基于四元域上自正交码的4维最优码的构造

李益群,赵学军,李瑞虎,王 雷
LI Yi-qun,ZHAO Xue-jun,LI Rui-hu,WANG Lei

空军工程大学 理学院 数理系,西安 710051
Air Force Engineering University,Xi'an 710051,China

LI Yi-qun,ZHAO Xue-jun,LI Rui-hu,et al.Construction of optimal codes for 4 dimensions based on quaternary self-orthogonal code.Computer Engineering and Applications,2008,44(28):51-52.

Abstract: The relations between length and minimum distance of 4 dimensions optimal or near optimal quaternary self-orthogonal codes are investigated,the generator matrices of such random optimal or near optimal self-orthogonal codes are constructed by combinatorial method.Especially,the optimal self-orthogonal codes that achieve the Griesmer bound are determined.
Key words: self-orthogonal code;Griesmer bound;optimal code;near optimal code

摘 要: 研究了 F_4 上维数为4的最优(或拟最优)自正交码的码长与极小距离之间的关系,用组合方法构造出任意码长的最优(或拟最优)自正交码的生成矩阵,确定了其中达到Griesmer界的码。
关键词: 自正交码;Griesmer界;最优码;拟最优码
DOI: 10.3778/j.issn.1002-8331.2008.28.017 **文章编号:** 1002-8331(2008)28-0051-02 **文献标识码:** A **中图分类号:** O157.4;TN919.3

自正交码是经典代数编码理论中一类非常重要的码,随着年的量子纠错理论的诞生,F_4 上一般自正交码的研究成为纠错码研究的热点和前沿问题[1-4],而最优码的特征和构造又是编码研究的中心问题。文献[2,5]刻划出了自正交码的特征,并进一步构造出一些具有给定特征的$[n,k,d]$自正交码,文献[6]给出了 F_4 上 $n\leqslant 29,k\leqslant 6$ 的最优自正交码的分类,文献[7]研究了 F_4 上任意码长的3维最优与拟最优自正交码的构造。

本文将进一步研究 F_4 上维数为4的最优自正交码的构造。

1 预备知识

设 $F_4=\{0,1,\omega,\varpi\}$ 是四元有限域,其中 $\varpi=\omega^2=\omega+1,\varpi^3=\omega^3=1$。$\forall x\in F_4,\bar{x}=x^2$ 称为 x 的共轭元。$F_4^n=\{\boldsymbol{X}=(x_1,x_2,\cdots,x_n)|x_i\in F_4\}$ 称为 F_4 上的 n 维线性空间,F_4^n 的 k 维子空间 C 称为码长为 n 的 k 维四元$[n,k]$线性码;如果 C 的Hamming距离为 d,则简记为 $C=[n,k,d]$。F_4^n 上的向量 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的Hermite内积为:$(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{X}\bar{\boldsymbol{Y}}^{\mathrm{T}}=x_1\bar{y}_1+x_2\bar{y}_2+\cdots+x_n\bar{y}_n$,若$(\boldsymbol{X},\boldsymbol{Y})=0$,则称 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ Hermite正交。

若 C 是一个四元$[n,k]$线性码,C 的Hermite对偶码记为 $C^{\perp}=\{\boldsymbol{X}|(\boldsymbol{X},\boldsymbol{Y})=0,\forall\boldsymbol{Y}\in C\}$。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 设自正交码 $C=[n,k,d]$,如果不存在 $C'=[n,k,d+2]$,则称 C 是最优的;如果不存在 $C'=[n,k,d+4]$,则称 C 是拟最优的。

引理1[5](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:$n\geqslant\sum_{i=0}^{k-1}\lceil d/q^{i-1}\rceil$。

引理2[5] 如果有自正交码$[n_1,k,d_1]$和$[n_2,k,d_2]$,通过并置它们生成矩阵,可构造出新的自正交码$[n_1+n_2,k,d_1+d_2]$。

