第 27 卷 第 1 期 量 子 电 子 学 报 Vol.27 No.1
2010 年 1 月 CHINESE JOURNAL OF QUANTUM ELECTRONICS Jan. 2010

DOI: 10.3969/j.issn.1007-5461.2010.01.005

用基本两位量子逻辑门实现n位量子逻辑门的研究

吕洪君， 郭俊旺， 彭 斐， 吴天昊， 解光军

（ 合肥工业大学电子科学与应用物理学院， 安徽 合肥 230009 ）

摘 要： 量子电路是实现量子态幺正演化的手段，一位和两位门是构成量子电路的基础。 Barenco 用基本的两位量子逻辑门实现 n 位量子逻辑门功能，张登玉在 Barenco 的工作基础上对用基本的两位量子逻辑门实现 n 位量子逻辑门功能进行了改进。通过对 Barenco 方案和张登玉方案的分析和研究，提出了一个用基本的两位量子逻辑门实现 n 位量子逻辑门功能的新方案，该方案结构更简单，且所用的两位门更易于实现，同时指出和改正了张文的不太准确的结论。

关键词： 量子信息；量子逻辑电路；量子逻辑门；幺正变换； Toffoli 门

中图分类号： O431.2 **文献标识码：** A **文章编号：** 1007-5461(2010)01-0026-05

n-bit quantum gate accomplished by two-bit quantum gates

LÜ Hong-jun, GUO Jun-wang, PENG Fei, WU Tian-hao, XIE Guang-jun

(School of Electronic Science and Applied Physics, Hefei University of Technology, Hefei 230009, China)

Abstract: Quantum circuits are the tools of realizing the unitary evolution of quantum state, and they are mainly made up of one-bit and two-bit quantum gates. Barenco proposed a method for constructing n-bit quantum gate by using basic two-bit quantum gates in 1995. Zhang proposed the improved method for constructing n-bit quantum gate by using basic two-bit quantum gates in 2001. The method for constructing n-bit quantum gate by using basic two-bit quantum gates is proposed by improving the two methods mentioned. The scheme is more simple and easier to implement and the incorrect conclusion by Zhang is amended.

Key words: quantum information; quantum logic circuit; quantum logical gate; unitary transformation; Toffoli gate

1 引 言

由电子计算机集成度引发的问题使人们预测经典电子计算机在今后的发展上会遇到极大的困难和挑战，甚至提出：按目前的发展速度，到本世纪 30 年代经典计算机发展水平将达到极限。为了解决这些困难， Feynman 在 1982 年提出用量子力学原理建设新型计算机 [1]— 量子计算机，由于量子计算机较经典计算机有不可比拟的优越性，量子计算机很快成为了人们研究的热点 [2,3]，而量子逻辑门则是其研究中一个比较重要的方向。研究表明 [4~6]：理论上所有的量子门都可以由那些一位门和两位门 (异或门) 组合起来实现其功能。

对单个量子位操作的一位门主要包括旋转操作、相移操作和 Pauli 操作，本文需用到的操作对应的幺正变换矩阵为

基金项目： 安徽省自然科学基金 (090412038) 和安徽省人才开发基金 (2007Z028) 资助项目

作者简介： 吕洪君 （ 1958 - ），硕士，副教授，主要从事量子信息方面的研究。 **E-mail:** lvhongjun1958@sina.com

收稿日期： 2009-07-23； **修改日期：** 2009-08-24

$$R_y(\theta)=\begin{pmatrix}\cos\frac{\theta}{2} & \sin\frac{\theta}{2}\\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix},\quad (\text{绕}y\text{轴转动}\theta\text{角}), \tag{1}$$

$$R_z(\alpha)=\begin{pmatrix}e^{i\frac{\alpha}{2}} & 0\\ 0 & e^{-\frac{\alpha}{2}}\end{pmatrix},\quad (\text{绕}z\text{轴转动}\alpha\text{角}), \tag{2}$$

$$\Phi(\delta)=\begin{pmatrix}e^{i\delta} & 0\\ 0 & e^{i\delta}\end{pmatrix},\quad (\delta\text{的相位变化}), \tag{3}$$

$$\sigma_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad (\text{泡利矩阵}). \tag{4}$$

两位门主要是控制非门

$$C_{\text{not}}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}. \tag{5}$$

Barenco[4] 研究了用基本的两位量子门实现任意 n 位量子逻辑功能的量子电路，张登玉 [7] 对 Barenco 方案进行了改进，使量子电路所需量子门数有所减少。本文在 Barenco 方案的基础上提出了对量子电路改进的新方案，改进后的方案不仅较前两者的方案有较多量子门数减少，而且所用的 V 门不随量子位的增加而变化，使得 V 门在使用中更方便且物理实现更容易。

