

量子 Turbo 乘积码*

肖海林[†] 欧阳缮 谢武

(桂林电子科技大学信息与通信学院, 桂林 541004)

(2009年12月28日收到; 2010年5月29日收到修改稿)

量子通信是经典通信和量子力学相结合的一门新兴交叉学科. 量子纠错编码是实现量子通信的关键技术之一. 构造量子纠错编码的主要方法是借鉴经典纠错编码技术, 许多经典的编码技术在量子领域都可以找到其对应的编码方法. 针对经典纠错码中最好码之一的 Turbo 乘积码, 提出一种以新构造的 CSS 型量子卷积码为稳定子码的量子 Turbo 乘积码. 首先, 运用群的理论及稳定子码的基本原理构造出新的 CSS 型量子卷积码稳定子码生成元, 并描述了其编码网络. 接着, 利用量子置换 SWAP 门定义推导出量子 Turbo 乘积码的交织编码矩阵. 最后, 推导出量子 Turbo 乘积码的译码迹距离与经典 Turbo 乘积码的译码距离的对应关系, 并提出量子 Turbo 乘积码的编译码实现方案. 这种编译码方法具有高度结构化, 设计思路简单, 网络易于实施的特点.

关键词: CSS 码, 量子卷积码, 量子 Turbo 乘积码, 量子纠错编码

PACS: 03. 65. Ta, 42. 30. Va, 42. 50. Ex

1. 引言

量子通信是通信技术的又一次划时代革命, 它在保密性、通信容量、通信距离等方面都具有十分明显的优势, 是未来通信发展的方向. 量子通信传送的是密钥而非密文本身, 是一个量子密钥分发过程^[1]. 目前采用的通信技术严重制约了量子密钥分发的比特率. 将多输入多输出 (MIMO) 技术应用于量子通信系统, 提高量子密钥分发的比特率, 促进量子通信向高速、大容量发展^[2,3]. 然而, 由于量子噪声和环境的影响, 使得量子密钥在分发过程中产生误码率. 为了提高量子密钥分发的效率和降低误码率, 增加量子通信的可靠性, 必须进行量子纠错编码^[4]. 受到经典纠错编码技术的启发, Shor^[5] 在 1994 年提出了一种用 9 量子位编码 1 位量子信息, 纠正任一量子位发生错误的编码方案. Shor 的方法促进了量子纠错编码理论的产生与发展. 通过借鉴经典纠错编码理论, 人们提出了一系列量子纠错编码方案. 其中以 CSS 型码^[6,7] 和稳定子码理论^[8,9] 最为成熟和重要. Ashikhim 等^[10] 于 2001 年在 CSS 码

基础上利用有限几何学的方法构造了量子低密度奇偶校验码 (LDPC). David 等^[11] 于 2004 年在 CSS 码基础上, 利用特殊稀疏序列, 提出了 4 种构造校验矩阵的方法得到新的量子 LDPC. 2008 年邢莉娟等^[12] 给出了 CSS 型量子卷积码的一种新的编译码方法, 描述了编译码网络. 该方法将码字基态变换为信息多项式与生成多项式的乘积, 然后用量子态上的多项式乘法操作实现编译码网络. 同年, 岳克峰等^[13] 利用有限几何中的点和线, 构造出 LDPC 码的校验矩阵, 并根据这种 LDPC 码的特点, 通过对校验矩阵的行或列变换得到其对偶码, 从而获得基于 CSS 码的量子 LDPC 码. 2009 年 Djordjevic^[14] 在 CSS 码基础上提出适合光纤通信的量子 LDPC 码, 它的编译码非常简单, 只取决于受控非门和 Hadamard 门操作.

Turbo 码是目前最受关注的经典纠错编码技术之一^[15,16], 它汲取了传统级联码的优点, 利用交织减少各成员码的相关性, 性能接近于香农极限^[17]. 同时开创性地引入迭代译码的思想, 译码也很简单. Turbo 乘积码^[18] (TPC) 是一种以经典码为子码的 Turbo 分组码, 在译码算法上采用了软输入软输

* 国家自然科学基金 (批准号: 60972084)、国家重点基础研究发展计划 (批准号: 2008CB317109) 和广西科学基金 (批准号: 桂科自 0991241) 资助的课题.

