

多值逻辑量子置换门的酉矩阵表示

王 冬^{1),2)} 陈汉武¹⁾ 朱皖宁¹⁾ 刘志昊¹⁾

¹⁾(东南大学计算机科学与工程学院 南京 210096)

²⁾(河南大学复杂智能网络系统研究所 河南 开封 475004)

摘 要 理论上量子可逆电路不存在能量耗散问题,因此量子计算系统对环境产生的负面影响可以达到最低.多值逻辑量子置换门是构建多值逻辑量子电路的基本单元.该文从数学的角度研究多值逻辑量子置换门的酉矩阵,提出了一种构造多值逻辑量子置换门酉矩阵的方法,并对其正确性进行了讨论.在此基础上,又给出了构造混合多值逻辑量子置换门酉矩阵的框架,利用此框架可以方便地构造任何混合逻辑量子置换门的酉矩阵.酉矩阵是量子门的数学模型,可以清晰地反映出量子门的数学性质.研究量子门的酉矩阵对验证量子门的正确性和可靠性,分析量子状态在电路中的演化过程及发展趋势具有一定的意义.

关键词 绿色计算;量子计算;多值逻辑;量子门;低功耗

中图法分类号 TP387 **DOI号**: 10.3724/SP.J.1016.2012.00639

Unitary Matrix of Multiple-Valued Quantum Permutation Gate

WANG Dong^{1),2)} CHEN Han-Wu¹⁾ ZHU Wan-Ning¹⁾ LIU Zhi-Hao¹⁾

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

²⁾(Institute of Complex Intelligent Network System, Henan University, Kaifeng, Henan 475004)

Abstract The negative effects to environment arose from quantum computing system can reach minimum in theory because there is no power dissipation in quantum reversible circuits. Multiple-valued quantum permutation gate is the basic unit to construct multiple-valued quantum circuits. In this paper, the unitary matrix of multiple-valued quantum permutation gate is studied from the view of mathematics. A method constructing the unitary matrix of multiple-valued quantum permutation gate is put forward, and its correctness is discussed constructively by permutation matrix. On the basis of it, a framework by which the unitary matrix of any hybrid quantum gate can be constructed is presented. Unitary matrix is mathematical model of quantum gate and can reflect quantum gate's mathematical properties clearly. The research on quantum gate's unitary matrix is significant to verify the correctness and reliability of quantum gate and to analyze the evolution process and development trend of quantum state in quantum circuits.

Keywords green computing; quantum computation; multiple-valued logic; quantum gate; low power

1 引 言

自哥本哈根大会之后,有效保护环境、合理利用

资源、建设低碳社会已经成为全球共识.目前计算机系统的广泛使用使得IT业的二氧化碳排放量已占全球总排放量的2%,IT行业对环境的负面影响日益突显.协调IT技术及产品和环境的关系,实施低

收稿日期:2011-08-05;最终修改稿收到日期:2012-01-10. 本课题得到国家自然科学基金(61070240,60873101)、河南省自然科学基金(102300410175)、江苏省高校自然科学基金(10KJB520021)、河南大学自然科学基金(09YBZR043)资助. 王 冬,女,1977年生,博士研究生,副教授,主要研究方向为量子计算、量子可逆逻辑电路综合. E-mail: juliaudd@qq.com; wdyumei@henu.edu.cn. 陈汉武,男,1955年生,博士,教授,博士生导师,主要研究领域为信息论、量子信息与量子计算. 朱皖宁,男,1983年生,博士研究生,主要研究方向为量子算法、量子可逆逻辑电路综合. 刘志昊,男,1982年生,博士研究生,主要研究方向为量子通信、量子信息处理.

功耗、低排放、高效率的“绿色计算”是最有效的解决方案之一^[1]. 量子计算是指利用微观粒子的状态作为信息的载体, 凭借着量子所特有的一些力学性质, 进行有效计算的新颖计算模式. 量子电路是进行量子计算的硬件基础, 具有可逆性, 要求其输入和输出之间存在一一映射, 因此电路中不存在扇入、扇出和反馈逻辑, 理论上不丢失输入信息, 不存在能量耗散问题, 从而可将芯片的运行速度和计算能力发挥到极致. Bennett^[2]证明采用可逆逻辑门构建可逆电路可有效降低计算能耗(理论上可以达到最低能耗). 因此量子计算系统对环境产生的负面影响可以达到最低.

