一类基于经典卷积码的量子稳定子码

邢莉娟，李 卓，王新梅
(西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071)

摘要：提出了一类新的量子稳定子码的构造方法.寻找量子稳定子码的问题可以转化为寻找 GF(4)上迹内积自正交的经典码问题.根据这一关系，首先证明了 GF(4)上经典卷积码迹内积自正交的充要条件，然后寻找满足该条件的经典卷积码，再将找到的经典卷积码通过“咬尾”变换得到具有简单分组结构的 tail-biting 码，证明了该类 tail-biting 码是迹内积自正交的，从而构造出对应的量子稳定子码.该类码构造方法简单，码距接近理论上限.

关键词：量子稳定子码；经典卷积码；tail-biting 码；迹内积；自正交
中图分类号：TN911.2 **文献标识码**：A **文章编号**：1001-2400(2008)02-0277-05

A class of quantum stabilizer codes based on classical convolutional codes

XING Li-juan, *LI Zhuo*, *WANG Xin-mei*
(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China)

Abstract: A new class of quantum stabilizer codes is presented. The problem of finding stabilizer quantum-error-correcting codes can be transformed into the problem of finding self-orthogonal codes over the Galois field GF(4) under a trace inner product. Based on this connection, the necessary and sufficient condition is proved under which classical convolutional codes over GF(4) are self-orthogonal with respect to the trace inner product, and then corresponding codes satisfying the condition are found. Tail-biting codes with a simple block structure are obtained by "tail-biting" transformation, which are self-orthogonal with respect to the trace inner product. Finally, relative quantum stabilizer codes are constructed. The code construction is simple, and the minimum distance of the code approaches the upper bound.

Key Words: stabilizer quantum-error-correcting codes; classical convolutional codes; tail-biting codes; trace inner product; self-orthogonal

近几十年来，量子通信与量子计算的研究已经引起人们极大的关注.由于量子系统在操作时不可避免会受到外界噪声的影响，必然导致量子状态发生错误，这已经成为量子信息领域的主要障碍之一.近年来发展起来的量子纠错编码技术能够有效地解决这一难题.迄今为止，许多种量子纠错码以及相关理论已经被发现和提出，其中以 CSS 码[1,2]和稳定子码[3,4]最为重要和成熟.笔者利用量子稳定子码与 GF(4)上经典码的对应关系[5]，给出了一种构造量子稳定子码的方法.

1 基础介绍

令 X,Y,Z 表示 pauli 算子，集合 $G=\{I,X,Y,Z\}$，GF(4) 为 $\{0,1,\alpha,\bar{\alpha}\}$.若忽略相位的影响，$G$ 中的乘法

收稿日期：2007-04-24
基金项目：国家部委基金资助(××060104)
作者简介：邢莉娟(1982-)，女，西安电子科技大学博士研究生 E-mail：yoyo_xing@126.com.

结构与 GF(4) 上的加法结构是相同的. 因此可通过如下的函数 $f(\cdot)$ 将集合 G 与 GF(4)上的元素对应起来.

$G \xrightarrow{f(\cdot)}$	GF (4)
I	0
X	α
Y	1
Z	$\bar{\alpha}$

给定 GF(4)上两个 n 长的向量 $\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})$, $\boldsymbol{b}=(b_0,b_1,\cdots,b_{n-1})$.

定义 1 厄米内积 $\langle \boldsymbol{a},\boldsymbol{b}\rangle=\sum_{i=0}^{n-1}\bar{a}_i b_i$, "—"表示元素的共轭.

定义 2 迹内积 $\mathrm{tr}\langle \boldsymbol{a},\boldsymbol{b}\rangle=\mathrm{tr}\sum_{i=0}^{n-1}\bar{a}_i b_i=\sum_{i=0}^{n-1}\mathrm{tr}(\bar{a}_i b_i)$,

$\mathrm{tr}(0)=\mathrm{tr}(1)=0, \mathrm{tr}(\alpha)=\mathrm{tr}(\bar{\alpha})=1$.

