第 57 卷 第 8 期 2008 年 8 月
1000-3290/2008/57(08)/4695-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.57, No.8, August, 2008


# 量子卷积码的编译码方法*

邢莉娟 李 卓 白宝明 王新梅

(西安电子科技大学综合业务网国家重点实验室，西安 710071)

(2007 年 10 月 18 日收到；2008 年 4 月 1 日收到修改稿)

对于量子卷积码理论的研究旨在保护长距离通信中的量子信息序列. 定义了量子态的多项式表示形式，根据 Calderbank-Shor-Steane(CSS)型量子码的构造方法，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. 最后借鉴经典卷积码的译码思想，给出了具有线性复杂度的量子 Viterbi 算法.

**关键词**：量子信息，量子卷积码，编译码，纠错算法

**PACC**：0367，0365，0210

## 1. 引 言

近年来，对量子通信和量子计算理论的研究，为未来信息技术的深入发展开辟了一个全新的领域. 量子信息科学是量子力学与信息科学相结合的产物，它是以量子物理为基础的一门新兴交叉学科. 量子通信系统是面向未来的全新通信技术，在安全和高效上具有经典通信无法比拟的优势. 近年来光纤量子通道传输技术的出现使得量子通信的实用化成为可能. 为了真正实现量子信息的可靠传输与处理，必须保证量子状态经过一定的时空距离传输后保持不变或能够正确恢复. 然而，由于量子系统在操作时不可避免地会受到外界噪声的影响，必然导致量子状态发生错误. 借助于经典纠错码理论，人们提出了一系列量子纠错码方案，其中以 Calderbank-Shor-Steane(CSS)型码[1—3]和稳定子码理论[4,5]最为成熟和重要. Grassl 和 Beth[6]在 1999 年给出了量子移位寄存器和量子态上的多项式乘法的实现方法，本文在此基础上给出了 CSS 型量子卷积码的编译码方法.

本文首先简单介绍了 CSS 型量子卷积码的构造方法，讨论编码方法及其实现网络，然后给出量子 Viterbi 纠错算法，最后通过对编码网络的逆操作得到译码网络.

## 2. CSS 型量子卷积码介绍

给定一个$[[n, n-2k, m]]$ CSS 型量子卷积码，其稳定子生成元可以表示为[7]

$$\boldsymbol{M} = \begin{pmatrix} M_{0,1} \\ M_{0,2} \\ \\ M_{0,2k} \\ M_{1,1} \\ M_{1,2} \\ \\ M_{1,2k} \end{pmatrix}. \tag{1}$$

这里

$$\begin{aligned} M_{0,1} &= g_1^1 \otimes g_1^2 \otimes \cdots \otimes g_1^{n+m} \otimes I \otimes \cdots, \\ M_{0,2} &= g_2^1 \otimes g_2^2 \otimes \cdots \otimes g_2^{n+m} \otimes I \otimes \cdots, \\ &\vdots \\ M_{0,2k} &= g_{2k}^1 \otimes g_{2k}^2 \otimes \cdots \otimes g_{2k}^{n+m} \otimes I \otimes \cdots, \\ M_{a,b} &= I^m \otimes M_{0,b} \quad (a > 0, 1 \leqslant b \leqslant 2k), \end{aligned} \tag{2}$$

其中 $m$ 称为编码存储. 在此规定，如果

$$\psi(D) = (\psi^{(1)}(D) \quad \psi^{(2)}(D) \quad \cdots \quad \psi^{(n)}(D)), \tag{3}$$

那么$|\psi(D)\rangle$表示量子态$|a_{1,0}\, a_{2,0} \cdots a_{n,0}\, a_{1,1} \cdots a_{n,1}$

* 国家自然科学基金(批准号：60496316，60472098)资助的课题.