量子计算具有并行、可逆及理论上无条件安全等特性, 在复杂计算和安全通信等领域被证明具有超越经典计算的潜力, 被认为是最具前景的计算和通信技术之一, 因此受到了越来越多的关注^[3]. 一次量子计算过程可以看作是一系列量子门作用在一个标准的初态上, 最后进行一次标准的测量^[4], 其中量子门的作用是实现量子状态的演化^[5-6]. 量子置换门是一类完成置换功能的量子门, 如 Toffoli 门、CNOT 门、Swap 门等^[7]. 多值逻辑量子置换门是二值逻辑量子置换门在多值逻辑空间中的扩展, 在多值逻辑量子计算中应用广泛, 发挥着重要作用^[8](多值逻辑是描述多级量子系统(multiple-level quantum system)所负载信息的理想数学工具^[9]). 与二值逻辑量子门相比, 多值逻辑量子门在存储和处理信息时具有更强的酉变换能力和灵活性, 实现相同的任务可使用更少的门, 并可有效减少量子寄存器的位数^[10].

2000 年 Muthukrishnan 和 Stroud^[9]设计并实现了在线性离子阱中构建一位和两位多值逻辑量子基本门(quantum primitive gate)的方案, 有力论述并证明了多值逻辑量子门物理实现的可行性. 2003 年 Daboul 等人^[11]提出量子混合门(quantum hybrid gate)的概念, 即所涉及的各量子位分别在不同的逻辑空间中的量子门, TS 门是已经物理实现的混合二值、三值逻辑量子置换门^[12]. 2009 年 Lanyon 等人^[8]利用线性光子系统实现了三值逻辑 Toffoli 门, 这是量子电路物理实现上的一项重大突破, 因为 Toffoli 门和 Hadamard 门可构成量子计算的一个通用门集. 酉性限制是对量子门的惟一限制, 每个酉矩阵都可定义一个有效的量子门^[5]. 酉矩阵是量子门的数学模型, 可清晰的反映出量子门的数学性质, 并可检验量子门物理实现的正确性, 因此研究量子

门的酉矩阵具有一定的意义.

基于多值逻辑量子置换门实现的置换功能, 本文提出了一种多值逻辑量子置换门的酉矩阵构造方法, 利用此方法可以简便的构造出多值逻辑量子置换门的酉矩阵. 在此基础上, 又给出了混合多值逻辑量子置换门的酉矩阵构造框架, 利用此框架可以构造任何混合逻辑量子置换门的酉矩阵. 量子门酉矩阵构造方法的给出有助于分析量子态的演化过程, 验证量子门及量子电路的正确性和可靠性.

2 多值逻辑量子置换门

定义 1. 设 $\Sigma = \{a_0, a_1, \dots, a_{n-1}\}$ 是一个 n 元集合. 集合 Σ 到 Σ 的 1-1 映射 f 叫做 Σ 上的一个置换, 表示为 $f = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{i_0} & a_{i_1} & \dots & a_{i_{n-1}} \end{pmatrix}$. Σ 上全部置换构成的集合称为 Σ 上的对称群, 记作 S_n , 其中元素个数为 $n!$. 对称群的每个子群叫做 Σ 上的置换群^[13].

定义 2. 实现置换函数功能的量子门称为量子置换门^[14].

定义 3. 一个 d 值逻辑量子位(qudit)的量子态可以用 d 个计算基态 $|0\rangle, |1\rangle, \dots, |d-1\rangle$ 的线性组合来表示:

$$|\psi\rangle = \sum_{m=0}^{d-1} c_m |m\rangle \quad (1)$$

其中 c_m 为概率幅(amplitude), 测量结果 m ($m \in \{0, 1, \dots, d-1\}$) 出现的概率是 $|c_m|^2$, 满足归一化条件: $\sum_{m=0}^{d-1} |c_m|^2 = 1$, 当有两个或多个 $c_m \neq 0$ 时, 称 $|\psi\rangle$ 为叠加态. 例如, 三值逻辑量子位的一个叠加态: $|\psi\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$.