根据定义 2,可以通过下式来判断集合 G 中的元素 G_1, G_2 是否对易:若 $\mathrm{tr}\langle f(G_1),f(G_2)\rangle=0$,算子 G_1, G_2 对易;若 $\mathrm{tr}\langle f(G_1),f(G_2)\rangle=1$,算子 G_1, G_2 反对易.

$$G_1G_2=(-1)^{\mathrm{tr}\langle f(G_1),f(G_2)\rangle}G_2G_1 \quad .$$

一个 GF(4)上的线性码迹内积自正交的充要条件为其也是厄米内积自正交的[6]. 因此,可以通过寻找 GF(4)上厄米内积自正交的线性码来构造相应的量子码.

定理 1 假设 C 是一个 GF(4) 上厄米内积自正交的线性码,参数为$[N,K]$,并且其对偶码 $C^{\perp}$ 的距离为 d,则由 C 可构造出参数为$[[N,N-2K,d]]$ 的非简并量子稳定子码[6].

2 自正交经典码的构造

第 1 步,构造一个 GF(4)上的线性卷积码 C,参数为$[n,k,m]$,其中 m 指编码存储. 则 C 的生成矩阵 $\boldsymbol{G}_{\infty}$ 如下式所示,迟延算子 D 表示延时一个时间单位.

$$\boldsymbol{G}_{\infty}=\begin{bmatrix}\boldsymbol{G}\\ D\boldsymbol{G}\\ D^2\boldsymbol{G}\\ \vdots\end{bmatrix}=\begin{bmatrix}\boldsymbol{G}_0 & \boldsymbol{G}_1 & \cdots & \boldsymbol{G}_{m-1} & \boldsymbol{G}_m & & \\ & \boldsymbol{G}_0 & \boldsymbol{G}_1 & \cdots & \boldsymbol{G}_{m-1} & \boldsymbol{G}_m & \\ & & \boldsymbol{G}_0 & \boldsymbol{G}_1 & \cdots & \boldsymbol{G}_{m-1} & \boldsymbol{G}_m \\ & & & \ddots & \ddots & & \ddots\end{bmatrix} \quad .$$

常见的厄米内积自正交卷积码的参数满足 $k=1$ 或 $n-k=1$[7],若无特殊说明,下面讨论的均为 GF(4)上参数为$k=1$ 的厄米内积自正交卷积码.

为了方便,也可以用迟延算子 D 表示 $\boldsymbol{G}_{\infty}$: $\boldsymbol{g}(D)=[g_1(D),g_2(D),\cdots,g_n(D)]$.

定理 2 设 C 是 GF(4)上的线性卷积码,其生成矩阵为 $\boldsymbol{g}(D)=[g_1(D),g_2(D),\cdots,g_n(D)]$,则当且仅当 $\sum_{j=1}^{n}g_j(D)\bar{g}_j(D^{-1})=0$ 成立时,C 是厄米内积自正交的.

证明 对于 $\boldsymbol{g}(D)=[g_1(D),g_2(D),\cdots,g_n(D)]$, 定义

$$g_j(D)=\sum_i g_{j,i}D^i \quad ,$$

$$D^l g_j(D)=\sum_i g_{j,i}D^{l+i}=\sum_i g_{j,i-l}D^i \quad ,$$

$$\langle \boldsymbol{g}(D),D^l\boldsymbol{g}(D)\rangle=\sum_{j=1}^{n}\langle g_j(D),D^l g_j(D)\rangle=\sum_{j=1}^{n}\sum_i \bar{g}_{j,i}g_{j,i-l} \quad ,$$

则有 $$\sum_{j=1}^{n}g_j(D)\bar{g}_j(D^{-1})=\sum_{j=1}^{n}g_j(D)\sum_i\bar{g}_{j,i}D^{-i}=\sum_{j=1}^{n}\sum_i\bar{g}_{j,i}D^{-i}g_j(D)=$$

$$\sum_{j=1}^{n}\sum_{i}\bar{g}_{j,i}D^{-i}\sum_{l}g_{j,i-l}D^{i-l}=\sum_{l}\sum_{j=1}^{n}\sum_{i}\bar{g}_{j,i}g_{j,i-l}D^{-i}D^{i-l}=$$

$$\sum_{l}\sum_{j=1}^{n}\sum_{i}\bar{g}_{j,i}g_{j,i-l}D^{-l}=\sum_{l}\langle\boldsymbol{g}(D),D^{l}\boldsymbol{g}(D)\rangle D^{-l}\quad .$$

所以，$\sum_{j=1}^{n}g_j(D)\bar{g}_j(D^{-1})=0$ 当且仅当$\langle\boldsymbol{g}(D),D^{l}\boldsymbol{g}(D)\rangle=0$，即 $\boldsymbol{g}(D)$ 与它所有的延时正交，也就是 C 是厄米内积自正交的.

