

两位量子纠错的编码方案及量子电路的实现

吕洪君 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 在无测量电路中, 提出两位纠错量子电路的概念。构造出纠两位错的量子编码方案及量子纠错电路, 此电路可以同时纠正量子信息中的一位错、两位错, 突破了以往量子电路只能纠正一位错的局限。引入编码电路编码输入信息的辅助位, 根据辅助位的不同判断输入信息的不同量子状态。在设计七量子位的纠错电路过程中, 提出了模块化思想, 以五量子位纠错电路为基础模块构建纠错电路, 简化了多量子位纠错电路的设计过程。

关键词 量子光学; 量子纠错码; 量子线路; 两位错; 辅助位

中图分类号 0431.2 **文献标识码** A **doi**: 10.3788/AOS201131.0527001

Coding and Correcting Circuits for Two-Quantum Errors

Lü Hongjun Xie Guangjun

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

Abstract Under the non-measuring circuits, it is used the truth table method to propose the concept of two quantum error-correcting circuits and then a circuit which can code and correct one-qubit error, two-qubits error is constructed. This quantum circuit can correct one-qubit error and two-qubits error at the same time, break through the former limit that the circuit can only correct one-qubit error. A coding circuit is recommended to encode auxiliary bits of inputting information and judge the different input-bits quantum states according to different auxiliaries. During the process of designing 7-qubits error correction circuit, a modular thinking is advanced based on the 5-qubits error-correction circuits which can simplify the multi-qubits error-correction circuit design process.

Key words quantum optics; quantum error-correction code; quantum circuit; two quantum error; auxiliary bit

OCIS codes 270.5565; 270.5568; 270.5585

1 引 言

量子计算机、量子密码学^[1]和量子通信^[2]是近年来量子信息科学的三个主要研究领域, 量子信息论之所以优越于经典信息论最主要特点是量子的相干性^[3~5]。然而在对量子比特的操作以及传输过程中, 由于环境的影响, 量子相干性将不可避免地随时间指数衰减, 这就是困扰整个量子信息论的消相干问题, 而这些引起量子错误的因素可统称为量子噪声。如果不及时纠正量子噪声引起的量子错误, 将有可能导致全部量子信息的谬误。为了消除消相干引起的错误需要及时对量子信息进行纠正。

Steane 利用与 Shor^[6,7]不同的方法通过研究多重粒子纠缠态的性质提出了量子纠错码方案, 由他们提出的量子纠错编码思想, 为解决量子操作中的

误码等问题提供了有效的解决方法。近年来, 各种不同的编码方案被提出进而得到完善和发展。Steane、Calderbank 和 Shor^[8]提出了 Calderbank-Shor-Steane(CSS)构造法; Calderbank 等^[9,10]基于经典编码理论, 利用实正交群的两个特殊离散子群建立了量子纠错码的二元正交几何框架, 独立地发现了一种实质上等价于量子纠错码的构造方法; Grass 和 Beth 明确了纠正删除错误的量子纠错码的物理实质和数学表示, 提出量子 BCH 码的概念; 此外, Rains 等考虑稳定子量子码以外的线性量子纠错码, 构造了许多不同类型的量子纠错码; Zanardi, Rasetti 和 Lidar 等提出无噪声量子码和无消相干子空间编码; Steane^[11]改进了 CSS 构造法, 确立了 Steane 构造法。

收稿日期: 2010-07-05; **收到修改稿日期**: 2010-12-09

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)资助课题。

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

在经典的纠错电路^[12]中,纠错之前需要对信息进行测量以获得错误信息,而在量子电路中,根据量子力学基本原理,测量会产生量子态的坍塌,破坏原量子态的信息,为了避免测量引起的坍塌效应,本文所搭建的电路通过引入辅助位,不需测量就可纠正编码量子态中的错误。目前,在量子纠错电路中纠正一位错拥有比较成熟的编码及纠错方案,研究者大都认为出现一位错的概率比较大。实际上,当对量子信息进行多次操作或长距离传输时,由于量子噪声的存在,量子信息有一定概率出现两位错。为了纠正量子信息中的两位错,本文构造了能同时纠正一、两位错的纠错电路。还通过引进模块化设计量子纠错电路的思想,以五量子位量子编码纠错电路为模块搭建了七量子位量子编码及纠错电路,简化了多量子位纠错电路设计与优化的过程。

