $f = \begin{pmatrix} x_1, x_2, \dots, x_{2^n} \\ x_{i_1}, x_{i_2}, \dots, x_{i_{2^n}} \end{pmatrix}$ 的函数

功能. 又因为 $(x_1, x_2, \dots, x_{2^n})$ 的全排列构成对称群 S_{2^n} , 其中每一个置换都是惟一的, 则在 $f = \begin{pmatrix} x_1, x_2, \dots, x_{2^n} \\ x_{i_1}, x_{i_2}, \dots, x_{i_{2^n}} \end{pmatrix}$ 中, x_k 惟一对应 x_{i_k} , 又从 σ 的定义知:

x_{i_k} 惟一对应 $e_{x_{i_k}+1}$, 所以 $\begin{pmatrix} e_{x_{i_1}+1} \\ e_{x_{i_2}+1} \\ \vdots \\ e_{x_{i_{2^n}}+1} \end{pmatrix}$ 是 n -qubit 可逆电路实现

置换 $f = \begin{pmatrix} x_1, x_2, \dots, x_{2^n} \\ x_{i_1}, x_{i_2}, \dots, x_{i_{2^n}} \end{pmatrix}$ 的惟一矩阵表示.

例 1 置换

$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 5 & 3 & 15 & 4 & 13 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 1 & 14 & 0 \end{pmatrix}$ 的矩阵如表 1.

表 1 置换 f 的矩阵表示

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\sigma(x_{i_1}) = \sigma(2) = e_{x_{i_1}+1} = e_{2+1} = e_3$$

$$\sigma(x_{i_2}) = \sigma(5) = e_{x_{i_2}+1} = e_{5+1} = e_6$$

$$\sigma(x_{i_3}) = \sigma(3) = e_{x_{i_3}+1} = e_{3+1} = e_4$$

$$\sigma(x_{i_4}) = \sigma(15) = e_{x_{i_4}+1} = e_{15+1} = e_{16}$$

$$\sigma(x_{i_5}) = \sigma(4) = e_{x_{i_5}+1} = e_{4+1} = e_5$$

$$\sigma(x_{i_6}) = \sigma(13) = e_{x_{i_6}+1} = e_{13+1} = e_{14}$$

$$\sigma(x_{i_7}) = \sigma(6) = e_{x_{i_7}+1} = e_{6+1} = e_7$$

$$\sigma(x_{i_8}) = \sigma(7) = e_{x_{i_8}+1} = e_{7+1} = e_8$$

$$\sigma(x_{i_9}) = \sigma(8) = e_{x_{i_9}+1} = e_{8+1} = e_9$$

$$\sigma(x_{i_{10}}) = \sigma(9) = e_{x_{i_{10}}+1} = e_{9+1} = e_{10}$$

$$\sigma(x_{i_{11}}) = \sigma(10) = e_{x_{i_{11}}+1} = e_{10+1} = e_{11}$$

$$\sigma(x_{i_{12}}) = \sigma(11) = e_{x_{i_{12}}+1} = e_{11+1} = e_{12}$$

$$\sigma(x_{i_{13}}) = \sigma(12) = e_{x_{i_{13}}+1} = e_{12+1} = e_{13}$$

$$\sigma(x_{i_{14}}) = \sigma(1) = e_{x_{i_{14}}+1} = e_{1+1} = e_2$$

$$\sigma(x_{i_{15}}) = \sigma(14) = e_{x_{i_{15}}+1} = e_{14+1} = e_{15}$$

$$\sigma(x_{i_{16}}) = \sigma(0) = e_{x_{i_{16}}+1} = e_{0+1} = e_1$$

定义 2 Toffoli 量子门, 记为 $TOF(C, T)$, 其中输入变量集合 $In = \{x_0, x_1, \dots, x_{n-1}\}$, 控制端集合 $C = \{x_{i_2}, x_{i_3}, \dots, x_{i_n}\}$, 受控端集合 $T = \{x_{i_1}\}$, 且 $C \cap T = \emptyset$, $C \cup T \subset In$. 输出变量集合映射为 $\{x_0, x_1, \dots, x_{i_1-1}, x_{i_1} \oplus \prod_{k=2}^n x_{i_k}, x_{i_1+1}, \dots, x_{n-1}\}$. 若 $\exists m \in \{2, 3, \dots, n\}$, $x_{i_m} = 0 \Rightarrow \prod_{k=2}^n x_{i_k} = 0$, 受控端 x_{i_1} 的输出为 $x_{i_1} \oplus \prod_{k=2}^n x_{i_k} = x_{i_1} \oplus 0 = x_{i_1}$; 若 $\forall m \in \{2, 3, \dots, n\}$, $x_{i_m} = 1 \Rightarrow \prod_{k=2}^n x_{i_k} = 1$, 受控端 x_{i_1} 的输出为 $x_{i_1} \oplus \prod_{k=2}^n x_{i_k} = x_{i_1} \oplus 1 = \bar{x}_{i_1}$. 控制端的数量决定了不同的 Toffoli 门, 如图 1 所示:

