F4上2维和3维的最优自正交码

马月娜，　赵学军，　冯有前

(空军工程大学理学院，陕西西安 710051)

摘　要：研究了F4上维数为2和3的最优(或拟最优)自正交码的码长与极小距离之间的关系，用组合方法构造相应维数的最优(或拟最优)自正交码的生成矩阵，确定出其中达到Griesmer界的码，并计算出所构造的2维最优(或拟最优)自正交码的重量多项式。

关键词：自正交码；Griesmer界；最优码

中图分类号：O236.6　　**文献标识码**：A　　**文章编号**：1009-3516(2005)05-0063-04

自正交码是一类特别重要的纠错码。在过去的40年中，自正交码(特别是其中的特例自对偶码)一直是人们研究的热门课题[1]。近几年来，由于量子纠错码的兴起，人们开始研究一般的自正交码，刻划出它们的特征并进一步构造出给定特征的自正交$[n,k,d]$码[1~2]。

本文将讨论F_4上低维数、短码长的线性最优自正交码的规律，用组合方法构造一系列维数$k=2$或3的最优(或拟最优)自正交码，并确定出其中达到Griesmer界的码。

1　预备知识

设F_4是包含四个元素的有限域，$\forall x\in F_4$，$\bar{x}=x^2$称为x的共轭元，记$F_4=\{0,1,\omega,\bar{\omega}\}$，其中$\bar{\omega}=\omega^2=\omega+1$且$\bar{\omega}^3=\omega^3=1$。$F_4$上的$n$维行线性空间记为$F_4^n$。$F_4^n$上的向量$\boldsymbol{X}$与$\boldsymbol{Y}$的Hermite内积为：$(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{X}\boldsymbol{Y}^+=\boldsymbol{X}\bar{\boldsymbol{Y}}^{\mathrm{T}}=x_1\bar{y_1}+x_2\bar{y_2}+\cdots+x_n\bar{y_n}$。若$(\boldsymbol{X},\boldsymbol{Y})=0$，称$\boldsymbol{X}$与$\boldsymbol{Y}$ Hermite正交。

F^n的k维子空间C称为四元$[n,k]$线性码，C的元素称为码字，称n为C的码长，k为C的维数。C的极小Hamming重量$w(C)=\min\{w(X)\mid X\neq 0,X\in C\}$；$C$的极小Hamming距离$d(C)=\min\{d(X,Y)\mid X\neq Y,$且$X,Y\in C\}$；当$d(C)=d$时，称$C$为$F_4$上参数为$[n,k,d]$的码，简记为$C=[n,k,d]$。

若C是一个四元$[n,k]$线性码，C的Hermite对偶码记为$C^{\perp}=\{X\mid(X,Y)=0,\forall Y\in C\}$。若$C\subseteq C^{\perp}$，称$C$为自正交的；若$C=C^{\perp}$，称$C$为自对偶的。

定义1　设$C=[n,k,d]$，如果不存在$[n,k,d+1]$，则称C是最优的；如果不存在$[n,k,d+2]$，则称C是拟最优的。

符号约定：为下文书写方便，将ω记为2、$\bar{\omega}$记为3。用$[n,k,d]$表示F_4上的码。用$\boldsymbol{I}_n$表示n维行向量$(1,1,\cdots,1)$，$\boldsymbol{A}_{k\times n}$表示$k\times n$的矩阵；特别地，用$\boldsymbol{O}_{k\times n}$表示$k\times n$的零矩阵。$d_{\max}(n,k)$表示线性$[n,k,d]$码极小距离的最大值。由文献[2]、[3]可知下面的3个引理成立。

引理1　F_4上自正交码的每个码字的重量为偶数。

引理2　(Griesmer界)q元域上任何线性$[n,k,d]_q$码的码长n、维数k和极小距离d之间存在如下关系：$n\geqslant\sum_{i=0}^{k-1}[d/q^i]$。

引理3　如果有自正交码$[n_1,k,d_1]$和$[n_2,k,d_1]$，通过并置它们的生成矩阵，可构造出新的自正交码$[n_1+n_2,k,d_1+d_2]$。

收稿日期：2004-11-24
基金项目：空军工程大学学术基金资助项目(2002X14)
作者简介：马月娜(1977-)，女，陕西西安人，讲师，硕士生，主要从事编码与密码学研究.