$\cdots a_{1,q-1}\cdots a_{n,q-1}\rangle$,其中

$$\psi^{(i)}(D) = \sum_{j=0}^{q-1} a_{i,j}D^j \qquad (a_{i,j} \in GF(2)).$$

CSS 型量子卷积码是以经典卷积码为基础的. 给定一个$[n,k,m_1]$经典二元卷积码 $C$,其对偶码 $C^{\perp}$为$[n,n-k,m_2]$卷积码,$m_1$ 和 $m_2$ 为编码存储. 如果满足 $C\subseteq C^{\perp}$,即码 $C$ 是自正交的,则通过 CSS 型量子码的一般构造方法[8],可以得到一个$[[n,n-2k,m]]$ CSS 型量子卷积码,其基态可以表示为(略去归一化系数)

$$|\psi_j(D)\rangle = \sum_{c\in C}|\boldsymbol{c}(D)+\boldsymbol{\omega}_j(D)\rangle, \qquad (4)$$

其中

$$\boldsymbol{\omega}_j(D) \in C^{\perp}/C.$$

常见的经典自正交卷积码一般满足[9] $k=1$ 或 $n-k=1$,所以本文中仅考虑 $k=1$ 的自正交经典卷积码. 若无特殊说明,以下讨论的皆为 CSS 型量子卷积码.

## 3. 编译码方法

给定一个$[n,1,m_1]$自正交卷积码 $C$,生成矩阵为 $\boldsymbol{g}(D)$,其对偶码 $C^{\perp}$是$[n,n-1,m_2]$卷积码,生成矩阵为 $\boldsymbol{g}^{\perp}(D)$. 假设 $\boldsymbol{c}(D)\in C$,$\boldsymbol{\omega}_j(D)\in C^{\perp}$分别为信息序列 $i(D)$,$\boldsymbol{j}(D)$的码字,则有

$$\boldsymbol{c}(D) = i(D)\boldsymbol{g}(D), \qquad (5)$$

$$\boldsymbol{\omega}_j(D) = \boldsymbol{j}(D)\boldsymbol{g}^{\perp}(D). \qquad (6)$$

由于 $C\subseteq C^{\perp}$,因此可以令 $\boldsymbol{g}^{\perp}(D)$中的第一行元素为 $\boldsymbol{g}(D)$,剩下的 $n-2$ 行元素表示为 $\tilde{\boldsymbol{g}}^{\perp}(D)$,即

$$\boldsymbol{g}^{\perp}(D) = \begin{bmatrix} \boldsymbol{g}(D) \\ \tilde{\boldsymbol{g}}^{\perp}(D) \end{bmatrix}. \qquad (7)$$

因而(4)式可以变换为

$$\begin{aligned}
|\psi_j(D)\rangle &= \sum_{c\in C}|\boldsymbol{c}(D)+\boldsymbol{\omega}_j(D)\rangle \\
&= \sum_{i(D)}|i(D)\boldsymbol{g}(D)+\boldsymbol{j}(D)\boldsymbol{g}^{\perp}(D)\rangle \\
&= \sum_{i(D)}\left|i(D)\boldsymbol{g}(D)+(j_1(D)\quad j_2(D)\quad\cdots\quad j_{n-1}(D))\begin{bmatrix}\boldsymbol{g}(D)\\ \tilde{\boldsymbol{g}}^{\perp}(D)\end{bmatrix}\right\rangle \\
&= \sum_{i(D)}\left|(i(D)\quad j_2(D)\quad\cdots\quad j_{n-1}(D))\begin{bmatrix}\boldsymbol{g}(D)\\ \tilde{\boldsymbol{g}}^{\perp}(D)\end{bmatrix}\right\rangle, \qquad (8)
\end{aligned}$$

其中关于 $i(D)$的求和表示取遍 $i(D)$的所有可能取值.

若将 $\boldsymbol{g}^{\perp}(D)$写为一般的数字表示形式,则第 $l$ 行可以表示为

$$\boldsymbol{g}_l^{\perp} = (g_{1,0}\,g_{2,0}\cdots g_{n,0}\,g_{1,1}\cdots g_{n,1}\cdots g_{1,m_2}\cdots g_{n,m_2}). \qquad (9)$$

定义

$$F_l(D) = \sum_{t=0}^{m_2}\sum_{s=1}^{n} g_{s,t}D^{nt+s-1}.$$

容易验证,在这种表示形式下,有下列关系式成立:

$$|i(D)\boldsymbol{g}(D)\rangle = |i(D^n)F_1(D)\rangle. \qquad (10)$$

因此,(8)式可以继续变换为

$$|\psi_j(D)\rangle = \sum_i\left|(i(D^n)\quad j_2(D^n)\quad\cdots\quad j_{n-1}(D^n))\times\begin{pmatrix}F_1(D)\\ \\ F_{n-1}(D)\end{pmatrix}\right\rangle. \qquad (11)$$

通过上述的分析可知,量子卷积码的任意一个码字基态可以用多项式乘法来实现. 编码过程分为两步进行.