2 量子纠错的基本概念

量子信息在操作过程中,由于量子噪声的影响,量子信息可能出现的错误一般分为3类:1)位反转错: $|0\rangle \rightarrow |1\rangle$ 或 $|1\rangle \rightarrow |0\rangle$;2)相位出错: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle = \alpha|0\rangle - \beta|1\rangle$ 或 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle = -\alpha|0\rangle + \beta|1\rangle$;3)位反转错和相位错误同时发生。

当找到可以纠正位反出错的量子线路时,只需要在每条线路的两端加上 Hadamard 门(H 门)(如图 1 所示)即可纠正相位出错。

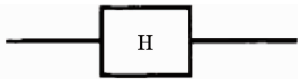


图 1 Hadamard 门

Fig. 1 Hadamard gate

首先对相位出错进行 H 门的变换:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (1)$$

$$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, \quad (2)$$

$$H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}. \quad (3)$$

例如:若 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 发生相位出错变为 $|\psi'\rangle = \alpha|0\rangle - \beta|1\rangle$, $|\psi\rangle$ 、 $|\psi'\rangle$ 在 H 门的作用下,

$$H|\psi'\rangle = \alpha(1/2)^{1/2}(|0\rangle + |1\rangle) - \beta(1/2)^{1/2}(|0\rangle - |1\rangle) = (1/2)^{1/2}(\alpha + \beta)|1\rangle + (1/2)^{1/2}(\alpha - \beta)|0\rangle, \quad (4)$$

$$H|\psi\rangle = \alpha(1/2)^{1/2}(|0\rangle + |1\rangle) + \beta(1/2)^{1/2}(|0\rangle - |1\rangle) = (1/2)^{1/2}(\alpha + \beta)|0\rangle + (1/2)^{1/2}(\alpha - \beta)|1\rangle. \quad (5)$$

通过(4)式,(5)式比较得出经 H 门作用,相位出错

变为位反转错。

因此,只要设计出位反转出错的纠正逻辑电路,则相位出错通过 H 门变为位反转错,再通过纠正逻辑电路,最后再通过 H 门变换恢复到初始相位。

由定理:若量子纠错码可以纠正错误 A 和 B,则可以纠正 A 和 B 的任意线性组合。可知纠错电路可以纠正位反转错和相位出错时,就可纠正位反转错和相位错误同时发生的情况。

3 五量子位的编码方案及量子电路的实现

为了增强量子信息的存储可靠性及纠错需要,可以用五量子位编码一位量子信息。设初始输入的一位量子信息为: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,在引入初态均为 $|0\rangle$ 态的四位辅助位时,以输入信息量子位为控制位,四位辅助位作为目标位,执行控制 NOT 操作:

$$(\alpha|0\rangle + \beta|1\rangle)|0000\rangle = \alpha|00000\rangle + \beta|10000\rangle \rightarrow \alpha|00000\rangle + \beta|11111\rangle$$

通过上述操作把量子态 $\alpha|0\rangle + \beta|1\rangle$ 中的信息存储在五量子位的纠缠态中。假设在量子信息的操作过程中,五量子位出现一位错、两位错和正确量子态的可能总量子态数共有 $N = C_5^1 + C_5^2 + 1 = 16$ 种。如果用 n 位辅助位来区别这些状态,则 $2^n \geq 16$,得 $n \geq 4$ 。所以至少需要4位辅助位来区别所有状态。用4位辅助位编码16种状态供选择的编码方式是多种多样的,通过分析和研究,选取如表1所示的编码方案(注:前面五位是量子信息位,括号中的为编码量子信息的辅助位)。