2 2 维最优自正交码的特征与构造

根据 Griesmer 界中码长与极小距离之间的关系,将维数 $k=2$ 的线性$[n,k,d]$自正交码 C 按码长 n 分成 5 种情况,并且可得到码 C 的极小距离 $d_{\max}(n,2)$ 满足以下结论:

$(i)n=5m,d_{\max}(n,2)\leqslant 4m$; $(ii)n=5m+1,d_{\max}(n,2)\leqslant 4m$;

$(iii)n=5m+2$,$d_{\max}(n,2)\leqslant 4m+1$; $(iv)n=5m+3$,$d_{\max}(n,2)\leqslant 4m+2$;

$(v)n=5m+4$,$d_{\max}(n,2)\leqslant 4m+3$,其中 $m=1,2,\cdots$。

由引理 1 和文献[3]可知,当 $n=5m+2$ 或 $5m+3$ 时,不存在达到 Griesmer 界的 2 维自正交码。

定理 1 设 $m\geqslant 1$

1) 当 $n=5m$、$5m+1$ 或 $5m+3$ 时,存在最优的、并达到 Griesmer 界的自正交码 $C=[n,2,d_{\max}(n,2)]$;

2)当 $n=5m+2$、$5m+4$ 时,则存在拟最优的自正交码 $C=[n,2,d_{\max}(n,2)-1]$。

证明 : 以下就$(i)\sim(v)$每种情况,具体构造出达到最优(或拟最优)自正交码的生成矩阵:

1) 当码长 $n=5m,m\geqslant 1$ 时,构造矩阵 $\boldsymbol{G}_{5m,2}$如下,则以 $\boldsymbol{G}_{5m,2}$为生成矩阵的码 C 是自正交的,且具有重量多项式 $A(z)=1+15z^{4m}$。由(i)可知 C 是最优的并且达到 Griesmer 界。

2) 当码长 $n=5m+1,m\geqslant 1$ 时,构造矩阵 $\boldsymbol{G}_{5m+1,2}$如下,则以 $\boldsymbol{G}_{5m+1,2}$为生成矩阵的码 C 是自正交的,且具有重量多项式 $A(z)=1+9z^{4m}+6z^{4m+2}$。由(ii)可知 C 是最优的并且达到 Griesmer 界。

3) 当码长 $n=5m+2,m\geqslant 2$ 时,构造矩阵 $\boldsymbol{G}_{5m+2,2}$如下,则以矩阵 $\boldsymbol{G}_{5m+2,2}$为生成矩阵的码 C 是自正交的,且具有重量多项式 $A(z)=1+9z^{4m}+6z^{4m+2}$。由(iii)可知 C 是拟最优的。

4) 当码长 $n=5m+3,m\geqslant 1$ 时,构造矩阵 $\boldsymbol{G}_{5m+3,2}$如下,则以矩阵 $\boldsymbol{G}_{5m+3,2}$为生成矩阵的码 C 是自正交的,且具有重量多项式 $A(z)=1+12z^{4m+2}+3z^{4m+4}$。由$(iv)$可知 C 是最优的且达到 Griesmer 界。

5) 当码长 $n=5m+4,m\geqslant 1$ 时,构造矩阵 $\boldsymbol{G}_{5m+4,2}$如下,则以矩阵 $\boldsymbol{G}_{5m+4,2}$为生成矩阵的码 C 是自正交的,且具有重量多项式以 $A(z)1+12z^{4m+2}$。由(v)可知 C 是拟最优的。

$$\boldsymbol{G}_{5m,2}=\begin{pmatrix}1_m & 1_m & 1_m & 1_m & 0_m\\ 0_m & 1_m & 21_m & 31_m & 1_m\end{pmatrix};\ \boldsymbol{G}_{5m+1,2}=\begin{pmatrix}1_{m+1} & 1_{m+1} & 1_{m-1} & 1_{m-1} & 0_{m+1}\\ 0_{m+1} & 1_{m+1} & 21_{m-1} & 31_{m-1} & 1_{m+1}\end{pmatrix};$$