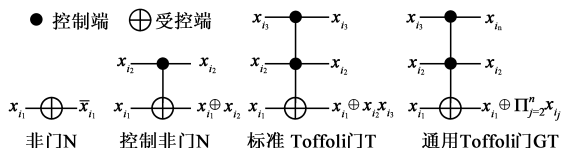


图1 Toffoli量子门

传统的 Toffoli 门是控制端置 1 对受控端进行控制, 而控制端置 0 对受控端进行控制也是常用的^[1,12,13], 这种情况等价于置 1 控制的控制点前后各加一个 X 门. 如图 2 所示:

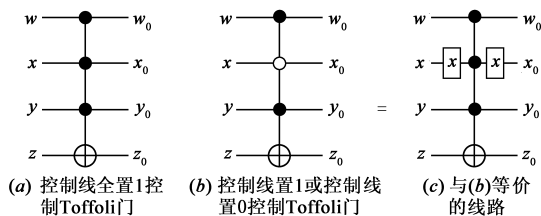


图2 两种控制条件的Toffoli门

图 2(a): $w_0 = w, x_0 = x, y_0 = y, z_0 = z \oplus uxy$

图 2(b): $w_0 = w, x_0 = x, y_0 = y, z_0 = z \oplus uxy$

图 2(c): 与图 2(b) 等价的应用传统的 Toffoli 门的线路

定义 3 设有两个不同的二进制数 s 和 t . 连接 s 和 t 的一个邻接矩阵定义为: 以 s 开头以 t 结束的一组二进制数组成的矩阵, 使得相邻的两个二进制数恰好仅有一位不同.

例 2 $s = 1001, t = 0111$, 连接 s 和 t 的邻接矩阵为:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \cdots \begin{matrix} s \\ d_1 \\ d_2 \\ t \end{matrix}$$

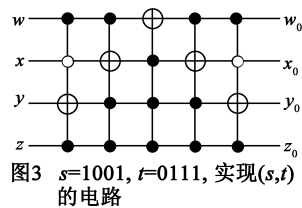
邻接矩阵可由一系列 Toffoli 门实现^[14], 由于:

$$(s, t) = (s, d_1) \cdot (d_1, d_2) \cdots (d_{n-1}, d_n) \cdot$$

$$(d_n, t) \cdot (d_n, d_{n-1}) \cdots (d_2, d_1) \cdot (d_1, s)$$

上式等号右边的每一个对换可用一个 Toffoli 门实现, 对于一个对换的两个二进制数, 让其中变化的那一位做受控端, 而其余不变的位做控制端.

例 3 同例 2: $s = 1001, t = 0111$, 根据其邻接矩阵有: $(s, t) = (s, d_1) \cdot (d_1, d_2) \cdot (d_2, t) \cdot (d_2, d_1) \cdot (d_1, s)$ 则实现 (s, t) 的电路, 如图 3 所示:

图3 $s=1001, t=0111$, 实现 (s, t) 的电路

3 基于矩阵变换的量子可逆电路综合算法

量子可逆电路综合问题就是找到一个门序列实现可逆函数的功能. 由于函数可逆, 所以问题可以转化为: 找到一个门序列, 将可逆函数变为恒等函数. 若可逆电路实现一个置换, 而置换又可用酉矩阵来表示, 因此实现置换的可逆电路综合问题又转化为: 找到将酉矩阵变换为单位矩阵的一个量子门序列. 由前文给出的置换的矩阵计算方法可知, 在置换的矩阵中每一行每一列都只有一个 '1', 其它位置全为 '0'. 将这种矩阵变换成单位矩阵只需逐次有序对调矩阵的两行, 对矩阵实施初等行变换即可, 而每一次对调过程都对应着一个量子门序列, 将这些量子门序列级联即构成实现给定置换的量子电路.

3.1 算法描述

基于以上分析, 给出基于矩阵变换的量子可逆电路综合算法.

第一步: 将给定置换表示成矩阵.

第二步: 依序对调矩阵的两行直到矩阵变为单位矩阵为止. 即首先对调两行, 将矩阵的第一行第一列变为 1, 再对调两行将矩阵的第二行第二列变为 1, 依此类推, 直到矩阵变为单位矩阵. 每次对调产生一个门序列的方法是: 设对调的两行为基 e_{k_1} 和 e_{k_2} , 则以 $(k_1 - 1, k_2 - 1)$ 构造邻接矩阵. 为一致性考虑, 规定统一用从右向左的顺序按位生成邻接矩阵. 依据定义 3 将每个邻接矩阵用对应的量子电路表示. 再将这些电路从后向前反向级联生成实现置换功能的量子可逆电路. 注意, 反向级联是因为算法采用把给定置换的矩阵向单位矩阵变换, 是逆向变换.

