第 9 卷第 5 期 空 军 工 程 大 学 学 报(自然科学版) Vol. 9 No. 5
2008 年 10 月 JOURNAL OF AIR FORCE ENGINEERING UNIVERSITY (NATURAL SCIENCE EDITION) Oct. 2008

二元最优自正交[15s + 10,4]码的分类

赵学军[1,2]，雷英杰[1]，冯有前[2]，郭罗斌[2]

(1. 空军工程大学 导弹学院，陕西 三原 713800;2. 空军工程大学 理学院，陕西 西安 710051)

摘 要:自正交码是一类重要的纠错码,其中的特殊类型——自对偶码一直是研究的重点。研究二元域码长为 $n=15s+10(s\geqslant 0)$ 的四维最优自正交码的特征,并且确定其完整分类。建立了最优[15s+10,4]自正交码的生成矩阵与两个线性方程组之间的联系,将确定最优[15s+10,4]自正交码的问题转化为求解线性方程组的问题。确定出所有最优[15s+10,4]自正交码的生成矩阵,并进一步得到互不等价的最优自正交码的完整分类,给出了互不等价且不含全零坐标的最优[15s+10,4]自正交码的生成矩阵和重量多项式。因此,二元域上最优[15s+10,4]自正交码的参数、结构特征和等价问题得到了完全解决。

关键词:二元线性码;自正交码;最优码

中图分类号: O157.4 **文献标识码**:A **文章编号**:1009-3516(2008)05-0091-04

自正交码是一类重要的纠错码,[1]其中的特殊类型——自对偶码一直为人们研究的重点。Pless 于 1972 年发表的论文[2]是这方面的奠基论文。自文献[1]发表后,有众多文章研究自对偶码,见文献[3-4]的评述及其后面的 300 多篇参考文献。

自对偶码是码率为 1/2 的自正交码,以往人们很少研究码率 <1/2 的自正交码。近年来,人们开始研究一般的码率 <1/2 的最优自正交[n,k]码,再使用这些最优[n,k]自正交码去研究自对偶码及新的自正交码[5-7]。在文献[8]中 Bouykliev 等人研究了码长小于 29、维数小于 7 的三元和四元最优自正交码的分类。在文献[9]中 Bouykliev 等人研究了码长小于 41、维数小于 16 的二元最优自正交码的分类。本文在文献[10]的基础上,讨论了二元最优自正交 [15s+10,4]码的分类。

1 二元自正交码和线性方程组

设 F_2^n 是在二元域 F_2 上的 n 维行向量空间,二元线性 $[n,k]$ 码 C 是 F_2^n 上的一个 k 维子空间。C 的对偶码 $C^\perp$ 定义为:$C^\perp=\{x\in F_2^n \mid x\cdot y=xy^{\mathrm{T}}=0,\forall y\in C\}$。若 $C\subseteq C^\perp$,则 C 是自正交码,若 $C=C^\perp$,则 C 是自对偶码。如果一个 $[n,k]$ 自正交码的重量是所有 $[n,k]$ 自正交码中最大的,则该自正交码被称为最优的。如果二元码 C' 可以由 C 通过初等行变换和列置换获得,则称这两个二元码 C 和 C' 等价。如果两个矩阵 G_1 和 G_2 生成等价的码,记为 $G_1\cong G_2$。我们用 $N_1(n,k)$ 表示不包含零分量的不等价的最优 $[n,k]$ 自正交码的个数。关于编码的基本概念见文献[11-13]。

用 $\boldsymbol{I}_n=(1,1,\cdots,1)_{1\times n}$ 和 $\boldsymbol{O}_n=(0,0,\cdots,0)_{0\times n}$ 分别表示长度为 n 的全 1 向量和全 0 向量。G_{15} 表示[15,4,8] 单形码的生成矩阵,矩阵 $G=(G_1,G_2)$ 表示由 G_1 和 G_2 的并置得到的矩阵。

我们采用线性方程组来刻画最优[n,4]自正交码。设 G 为码 C 的生成矩阵

$$G=\begin{pmatrix} I_{2m} & O_{n-2m} \\ X & Y \end{pmatrix} \tag{1}$$

收稿日期:2007-07-13
基金项目:国家自然科学基金资助项目(60573040)
作者简介:赵学军(1972-),男,四川三台人,讲师,博士生,主要从事代数编码与密码,信号与信息处理研究;
E-mail:zlycczlycc@163.com
雷英杰(1956-),男,陕西渭南人,教授,博士生导师,主要从事智能信息处理、信息融合、智能决策等研究.