$$\boldsymbol{G}_{5m+2,2}=\begin{pmatrix}1_{m+2} & 1_{m+2} & 1_{m-2} & 1_{m-2} & 0_{m+2}\\ 0_{m+2} & 1_{m+2} & 21_{m-2} & 31_{m-2} & 1_{m+2}\end{pmatrix};\boldsymbol{G}_{5m+3,2}=\begin{pmatrix}1_{m+1} & 1_{m+1} & 1_{m-1} & 1_{m-1} & 0_{m+1}\\ 0_{m+1} & 1_{m+1} & 21_{m-1} & 31_{m-1} & 1_{m+1}\end{pmatrix};$$

$$\boldsymbol{G}_{5m+4,2}=\begin{pmatrix}1_{m+2} & 1_m & 1_m & 1_m & 0_{m+2}\\ 0_{m+2} & 1_m & 21_m & 31_m & 1_{m+2}\end{pmatrix}。$$

总结以上讨论,则定理得证。

3 3 维最优自正交码的特征与构造

文献[5]构造出 F_4 上码长 $n\leqslant 16,k=3$ 的自正交$[n,k,d]$ 码 C 。下面研究 F_4上 $n\geqslant 16,k=3$ 的线性$[n,k,d]$ 码 C ,根据 Griesmer 界中码长与极小距离之间的关系,将此码按码长 n 分成以下 16 种情况(具体分类见表 1)。

表 1 码长为 n 的 3 维自正交码的距离上限

n	$d_{\max}$	m	n	$d_{\max}$	m
$16m$	$\leqslant 12m$	$\leqslant 8$	$16m+10$	$12m+6$	0
$16m+1$	$\leqslant 12m$	$\leqslant 8$		$12m+7$	$[1,8]$
$16m+2$	$\leqslant 12m+1$	$\leqslant 8$	$16m+11$	$12m+7$	1
$16m+3$	$\leqslant 12m+2$	$[1,4]$		$12m+8$	$[2,8]$
	$\leqslant 12m+3$	$[5,8]$		$12m+8$	<2
$16m+4$	$12m+3$	$\leqslant 8$	$16m+12$	$12m+9$	$[3,8]$

续表

n	$d_{\max}$	m	n	$d_{\max}$	m
$16m+5$	$12m+4$	$\leqslant 8$	$16m+13$	$12m+9$	$\leqslant 2$
$16m+6$	$12m+4$	$\leqslant 8$		$12m+10$	$[3,8]$
$16m+7$	$12m+4$	1	$16m+14$	$12m+10$	$\leqslant 2$
	$12m+5$	$[2,8]$		$12m+11$	$[3,6]$
$16m+8$	$12m+5$	1		$12m+12$	$[7,8]$
	$12m+6$	$[2,8]$		$12m+11$	$m\leqslant 2$
$16m+9$	$\leqslant 12m+6$	$\leqslant 1$	$16m+15$	$12m+12$	$[3,8]$
	$\leqslant 12m+7$	$[2,8]$			

我们用构造的方法是：以一些特殊自正交码的生成矩阵为模块，组合出新的最优（或拟最优）自正交码。在给出具体构造之前，先对构造中需要用到的这些特殊最优自正交码的生成矩阵加以说明：

$$\boldsymbol{G}_{6,3}=\begin{pmatrix}1&1&1&1&1&1\\0&1&0&1&2&2\\0&0&1&2&1&2\end{pmatrix},\quad \boldsymbol{G}_{16,3}=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\0&1&0&2&2&1&2&0&3&3&2&3&0&1&1&3\\0&0&1&1&3&1&0&2&2&1&2&0&3&3&2&3\end{pmatrix}$$

$$\boldsymbol{G}_{7,3}=\begin{pmatrix}1&1&1&1&0&0&0\\0&0&1&1&1&1&0\\1&0&1&0&1&0&1\end{pmatrix},\quad \boldsymbol{G}_{15,3}=\begin{pmatrix}0&0&0&1&1&1&1&1&1&1&1&1&1&1&1\\0&1&1&2&3&2&3&0&1&2&3&0&1&2&3\\1&0&1&0&0&1&1&2&2&2&2&3&3&3&3\end{pmatrix}$$