[†] E-mail: xhl_xiaohailin@163.com

出的迭代译码思想. 在码率较高的情况下, 编码增益较大, 而且在译码性能上获得了近似 Turbo 卷积码译码的编码增益. 相对于经典 Turbo 乘积码, 量子 Turbo 乘积码成为量子纠错码研究的新方向, 而且构造好的稳定子码也是量子 Turbo 乘积码的重要技术.

2. 经典 Turbo 乘积码

经典 Turbo 乘积码就是采用软输入软输出迭代译码的乘积码, 是传统 Turbo 卷积码技术的一种延伸, 也称为 Turbo 分组码. 从编码的角度看, 它就是乘积码而已. 从译码的角度看, 它采用的是与 Turbo 码类似的迭代译码结构, 只是构成 Turbo 乘积码的子码通常是一些线性分组码或卷积码, 所以在 SISO 译码算法上有别于 Turbo 译码器中常用的算法^[19]. 乘积码是通过将两组或多组经典码排列在一个二维或多维的阵列中而构成的, 其最小距离等于子码最小距离的乘积. 乘积码实际上也是一种特殊的串行级联码, 子码的级联顺序可以任意交换而不影响码的结构和性能. Turbo 乘积码引入乘积码的概念, 用两个或多个短的经典码简单而有效率地构造长码. 其编码器由两个或多个块编码器串行级联而成, 这些编码器被简单的行/列交织器分隔开来. 二维 Turbo 乘积码的乘积码结构框图如图 1 所示.

图 1 中 $C_1[n_1, k_1]$ 和 $C_2[n_2, k_2]$ 是两个经典码, n_i 为码长, k_i 为信息比特数. Turbo 乘积码的编码器结构方框图如图 2 所示.

在译码过程中, 译码模块 A 输出的外赋信息经过交织后送入译码模块 B, 而译码模块 B 输出的外赋信息解交织后又反馈到译码模块 B, 经过多次迭代后译码模块 B 的译码输出经判决后得到译码结果. 在译码器中, 两个译码模块均采用 Chase 算法, 它的性能接近于最大似然译码. 该算法的基本原理是: 利用硬判决译码器, 根据不同的试探序列产生几个候选码字, 然后把它们与接收序列进行比较, 挑选一个与接收序列有最小软距离的候选码字作

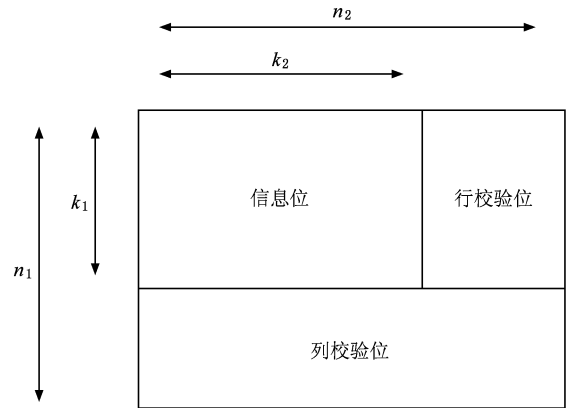


图 1 二维 Turbo 乘积码结构框图



图 2 Turbo 乘积码的编码器结构方框图

为译码器的输出码字. Turbo 乘积码的译码器结构方框图如图 3 所示.

Turbo 乘积码在信噪比较高时具有更加稳定的译码输出, 它解决了译码结果的涨落问题, 收敛速度也较快. 此外, Turbo 乘积码可以用一个子译码单元来完成多次迭代, 这意味着可以大大减少实现电路的复杂度, 同时将减小译码时延.