2　Barenco 和张登玉的方案

2.1 Barenco 的方案

对于一个任意的 2×2 的幺正矩阵 U，一个四位控制 U 门 $\Lambda_3(U)$ 可以用图 1 的网络来实现。这里 $V^4=U, VV^+=I$，因此有一个 V^+ 的作用就可以抵消一个 V 的作用。设前三位的输入分别是 x_1、x_2、x_3，作用于第 4 位上的算符是 V 和 V^+，它们作用的条件从左到右依次为：x_1、$x_1\oplus x_2$、$x_1\oplus x_3$、$x_1\oplus x_2\oplus x_3$、x_3、x_2。只有当条件为 1 时，其对应的 V 和 V^+ 才会发生作用，得到如下的关系式

$$x_1+x_2+x_3-(x_1\oplus x_2)-(x_1\oplus x_3)+(x_1\oplus x_2\oplus x_3)=4\times(x_1\Lambda x_2\Lambda x_3), \tag{6}$$

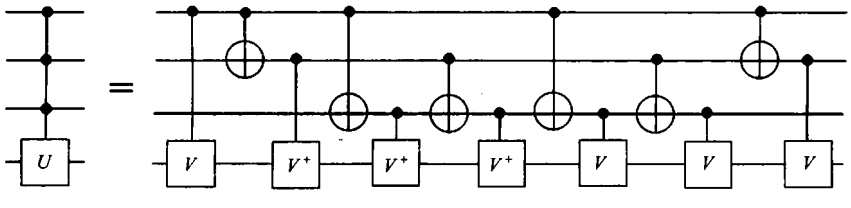

Fig.1　Quantum circuit of $\Lambda_3(U)$

当且仅当 x_1、x_2、x_3 同时为 1 时，有 4 个 V 先后作用在第 4 位上，而在其他情况下第 4 位的作用都相当于 I。所以令 $V^4=U$，即可实现所需逻辑功能。

对于一个任意的 2×2 的幺正矩阵 U，一个 $\Lambda_4(U)$ 可以用图 2 所示网络实现。用上面构建 $\Lambda_3(U)$ 门的方法同样可以来构建 $\Lambda_4(U)$ 门。设前四个量子位的输入分别是 x_1、x_2、x_3、x_4，由等式

$$\begin{aligned}x_1+x_2+x_3+x_4-(x_1\oplus x_2)-(x_1\oplus x_3)-(x_1\oplus x_4)+(x_1\oplus x_2\oplus x_3)+(x_1\oplus x_2\oplus x_4)+\\ (x_1\oplus x_3\oplus x_4)+(x_2\oplus x_3\oplus x_4)-(x_1\oplus x_2\oplus x_3\oplus x_4)=8\times(x_1\Lambda x_2\Lambda x_3\Lambda x_4),\end{aligned} \tag{7}$$

可以看出，当且仅当 x_1 、 x_2 、 x_3 、 x_4 都为 1 时，有 8 个 V 先后作用在第 5 量子位上，而在其他情况下，作用的第 5 量子位上的算符都相当于 I ，所以令 $V^8=U$ 时，即可实现 $\Lambda_4(U)$ 门。

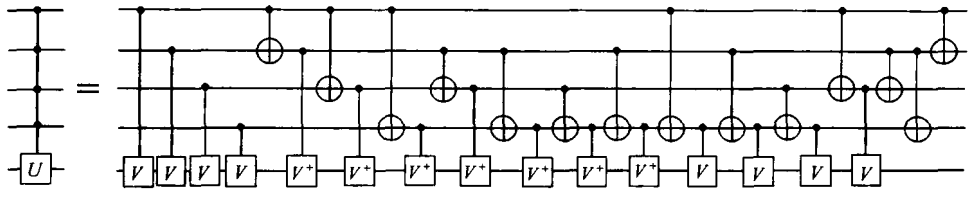

Fig.2 Quantum circuit of $\Lambda_4(U)$

对于一个任意 2×2 的幺正矩阵 U ，一个 $\Lambda_{n-1}(U)$ 门同样可以用上面的思路来实现。设前 $n-1$ 位的输入分别为 x_1 、 x_2 、 $\cdots$ 、 x_{n-1} ，则等式

$$\sum_{k_1}x_{k_1}-\sum_{k_1<k_2}(x_{k_1}\oplus x_{k_2})+\sum_{k_1<k_2<k_3}(x_{k_1}\oplus x_{k_2}\oplus x_{k_3})-\cdots+(-1)^{n-2}(x_1\oplus x_2\oplus\cdots\oplus x_{n-1})=2^{n-2}\times(x_1\Lambda x_2\Lambda\cdots\Lambda x_{n-1}),\tag{8}$$