同理，用相同的方法寻找 C 的对偶码 $C^{\perp}$，$C^{\perp}$ 为 GF(4) 上的参数为$[n,n-1]$的线性卷积码. 令 $C^{\perp}$ 的生成矩阵为

$$\boldsymbol{H}(D)=\begin{bmatrix}h_{(1,1)}(D) & h_{(1,2)}(D) & \cdots & h_{(1,n)}(D)\\ h_{(2,1)}(D) & h_{(2,2)}(D) & \cdots & h_{(2,n)}(D)\\ \vdots & \vdots & & \vdots\\ h_{(n-1,1)}(D) & h_{(n-1,2)}(D) & \cdots & h_{(n-1,n)}(D)\end{bmatrix},$$

则 C 与 $C^{\perp}$ 必满足　　$\sum_{j=1}^{n}h_{(i,j)}(D)\bar{g}_j(D^{-1})=0\quad,\quad i=1,2,\cdots,n-1\quad .$

例 1　参数为$[3,1,2]$的线性卷积码 C，生成矩阵 $\boldsymbol{g}(D)=[1+D+D^2,1+\alpha D+D^2,1+D]$.

由定理 2 可知

$$\sum_{j=1}^{n}g_j(D)\bar{g}_j(D^{-1})=(1+D+D^2)(1+D^{-1}+D^{-2})+$$

$$(1+\alpha D+D^2)(1+\bar{\alpha}D^{-1}+D^{-2})+(1+D)(1+D^{-1})=0\quad ,$$

所以 C 是厄米内积自正交的. 并根据 $\sum_{j=1}^{n}h_{(i,j)}(D)\bar{g}_j(D^{-1})=0$ 找到对偶码 $C^{\perp}$，其生成矩阵为

$$\boldsymbol{H}(D)=\begin{bmatrix}\alpha D & \bar{\alpha}D & 1+D\\ 1 & 1+\bar{\alpha}D & 1+\bar{\alpha}D\end{bmatrix}\quad .$$

第 2 步，由线性卷积码 C 经过适当变换得到 tail-biting 码 B[8]. 在经典编码理论中，tail-biting 码是一种性能优异的线性分组码，其可以达到与卷积码相同的码率，同时具有简单的分组码结构，大大降低了编译码器的复杂度. 为了保持码率不变，B 的参数可以写为$[n(L+m),L+m]$，L 取任意正整数. 其生成矩阵可以表示为

$$\boldsymbol{G}_B=\begin{bmatrix}\boldsymbol{G}_0 & \boldsymbol{G}_1 & \cdots & \boldsymbol{G}_m & \boldsymbol{0} & \cdots & \cdots & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{G}_0 & \cdots & \boldsymbol{G}_{m-1} & \boldsymbol{G}_m & \boldsymbol{0} & \cdots & \boldsymbol{0}\\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots\\ \boldsymbol{G}_1 & \boldsymbol{G}_2 & \cdots & \boldsymbol{0} & \cdots & \boldsymbol{0} & \cdots & \boldsymbol{G}_0\end{bmatrix}\quad .$$

显然，若 C 是厄米内积自正交的，则由其得到的 B 也是厄米内积自正交的. $B^{\perp}$ 可由 $C^{\perp}$ 用同样的方法得到，其码参数为$[n(L+m),(n-1)(L+m),d]$.