符号约定:为下文书写方便,将 ω 记为2、ϖ 记为3。用$[n,k,d]$表示 F_4 上的码,$\boldsymbol{G}_{n,k}$ 表示码长为 n、维数为 k 的自正交码 $C_{n,k}$ 的生成矩阵。$\widetilde{\boldsymbol{G}}_{n,4}$ 表示对 $\boldsymbol{G}_{n,3}$ 再添加一行全0向量而形成的 $4\times n$ 阶矩阵(其中 $\boldsymbol{G}_{n,3}$ 取自文献[7]),$\overline{\boldsymbol{G}}_{n,4}$ 表示对 $\boldsymbol{G}_{n,4}$ 做线性变换,将其最后一行改为具有最大重量的码字,$\hat{\boldsymbol{G}}_{n,4}$ 表示从系统码的生成矩阵 $\boldsymbol{G}_{n,4}$ 中删除第一列。

2 4维最优自正交码的特征与构造

下面将码长 n 分成以下85种情况:$n=85m+i,i=0,1,\cdots,84,m\geqslant 0$,来研究 F_4 上的线性$[n,k,d]$码和自正交$[n,k,d]$码 C 的极小距离的最大值。这里 $d_{\max}$ 表示自正交$[n,k,d]$码 C 的极小距离可能达到的最大值,dg 表示由Grismer界确定的线性$[n,k,d]$码 C 的极小距离最大值。根据引理1,可得表1。

根据码长的分类,可以构造出码长为 n,维数 $k=4$ 时最优(或拟最优)自正交码的生成矩阵。

以码长 $n\leqslant 85$ 的码的生成矩阵为模块,组合出新的生成矩阵,从而构造出任意码长的最优(或拟最优)自正交码。即有下面的定理:

定理1 当 $n=85m+i,i=31,33,36,39,44,52,54,57,59$ 时,则存在拟最优自正交码 $C=[n,4,dg(n,4)-2]$。

证明 当自正交码 $C=[n,4,d]$ 的码长 $86\leqslant n\leqslant 170$ 时,根据引理2,可以组合出如下码长的自正交码的生成矩阵:

(1)$\boldsymbol{G}_{n,4}=(\boldsymbol{G}_{85,4}\ \boldsymbol{G}_{i,4})$,$n=85m+i,i=31,33,36,39,44,52,54,$

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60573040);空军工程大学理学院科研基金。
作者简介: 李益群(1972-),女,讲师,研究方向:代数编码及密码。
收稿日期: 2007-11-14 **修回日期:** 2008-02-03