表 1 五量子位信息辅助位的编码表

Table 1 Auxiliary bits/coding table of five-bits

Input	Output	Input	Output
No error		00011(0000)	00011(0001)
00000(0000)	00000(0000)	00101(0000)	00101(0010)
Single-bit error		01001(0000)	01001(0100)
00001(0000)	00001(1111)	10001(0000)	10001(1000)
00010(0000)	00010(1110)	00110(0000)	00110(0011)
00100(0000)	00100(1101)	01010(0000)	01010(0101)
01000(0000)	01000(1011)	10010(0000)	10010(1001)
10000(0000)	10000(0111)	01100(0000)	01100(0110)
		10100(0000)	10100(1010)
Two-qubits error		11000(0000)	11000(1100)

表 1 所示的是输入量子信息为 $|0\rangle$ 时,不同量子信息状态所对应的编码表,当量子信息为 $|1\rangle$ 时,编码状态与表1完全对称,完整的编码表如表2所示。

表 2 纠错过程中的量子态转化

Table 2 Input states transformation in error correction

Input	Coded	Step-one	Step-two
		(Corresponding in part N' function)	(Corresponding in part M' function)
00000(0000)	00000(0000)	00000(0000)	00000(0000)
11111(0000)	11111(0000)	11111(0000)	11111(0000)
00001(0000)	00001(1111)	11111(1111)	00000(1111)
11110(0000)	11110(1111)	00000(1111)	11111(1111)
00010(0000)	00010(1110)	11111(1110)	00000(1110)
11101(0000)	11101(1110)	00000(1110)	11111(1110)
00100(0000)	00100(1101)	11111(1101)	00000(1101)
11011(0000)	11011(1101)	00000(1101)	11111(1101)
01000(0000)	01000(1011)	11111(1011)	00000(1011)
10111(0000)	10111(1011)	00000(1011)	11111(1011)
10000(0000)	10000(0111)	11111(0111)	00000(0111)
01111(0000)	01111(0111)	00000(0111)	11111(0111)
00011(0000)	00011(0001)	00000(0001)	00000(0001)
11100(0000)	11100(0001)	11111(0001)	11111(0001)
00101(0000)	00101(0010)	00000(0010)	00000(0010)
11010(0000)	11010(0010)	11111(0010)	11111(0010)
01001(0000)	01001(0100)	00000(0100)	00000(0100)
10110(0000)	10110(0100)	11111(0100)	11111(0100)
10001(0000)	10001(1000)	00000(1000)	00000(1000)
01110(0000)	01110(1000)	11111(1000)	11111(1000)
00110(0000)	00110(0011)	00000(0011)	00000(0011)
11001(0000)	11001(0011)	11111(0011)	11111(0011)
01010(0000)	01010(0101)	00000(0101)	00000(0101)
10101(0000)	10101(0101)	11111(0101)	11111(0101)
10010(0000)	10010(1001)	00000(1001)	00000(1001)
01101(0000)	01101(1001)	11111(1001)	11111(1001)
01100(0000)	01100(0110)	00000(0110)	00000(0110)
10011(0000)	10011(0110)	11111(0110)	11111(0110)
10100(0000)	10100(1010)	00000(1010)	00000(1010)
01011(0000)	01011(1010)	11111(1010)	11111(1010)
11000(0000)	11000(1100)	00000(1100)	00000(1100)
00111(0000)	00111(1100)	11111(1100)	11111(1100)

另外,设计的表 1 有三个特点:当五位量子态出现 1~2 位错时,量子信息通过编码线路后,利用四位辅助位,可以完全区分五位量子态的 16 种不同状态;当五位量子态中最后一位为 $|1\rangle$ 时,辅助位中 $|1\rangle$ 的个数为奇数,当五位量子态中最后一位为 $|0\rangle$ 时,辅助位中 1 的个数为偶数;在两位错中,辅助位的状态与五位量子态的前四位完全一致。根据表 1 构造的量子编码电路如图 2 所示。