3. 量子 Turbo 乘积码

3.1. 新构造 CSS 型量子卷积码

通过 Steane 码, 人们找到了经典码与量子码间构造的桥梁. CSS 码是 Calderbank, Shor 和 Steane 等^[20-22]首先提出的一类量子纠错码. 其原则是将经典码看作 Hilbert 空间中的量子态, 利用原码及其对偶码的级联分别纠正比特翻转和相位翻转错误. CSS 码结合了级联码和对偶码两种编码思想, 与经典码具有良好的对应关系, 从而可以利用经典纠错

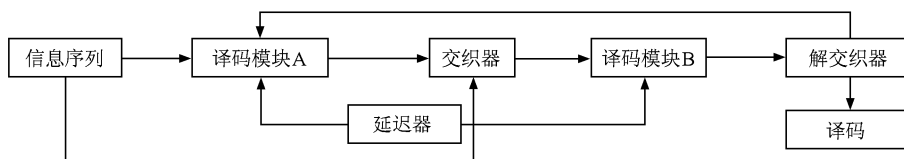


图 3 Turbo 乘积码的译码器结构方框图

码来构造量子纠错码,而且具有非常直观的代数结构,非常易于分析.为了与经典纠错码相区别,习惯上用符号 $[[n, k, m]]$ 表示码长为 n 的量子位,信息为 k 量子位的量子码, m 为约束长度.

设 $x \in C_1$ 且为 C_1 中的任意一个码字,定义量子态

$$|x + C_1\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle, \quad (1)$$

其中,“+”为按比特的“模2”方式加. C_1 和 C_2 分别为 $[n, k_1]$ 和 $[n, k_2]$ 经典卷积码,且有 $C_2 \subset C_1$.利用 C_1 和 C_2 的对偶码 C_2^\perp 可纠正 t 个比特翻转差错和相位翻转差错.量子CSS(C_1, C_2)码具有如下形式的一个检验矩阵

$$A = \begin{bmatrix} \mathbf{H}(C_2^\perp) & | & 0 \\ 0 & | & \mathbf{H}(C_1) \end{bmatrix}, \quad (2)$$

其中,检验矩阵满足对易条件 $\mathbf{H}(C_2^\perp)\mathbf{H}(C_1)^T = 0$.由于假定 $C_2 \subset C_1$,我们有 $\mathbf{H}(C_2^\perp)\mathbf{H}(C_1)^T = [\mathbf{H}(C_1)\mathbf{G}(C_2)]^T = 0$,这里 $\mathbf{G}(C) = [\mathbf{G}(C_1) | \mathbf{G}(C_2)]$ 为生成矩阵.量子Turbo乘积码是通过CSS(C_1, C_2)型量子卷积码为稳定子码进行级联得到.我们首先构造出新的CSS(L_1, L_2)型量子卷积码,且有 $L_1^\perp \leq L_2$.

假设(C_1, C_2)是 $[[n, k]]$ 在有限空间 F_q 编码对,且满足

$$\begin{aligned} C_1 &= C_2^\perp + \text{span}\{g_1^1, \dots, g_k^1\} \\ C_2 &= C_1^\perp + \text{span}\{g_1^2, \dots, g_k^2\}, \end{aligned} \quad (3)$$

这里 $C_1, C_2 \leq F_q$, $\text{span}\{\cdot\}$ 表示线性张量子空间.向量 g_i^1, g_j^2 ($i, j = 1, \dots, k$)满足 $g_i^1 \cdot g_j^2 = \delta_{ij}$,相应的结构图如图4所示.

同样假设(D_1, D_2)是 $[[N, K]]$ 在有限空间 F_{q^k} 编码对.将(C_1, C_2)和(D_1, D_2)进行级联,必须在 F_q 和 F_{q^k} 进行变换,引入两个变换空间的关系式.我们选择 $e_1 = \{e_1^1, e_2^1, \dots, e_k^1\}$ 是 F_q 空间的一组基,选择 $e_2 = \{e_1^2, e_2^2, \dots, e_k^2\}$ 是 F_{q^k} 空间的一组基. F_{q^k} 是 F_q 线性矢量空间,则满足 F_q 双线性变换 f_i ,即

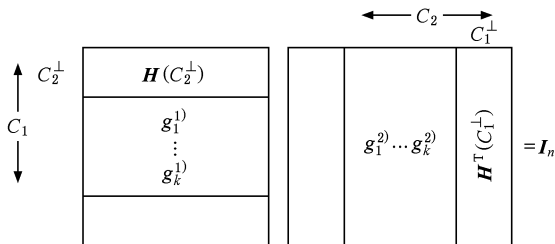


图4 CSS(C_1, C_2)型量子卷积结构示意图

$$\begin{aligned} f_i &: F_{q^k} \times F_{q^k} \rightarrow F_q \\ (e_1, e_2) &\rightarrow \text{Tr}\{F_{q^k/F_q} e_1 e_2\} = \pi_1(e_1) \cdot \pi_2(e_2), \end{aligned} \quad (4)$$