引理 1 设参数为$[n,k+1,2m]$的自正交码C的生成矩阵为G(G的形式如式(1)所示),由$(X\quad Y)$、X和Y生成的码分别记为C_0,C_1和C_2。则C_0是$[n,k]$自正交码,C_1和C_2是偶码,且$d(C_1)\leqslant d(C_2)$,$d(C_2)\geqslant 2\lceil \frac{m}{2}\rceil$。

令$\boldsymbol{\alpha}_i(0\leqslant i\leqslant 7)$为二元列向量,其中$\boldsymbol{\alpha}_0=(0,0,0)^{\mathrm{T}},\boldsymbol{\alpha}_1=(0,0,1)^{\mathrm{T}},\cdots,\boldsymbol{\alpha}_7=(1,1,1)^{\mathrm{T}}$。设$M$为$3\times n$的矩阵,如果$M$的列中有$l_i$个$\boldsymbol{\alpha}_i(0\leqslant i\leqslant 7)$,$M$简记为$M=(l_0\boldsymbol{\alpha}_0,l_1\boldsymbol{\alpha}_1,\cdots,l_7\boldsymbol{\alpha}_7)$,由$M$生成的码记为$C_M$,向量$L_M=(l_1,l_2,\cdots,l_7)$叫做$M$的定义向量。由文献[9],$M$的重量向量$W_M=(m_1,m_2,\cdots,m_7)$满足$m_1+m_2+\cdots+m_7=4(l_1+l_2+\cdots+l_7)$和$W_M^{\mathrm{T}}=DL_M^{\mathrm{T}}$,其中$D$和$D^{-1}$为有理数域上的如下可逆矩阵。

$$D=\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\0&1&1&1&1&0&1\\1&0&1&0&1&0&1\\1&0&1&1&0&1&0\\1&1&0&0&1&1&0\\1&1&0&1&0&0&1\end{pmatrix}$$

$$D^{-1}=\frac{1}{4}\begin{pmatrix}-1&-1&-1&1&1&1&1\\-1&1&1&-1&-1&1&1\\-1&1&1&1&1&-1&-1\\1&-1&1&1&-1&1&-1\\1&1&-1&-1&1&1&-1\\1&1&-1&1&-1&-1&1\\1&-1&1&-1&1&-1&1\end{pmatrix}$$

设最优自正交码$C=[n,4,2m]$,G为C的生成矩阵,其中G,X,Y,C_0,C_1,C_2如引理1所示,设$X=(r_1\alpha_1,r_2\alpha_2,\cdots,r_7\alpha_7)$,$Y=(l_0\alpha_0,l_1\alpha_1,\cdots,l_7\alpha_7)$,$X$的重量向量为$W_X=(x_1,x_2,\cdots,x_7)$,$Y$的重量向量为$W_Y=(y_1,y_2,\cdots,y_7)$,并且$W_X^{\mathrm{T}}=DL_X^{\mathrm{T}}$和$W_Y^{\mathrm{T}}=DL_Y^{\mathrm{T}}$。将确定$G$的问题转化为确定$X$和$Y$。依据引理1,可建立如下线性方程组:

$$\begin{cases}L_X^{\mathrm{T}}=D^{-1}W_X^{\mathrm{T}},\\x_i\equiv 0(\mathrm{mod}2),\quad 1\leqslant i\leqslant 7,\\2\lceil \frac{m}{2}\rceil\leqslant y_i\leqslant n-2m,\\x_1+x_2,\cdots+x_7=4(n-2m),\\r_1\geqslant r_2\geqslant r_i,3\leqslant i\leqslant 7,r_4\geqslant r_j,\quad j=5,6,7\end{cases}\tag{2}$$