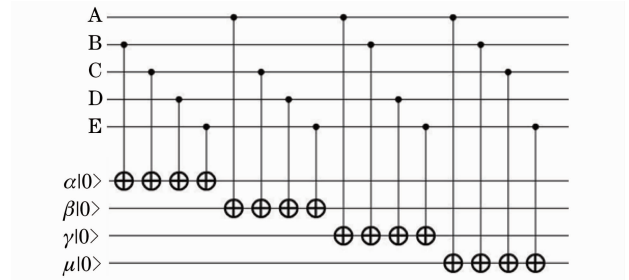


图 2 五量子位信息辅助位的编码电路

Fig. 2 Auxiliary bit' coding circuit of five-bits

图中辅助位 $\alpha, \beta, \gamma, \mu$ 初始都制备在 $|0\rangle$, 其中辅助位 α 的输出由 B、C、D、E 四位控制, 辅助位 β 的输出由 A、C、D、E 四位控制, 辅助位 γ 的输出由 A、B、D、E 四位控制, 辅助位 μ 的输出由 A、B、C、E 四位控制。例如当量子信息输入 $|ABCDE\rangle$ 为 $|00011\rangle$ 时, 经过此编码电路使辅助位 $\alpha, \beta, \gamma, \mu$ 分别翻转 2 次、2 次、2 次、1 次, 最终辅助位由 (0000) 输出为 (0001)。

4 纠错方案及其量子线路的实现

当输入信息经过图 2 所示的编码电路后, 根据编码方案的规律, 可以把纠错电路分成两部分, 第一部分(N)纠两位错, 第二部分(M)纠一两位错, 纠错中的量子态转化过程如表 2 所示。