当且仅当 x_1 、 x_2 、 $\cdots$ 、 x_{n-1} 同时为 1 时，有 2^{n-2} 个 V 作用在第 n 位上，其它情况下作用在第 n 位的算符都相当于 I ，那么令 $V^{2^{n-2}}=U$, 即可实现 $\Lambda_{n-1}(U)$ 的功能。通过统计可以得出：对于 $\Lambda_{n-1}(U)$ 门有 2^{n-2} 个 $\Lambda_1(V)$ 门和 $2^{n-2}-1$ 个 $\Lambda_1(V^+)$ 门以及 $2^{n-1}-2$ 个 $\Lambda_1(\sigma_x)$ 门，所以需要两位门的个数为 2^n-3 。

2.2 张登玉的方案

重点介绍张登玉对受控非门的实现方案。

$\Lambda_3(\sigma_x)$ 门如果用 Barenco 的方案来实现，则如图 3 所示 (其中 $V^4=\sigma_x, VV^+=I$) 。

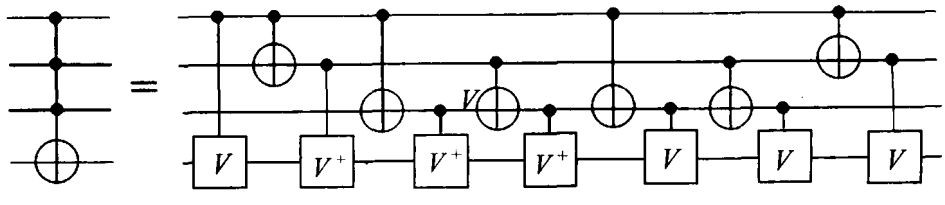

Fig.3 Quantum circuit of $\Lambda_3(\sigma_x)$

$\Lambda_3(\sigma_x)$ 用图 4 的网络来替换 (这里 $V^4=\sigma_x, VV^+=I$), 相对 Barenco 实现 $\Lambda_3(\sigma_x)$ 节省了 2 个 $\Lambda_1(\sigma_x)$ 且第 4 位上实现了其逻辑功能。

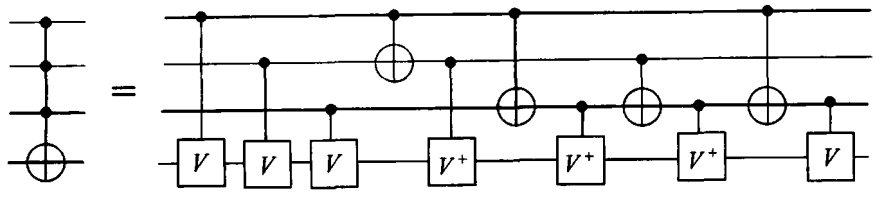

Fig.4 Quantum circuit of $\Lambda_3(\sigma_x)$

张登玉从四位、五位门得出构建 n 位网络可以比 Barenco 方案节省 2^{n-3} 个 $\Lambda_1(\sigma_x)$ 门，实际上仔细分析 6 位门时，我们发现只节省了 6 个门而非 8 个门。因为从构建 $\Lambda_{n-1}(\sigma_x)$ 门的角度讲，由等式

$$\sum_{k_1}x_{k_1}-\sum_{k_1<k_2}(x_{k_1}\oplus x_{k_2})+\sum_{k_1<k_2<k_3}(x_{k_1}\oplus x_{k_2}\oplus x_{k_3})-\cdots+(-1)^{n-2}(x_1\oplus x_2\oplus\cdots\oplus x_{n-1})=2^{n-2}\times(x_1\Lambda x_2\Lambda\cdots\Lambda x_{n-1}),\tag{9}$$

可以看出，这些条件中只有初始的输入 x_1 、 x_2 、 $\cdots$ 、 x_{n-1} 不用通过增加 $\Lambda_1(\sigma_x)$ 来实现，其它作用在第 n 位上的 $\Lambda_1(V)$ 门和 $\Lambda_1(V^+)$ 门的条件 $x_1\oplus x_2, x_1\oplus x_3\cdots$ 都需要增加 $\Lambda_1(\sigma_x)$ 来实现，所以 $\Lambda_{n-1}(\sigma_x)$