例 2　例 1 中参数为$[3,1,2]$的线性卷积码 C，其生成矩阵为

$$\boldsymbol{G}_{\infty}=\left[\begin{array}{ccc:ccc:ccc:ccc:ccc:c}1&1&1&1&\alpha&1&1&1&0&0&0&0&0&0&0&\cdots\\ 0&0&0&1&1&1&1&\alpha&1&1&1&0&0&0&0&\cdots\\ 0&0&0&0&0&0&1&1&1&1&\alpha&1&1&1&0&\cdots\\ \multicolumn{3}{c:}{\cdots}&\multicolumn{3}{c:}{\cdots}&\multicolumn{3}{c:}{\cdots}&\multicolumn{3}{c:}{\cdots}&\multicolumn{3}{c:}{\cdots}&\cdots\end{array}\right]\quad .$$

令 $L=3$，由 C 可以得到一个参数为$[15,5]$ 的 B，其生成矩阵 $\boldsymbol{G}_B$ 为

$$\boldsymbol{G}_B=\left[\begin{array}{ccc:ccc:ccc:ccc:ccc}1&1&1&1&\alpha&1&1&1&0&0&0&0&0&0&0\\ 0&0&0&1&1&1&1&\alpha&1&1&1&0&0&0&0\\ 0&0&0&0&0&0&1&1&1&1&\alpha&1&1&1&0\\ 1&1&0&0&0&0&0&0&0&1&1&1&1&\alpha&1\\ 1&\alpha&1&1&1&0&0&0&0&0&0&0&1&1&1\end{array}\right]\quad .$$

在例 1 中已经证得 C 是厄米内积自正交的,因此 B 也是厄米内积自正交的. 同理,由 $C^{\perp}$ 可以得到参数为[15,10,4]的 $B^{\perp}$,其生成矩阵为

$$\boldsymbol{G}_{B^{\perp}}=\left[\begin{array}{ccc:ccc:ccc:ccc:ccc}
0 & 0 & 1 & \alpha & \bar{\alpha} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 1 & 1 & 0 & \bar{\alpha} & \bar{\alpha} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & \alpha & \bar{\alpha} & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 1 & 1 & 0 & \bar{\alpha} & \bar{\alpha} & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha & \bar{\alpha} & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \bar{\alpha} & \bar{\alpha} & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha & \bar{\alpha} & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \bar{\alpha} & \bar{\alpha}\\
\alpha & \bar{\alpha} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & \bar{\alpha} & \bar{\alpha} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1
\end{array}\right].$$

3 量子稳定子码的构造

上文已经找到了 GF(4)上厄米内积自正交的线性码,根据定理 1,可以构造出相应的量子稳定子码. 将 B 的生成矩阵 $\boldsymbol{G}_B$ 中的每一行生成元分别乘以 1 和 α,然后将得到的结果通过函数 $f^{-1}(\cdot)$ 映射到集合 G 中的元素,这样就得到了相应量子码的稳定子生成元. 显然,若 $\boldsymbol{G}_B$ 共有 $L+m$ 行,通过上述的计算,可以得到对应的 $2(L+m)$ 个稳定子生成元,若其对偶码 $B^{\perp}$ 的距离为 d,就得到了参数为[[$n(L+m),(L+m)(n-2),d$]]的量子码,这样的量子码最多可以纠正 $\lfloor (d-1)/2 \rfloor$ 位错误.

例 3 已知例 2 中参数为[15,5]的码 B,并且 $B^{\perp}$ 的距离 $d=4$. 根据定理 1,可以构造出参数为[[15,5,4]]的非简并量子稳定子码. 其稳定子生成元如下所示,其中 M_i 代表第 i 个生成元.