根据表 2 的量子态转化过程构造的纠错量子电路如图 3 所示。

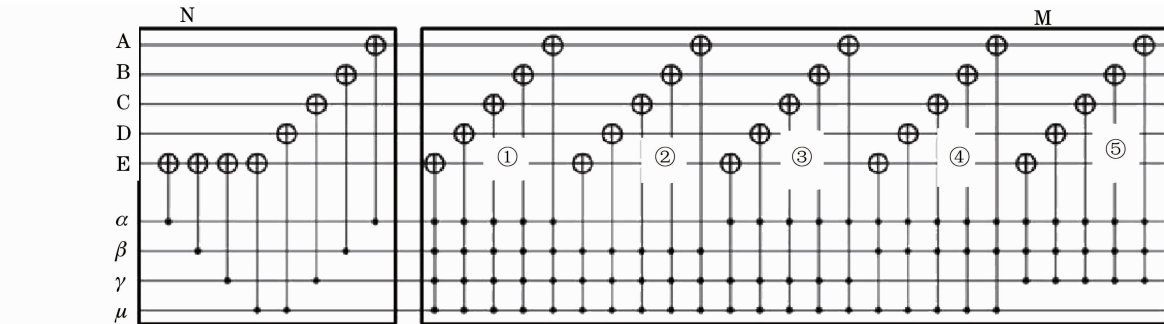


图 3 五量子位信息纠错电路

Fig. 3 Five-bits error-correction circuit

初始输入经过编码后,在 N 电路部分,A、B、C、D 四位分别由辅助位 α 、 β 、 γ 、 μ 控制翻转,E 位由 α 、 β 、 γ 、 μ 共同控制翻转。由表 2 可以看出,当存在两位错时,经过 N 电路部分的控制操作就可得到正确的输出。若当输入量子信息中存在的是一位错时,经过 N 电路部分后得到是与正确信息完全相反的量子状态,需经 M 电路部分纠错后才能得到正确信息;在 M 电路部分,以辅助位 α 、 β 、 γ 、 μ 中状态为 $|1\rangle$ 的位为控制位,对五位量子信息进行控制操作。其中部分①是当辅助位 α 、 β 、 γ 、 μ 四位全为 $|1\rangle$ 时,对五位量子位进行控制 NOT 操作,部分②当辅助位 β 、 γ 、 μ 为 $|1\rangle$ 时,对五位量子位进行控制 NOT 操作,部分③当辅助位 α 、 γ 、 μ 为 $|1\rangle$ 时,对五位量子位进行控制 NOT 操作,部分④当辅助位 α 、 β 、 μ 为 $|1\rangle$ 时,对五位量子位进行控制 NOT 操作,部分⑤当辅助位

α 、 β 、 γ 为 $|1\rangle$ 时,对五位量子位进行控制 NOT 操作。五位的量子信息通过此部分后,可得到正确的输出。

例如当初始输入为 $|00101\rangle(0000)$,经过编码电路为 $|00101\rangle(0010)$,在经过 N 电路部分时,A、B、C、D、E 五位分别经过 0 次、0 次、1 次、0 次、1 次翻转输出 $|00000\rangle(0010)$,得到正确的量子信息。当初始输入为 $|01000\rangle(0000)$ 经过编码电路为 $|01000\rangle(1011)$,在经过 N 部分时,A、B、C、D、E 五位分别经过 1 次、1 次、0 次、1 次、3 次翻转得到输出 $|11111\rangle(1011)$,五位量子信息进入 M 电路部分时,只有③电路对五位量子位做控制 NOT 操作,最后量子信息输出 $|00000\rangle(1011)$,得到正确的量子信息。图 4 给出五量子位编码纠错的量子电路。