式中 $\text{Tr}\{\cdot\}$ 表示求迹, $\pi_i(\cdot)$ ($i = 1, 2$)为 F_{q^k} 空间到 F_q 空间的线性内射变换.CSS(L_1, L_2)型量子卷积码构造表达式为

$$\begin{aligned} L_1 &= \pi_1(D_1) + \overline{C_2^\perp}, \\ L_2 &= \pi_2(D_2) + \overline{C_1^\perp}, \end{aligned} \quad (5)$$

其中 $\overline{C_i^\perp} = \bigoplus_i^k C_i^\perp$ ($i = 1, 2$),“ \oplus ”为对称差运算. C_1^\perp 和 C_2^\perp 相互正交, $\overline{C_2^\perp}$ 也正交于 $\overline{C_1^\perp}$.由(4)式可以知道 $\pi_1(D_1)$ 和 $\pi_2(D_1^\perp)$ 相互正交.根据(2)式,如果满足 $L_1^\perp \subseteq L_2$,CSS(L_1, L_2)型量子卷积码对应的检验矩阵为

$$A = \begin{bmatrix} \mathbf{H}(L_2^\perp) & | & 0 \\ 0 & | & \mathbf{H}(L_1) \end{bmatrix}, \quad (6)$$

其中 $\mathbf{H}(L_2^\perp)$ 和 $\mathbf{H}(L_1)$ ^T,满足 $\mathbf{H}(L_2^\perp)\mathbf{H}(L_1)^T = 0$.在有限 F_q 空间 L_1 的生成矩阵的表示为

$$\mathbf{G}(L_1) = \begin{bmatrix} \mathbf{H}(C_2^\perp) \\ \pi^\perp(D_1) \end{bmatrix}, \quad (7)$$

式中 $\mathbf{H}(C_2^\perp)$ 是 C_1 的奇偶校验矩阵元组成的对角矩阵.矩阵单元为 $N \times (N - K_1)$,其中 K_1 为 D_1 的空间维数. $\pi^\perp(D_1)$ 是 $K \times N$ 矩阵,它的行矩阵元是由 g_j^2 ($j = 1, 2, \dots, k$)的子空间线性展开,写成 $\text{span}\{|x + \pi(D_1^\perp)\rangle | x \in C_2^\perp\}$.CSS(L_1, L_2)型量子卷积码存在一个量子纠错码 $[[nN, kK, m]]$,其基态(略去归一化系数)可以表示为

$$|\psi(L_i)\rangle = \sum_{C_i, D_i \in L_i^\perp} |\mathbf{H}(C_i) + \pi(D_i)\rangle, \quad (8)$$

其中 $|\pi(D_i)\rangle$ 表示量子态 $|g_1^1, g_2^1, g_1^2, g_2^2, \dots, g_k^1, g_k^2\rangle$,其对应的生成多项式为

$$\psi(L_i) = \sum_i^k \eta_i g_i^{1,2}, \quad (9)$$

其中 k 重向量 $(\eta_1, \eta_2, \dots, \eta_k)$ ($\eta_i \in GF(2^s)$)在伽罗华域 $GF(2^s)$ 上形成一个向量空间,共有 2^{ks} 个元素.在组合数学中, $GF(2^s)$ 上的 2^{ks} 个 k 重向量形成 $GF(2^s)$ 上的 k 维欧氏几何.多项式 $\psi(L_i)$ 取决于第 i 个输出端和编码存储单元之间如何用加法器和乘除器连接.给定一定参数为 $[[nN, kK, m]]$ 的量子卷积码,其生成元可以用左右两个 $GF(2^s)$ 上的 $(nN - kK) \times nN$ 矩阵来表示.这里矩阵行对应不同的生成元,列对应不同的量子位.构造CSS(L_1, L_2)型量子卷积码的稳定子码生成元矩阵为

$$\mathbf{M} = [\mathbf{M}_x | \mathbf{M}_z]$$

$$= [\pi(D_1) \oplus (C_1^\perp \oplus C_2^\perp \oplus \dots \oplus C_n^\perp) \times |g_1^1\rangle \otimes |g_1^2\rangle \otimes |g_2^1\rangle \otimes |g_2^2\rangle \otimes \dots \otimes |g_n^1\rangle \otimes |g_n^2\rangle \otimes_{i=1}^n \sigma_i], \quad (10)$$