可以省去 $n-2$ 个 $\Lambda_1(\sigma_x)$ 门，最终 $\Lambda_{n-1}(\sigma_x)$ 需要 $2^n-3-(n-2)$ 个两位门来实现。这样对于任意的 $W(W=R_z(\alpha)R_y(\theta)R_z(\beta)),\Lambda_{n-1}(W)$ 需要 $2^n-2n+3(n\geq 3)$ 个两位门来实现，其中需要 $\Lambda_1(A),\Lambda_1(B)$ 和 $\Lambda_1(C)$ 各一个，需 $\Lambda_{n-2}(\sigma_x)$ 两个 (这里 $ABC=I, A\sigma_xB\sigma_xC=W$)。

3　用基本的两位量子门实现 n 位量子逻辑功能的新方案

已经证明，全部的 1 位量子门和受控非门可以构成量子计算的通用门集。这里提出一个实现任意受控运算的新方案，可以用数学归纳法的形式给出。

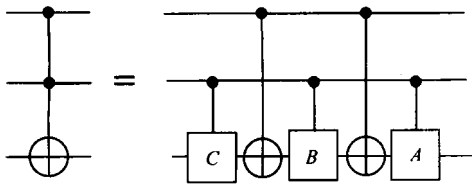

Fig.5　Quantum circuit of $\Lambda_2(\sigma_x)$

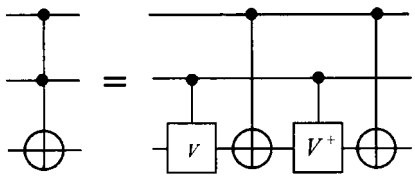

Fig.6　Quantum circuit of $\Lambda_2(\sigma_x)$

定理：对于任意 2×2 的幺正矩阵 $W, W=R_z(\alpha)R_y(\theta)\times R_z(\beta)$，存在矩阵 A、B、C，使得 $ABC=I$ 且 $A\sigma_xB\sigma_xC=W$。根据以上定理，当 $n=3$ 时，$\Lambda_2(\sigma_x)$ 门可以按照图 5 所示实现，其中 n 为量子逻辑电路的位数。

令 $A=V=\dfrac{1}{1+\mathrm{i}}\begin{pmatrix}1 & \mathrm{i}\\ \mathrm{i} & 1\end{pmatrix}, B=V^+, C=I$。则 $ABC=I$，且 $A\sigma_xB\sigma_xC=\sigma_x$，满足以上定理的条件。因此 $\Lambda_2(\sigma_x)$ 门可以按图 6 所示来实现。且当 $n=3$ 时，所需门的总个数满足公式 $2^{n-1}+2^{n-2}-2$。

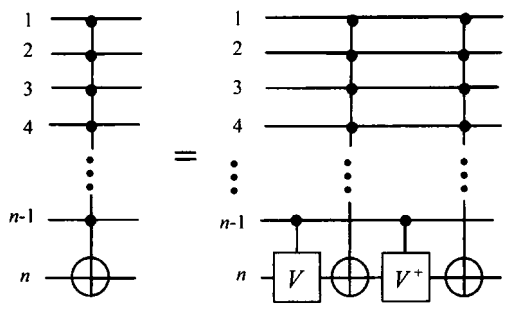

Fig.7　Quantum circuit of $\Lambda_{n-1}(\sigma_x)$

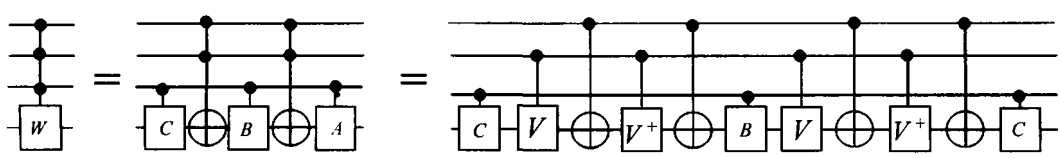

Fig.8　Quantum circuit of $\Lambda_3(W)$

假设 $n-1$ 位门 $\Lambda_{n-2}(\sigma_x)$ 可以实现，且所需门的个数满足公式 $2^{n-1}+2^{n-2}-2$，则 n 位门 $\Lambda_{n-1}(\sigma_x)$ 可以按图 7 方式实现。此时所需门的总个数为 $2(2^{n-2}+2^{n-3}-2)+2=2^{n-1}+2^{n-2}-2$。

由数学归纳法可知，所有的受控非门都可以按上述方法递归地给出，而且所需的门的总数为 $2^{n-1}+2^{n-2}-2$。类比上面的过程，可以得到一般的受控门的构造方法。