$$\begin{cases}L_X^{\mathrm{T}}=D^{-1}W_X^{\mathrm{T}},\\y_i\equiv 0(\mathrm{mod}2),\\x_i+y_i\geqslant 2m,\quad 1\leqslant i\leqslant 7\\y_i-x_i\geqslant 0,\quad 1\leqslant i\leqslant 7\\r_i+l_i\equiv r_j+l_j(\mathrm{mod}2),\quad 1\leqslant i,j\leqslant 7\\l_0=2m-(l_1+l_2\cdots+l_7)\end{cases}\tag{3}$$

由式(2)不难得到X的所有非负整数解,由式(3)可得到Y的所有非负整数解,由此可得所有的最优$[n,4,2m]$自正交码。

2 最优自正交$[15s+10,4]$码的分类

设最优自正交码$C=[15s+10,4,d]$,由 Griesmer 界知,$d=8s+4$。其中C的生成矩阵如式(1)所示。根据引理1和Griesmer界可知,$d(C_2)=4s+2$。由于$4(7s+6)=7\times(4s+2)+10$,因此C_2的重量向量W_Y

$=(4s+2+2\lambda_1,4s+2+2\lambda_2,\cdots,4s+2+2\lambda_7)$,其中 $\lambda_1+\lambda_2+\cdots+\lambda_7=5(\lambda_i\geqslant 0)$,同理, $\boldsymbol{W}_X=(4s+2+2\mu_1,4s+2+2\mu_2,\cdots,4s+2+2\mu_7)$,其中 $-\lambda_i\leqslant\mu_i\leqslant\lambda_i,i=1,2,\cdots,7$。这里先确定出所有[15s+10,4]的生成矩阵,再给出分类,结果如下:

定理 1 设 $n=15s+10,s\geqslant 0$,则有

1)如果 $s=0$,则 $N_1(10,4)=3$,这 3 个没有全零坐标分量的不等价的最优自正交[10,4,4] 码有生成矩阵 $\boldsymbol{G}_{10,1},\boldsymbol{G}_{10,2},\boldsymbol{G}_{10,3}$,其中 $\boldsymbol{G}_{10,i}(1\leqslant i\leqslant 3)$为

$$G_{10,i}=\begin{pmatrix}\boldsymbol{I}_4 & \boldsymbol{O}_6\\ X_i & Y_i\end{pmatrix},\quad (1\leqslant i\leqslant 3) \tag{4}$$

式中: $\boldsymbol{X}_1=(\alpha_0,\alpha_3,\alpha_5,\alpha_6)$; $\boldsymbol{Y}_1=(3\alpha_1,\alpha_2,\alpha_4,\alpha_7)$; $\boldsymbol{X}_2=(2\alpha_0,2\alpha_7)$; $\boldsymbol{Y}_2=(2\alpha_1,2\alpha_2,4)$; $\boldsymbol{X}_3=(\alpha_0,\alpha_1,\alpha_6,\alpha_7)$; $\boldsymbol{Y}_3=(2\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)$;他们的重量多项式 $W_{10,i}$分别为: $W_{10,1}=1+7y^4+7y^6+y^{10}$; $W_{10,2}=1+10y^4+5y^8$; $W_{10,3}=1+6y^4+8y^6+y^8$。

2)如果 $s=1$,则 $N_1(25,4)=6$,这 6 个没有全零坐标分量的不等价的最优自正交[25,4,12] 码有生成矩阵 $\boldsymbol{G}_{25,1},\boldsymbol{G}_{25,2},\cdots,\boldsymbol{G}_{25,6}$,其中 $\boldsymbol{G}_{25,j}(1\leqslant j\leqslant 6)$为

$$\boldsymbol{G}_{25,j}=(\boldsymbol{G}_{15},\boldsymbol{G}_{10,j}),\quad (1\leqslant j\leqslant 3)\ ,\boldsymbol{G}_{25,j}=\begin{pmatrix}\boldsymbol{I}_{12} & \boldsymbol{O}_{13}\\ \boldsymbol{U}_j & \boldsymbol{V}_i\end{pmatrix},\quad (4\leqslant j\leqslant 6) \tag{5}$$