M_1:$Y\ Y\ Y\ Y\ X\ Y\ Y\ Y\ I\ I\ I\ I\ I\ I\ I$

M_2:$I\ I\ I\ Y\ Y\ Y\ Y\ X\ Y\ Y\ Y\ I\ I\ I\ I$

M_3:$I\ I\ I\ I\ I\ I\ Y\ Y\ Y\ Y\ X\ Y\ Y\ Y\ I$

M_4:$Y\ Y\ I\ I\ I\ I\ I\ I\ I\ Y\ Y\ Y\ Y\ X\ Y$

M_5:$Y\ X\ Y\ Y\ Y\ I\ I\ I\ I\ I\ I\ I\ Y\ Y\ Y$

M_6:$X\ X\ X\ X\ Z\ X\ X\ X\ I\ I\ I\ I\ I\ I\ I$

M_7:$I\ I\ I\ X\ X\ X\ X\ Z\ X\ X\ X\ I\ I\ I\ I$

M_8:$I\ I\ I\ I\ I\ I\ X\ X\ X\ X\ Z\ X\ X\ X\ I$

M_9:$X\ X\ I\ I\ I\ I\ I\ I\ I\ X\ X\ X\ X\ Z\ X$

M_{10}:$X\ Z\ X\ X\ X\ I\ I\ I\ I\ I\ I\ I\ X\ X\ X$

表 1 由 tail-biting 码构造出的稳定子码

码率	B	$B^{\perp}$	稳定子码	d_{opt}	码率	B	$B^{\perp}$	稳定子码	d_{opt}
1/3	[15,5]	[15,10,4]	[[15,5,4]]	4	1/6	[30,5]	[30,25,3]	[[30,20,3]]	4
1/3	[24,8]	[24,16,5]	[[24,8,5]]	5-6	1/10	[40,4]	[40,36,3]	[[40,32,3]]	3
1/5	[15,3]	[15,12,3]	[[15,9,3]]	3	1/16	[80,5]	[80,75,3]	[[80,70,3]]	3-4

表 1 列出了一些由 B 构造出的稳定子码,其中 d_{opt} 为相同参数下码距的理论上界[6],根据以上所述的构造方法得到的稳定子码基本都达到了上界值,因此是一类纠错能力良好的量子码.

4 结 束 语

根据量子稳定子码与 GF(4)上经典码的对应关系,在 GF(4)上找到了基于经典卷积码的 tail-biting 码,

并满足迹内积自正交的条件,然后构造出了相应的量子稳定子码.这种稳定子码构造方法简单,并且码距基本可以达到理论的上界值,具有较好的纠错能力.

参考文献:

[1] Calderbank A R, Shor P W. Good Quantum Error-correcting Codes Exist[J]. Phys Rev A, 1996, 54(2): 1098-1105.

[2] MacKay D J C, Mitchisom G, McFadden P L. Sparse-graph Codes for Quantum Error Correction[J]. IEEE Trans on Inform Theory, 2004, 50(7): 2315-2330.

[3] Gottesman D. Class of Quantum Error-correcting Codes Saturating the Quantum Hamming Bound[J]. Phys Rev A, 1996, 54(3): 1862-1868.

[4] Ketkar A, Klappenecker A, Kumor S, et al. Nonbinary Stabilizer Codes over Finite Fields[J]. IEEE Trans on Inform Theory, 2006, 52(12): 4892-4914.

[5] Gulliver T A, Kim J L. Circulant Based Extremal Additive Self-dual Codes over GF(4)[J]. IEEE Trans on Inform Theory, 2004, 50(2): 359-366.

[6] Calderbank A R, Rains E M, Shor P W, et al. Quantum Error Correction Via Codes over GF(4)[J]. IEEE Trans on Inform Theory, 1998, 44(4): 1369-1387.

[7] 王新梅, 肖国镇. 纠错码——原理与方法[M]. 第二版. 西安: 西安电子科技大学出版社, 2001.

[8] Lin S, Costello D J. Error Control Coding[M]. 2nd. New Jersey: Prentice-Hall, Inc, 2004.

(编辑: 郭　华)

简　讯

2007 全国大学生电子设计竞赛陕西赛区颁奖典礼在我校举行　日前,由陕西省教育厅主办、我校承办、惠普公司协办的 2007 年全国大学生电子设计竞赛陕西赛区(惠普杯)比赛圆满结束,2008 年 1 月 4 日在我校进行了颁奖典礼.本届竞赛陕西赛区共有 35 所高校的 400 支队伍参赛.其中我校获得 5 个国家一等奖,9 个国家二等奖,获省级一等奖 17 个,二等奖 7 个,三等奖 3 个.获奖数在全国 767 所参赛高校中排名并列第三,在全省 35 所参赛高校中排名第一.

摘自《西电科大报》2008.1.10