其中“ \otimes ”表示是张量积, $G_n = \{ \otimes_{n=1}^i \sigma_n : \sigma_n \in \{I, X, Y, Z\}, 1 \leq i \leq n \}$ 为 n 量子位 Pauli 算子群.

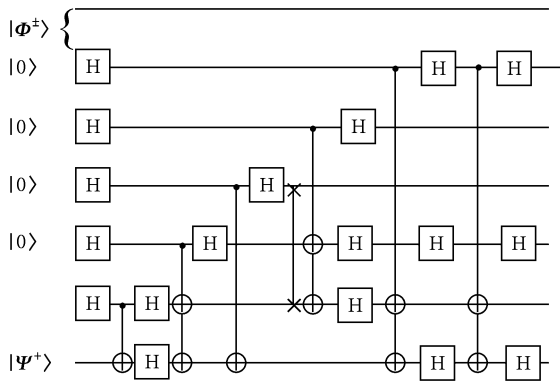


图5 参数为[[6,1,3]]的CSS(L₁, L₂)型量子卷积码的编码网络 “H”表示 Hadamard 门

从图5中我们发现,新构造的CSS型量子卷积码的编译码网络只包含 Hadamard 门与控制非门,涉及相位翻转操作的算子都可以忽略. 编译码的复杂度大大降低,网络的结构非常简单. 此外,我们新构造的CSS型量子卷积码可以实现由短的CSS型量子卷积码的级联取代长卷积码,降低了系统的复杂度,而且它的稳定子生成码包含 Pauli 算子群代数中的算子. 量子编码的汉明距离可以用 Pauli 算子的最小重量表示^[23]. 在二元对称信道中,最大后验概率等效于最小汉明距离. 在量子 Turbo 乘积码译码过程中,将 Pauli 算子群的维数赋予不同的置信系数作为译码输出,从而可以在译码复杂度和译码性能之间进行灵活选择.

3.2. 量子交织器

交织矩阵的应用是 Turbo 系列码性能优越的重要原因,它改变了 Turbo 系列码的重量分布,使产生小重量码字的输入序列在通过交织矩阵后以很大的概率产生大重量码字. 通过选取好的交织矩阵,可以提高 Turbo 系列码的自由距离,减少低重量码字的个数,最大限度地发挥交织器的作用. 在量子通信中,量子交织器是利用量子置换 SWAP 门操作^[24]来实现,量子置换定义为

$$\text{SWAP} = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + e^{i\pi} |\Psi^-\rangle\langle\Psi^-| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$|\Phi^\pm\rangle = (1/\sqrt{2})(|00\rangle \pm |11\rangle)$$

$$|\Psi^\pm\rangle = (1/\sqrt{2})(|01\rangle \pm |10\rangle), \quad (11)$$

其中 $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle$ 和 $|\Psi^-\rangle$ 为四个 Bell 态. 对于两量子比特的量子置换操作算符表示为^[25]

$$V = \Pi_+ + e^{i\phi} \Pi_-, \quad (12)$$

其中 $\Pi_- = |\Psi^-\rangle\langle\Psi^-|, \Pi_+ = I - \Pi_-$ (I 为单位矩阵), ϕ 表示相移. 当 $\phi = \pi$ 时为无相消子空间^[26], 对应产生算子 a^+ 在海森堡绘景中描述为

$$a^+ = \Pi_- a_1^+ + \Pi_+ a_2^+, \quad (13)$$

其中 $a_1^+, a_2^+ \in SU(2)$. 在此基础上,我们引入哈密顿算子

$$H = J(t) S_1 \cdot S_2, \quad (14)$$

其中 $S = \{\sigma_x, \sigma_y, \sigma_z\}$ 为 Pauli 矩阵的矢量. $J(t)$ 为量子态的耦合常数^[27], 在无消相干子空间且满足 $J(t) = 1$. a_1^+, a_2^+ 和 H 的 U 变换表达式为