定义 4. k 个 d 值逻辑量子位的复合量子系统的状态可以用 d^k 个计算基态: $|\underbrace{0, 0, \dots, 0}_{k\text{个}}\rangle, |\underbrace{0, 0, \dots, 1}_{k\text{个}}\rangle, \dots, |\underbrace{d-1, d-1, \dots, d-1}_{k\text{个}}\rangle$ (用十进制表示即为 $|0\rangle, |1\rangle, \dots, |d^k-1\rangle$) 的线性组合来表示:

$$|\phi\rangle = \sum_{n=0}^{d^k-1} c_n |n\rangle \quad (2)$$

其中 c_n 为概率幅, 测量结果 n ($n \in \{0, 1, \dots, d^k-1\}$) 出现的概率是 $|c_n|^2$, 满足归一化条件 $\sum_{n=0}^{d^k-1} |c_n|^2 = 1$.

k 个 d 值逻辑量子位的复合量子系统可构成一个 d 值逻辑的 k 位量子寄存器. 例如两个三值逻辑量子位所组成的量子寄存器的可能状态之一是

$$|\phi\rangle = \frac{1}{3}(|00\rangle + |01\rangle + |02\rangle + |10\rangle + |11\rangle + |12\rangle + |20\rangle + |21\rangle + |22\rangle).$$

定义 5. 在多值逻辑空间中实现置换函数功能的量子门叫做多值逻辑量子置换门. 有些量子置换门所涉及的量子位分别处于不同的逻辑空间, 这种门叫做混合多值逻辑量子置换门.

3 多值逻辑量子置换门的酉矩阵表示

置换门实现置换的功能, 即置换门的输出是其输入的一个置换. 置换门的酉矩阵是置换矩阵(单位矩阵的某些行和列交换后得到的矩阵). 可依据置换门所完成的置换功能写出它的酉矩阵.

若 d 值逻辑 k 位置换门 U 所完成的置换功能为

$$U: \begin{pmatrix} 0 & 1 & \cdots & d^k - 1 \\ U(0) & U(1) & \cdots & U(d^k - 1) \end{pmatrix} \quad (3)$$

它对应的 $d^k \times d^k$ 的置换矩阵 P_U 为: 在第 i 列 ($i \in \{0, 1, \dots, d^k - 1\}$) 只有第 $U(i)$ 位上元素为 1, 其余全为 0 的矩阵. P_U 可以写作:

$$P_U = [e_{U(0)} \ e_{U(1)} \ \cdots \ e_{U(d^k - 1)}] \quad (4)$$

其中每个 $e_{U(i)}$ 表示正则基^[15]中的一个, 也就是第 $U(i)$ 位上元素为 1, 其余全为 0 的 d^k 元列向量.

置换门酉矩阵的构造方法也可以简单地描述为: 依次排列从 $U(0)$ 到 $U(d^k - 1)$ 所对应的量子态的列向量.

令 P_U 为量子门的酉矩阵, 则有 $P_U(0, 1, \dots, d^k - 1) = (U(0), U(1), \dots, U(d^k - 1))$, 由于 $0, 1, \dots, d^k - 1$ 所对应的量子态的列向量依次排列构成单位矩阵 I , 所以有 $P_U I = (U(0), U(1), \dots, U(d^k - 1))$, 则 P_U 就等于 $U(0), U(1), \dots, U(d^k - 1)$ 所对应的量子态的列向量依次排列构成的矩阵, 而 $e_{U(0)}, e_{U(1)}, \dots, e_{U(d^k - 1)}$ 正好分别就是 $U(0), U(1), \dots, U(d^k - 1)$ 所对应的量子态的列向量, 所以式(4)是正确的.

例 1. 三值逻辑 CNOT 门是两位的三值逻辑量子置换门, 目前它所实现的置换功能按照不同的实现方案可分为两种:

(1) 第一量子位的输出状态始终等于其输入状态, 第二量子位的输出状态为: 当第一量子位的输入状态为 $|2\rangle$ 时, 第二量子位的输出状态等于其输入状

态进行加 1 模 3, 否则第二量子位的输出状态等于其输入状态^[9,16]. 这种实现方案可用图 1 表示.