加上 H 门后完整的五位编码纠错量子线路电路如图 5 所示。

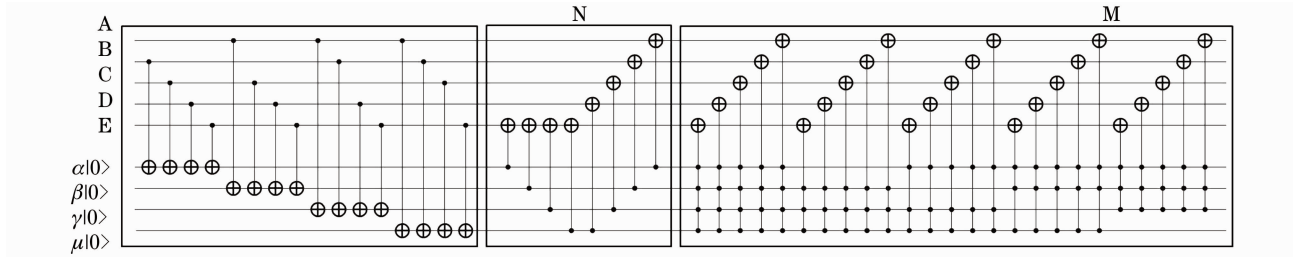


图 4 编码纠错量子线路

Fig. 4 Coding and error-correction quantum circuit of five-qubits

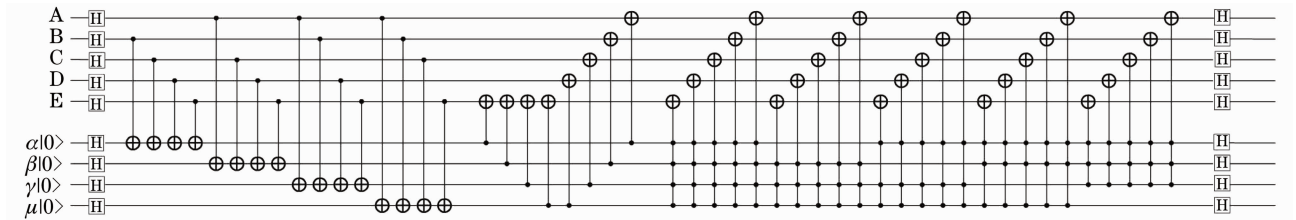


图 5 完整的五位编码纠错量子线路

Fig. 5 Complete five-qubits error-correction quantum circuit with Hadamard gate

5 七量子位的编码纠错方案及量子电路模块化实现

在量子纠错编码中,根据要求往往需要多位编码,随着位数的增多,编码纠错量子电路变得复杂起来,通过分析和研究,可以使用模块化编码纠错量子电路方案。在七量子位量子纠错电路构造过程中,首先对七量子位的前五位使用五量子位构建的编码及纠错电路对其进行编码和纠错;然后,以纠正过的五量子位中的任意一位为基准,再对剩下的两位进行编码及纠错。例如:有 A、B、C、D、E、F、G 七量子位,先对 A、B、C、D、E 进行五量子位的纠错,那么

A、B、C、D、E 通过纠错后,以其中任意一位为基准,再对 F、G 进行纠错。图 6 所示的七量子位的纠错电路就是在五量子位的编码及纠错量子电路上通过增加两位辅助位来实现的(注:图 6 左方框中为五量子位的编码及纠错量子电路)。

例如,当输入 $|ABCDEFG\rangle$ 为 $|0000101\rangle$ 时,F、G 两位信息为 $|01\rangle$,首先对 A、B、C、D、E 五量子位纠错,经过五量子位的纠错电路(图 6 左方框中的电路),A、B、C、D、E 的输出为 $|00000\rangle$, α 、 β 、 γ 、 μ 辅助位为 $|1111\rangle$;以 E 为控制位,F、G 位为目标位进行控制 NOT 操作,F 位为 $|0\rangle$,所以辅助 ν 位为 $|0\rangle$ 保持不变;G 位为 $|1\rangle$,辅助位 ω 被置成 $|1\rangle$,而后以辅

助位 α 为控制位 G 为目标位进行控制 NOT 操作, G 位变为 $|0\rangle$, 最后七位量子位输出为 $|000000\rangle$, 辅助位输出为 $|111101\rangle$ 。

如果要对九量子位信息进行纠错编码, 把图 6

所示的七量子比特编码纠错电路作为模块, 构造九量子位编码纠错电路, 逐级套用, 可得到任意 n 量子位模块化编码纠错电路。

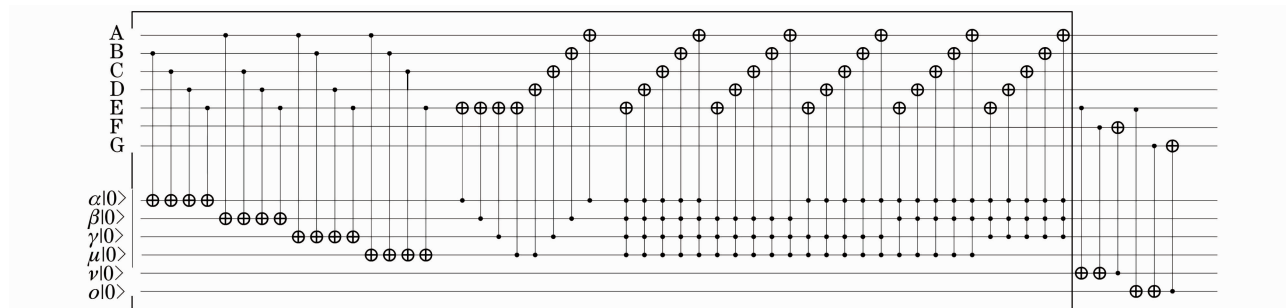


图 6 七量子位编码纠错电路

Fig. 6 Quantum circuit of error-correction in 7-qubit

6 结 论

提出的五量子位的编码方案及量子纠错电路完全实现了对一位、两位纠错的需要; 在编码方案中引入辅助位, 用 4 位辅助位来分辨 16 种不同的信息状态, 实现了辅助位的最大化利用; 纠错电路中使用的都是简单的 Toffoli 门, 易于物理上的实现; 在设计多量子位的纠错电路时, 引入模块化思想, 在构造七量子位纠错电路的过程中以五量子位纠错电路为基础模块, 使纠错电路的构造方便简洁, 简化设计过程, 构建的电路结构简单且各部分的功能明确, 这为多量子位纠错电路的设计与优化提供了新思路。