4 位门 $\Lambda_3(W)$ 的构造方法如图 8 所示。其中 $ABC=I, A\sigma_xB\sigma_xC=W, V^2=\sigma_x, VV^+=I$。

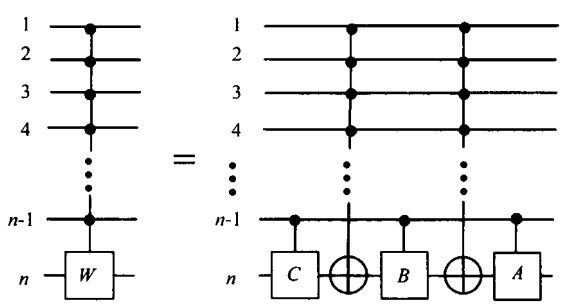

Fig.9　Quantum circuit of $\Lambda_{n-1}(W)$

n 位门网络即 $\Lambda_{n-1}(W)$ 门如图 9 所示。用数学归纳法不难证明该网络共需 $2^{n-1}+2^{n-2}-1$ 个两位门，其中 $\Lambda_1(A)$、$\Lambda_1(B)$ 和 $\Lambda_1(C)$ 各一个、$2^{n-2}+2^{n-3}-2$ 个 $\Lambda_1(V)$ 门和 $2^{n-2}+2^{n-3}-2$ 个 $\Lambda_1(V^+)$ 门。门的种类和数量都大大减少，而且网络构建相对容易，多位的 Toffoli 门移植性强，不用新门即可实现由基本门加上 $\Lambda_1(V)$ 和 $\Lambda_1(V^+)$ 门直接构造 $\Lambda_{n-1}(\sigma_x)$ 门。

4 结 论

本文所提出的一个新的由基本的两位门实现 n 位量子逻辑功能的量子电路，与前人的方案相比具有如下特点：

1) 本文的方案所需两位门的数量少。 Barenco 的方案需用 $2^n-3(n\geq 3)$ 个两位门，张登玉方案需用 $2^n-2n+3(n\geq 3)$ 个两位门，而本文方案仅需 $2^{n-1}-2^{n-2}-1(n>3)$ 个两位门即可实现相同功能。

2) 本文的方案所需两位门的种类少。在 Barenco 的方案中 $V^{2^{n-2}}=U$, 对于 n 的取值不同， $\Lambda_1(V)$ 和 $\Lambda_1(V^+)$ 也有所不同. 在张登玉的方案中 $V^{2^{n-3}}=\sigma_x$, 因此同样对于 n 的取值不同， $\Lambda_1(V)$ 和 $\Lambda_1(V^+)$ 也会不同. 而本文方案中的 $\Lambda_1(V)$ 和 $\Lambda_1(V^+)$ 是固定的，即使对于不同 n 的多位 Toffoli 门， $V=\frac{1}{1+\mathrm{i}}\begin{pmatrix}1 & \mathrm{i}\\ \mathrm{i} & 1\end{pmatrix}$ 都是恒定的。

3) 本文方案的网络构建简单，移植性好，可直接由基本门加上 $\Lambda_1(V)$ 和 $\Lambda_1(V^+)$ 门来构建任意 $n(n\geq 3)$ 位的 Toffoli 门。

值得一提的是，在张登玉方案中，其与 Barenco 方案所用两位门个数进行对比，得出的结论是 n 位门节省 $2^{n-3}(n\geq 3)$ 个两位门. 实际上，我们通过分析发现，张登玉的方案较 Barenco 的方案只节省了 $2n-6$ 个两位门。

参考文献：

[1] Feynman R P. Simulating physics with computers [J]. *Int. J. Theor. Phys.*, 1982, 21: 457-488.

[2] Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer [C]. *Proc. of Roy. Soc. London. A*, 1985, 400: 97-117.

[3] Birnbaum J. Williams R S. Physics and the information revolution [J]. *Physics Today*, 2000, 53: 38-42.

[4] Barenco A, Bennett C H, Cleve R, *et al.* Elementary gates for quantum computation [J]. *Phys. Rev. A*, 1995, 52(5): 3457-3467.

[5] Sleator T. Realizable universal quantum logic gates [J]. *Phys. Rev. Lett. A*, 1995, 74(20): 4087-4090.

[6] Divincenzo D P. Two-bit gates are universal for quantum computation [J]. *Phys. Rev. A*, 1995, 51(2): 1015-1022.

[7] Zhang Dengyu. Two-bit quantum gates to implement n-bit quantum gates [J]. *Journal of Optoelectronics • Laser* (光电子 • 激光), 2001, 12(11): 1190-1192 (in Chinese).