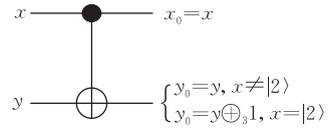


图 1 三值逻辑 CNOT 门的第 1 种实现方案

按照此种实现方案, 三值逻辑 CNOT 门实现的置换为 $|00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, |02\rangle \mapsto |02\rangle, |10\rangle \mapsto |10\rangle, |11\rangle \mapsto |11\rangle, |12\rangle \mapsto |12\rangle, |20\rangle \mapsto |21\rangle, |21\rangle \mapsto |22\rangle, |22\rangle \mapsto |20\rangle$. 依据上述给出的多值逻辑量子置换门的酉矩阵构造方法可生成其酉矩阵, 如图 2 所示(行号为输入, 列号依次为相应输入的输出).

	$ 00\rangle$	$ 01\rangle$	$ 02\rangle$	$ 10\rangle$	$ 11\rangle$	$ 12\rangle$	$ 21\rangle$	$ 22\rangle$	$ 20\rangle$
$ 00\rangle$	1	0	0	0	0	0	0	0	0
$ 01\rangle$	0	1	0	0	0	0	0	0	0
$ 02\rangle$	0	0	1	0	0	0	0	0	0
$ 10\rangle$	0	0	0	1	0	0	0	0	0
$ 11\rangle$	0	0	0	0	1	0	0	0	0
$ 12\rangle$	0	0	0	0	0	1	0	0	0
$ 20\rangle$	0	0	0	0	0	0	0	1	0
$ 21\rangle$	0	0	0	0	0	0	1	0	0
$ 22\rangle$	0	0	0	0	0	0	0	1	0

图 2 实现第 1 种置换功能的三值逻辑 CNOT 门的酉矩阵

(2) 第一量子位的输出状态始终不变, 第二量子位的输出状态等于第一、二量子位的输入之和(是模 3 加运算)^[17]. 这种实现方案可用图 3 表示.

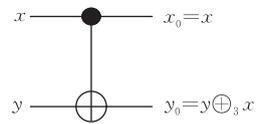


图 3 三值逻辑 CNOT 门的第 2 种实现方案

按照此种实现方案, 三值逻辑 CNOT 门实现的置换为 $|00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, |02\rangle \mapsto |02\rangle, |10\rangle \mapsto |11\rangle, |11\rangle \mapsto |12\rangle, |12\rangle \mapsto |10\rangle, |20\rangle \mapsto |22\rangle, |21\rangle \mapsto |20\rangle, |22\rangle \mapsto |21\rangle$. 依据上述方法可生成其酉矩阵如图 4 所示.

	$ 00\rangle$	$ 01\rangle$	$ 02\rangle$	$ 11\rangle$	$ 12\rangle$	$ 10\rangle$	$ 22\rangle$	$ 20\rangle$	$ 21\rangle$
$ 00\rangle$	1	0	0	0	0	0	0	0	0
$ 01\rangle$	0	1	0	0	0	0	0	0	0
$ 02\rangle$	0	0	1	0	0	0	0	0	0
$ 10\rangle$	0	0	0	0	0	1	0	0	0
$ 11\rangle$	0	0	0	1	0	0	0	0	0
$ 12\rangle$	0	0	0	0	1	0	0	0	0
$ 20\rangle$	0	0	0	0	0	0	0	1	0
$ 21\rangle$	0	0	0	0	0	0	0	0	1
$ 22\rangle$	0	0	0	0	0	0	1	0	0

图 4 实现第 2 种置换功能的三值逻辑 CNOT 门的酉矩阵

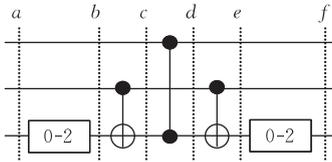


图 6 TS 门

图 6 中, a 点和 b 点之间为 0-2 门。0-2 门是三值逻辑一位量子门, 是置换门, 置换功能为 $|0\rangle \mapsto |2\rangle, |1\rangle \mapsto |1\rangle, |2\rangle \mapsto |0\rangle$ 。依据第 3 小节置换门矩阵的生成方法, 可给出 0-2 门的矩阵为

$$U_{0-2} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

TS 门的 3 个量子位上的输入都只有状态 $|0\rangle$ 和 $|1\rangle$, 虽然第三位作用在三值逻辑空间, 但状态 $|2\rangle$ 并不作为第三位的输入状态, 表 1 显示了对于所有可能的输入状态, 在 TS 门各点上状态的变化情况。