参 考 文 献

- Hu Xing, Yu Jijun, Ning Xiaoling *et al.*. Quantum identity authentication using three-particle W state [J]. *Acta Optica Sinica*, 2009, **29**(6): 1680~1683
胡 杏, 郁季军, 宁小玲 等. 基于三粒子 W 态的身份认证[J]. *光学学报*, 2009, **29**(6): 1680~1683
- Chen Yan, Yang Hongyu, Deng Ke. Effects of photon-number-splitting attacks on the security of satellite-to-ground quantum Key distribution systems[J]. *Acta Optica Sinica*, 2009, **29**(11): 2989~2993
陈 彦, 杨红宇, 邓 科. 光子数分束攻击对星地量子密钥分配系统安全的影响[J]. *光学学报*, 2009, **29**(11): 2989~2993
- Cai Xunming, Fan Menghui. The entanglement of two atoms in a coherent field of time-varying frequency[J]. *Acta Optica Sinica*, 2009, **29**(9): 2570~2576
蔡勋明, 范梦慧. 频率变化的相干态光场中两原子纠缠演化[J]. *光学学报*, 2009, **29**(9): 2570~2576
- Zheng Xiaolan, Chen Zihong. Nonclassical properties of fields in pair coherent states interacting with two two-level atoms [J]. *Acta Optica Sinica*, 2010, **30**(10): 3054~3058
郑小兰, 陈子翊. 对相干态与原子作用后非经典性质的演化[J]. *光学学报*, 2010, **30**(10): 3054~3058
- Guo Zhanying, Zhang Xinhai, Fang Jianxing *et al.*. Probabilistic teleportation of an arbitrary n-particle entangled state and Its quantum logic circuit [J]. *Acta Optica Sinica*, 2008, **28**(2): 387~391
郭战营, 张新海, 方建兴 等. 任意 n 粒子纠缠态的概率传送及其量子逻辑线路[J]. *光学学报*, 2008, **28**(2): 387~391
- Shor P. W.. Scheme for reducing decoherence in quantum computer memory [J]. *Phys. Rev. A.*, 1995, **52**(4): 2493~2496
- Man-Duen Choi, David W. Kribs. Quantum error correcting codes from the compression formalism [J]. *Reports on Mathematical Physics*, 2006, **58**(1): 77~91
- Xing Lijuan, Li Zhuo, Wang Xinmei. Encoding and decoding of CSS-type quantum convolution codes [J]. *Journal of Beijing University of Post and Telecommunications*, 2008, **31**(6): 121~124
邢莉娟, 李 卓, 王新梅. CSS 型量子卷积码的编译码方法[J]. *北京邮电大学学报*, 2008, **31**(6): 121~124
- Gottesman D.. An introduction to quantum error correction [C]. *Proc. Symposia in Applied Mathematics*, 2002, **58**: 221~235
- Calderbank A. R., Shor P. W.. Good quantum error-correcting codes exist [J]. *Phys. Rev. A.*, 1996, **54**(2): 1098~1105
- Steane A.. Multiple particle interference and quantum error correction [J]. *Proc. R. Soc. London A*, 1996, **452**(1954): 2551~2576
- Daxiu Wei, Jun Luo, Xianping Sun *et al.*. Three-qubit quantum error-correction scheme based on quantum cloning [J]. *Phys. Lett. A*, 2004, **329**(4-5): 294~297