式中: $\boldsymbol{U}_4=(3\alpha_0,\alpha_2,2\alpha_3,\alpha_4,2\alpha_5,\alpha_6,2\alpha_7)$; $\boldsymbol{V}_4=(4\alpha_1,3\alpha_2,3\alpha_4,\alpha_6,2\alpha_7)$; $\boldsymbol{U}_5=(2\alpha_0,\alpha_1,2\alpha_2,\alpha_3,\alpha_4,2\alpha_5,\alpha_6,2\alpha_7)$; $\boldsymbol{V}_5=(4\alpha_1,3\alpha_2,2\alpha_4,\alpha_5,2\alpha_6,\alpha_7)$; $\boldsymbol{U}_6=(2\alpha_0,2\alpha_1,2\alpha_2,2\alpha_5,2\alpha_6,2\alpha_7)$; $\boldsymbol{V}_6=(3\alpha_1,3\alpha_2,\alpha_3,2\alpha_4,\alpha_5,\alpha_6,\alpha_7)$。重量多项式 $W_{25,j}$分别为: $W_{25,1}=1+7y^{12}+7y^{14}+y^{18}$; $W_{25,2}=1+10y^{12}+5y^{16}$; $W_{25,3}=1+6y^{12}+8y^{14}+y^{16}$; $W_{25,4}=1+11y^{12}+3y^{16}+y^{20}$; $W_{25,5}=1+10y^{12}+5y^{16}$; $W_{25,6}=1+10y^{12}+5y^{16}$。

3)如果 $s\geqslant 2$,则 $N_1(n,4)=17$,这 17 个没有全零坐标分量的不等价的最优自正交[n,4,8s]码有生成矩阵 $\boldsymbol{G}_{n,k}$如下所示:

$$\boldsymbol{G}_{n,k}=((s-1)\boldsymbol{G}_{15},\boldsymbol{G}_{25,k}),\quad (1\leqslant k\leqslant 6),\boldsymbol{G}_{n,k}=((s-2)\boldsymbol{G}_{15},\boldsymbol{G}_{40,k}),\quad (7\leqslant k\leqslant 17) \tag{6}$$