表 1 TS 门在各点的状态变化

a	b	c	d	e	f
$ 000\rangle$	$ 002\rangle$	$ 002\rangle$	$ 002\rangle$	$ 002\rangle$	$ 000\rangle$
$ 001\rangle$	$ 001\rangle$	$ 001\rangle$	$ 001\rangle$	$ 001\rangle$	$ 001\rangle$
$ 010\rangle$	$ 012\rangle$	$ 012\rangle$	$ 012\rangle$	$ 012\rangle$	$ 010\rangle$
$ 011\rangle$	$ 011\rangle$	$ 010\rangle$	$ 010\rangle$	$ 011\rangle$	$ 011\rangle$
$ 100\rangle$	$ 102\rangle$	$ 102\rangle$	$ 102\rangle$	$ 102\rangle$	$ 100\rangle$
$ 101\rangle$	$ 101\rangle$	$ 101\rangle$	$- 101\rangle$	$- 101\rangle$	$- 101\rangle$
$ 110\rangle$	$ 112\rangle$	$ 112\rangle$	$ 112\rangle$	$ 112\rangle$	$ 110\rangle$
$ 111\rangle$	$ 111\rangle$	$ 110\rangle$	$ 110\rangle$	$ 111\rangle$	$ 111\rangle$

5 结 论

随着计算机系统及网络应用日益广泛与深入, 节省系统能耗、降低系统排放、构建环境友好的绿色计算系统成为计算机科学的一个重要研究方向。由于理论上量子计算模式对环境产生的负面影响可以达到最低从而成为绿色计算的备选模式之一。

与二值逻辑量子计算相比, 多值逻辑量子计算更自然, 运算能力更强, 实现相同的计算任务需要的量子位更少, 因此更具优势。

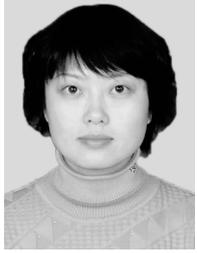
多值逻辑量子置换门是多值逻辑量子计算中一类重要的量子门。我们提出了一种依据多值逻辑量子置换门所实现的置换功能构造其酉矩阵的方法, 用此方法可以简便的计算出多值逻辑量子置换门的酉矩阵。在此基础上, 我们又给出了混合多值逻辑量子置换门的酉矩阵构造框架, 利用此框架可以方便的计算出混合多值逻辑量子置换门的酉矩阵。酉矩阵是量子门的数学模型, 可以清晰的反映出量子