第一步,对(11)式中的各项实现多项式乘法操作. 假设每次输入 $q$ 个时刻的信息,则 $i(D^n)$与 $j_2(D^n)\cdots j_{n-1}(D^n)$的最高次数可以达到$n(q-1)$,$F_l(D)$的最高次数可以达到 $n(m_2+1)-1$. 因此每个多项式乘法的输出必须达到 $n(q+m_2)$位,如果实际输出达不到这个位数,则我们在高位补充相应位数的$|0\rangle$态. 在网络中可以用 Hadamard 变换来实现 $i(D^n)$取遍所有值. 下面讨论如何根据$F_l(D)$中的多项式实现相应的乘法网络. 若 $F_l(D)$中的多项式的常数项为 1,那么我们直接按照文献[6]中的方法实现乘法网络 若多项式中常数项为 0,则我们可以从多项式中提出一个 $D^i$,使多项式的常数项变为 1 后实现乘法网络,然后在高位补 $i$ 个$|0\rangle$态,接着进行 $i$ 个循环移位[6],这样就实现了常数项为 0 的

多项式乘法网络.

第二步，对码字基态$|\psi_j(D)\rangle$的实现. 在量子网络中控制非门可以实现量子态相加的功能. 因此我们可以将 $\sum_i |i(D^n)F_1(D)\rangle$ 作为受控位，$\left|(j_2(D^n)\ \cdots\ j_{n-1}(D^n))\begin{bmatrix}F_2(D)\\ \\ F_{n-1}(D)\end{bmatrix}\right\rangle$ 作为控制位，这样，受控位的输出即为所要的码字基态.

例　以[3,1,2]自正交卷积码为例，其对偶码为[3,2,2]卷积码，生成矩阵分别为

$$\boldsymbol{g}(D)=[1+D+D^2\quad 1+D^2\quad 1],$$

$$\boldsymbol{g}^{\perp}(D)=\begin{bmatrix}1+D+D^2 & 1+D^2 & 1\\ D & D & 1\end{bmatrix}.$$

由上述经典码用 CSS 的构造方法得到一个[[3,1,6]]量子卷积码. 令 $q=2$，$\boldsymbol{j}(D)=(1\quad 1+D)$，则相应的码字基态为

$$\begin{aligned}|\psi_j(D)\rangle&=\sum_i\left|(i(D^n)\quad j_2(D^n)\quad\cdots\quad j_{n-1}(D^n))\begin{bmatrix}F_1(D)\\ \\ F_{n-1}(D)\end{bmatrix}\right\rangle\\&=\sum_i\left|(i(D^3)\quad 1+D^3)\begin{bmatrix}1+D+D^2+D^3+D^6+D^7\\ D^2+D^3+D^4\end{bmatrix}\right\rangle\\&=|D^2+D^3+D^4+D^5+D^6+D^7\rangle+|D^2+D^7+D^9+D^{10}\rangle\\&\quad+|1+D+D^4+D^5\rangle+|1+D+D^3+D^6+D^9+D^{10}\rangle.\end{aligned}$$

其编码网络如图 1 所示，图中 $H$ 表示 Hadamard 门，$R$ 表示循环移位单元. 网络受控位的输出即为码字基态的多项式系数.