$$\boldsymbol{G}_{8,3}=\begin{pmatrix}1&1&1&1&1&1&1&1\\0&1&1&1&1&0&0&0\\0&0&1&2&3&1&2&3\end{pmatrix},\quad \boldsymbol{G}_{14,3}=\begin{pmatrix}1&1&1&1&0&1&1&1&1&0&1&1&1&1\\2&3&2&3&1&0&1&2&3&1&0&2&1&3\\0&0&1&1&2&2&2&2&2&3&3&3&3&3\end{pmatrix}$$

$$\boldsymbol{G}_{11,3}=\begin{pmatrix}1&1&1&1&1&1&0&0&0&0&0\\0&1&1&2&2&0&1&1&1&1&0\\0&0&1&3&1&3&1&2&3&0&1\end{pmatrix},\quad \boldsymbol{G}_{13,3}=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&0&0&0\\0&1&0&1&1&1&2&2&3&3&0&1&1\\2&2&3&3&1&0&0&3&0&2&1&2&3\end{pmatrix}$$

$$\boldsymbol{G}_{10,3}=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1\\0&1&1&1&1&2&2&3&3&0\\0&0&1&2&3&1&3&1&2&1\end{pmatrix},\quad \boldsymbol{G}_{12,3}=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&0&0\\0&1&0&1&1&1&2&2&3&3&1&1\\0&0&1&1&2&3&1&2&1&3&2&3\end{pmatrix}$$

$$\boldsymbol{G}_{9,3}=\begin{pmatrix}1&1&1&1&1&1&0&0&0\\0&1&1&2&2&0&1&1&0\\0&0&1&1&2&2&0&3&1\end{pmatrix},\boldsymbol{G}_{21,3}=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0\\0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3&0&1&1&1&1\\0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3&1&0&1&2&3\end{pmatrix}$$

为使下文中所构造的自正交码的生成矩阵形式上统一，特别地用 $\boldsymbol{G}_{5,3}$ 表示 $\begin{pmatrix}0&0&0&0&0\\0&1&1&1&1\\1&0&1&2&3\end{pmatrix}$。

定理2　设 $0\leqslant m\leqslant 8$

1）当 $n=16m$、$16m+1$、$16m+3(1\leqslant m\leqslant 4)$、$16m+6$、$16m+5$、$16m+7(m=1)$、$16m+8(2\leqslant m\leqslant 8)$、$16m+9(m=1)$、$16m+10(m=0)$、$16m+11(2\leqslant m\leqslant 8)$、$16m+12(m\leqslant 2)$、$16+13(3\leqslant m\leqslant 8)$、$16m+14(m\leqslant 2$ 或 $7\leqslant m\leqslant 8)$ 或 $16m+15(3\leqslant m\leqslant 8)$ 时，存在最优的、并达到 Griesmer 界的自正交码 $C=[n,3,d_{\max}(n,2)]$。

2）当 $n=16m+2$、$16m+3(5\leqslant m\leqslant 8)$、$16m+4$、$16m+7(2\leqslant m\leqslant 8)$、$16m+8(m=1)$、$16m+9(2\leqslant m\leqslant 8)$、$16m+10(1\leqslant m\leqslant 8)$、$16m+11(m=1)$、$16m+12(3\leqslant m\leqslant 8)$、$16m+13(m\leqslant 2)$、$16m+14(3\leqslant m\leqslant 6)$ 或 $16m+15(m\leqslant 2)$ 时，则存在拟最优自正交码 $C=[n,3,d_{\max}(n,2)-1]$。

证明：分类构造出维数 $k=3$ 时最优（或拟最优）自正交码的生成矩阵

1）$\boldsymbol{G}_{n,3}=(\boldsymbol{G}_{12,3}\quad \boldsymbol{G}_{t,3})$，其中 $n=12+t,t\in\{5,6,7\}$；

2）$\boldsymbol{G}_{n,3}=(\boldsymbol{G}_{16,3}\quad \boldsymbol{G}_{t,3})$，其中 $n=16+t,t\in\{5,6,7,8,9,10,11,12,13,14,15,16,17,18\}$；

3）$\boldsymbol{G}_{n,3}=(\boldsymbol{G}_{21,3}\quad \boldsymbol{G}_{t,3})$，其中 $n=21+t,t\in\{14,15,16,17,18,20,21,22,23,24\}$；

4）$\boldsymbol{G}_{n,3}=(\boldsymbol{G}_{37,3}\quad \boldsymbol{G}_{t,3})$，其中 $n=37+t,t\in\{9,10,14,15,16,17,18\}$；