第三步: 优化电路, 优化规则为:

(1) 若 Toffoli 门 $A = TOF(x_1, x_2, \dots, x_{k-1}; x_k)$ 与 $B = TOF(y_1, y_2, \dots, y_{l-1}; y_l)$, 满足: $x_k \notin \{y_1, y_2, \dots, y_{l-1}\}$; 或者 $\exists x_i \in \{x_1, x_2, \dots, x_{k-1}\}$ and $y_i \in \{y_1, y_2, \dots, y_{l-1}\}$, 满足 $x_i = \bar{y}_i$. 则 A 与 B 互不影响, 可以交换 A, B 的位置. 交换相邻的两个门, 将受控端在同一条线上的量子门尽量排列在一起, 为下一步的合并

与移除优化操作做准备.

(2)相邻的两个 Toffoli 门,如果受控端相同而控制端只有一位不同,则可以把不同的控制端去掉,留下相同的控制端和受控端合并成 1 个 Toffoli 门.

(3)如果存在连续两个完全相同的 Toffoli 门则可以将这两个 Toffoli 门一起移除.

3.2 算法举例

考虑例 1,生成可逆电路的步骤如下:

(1)将置换

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 5 & 3 & 15 & 4 & 13 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 1 & 14 & 0 \end{pmatrix}$$

表示成矩阵,如表 1.

(2)将其变换为单位矩阵需对调的行为 (r_{16}, r_1) , (r_{14}, r_2) , (r_{16}, r_3) , (r_{16}, r_4) , (r_{14}, r_6) . 每一行对应的基为: (e_1, e_3) , (e_2, e_6) , (e_3, e_4) , (e_4, e_{16}) , (e_6, e_{14}) . 构造邻接矩阵:

$$\begin{matrix} (0,2) & (1,5) & (2,3) \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \\ (3,15) & (5,13) \\ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \end{matrix}$$

每个邻接矩阵对应一个 Toffoli 门序列,将这些门序列从后向前反向级联即生成实现给定置换的量子可逆逻辑电路,如图 4 所示:

(3)利用优化规则实施优化后的电路,如图 5 所示:

至此,给定置换被表示为 5 个 Toffoli 门的级联,电路综合过程完成.

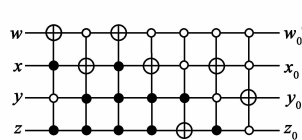


图4 实现置换 f 的电路

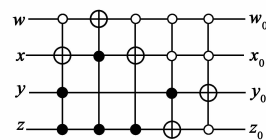


图5 实现置换 f 的优化电路

4 算法性能分析

定理 1 令 N 为 n -qubit 可逆电路实现的置换中不同于输入的输出的个数,基于矩阵初等变换的 n -qubit 可逆逻辑电路综合算法优化前所使用的 Toffoli 门最多为: $(2n-1) \cdot N$.

证明:因为在 n -qubit 可逆电路实现的置换中有 N 个不同于输入的输出,则将置换的矩阵变换为单位矩阵所需对调的行最多为 N 对.而每一对调行表示成邻接矩阵后,可用最多 $2n-1$ 个 Toffoli 门实现,所以实现置换的 Toffoli 门的数量最多为: $(2n-1) \cdot N$.

由于对量子相位的控制是一项复杂的技术,并且

量子系统固有的退相干效应将严重影响量子逻辑门的可靠性,因此制备高可信度的量子逻辑门是困难的.所以实现同一功能的量子电路所使用的量子逻辑门的数量成为衡量量子电路设计优劣的重要指标.目前较为成熟的 4 量子比特可逆电路构造性算法所使用的量子门数量最多为: $2n \cdot N$,在最坏情况下比我们的算法多 N 个量子门,并且我们的算法还提出了优化规则对电路实施优化,优化后 Toffoli 门的数量和复杂度都将进一步降低. n -qubit 可逆电路共有 $2^n!$ 个,其中 $N > 2^{n-1}$ 的电路数量将超过 n -qubit 可逆电路总数的一半以上,所以随着量子比特数的增加, N 较大的情况是普遍存在的,则我们的可逆电路设计方法的优势将更加突出.