门的数学性质, 因此研究量子门的酉矩阵对于验证量子门的正确性和可靠性, 构造新型量子门, 分析量子状态在电路中的演化过程及其发展趋势具有一定的意义。

参 考 文 献

- [1] Guo Bing, Shen Yan, Shao Zi-Li. The redefinition and some discussion of green computing. Chinese Journal of Computers, 2009, 32(12): 2311-2319(in Chinese)
(郭兵, 沈艳, 邵子立. 绿色计算的重定义与若干探讨. 计算机学报, 2009, 32(12): 2311-2319)
- [2] Bennett C H. Logical reversibility of computation. IBM Journal of Research and Development, 1973, 17(6): 525-532
- [3] Plesch M, Brukner C. Quantum-state preparation with universal gate decompositions. Physical Review A, 2011, 83(3): 032302/1-5
- [4] Guo Z H, Cao H X, Chen Z L, Yin J C. Operational properties and matrix representations of quantum measures. Chinese Science Bulletin, 2011, 56(16): 1671-1678
- [5] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000
- [6] Zhang Y, Cao H X, Li L. Realization of allowable generalized quantum gates. Science China: Physics, Mechanics & Astronomy, 2010, 53(10): 1878-1883
- [7] Toffoli T. Reversible computing. Lecture Notes in Computer Science, 1980, 85: 632-644
- [8] Lanyon B P, Barbieri M, Almeida M P et al. Simplifying quantum logic using higher-dimensional hilbert spaces. Nature Physics, 2009, 5(2): 134-140
- [9] Muthukrishnan A, Stroud C R. Multivalued logic gates for quantum computation. Physical Review A, 2000, 62(5): 052309/1-8
- [10] Bullock S S, O'leary D P, Brennen G K. Asymptotically optimal quantum circuits for d-level systems. Physical Review Letters, 2005, 94(23): 230502/1-4
- [11] Daboul J, Wang X, Sanders B C. Quantum gates on hybrid qudits. Journal of Physics A: Mathematical and General, 2003, 36(10): 2535-2536
- [12] Lanyon B P, Barbieri M, Almeida M P et al. Quantum computing using shortcuts through higher dimensions. arXiv Quantum Physics, 2008, 0804.0272: 1-7
- [13] Dixon J D, Mortimer B. Permutation Group. New York: Springer, 1996
- [14] Li Zhi-Qiang, Li Wen-Qian, Chen Han-Wu. Algorithm of optimizing quantum reversible logic synthesis. Journal of Software, 2009, 20(9): 2332-2343(in Chinese)
(李志强, 李文骞, 陈汉武. 量子可逆逻辑综合的关键技术及其算法. 软件学报, 2009, 20(9): 2332-2343)

- [15] Fang Bao-Rong, Zhou Ji-Dong, Li Yi-Min et al. *Matrix Theory*. Beijing: Tsinghua University Press, 2004(in Chinese) (方保镛, 周继东, 李医民等. 矩阵论. 北京: 清华大学出版社, 2004)
- [16] Yang G W, Xie F, Song X Y, Perkowski M A. Universality of 2-qudit ternary reversible gates. *Journal of Physics A: Mathematical and General*, 2006, 39(24): 7763-7773
- [17] Khan M H A. Quantum realization of multiple-valued Feynman and Toffoli gates without ancilla input//Proceedings of the 39th International Symposium on Multiple-Valued Logic (ISMVL 2009). Naha Okinawa, Japan, 2009: 103-108
- [18] Ralph T C, Resch J, Gilchrist A. Efficient toffoli gates using qudits. *Physical Review A*, 2007, 75(2): 022313/1-5



WANG Dong, born in 1977, Ph. D. candidate, associate professor. Her current research interests include quantum computation and quantum reversible logic circuit synthesis.

CHEN Han-Wu, born in 1955, Ph. D., professor, Ph. D. supervisor. His current research interests include in-

formation theory, quantum information and quantum computation.

ZHU Wan-Ning, born in 1983, Ph. D. candidate. His current research interests include quantum inspired algorithm, quantum reversible logic circuit synthesis.

LIU Zhi-Hao, born in 1982, Ph. D. candidate. His current research interests include quantum communication, quantum information processing.

Background

This work is supported by the National Natural Science Foundation of China under grant Nos. 61070240, 60873101, Natural Science Foundation of Henan Province under grant No. 102300410175, Natural Science Foundation for Colleges of Jiangsu Province under grant No. 10KJB520021, and Natural Science Foundation of Henan University under grant No. 09YBZR043. In these projects, quantum gates, quantum circuit synthesis methods and application of them are studied. There is no power dissipation in quantum circuits, thus the negative impact to environment arose from quantum computing system can reach minimum. Compared with classical computer, it is believed that quantum computer have potentially greater computation and simulation power.

In fact, since 2004 the authors have been focusing on quantum circuit synthesis because quantum circuits are the basic blocks to build quantum computer. We also have proposed some synthesis methods and matrix presentation methods of quantum circuits. In this paper, a simple and effective method to construct the unitary matrix of multiple-valued quantum permutation gate is put forward, and its correctness is discussed. On the basis of it, a framework by which unitary matrix of any hybrid quantum gate can be constructed is presented. Unitary matrix is mathematical model of quantum gate, by which quantum states' evolution in quantum circuits can be calculated step by step. And this is meaningful to verify the correctness and validity of quantum circuits.