表 1 码长为 n 的 4 维自正交码的距离上限

n	dso	dg	n	dso	dg	n	dso	dg	n	dso	dg
85m+1	64m	64m	85m+22	64m+14	64m+16	85m+43	64m+32	64m+32	85m+64	64m+48	64m+48
85m+2	64m	64m	85m+23	64m+16	64m+16	85m+44	64m+32	64m+32	85m+65	64m+48	64m+48
85m+3	64m	64m	85m+24	64m+16	64m+16	85m+45	64m+32	64m+32	85m+66	64m+48	64m+48
85m+4	64m	64m+1	85m+25	64m+16	64m+17	85m+46	64m+32	64m+33	85m+67	64m+48	64m+49
85m+5	64m+2	64m+2	85m+26	64m+18	64m+18	85m+47	64m+34	64m+34	85m+68	64m+50	64m+50
85m+6	64m+2	64m3	85m+27	64m+18	64m+19	85m+48	64m+34	64m+35	85m+69	64m+50	64m+51
85m+7	64m+4	64m4	85m+28	64m+20	64m+20	85m+49	64m+36	64m+36	85m+70	64m+52	64m+52
85m+8	64m+4	64m+4	85m+29	64m+20	64m+20	85m+50	64m+36	64m+36	85m+71	64m+52	64m+52
85m+9	64m+4	64m+5	85m+30	64m+20	64m+21	85m+51	64m+36	64m+37	85m+72	64m+52	64m+53
85m+10	64m+6	64m+6	85m+31	64m+22	64m+22	85m+52	64m+36	64m+38	85m+73	64m+54	64m+54
85m+11	64m+6	64m+7	85m+32	64m+22	64m+23	85m+53	64m+38	64m+39	85m+74	64m+54	64m+55
85m+12	64m+8	64m+8	85m+33	64m+24	64m+24	85m+54	64m+38	64m+40	85m+75	64m+56	64m+56
85m+13	64m+8	64m+8	85m+34	64m+24	64m+24	85m+55	64m+40	64m+41	85m+76	64m+56	64m+56
85m+14	64m+8	64m+9	85m+35	64m+24	64m+25	85m+56	64m+40	64m+41	85m+77	64m+56	64m+57
85m+15	64m+10	64m+10	85m+36	64m+24	64m+26	85m+57	64m+40	64m+42	85m+78	64m+58	64m+58
85m+16	64m+10	64m+11	85m+37	64m+26	64m+27	85m+58	64m+42	64m+43	85m+79	64m+58	64m+59
85m+17	64m+10	64m+12	85m+38	64m+28	64m+28	85m+59	64m+42	64m+44	85m+80	64m+60	64m+60
85m+18	64m+12	64m+12	85m+39	64m+28	64m+28	85m+60	64m+44	64m+44	85m+81	64m+60	64m+60
85m+19	64m+12	64m+13	85m+40	64m+28	64m+29	85m+61	64m+44	64m+45	85m+82	64m+60	64m+61
85m+20	64m+12	64m+14	85m+41	64m+30	64m+30	85m+62	64m+46	64m+46	85m+83	64m+62	64m+62
85m+21	64m+12	64m+15	85m+42	64m+30	64m+31	85m+63	64m+46	64m+47	85m+84	64m+62	64m+63

57,59,对应码的极小距离分别为:$d(116,4)=84$,$d(118,4)=86$,$d(121,4)=88$,$d(137,4)=100$,$d(139,4)=102$,$d(142,4)=104$,$d(144,4)=106$。

利用上面的结论,自正交码 $C=[n,4,d]$的码长 $n\geqslant 170$ 时,设 $n=85m+s$,$m\geqslant 2$,$s=31,33,36,39,44,52,54,57,59$ 时,可以构造出:$\boldsymbol{G}_{n,4}=\left(\underbrace{\boldsymbol{G}_{85,4}\ \boldsymbol{G}_{85,4}\ \cdots\ \boldsymbol{G}_{85,4}}_{m-1}\quad \boldsymbol{G}_{k,4}\right)$,其中 $k=85+s$。$\boldsymbol{G}_{n,4}$ 所生成码的极小距离 $d=64(m-1)+d_{t,4}$,$d_{t,4}$ 是自正交码$<\boldsymbol{G}_{t,4}>$的极小距离的最大值。

综上所述,定理成立。

定理 2 当 $n=85m+t$,$1\leqslant t\leqslant 84$ 且 $t\neq 31,33,36,39,44,52,54,57,59$ 时,存在最优自正交码 $C=[n,4,d_{so}(n,4)]$,且 $n=85m+k$,$k=0,10,12,15,17,20,22,26,28,41,43,47,49,62,64,68,70,73,75,78,80,83$ 时,最优的码 $C=[n,4,d_{so}(n,4)]$达到 Griesmer 界。

证明 当自正交码 $C=[n,4,d]$的码长 $86\leqslant n\leqslant 170$ 时,根据引理 2,可以组合出如下码长的自正交码的生成矩阵:

(1)$\boldsymbol{G}_{n,4}=(\boldsymbol{G}_{85,4}\ \boldsymbol{G}_{t,4})$,其中 $t\neq 10,12,15,26,31,33,36,38,39,44,45,47,49,50,52,53,54,55,57,59,60,61,62,63,65,75,83$,对应码的极小距离见表 1。

(2)$\boldsymbol{G}_{n,4}=(\boldsymbol{G}_{64,4}\ \boldsymbol{G}_{t,4})$,其中 $n=64+t$,$t=24,25,64,65$,对应码的极小距离见表 1。