我们的算法还是生成多量子可逆电路的通用算法,能够构建任意 n -qubit 可逆逻辑电路,而目前实现多量子 ($n \geq 4$) 可逆电路仍然是个难题,我们的算法并不受量子比特数的限制,很容易扩展到更高维的 Hilbert 空间,解决此问题,其基本思路为:首先将量子可逆逻辑电路实现的 2^n 个数的置换转换成 $2^n \times 2^n$ 的矩阵,当然,随着 n 的加大,矩阵的规模将增加.认真分析此矩阵的特点发现:矩阵是每一行每一列只有一个 1,其余位置全为 0 的稀疏矩阵.为降低矩阵对内存空间的消耗,只记录矩阵中 1 的位置,则只需一个具有 $\Theta(2^n)$ 个元素的数组.将矩阵调整为单位矩阵的过程即是将此数组中的元素交换排序的过程.利用两个交换元素的邻接矩阵产生局部电路,最后将所有交换元素的局部电路逆向连接,再使用 3 个优化规则简化电路即可.我们的算法思想简单精巧,计算机实现方便容易.

5 结论

酉矩阵是量子门的数学模型,能够形式化地描述量子系统的演化(如量子相位的部分转移等)和量子计算的数学属性.因此,量子电路的酉矩阵表示能够更加全面清晰地反映量子可逆电路的代数特征.依据此思想,本文提出基于矩阵初等变换的 4 量子比特可逆电路综合算法.该算法利用量子电路的酉矩阵表示及变换和邻接矩阵的电路转化规则,总能以较小的量子代价生成任意给定置换的 4 量子比特最优或近似最优电路.进一步的工作为:寻找更多更高效的电路优化规则或方法对生成的 4 量子比特可逆逻辑电路进行优化.

参考文献:

- [1] M A Nielsen, I L Chuang. Quantum Computation and Quantum Information [M]. Cambridge, England: Cambridge University Press, 2000. 4-40.
- [2] C Bennett. Logical reversibility of computation [J]. IBM Journal of Research and Development, 1973, 17(6): 525-532.

- [3] A Barceno, C Bennett, et al. Elementary gates for quantum computation [J]. Physical Review A, 1995, 52(5): 3457 – 3467.
- [4] D Maslov, G W Dueck, D M Miller. Toffoli network synthesis with templates [J]. IEEE Transactions on CADICS, 2005, 24(6): 807 – 817.
- [5] D M Miller, D Maslov, G W Dueck. A Transformation based algorithm for reversible logic synthesis [A]. Proceedings-Design Automation Conference [C]. New York: Institute of Electrical and Electronics Engineers Inc, 2003. 318 – 323.
- [6] V V Shende, A K Prasad, I L Markov, et al. Synthesis of reversible logic circuits [J]. IEEE Transactions on CADICS, 2003, 22(6): 710 – 722.
- [7] G W Yang, X Y Song, et al. Fast synthesis of exact Minimal reversible circuits using group theory [A]. Proceedings of the 2005 Conference on Asia South Pacific Design Automation [C]. New York: ACM, 2005. 1002 – 1005.
- [8] 李志强, 陈汉武, 徐宝文, 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, Xu Bao-wen, et al. Fast algorithms for 4-qubit reversible logic circuits synthesis [J]. Acta Electronic Sinica, 2008, 36(11): 2081 – 2089. (in Chinese)
- [9] G W Yang, F Xie, X Y Song, et al. A constructive algorithm for reversible logic synthesis [A]. 2006 IEEE Congress on Evolutionary Computation [C]. Piscataway: Inst of Elec and Elec Eng Computer Society, 2006. 2416 – 2421.
- [10] J D Dixon, B Mortimer. Permutation Group [M]. New York, America: Springer, 1996. 50 – 70.
- [11] L Storme, A De Vos, G Jacobs. Group theoretical aspects of reversible logic gates [J]. Journal of Universal Computer Science, 1999, 5(5): 307 – 321.
- [12] Y Zheng, C Huang. A novel Toffoli network synthesis algorithm for reversible logic [A]. Proceedings of the 2009 Asia and South Pacific Design Automation Conference [C]. Piscataway: Institute of Electrical and Electronics Engineers Inc, 2009. 739 – 744.
- [13] M Saeedi, M Sedighi, M S Zamani. A novel synthesis algorithm for reversible circuits [A]. IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers [C]. New York: Institute of Electrical and Electronics Engineers Inc, 2007. 65 – 68.
- [14] G W Yang, X Y Song, et al. Group theory based synthesis of binary reversible circuits [J]. Lecture Notes in Computer Science, 2006, 3959 LNCS: 365 – 374.

作者简介:



王 冬 女, 1977 年生于河南焦作, 博士研究生、副教授. 主要研究方向为量子计算、量子可逆逻辑综合.

E-mail: 122062815@qq.com



陈汉武 男, 1955 年生于江苏南京, 教授、博士生导师. 主要研究方向为经典信息论, 量子信息与量子计算, 数理解析.

E-mail: hw_chen@seu.edu.cn

安 博 男, 1986 年生于河南南阳, 硕士研究生. 主要研究方向为量子计算、量子可逆逻辑综合.

杨忠明 男, 1983 年生于安徽滁州, 硕士研究生. 主要研究方向为量子计算、量子可逆逻辑综合.