编码后的信息在传输过程中，不可避免地会受到噪声的影响. 借助于经典编码理论的纠错算法思想，对量子编码领域的纠错算法进行讨论. 首先，对

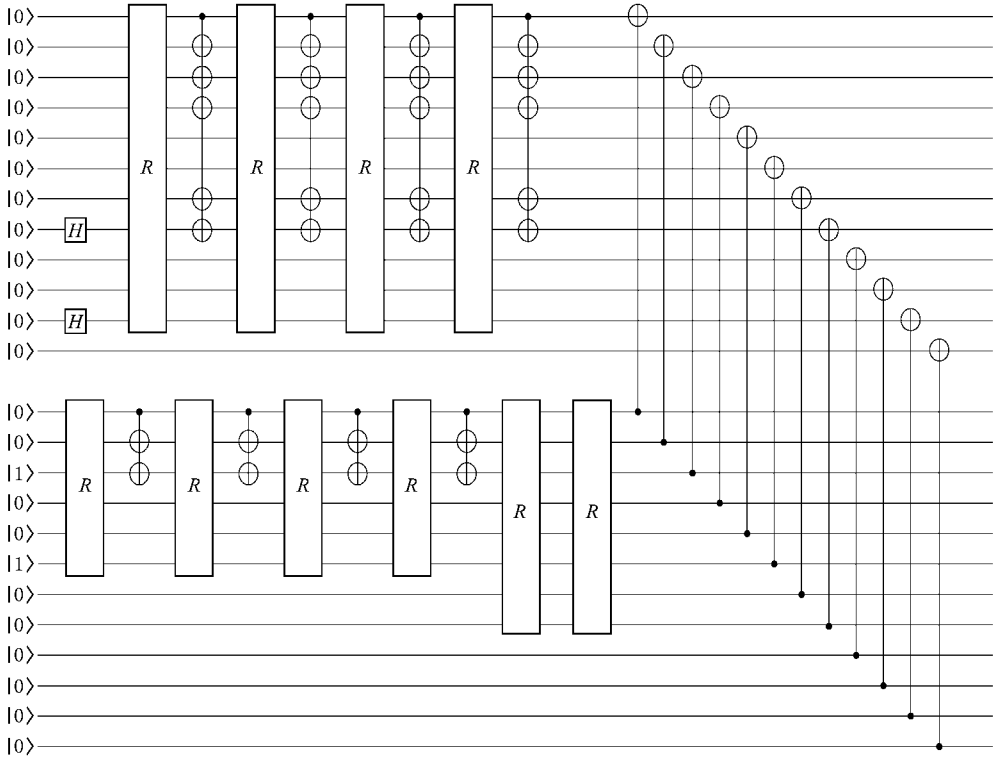


图 1　[[3,1,6]]量子卷积码基态编码网络

指错子 $S$ 进行测量. 令

$$f_{M_{j,i}}(E)=\begin{cases}1 & ([M_{j,i},E]=0),\\ -1 & (\{M_{j,i},E\}=0),\end{cases}\tag{12}$$

则

$$S=\left(f_{M_{0,1}}(E),\cdots,f_{M_{0,2k}}(E),f_{M_{1,1}}(E),\cdots\right).$$

对指错子 $S$ 测量时,先制备一个辅助态 $|0\rangle$,经过 Hadamard 变换,然后以该辅助位作为控制位对接收到的状态 $|\psi\rangle$ 进行 $M_{j,i}$ 操作,经过 Hadamard 再次变换后用 $\{|0\rangle,|1\rangle\}$ 这组基进行测量,最后得到的就是 $f_{M_{j,i}}(E)$.

经典 Viterbi 纠错算法是一种最大似然译码算法,其复杂度随着接收序列的长度而线性增长. 借鉴经典 Viterbi 算法的译码思想,我们给出适用于量子卷积码的纠错算法. 与分组码的纠错算法不同,不用同时计算出接收序列的所有指错子,而是接收一段后对该段进行计算、比较. 在每次计算一段指错子后,挑选一定数量重量最轻的错误矢量 $E_j$ 作为最可能发生的错误矢量集 $\varepsilon_j$. 如此循环迭代,使得 $\varepsilon$ 中的错误矢量 $E$ 长度逐渐增长,直到最后生成与序列长度相等的错误矢量,也就是需要纠正的错误,整个译码过程完成. 由于量子卷积码的生成元之间互相有 $m$ 位的重叠,因此每次译码时我们最多保存 $4^m$ 个错误矢量. 这样,保证了量子 Viterbi 算法也具有线性复杂度. 具体的算法可分为四个步骤进行. 对于 $j=0,\cdots,q-1$,假设 $q$ 为输入的总时刻.

步骤 1 计算稳定子生成元 $M_{j,1}$ 到 $M_{j,2k}$ 的指错子 $S_j$.