$$U = (a_1 \otimes a_2) e^{-iH} (a_1^+ \otimes a_2^+), \quad (15)$$

其中 a_1, a_2 分别为 a_1^+, a_2^+ 对应的湮灭算子. (13), (14) 和 (15) 式得到多量子比特交织的表达式为

$$U = (a_1 \otimes a_2) \text{SWAP}(a_1^+ \otimes a_2^+) \Rightarrow \begin{bmatrix} u_+ & u_- \\ v_- & v_+ \end{bmatrix} = V_{j=1}^{N-1} \begin{bmatrix} u_{j+} & u_{j-} \\ v_{j-} & v_{j+} \end{bmatrix}, \quad (16)$$

其中 $u_\pm, v_\pm \in U$, 且满足 $v_{j\pm} = \mp (-1)^{s_j+s_{j+1}} u_{j\mp}$ 和 $u_{j\pm} = [1 \pm (-1)^{s_j}]/2, s_j, s_{j+1} \in (a, a^+)$. 从(16)式中得出量子交织编码矩阵对应于 Pauli 算子群代数中的算子,可以称为错样算子. 错样算子在态空间中的表示是可约的. 每个不可约表示对应一种量子错误,其中具有最小维数的不可约表示称为最简不可约表示. 将最简不可约表示的维数和重数赋予不同的概率提高量子 Turbo 乘积码的自由距离,产生大重量码字. 此外,译码时,最简不可约表示对应的错误还可以作为译码的依据.

3.3. 量子 Turbo 乘积码译码

在经典译码中,常采用编译码之间的最小距离(欧式距离或者汉明距离)的序列作为最佳估计序列,而量子编译码之间的距离用迹距离来描述^[28].

因此,寻求经典 Turbo 乘积码的译码距离和量子 Turbo 乘积码的译码距离存在某种对应关系对译码工作是十分重要的.

在量子 Turbo 乘积码中,把发送码字记做 $|S\rangle = \sum_i s_i |i\rangle\langle i|$, 经过信道传输后的接收码字记做 $|R\rangle = \sum_i r_i |i\rangle\langle i|$. $|R\rangle$ 和 $|S\rangle$ 的之间关系表示为 $|R\rangle = |S + G\rangle$ (“+”表示模 2 法则), $|G\rangle = \sum_i g_i |i\rangle\langle i|$ 为加性量子白噪声. 在 Bloch 向量空间, CSS 型量子 Turbo 乘积码的编译距离可以表示为

$$D(\alpha, \beta) = \frac{1}{2} \text{Tr} \{ |\alpha - \beta| \},$$

$$\alpha = \frac{I + S \cdot \sigma}{2},$$

$$\beta = \frac{I + S \cdot \sigma}{2}, \quad (17)$$

其中 σ 为 Pauli 矩阵向量, $\alpha \in S, \beta \in R$. 简化(17)式可得到

$$D(\alpha, \beta) = \frac{1}{2} \text{Tr} \{ |\alpha - \beta| \}$$

$$= \frac{1}{4} \text{Tr} \{ |(\mathbf{R} - \mathbf{S}) \cdot \boldsymbol{\sigma}| \}$$

$$= \frac{1}{2} |r - s|, \quad (18)$$

其中利用广义测量得到 $(\mathbf{R} - \mathbf{S}) \cdot \boldsymbol{\sigma}$ 本征态的特征值为 $\pm |r - s|$, 从(18)式中得到量子 Turbo 乘积码的编译码之间的距离等于 Bloch 球上它们之间经典距离的一半. 因此,可以将经典 Turbo 乘积码的译码距离与量子系统中量子 Turbo 乘积码的译码距离进行对应,这对量子 Turbo 乘积译码工作非常重要. 因此在量子 Turbo 乘积码的编译码器的形式上与经典串行级联卷积码基本上相同. 这样可以选用经典 Turbo 乘积码的设计方案非常方便地构造量子 Turbo 乘积码. 从(18)式中我们还发现量子 Turbo 乘积码不涉及纠错算法,只是将错样转化为 Pauli 算子群代数上的算子,提高算法的可操作性,其对应的编译码器如图 6 所示.