5）$\boldsymbol{G}_{n,3}=(\boldsymbol{G}_{42,3}\quad \boldsymbol{G}_{t,3})$，其中 $n=42+t,t\in\{6,7,8,14,15,16,17,18,20,21\}$；

6) $G_{n,3}=(G_{48,3}\quad G_{t,3})$,其中 $n=48+t,t\in\{17,18,19\}$;

7) $G_{n,3}=(G_{58,3}\quad G_{t,3})$,其中 $n=58+t,t\in\{16,17,18\}$;

8) $G_{n,3}=(G_{63,3}\quad G_{t,3})$,其中 $n=63+t,t\in\{6,7,8,9,10,14,15,16,17,18,20,21,22,23,24,32,33,34,40,42,46,48,49,53,54,56,58,61,62,63\}$;

9) $G_{n,3}=(G_{64,3}\quad G_{t,3})$,其中 $n=64+t,t\in\{40,42,43,44,46,49,50,51,54,56,58,59,64\}$;

10) $G_{n,3}=(G_{84,3}\quad G_{t,3})$,其中 $n=84+t,t\in\{6,7,8,14,15,16,17,18\}$

除了以上的构造类型外,还有几种特殊的构造形式,如:

$$G_{20,3}=(G_{14,3}\quad G_{6,3}),G_{27,3}=(G_{22,3}\quad G_{5,3}),G_{64,3}=(G_{32,3}\quad G_{32,3}),G_{88,3}=(G_{72,3}\quad G_{16,3})$$

$$G_{89,3}=(G_{72,3}\quad G_{17,3}),G_{93,3}=(G_{77,3}\quad G_{16,3}),G_{94,3}=(G_{77,3}\quad G_{17,3}),G_{127,3}=(G_{84,3}\quad G_{21,3}\quad G_{22,3})$$

4 结束语

低维最优自正交$[n,k,d]$码的码长n、维数k和极小距离d之间存在的这些规律,通过定理和列表详细的表述出来,并构造出生成矩阵。尽管如此,其中个别几个最优自正交码的构造还没能解决,例如 ,$G_{40,3}$,$G_{61,3}$,$G_{62,3}$,$G_{82,3}$。当维数增加时,码长n、维数k和极小距离d之间的规律性就会变得更为复杂(见文献[3]、[6]),如何将本文的构造方法推广到一般情形,还有待于进一步讨论。

参考文献:

[1] Rains E M, Sloane N J A. Self - dual codes. In Handbook of Coding Theory [M]. Netherlands: Elsevier, 1998.

[2] Calderbank A R, Rains E M. Quantun Error Correction Via Codes Over GF(4) [J]. IEEE Trans. Inf. Theory, 1998,44:1369 - 1387.

[3] Brouwer A E. Bound on the Size of Linear Codes. In Handbook of Coding Theory [M]. Netherlands: Elsevier, 1998.

[4] Hamada N. The Nonexistence of Some Quaternary Linear Codes Meeting the Griesmer Bound and the Bound for N4(5,d) [J]. Math. Japon. 1996,43:7 - 21.

[5] 李瑞虎. 加性量子纠错码研究[D]. 西安:西北工业大学,2004.

[6] Bhandari M C, Garg M S. Optimal Codes of Dimension 3 and 4[J]. IEEE Trans. Inf. Theory, 1992, 38:1564 - 1567.

(编辑:田新华)

Optimal Quaternary Self - Orthogonal Codes of Dimensions Two and Three

MA Yue -ha, ZHAO Xue -jun, FENG You -qian

(Science Institute, Air Force Engineering University, Xi'an, Shaanxi 710051, China)

Abstract: The optimal or near optimal quaternary serf - orthogonal codes of dimensions 2 and 3 are investigated in this paper, and the relations between the optimal self - orthogonal code length, dimension and the minimum distance are found. By means of constructing the generator matrices of such optimal or near optimal self - orthogonal codes, the optimal codes of dimensions 2 and 3 that achieve the Griesmer bound are determined. Especially, the weight polynomial of the optimal or near optimal quaternary serf - orthogonal codes of dimensions 2 is obtained.

Key words: self - orthogonal code; Griesmer bound ; optimal code