(3)$\boldsymbol{G}_{n,4}=(\boldsymbol{G}_{64,4}\ \widetilde{\boldsymbol{G}}_{t,4})$,其中 $n=64+t$,$t=22,23$,对应码的极小距离见表 1。

(4)$\boldsymbol{G}_{n,4}=(\boldsymbol{G}_{128,4}\ \widetilde{\boldsymbol{G}}_{t,4})$,其中 $n=128+t$,$t=6,7,10,12,17,18,20,22$,对应码的极小距离见表 1。

(5)$\boldsymbol{G}_{n,4}=(\boldsymbol{G}_{64,4}\ \overline{\boldsymbol{G}}_{17,4}\ \widetilde{\boldsymbol{G}}_{t,4})$,其中 $n=81+t$,$t=9,10,14,16$,对应码的极小距离见表 1。$\boldsymbol{G}_{122,4}=(\boldsymbol{G}_{64,4}\ \overline{\boldsymbol{G}}_{42,4}\ \widetilde{\boldsymbol{G}}_{16,4})$,$\boldsymbol{G}_{130,4}=(\boldsymbol{G}_{64,4}\ \boldsymbol{G}_{34,4}\ \widetilde{\boldsymbol{G}}_{32,4})$对应码的极小距离见表 1。

(6)$\boldsymbol{G}_{n,4}=(\hat{\boldsymbol{G}}_{85,4}\ \hat{\boldsymbol{G}}_{t,4})$,其中 $n=85+t-2$,$t=17,28,41,64,85$,对应码的极小距离见表 1。

(7)$\boldsymbol{G}_{132,4}=(\hat{\boldsymbol{G}}_{64,4}\ \hat{\boldsymbol{G}}_{64,4}\ \widetilde{\boldsymbol{G}}_{6,4})$,对应码的极小距离见表 1。

(8)$\boldsymbol{G}_{160,4}=(\boldsymbol{G}_{80,4}\ \boldsymbol{G}_{80,4})$,对应码的极小距离见表 1。

(9)$\boldsymbol{G}_{92,4}=(\overline{\boldsymbol{G}}_{86,4}\ \widetilde{\boldsymbol{G}}_{6,4})$,对应码的极小距离见表 1。

当自正交码 $C=[n,4,d]$的码长 $n\geqslant 170$ 时,设 $n=85m+s$,$m\geqslant 2$,$1\leqslant s\leqslant 84$,利用(1)~(7)的结论,可以构造出:

$\boldsymbol{G}_{n,4}=\left(\underbrace{\boldsymbol{G}_{85,4}\ \boldsymbol{G}_{85,4}\ \cdots\ \boldsymbol{G}_{85,4}}_{m-1}\quad \boldsymbol{G}_{k,4}\right)$,其中 $t=85+s$。

综上所述,定理成立。

3 结束语

本文用组合方法构造了码长为 n、维数为 4 的最优(或拟最优)自正交码的生成矩阵,并确定出其中达到 Griesmer 界的码,总结出码长 n 和极小距离 d 之间存在的规律。但是,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[4-5]),这还有待于进一步讨论。

参考文献:

[1] Calderbank A R,Rains E M.Quantum error correction via codes over GF(4)[J].IEEE Trans Inf Theory,1998,44:1369-1387.

[2] 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.

[3] 李瑞虎.加性量子纠错码研究[D].西安:西北工业大学,2004.

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

[5] Pless V S,Huffman W C.Handbook of coding theory [M].Amsterdam.The Netherlands:Elsevier,1998:179-294,295-432.

[6] Bouklieve Iliya,Ötergard Patric R J.Classification of self-orthogonal codes over F_3 and F_4[J].Society for Industrial and Applied Mathematics,2005,19(2):363-370.

[7] 李益群,刘三阳,王雷.F_4 上的 3 维最优自正交码[J].西北大学学报,2006,36(6):871-874.