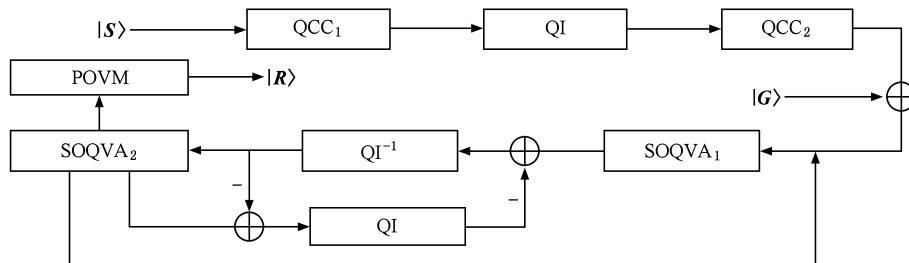


图 6 量子 Turbo 乘积码的编译码器 QCC₁ 为量子卷积码, QI 为量子交织器, SOQVA₁ 为软输出量子 Viterbi 译码器, QI⁻¹ 为量子去交织器, POVM 为广义测量, ⊕ 为模 2 加

4. 结 论

量子纠错码技术是实现量子通信和量子计算实用化的基础. 迄今为止, 量子纠错码理论日趋完善, 许多经典的编译码技术在量子领域都可以找到其对应的编译码方法. 针对经典纠错码中最好码之一的 Turbo 乘积码, 研究了量子 Turbo 乘积码的编译码方法, 它通过 CSS 型量子卷积码级联, 采用了经典类比的方法, 因此在编译码器的形式上与经典串行级联卷积码基本上相同. 这样可以选用经典 Turbo 乘积码的设计方案非常方便地构造出量子 Turbo 乘积码, 并从理论推导中得到这种对应的关系. 我们首先运用群的理论及稳定子码的基本原理

构造出新的 CSS 型量子卷积码稳定子码生成元, 并描述了其编码网络. 接着, 利用量子置换 SWAP 门定义推导出量子 Turbo 乘积码的交织编码矩阵, 这种量子交织编码矩阵对应于 Pauli 算子群代数中的错样算子. 对错样算子的最简不可约表示的维数和重数赋予不同的概率能提高量子 Turbo 乘积码的自由距离, 产生大重量码字. 最后, 推导出量子 Turbo 乘积码的译码迹距离与经典 Turbo 乘积码的译码距离的对应关系, 并提出量子 Turbo 乘积码的编译码实现方案. 这种编译码方法具有高度结构化, 设计思路简单, 网络易于实施的特点. 量子 Turbo 乘积码不仅可以拓展量子纠错编码技术的研究领域, 而且可能解决经典方法难以解决的编码理论难题.