步骤 2 列出步骤 1 的 $\varepsilon_{j-1}$ 中差错扩展得到并与 $S_j$ 一致的所有错误矢量 $E_j$. 这时错误矢量作用于接收序列的 1 到 $jn+m$ 量子比特上.

步骤 3 对于 $m$ 位上所有状态中的每一个状态,计算以该状态结尾的所有错误矢量的重量. 挑选其中最轻重量的错误矢量并记录下来,若有相同最轻重量的错误矢量,则任意挑选其中的一个错误矢量加以记录.

步骤 4 经过上述三个步骤,得到了第 $j$ 步中最可能发生的错误矢量集 $\varepsilon_j$,一共包含 $4^m$ 个错误矢量.

当计算出所有长度的错误矢量集后,挑选最轻重量的错误矢量作为最有可能发生的错误. 然后用相应逆操作恢复出原有编码态,纠错完成.

对接收序列完成纠错后,即可进行译码. 译码网络只需简单地逆向执行编码过程,即输入编码后状态,然后逆向执行上述编码过程的每一步,最后恢复出所有信息位,译码完成. 例如对上述举例的译码,只需从图 1 的右端送入编码后的量子比特,信息在左端相应位被恢复.

## 4. 结 论

CSS 型量子纠错码以经典线性码为基础,是量子稳定子码类中的一个重要子类. 首先提出了 CSS 型量子卷积码的一种新的编译码方法. 由于经典卷积码可以表示为多项式形式,通过适当变换给出了 CSS 型量子卷积码码字基态的多项式表示形式. 这样编码一个码字基态就可以通过量子态上的多项式乘法网络实现. 这种方法具有高度结构化、思路简单的特点,且编译码网络易于实现. 本文将经典卷积码的纠错算法思想移植到量子领域,详细给出了具有线性复杂度的量子 Viterbi 算法,通过逐段迭代译码找到最有可能发生的错误矢量.


[1] Calderbank A R, Shor P W 1996 *Phys. Rev.* A **54** 1098

[2] Stean A 1996 *Proc. Roy. Soc. Lond.* A **452** 2551

[3] Li Z, Xing L J 2007 *Acta Phys. Sin.* **56** 5602 (in Chinese) [李卓、邢莉娟 2007 物理学报 **56** 5602]

[4] Matsumoto R 2002 *IEEE Trans. Inform. Theory* **48** 2122

[5] Li Z, Xing L J 2008 *Acta Phys. Sin.* **57** 28 (in Chinese) [李卓、邢莉娟 2008 物理学报 **57** 28]

[6] Grassl M, Beth T 2000 *Proc. Roy. Soc. Lond.* A **456** 2689

[7] Ollivier H, Tillich J P 2003 *Phys. Rev. Lett.* **91** 177902

[8] Li C Z 2000 *Quantum Communication and Quantum Computation* (Changsha: National University of Defense Technology Press) p297 (in Chinese) [李承祖 2000 量子通信和量子计算 (长沙:国防科技大学出版社) 第 297 页]

[9] Wang X M, Xiao G Z 2001 Error-correcting Codes——Principle and Method (Xi'an: Xidian University Press) p378 (in Chinese) [王新梅、肖国镇 2001 纠错码——原理与方法 (西安:西安电子科技大学出版社) 第 378 页]

# Encoding and decoding of quantum convolutional codes*

Xing Li-Juan Li Zhuo Bai Bao-Ming Wang Xin-Mei
(*State Key Laboratory of Integrated Service Networks*, *Xidian University*, *Xi'an* 710071, *China*)
(Received 18 October 2007; revised manuscript received 1 April 2008)

Abstract

The research on quantum convolutional codes is aimed at protecting a flow of information over long distance communications. The polynomial representation of a quantum state is defined. Based on the Calderbank-Shor-Steane(CSS)-type construction of quantum codes, a new method for encoding and decoding of CSS-type quantum convolutional codes is presented and corresponding networks are described. The basis state of the code is transformed into the product of an information polynomial by the generator polynomial. Then networks can be realized by operations of polynomial multiplication. Finally, inspired by classical convolutional decoding idea, a quantum Viterbi algorithm with linear complexity is put forward.

**Keywords**: quantum information, quantum convolutional codes, encoding and decoding, correcting algorithm
**PACC**: 0367, 0365, 0210

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60496316, 60472098).