- [1] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3124
- [2] Xiao H L, Ouyang S, Nie Z P 2009 *Acta Phys. Sin.* **58** 3685 (in Chinese) [肖海林、欧阳缮、聂在平 2009 物理学报 **58** 3685]
- [3] Xiao H L, Ouyang S, Nie Z P 2009 *Acta Phys. Sin.* **58** 6779 (in Chinese) [肖海林、欧阳缮、聂在平 2009 物理学报 **58** 6779]
- [4] Kremsky I, Hsieh M H, Brun T A 2008 *Phys. Rev. A* **78** 012341
- [5] Shor P W 1995 *Phys. Rev. A* **52** 2493
- [6] Calderbank A R, Shor P W 1996 *Phys. Rev. A* **54** 1098
- [7] Dave B 2008 *Phys. Rev. A* **78** 042324
- [8] Gottesman D 1996 *Phys. Rev. A* **54** 1862
- [9] Alexei A, Emanuel K 2001 *IEEE Trans. Inf. Theory* **47** 3065
- [10] Ashikhim A, Litsyn S, Tsfasman M 2001 *IEEE Trans. Inf. Theory* **47** 1206
- [11] David J C, Mitchison G, McFadden P L 2004 *IEEE Trans. Inf. Theory* **50** 2315
- [12] Xing L Z, Li Z, Bao B M, Wang X M 2008 *Acta Phys. Sin.* **57** 4695 (in Chinese) [邢莉娟、李卓、白宝明、王新梅 2008 物理学报 **57** 4695]
- [13] Yue K F, Zhao S M, Li M M 2008 *Journal of Nanjing University of Posts and Telecomm* **28** 44 (in Chinese) [岳克峰、赵生妹、李苗苗 2008 南京邮电大学学报 **28** 44]
- [14] Djordjevic I B 2009 *IEEE Photonics Technology Lett.* **21** 842
- [15] Vucetic B, Li Y H, Perez L C, Jiang F 2007 *IEEE Proc.* **95** 1323
- [16] Huebner A, Zigangirov K S, Costello D J 2008 *IEEE Trans. Inf. Theory* **54** 3024
- [17] Liese F, Vajda I 2006 *IEEE Trans. Inf. Theory* **52** 4394
- [18] Chen G T, Cao L, Yu Lun, Chen C W 2009 *IEEE Trans. Comm.* **57** 307
- [19] Xu C L, Liang Y C, Leon W S 2008 *IEEE Trans. Wire. Comm.* **7** 43
- [20] Calderbank A R, Shor P W 1996 *Phys. Rev. A* **54** 1098
- [21] Steane A M 1999 *IEEE Trans. Inf. Theory* **45** 2492
- [22] Fletcher A S, Shor P W, Win M Z 2008 *IEEE Trans. Inf. Theory* **54** 5705
- [23] Zhang Q, Tang C J, Gao F 2002 *Acta Phys. Sin.* **51** 15 (in Chinese) [张权、唐朝京、高峰 2002 物理学报 **51** 15]
- [24] Jaromir F 2009 *Phys. Rev. A* **79** 012330
- [25] Heng F, Vwani R, Thomas S 2005 *Phys. Rev. A* **72** 052323
- [26] Zhang Q, Zhang E Y, Tang C J 2002 *Acta Phys. Sin.* **51** 1676 (in Chinese) [张权、张尔杨、唐朝京 2002 物理学报 **51** 1676]
- [27] Tetsufumi T, Liu Y X, Hu X D, Franco N 2009 *Phys. Rev. Lett.* **102** 100501
- [28] Zhang M, Dai H Y, Xi Z R, Xie H W, Hu D W 2007 *Phys. Rev. A* **76** 042335

Quantum turbo product codes^{*}

Xiao Hai-Lin[†] Ouyang Shan Xie Wu

(School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China)

(Received 28 December 2009; revised manuscript received 29 May 2010)

Abstract

Quantum communication is a growing interdisciplinary field which combines classical communications and quantum mechanics. Quantum error correction coding is one of the key techniques in quantum communication. Nearly all of the classical error correction coding schemes have been transplanted to the domain of quantum communication, and the quantum counterparts of classical error correction coding techniques have been found. Based on the classical turbo product codes (TPCs) which is one of the most outstanding schemes in classical coding region, a new structure of the CSS-type quantum convolutional codes (QCC) as stabilizer sub-code of the quantum turbo product codes (QTPC) is presented. Firstly, CSS-type QCC stabilizer generator is constructed with the help of group theory and the basic principle of stabilizer coders, and the corresponding networks are described. Secondly, the interleaved coded matrix of the QTPC is obtained by quantum permutation SWAP gate definition. Finally, the corresponding relation between the quantum trace distance of QTPC decoding and the distance of classical TPCs decoding is obtained, and the scheme of QTPCs coding and decoding is completed. The coding and decoding of QTPCs have a highly regular structure and a simple design idea, and the networks are easy to realize.

Keywords: CSS coding, quantum convolutional codes, quantum turbo product codes, quantum error correcting coding

PACS: 03.65.Ta, 42.30.Va, 42.50.Ex

^{*} Project supported by the National Natural Science Foundation of China (Grant No. 60972084), the National Basic Research Program of China (Grant No. 2008CB317109), and the Guangxi Science Foundation of China (Grant No. 0991241).

[†] E-mail: xhl_xiaohailin@163.com