式中: $\boldsymbol{G}_{40,k}=\begin{pmatrix}1_{20} & 0_{20}\\ \boldsymbol{P}_k & \boldsymbol{Q}_k\end{pmatrix},(7\leqslant k\leqslant 17)$; $\boldsymbol{P}_7=(5\alpha_0,5\alpha_3,5\alpha_5,5\alpha_6)$; $\boldsymbol{Q}_7=(5\alpha_1,5\alpha_2,5\alpha_3,5\alpha_7)$; $\boldsymbol{P}_8=(4\alpha_0,\alpha_1,\alpha_2,4\alpha_3,4\alpha_4,4\alpha_5,4\alpha_6,4\alpha_7)$; $\boldsymbol{Q}_8=(5\alpha_1,5\alpha_2,5\alpha_4,5\alpha_7)$; $\boldsymbol{P}_9=(3\alpha_0,2\alpha_1,2\alpha_2,3\alpha_3,2\alpha_4,3\alpha_5,3\alpha_6,2\alpha_7)$; $\boldsymbol{Q}_9=(5\alpha_1,5\alpha_2,5\alpha_4,5\alpha_7)$; $\boldsymbol{P}_{10}=(4\alpha_0,2\alpha_1,2\alpha_2,4\alpha_3,2\alpha_4,3\alpha_5,3\alpha_6,2\alpha_7)$; $\boldsymbol{Q}_{10}=(5\alpha_1,5\alpha_2,4\alpha_4,\alpha_5,\alpha_6,5\alpha_7)$; $\boldsymbol{P}_{11}=(3\alpha_0,2\alpha_1,2\alpha_2,3\alpha_3,3\alpha_4,3\alpha_5,3\alpha_6,2\alpha_7)$; $\boldsymbol{Q}_{11}=(5\alpha_1,5\alpha_2,4\alpha_4,\alpha_5,\alpha_6,4\alpha_7)$; $\boldsymbol{P}_{12}=(3\alpha_0,2\alpha_1,2\alpha_2,3\alpha_3,3\alpha_4,3\alpha_5,3\alpha_6,2\alpha_7)$; $\boldsymbol{Q}_{12}=(5\alpha_1,5\alpha_2,3\alpha_4,2\alpha_5,2\alpha_6,3\alpha_7)$; $\boldsymbol{P}_{13}=(4\alpha_0,2\alpha_1,2\alpha_2,4\alpha_3,4\alpha_4,4\alpha_5,2\alpha_7)$; $\boldsymbol{Q}_{13}=(4\alpha_1,4\alpha_2,2\alpha_3,4\alpha_4,2\alpha_5,2\alpha_6,2\alpha_7)$; $\boldsymbol{P}_{14}=(3\alpha_0,3\alpha_1,3\alpha_2,\alpha_3,4\alpha_5,4\alpha_6,2\alpha_7)$; $\boldsymbol{Q}_{14}=(4\alpha_1,4\alpha_2,2\alpha_3,3\alpha_4,3\alpha_5,3\alpha_6,\alpha_7)$; $\boldsymbol{P}_{15}=(2\alpha_0,4\alpha_1,4\alpha_2,4\alpha_4,2\alpha_6,4\alpha_7)$; $\boldsymbol{Q}_{15}=(4\alpha_1,4\alpha_2,2\alpha_3,3\alpha_4,2\alpha_5,4\alpha_7)$; $\boldsymbol{P}_{16}=(3\alpha_0,3\alpha_1,4\alpha_2,2\alpha_4,2\alpha_5,3\alpha_6,3\alpha_7)$; $\boldsymbol{Q}_{16}=(4\alpha_1,3\alpha_2,3\alpha_3,3\alpha_4,3\alpha_5,2\alpha_6,2\alpha_7)$; $\boldsymbol{P}_{17}=(3\alpha_0,3\alpha_1,3\alpha_2,3\alpha_3,3\alpha_4,4\alpha_5,4\alpha_7)$; $\boldsymbol{Q}_{17}=(4\alpha_1,4\alpha_2,3\alpha_4,3\alpha_5,3\alpha_6,\alpha_7)$。

这 17 个码的重量多项式分别为: $W_{40,i}=1+y^8(W_{25,i}-1),1\leqslant i\leqslant 6$; $W_{40,7}=1+14y^{20}+y^{20}$; $W_{40,8}=1+12y^{20}+2y^{24}+y^{36}$; $W_{40,9}=1+13y^{20}+y^{28}+y^{32}$, $W_{40,10}=1+12y^{20}+2y^{24}+y^{32}$; $W_{40,11}=1+12y^{20}+y^{24}+2y^{28}$, $W_{40,12}=1+11y^{20}+3y^{24}+y^{28}$; $W_{40,13}=1+11y^{20}+3y^{24}+y^{28}$, $W_{40,14}=1+11y^{20}+3y^{24}+y^{28}$; $W_{40,15}=1+12y^{20}+2y^{24}+y^{32}$, $W_{40,16}=1+10y^{20}+5y^{24}$; $W_{40,17}=1+12y^{20}+y^{24}+2y^{28}$。

注:当 $s=0,1$ 时,相应的[15s+10,4] 自正交码为[10,4]和[25,4] ,我们关于[10,4]和[25,4]在第 2 节中的分类结果与文献[8]中的一致。

3 结束语

本文建立了最优自正交码的生成矩阵与线性方程组之间的关系,将确定最优自正交码问题转化为求解两个整系数方程组的整数解,从而确定出所有二元最优[15s+10,4]自正交码的生成矩阵。再由最优自正交码的生成矩阵给出互不等价的最优 [15s+10,4]自正交码的分类,完整的解决了这种码长的最优自正交码的距离、结构特征和等价问题。

参考文献:

[1] 赵全习,郭罗斌,赵学军,等. 四维最优二元自正交码及其结构[J]. 空军工程大学学报:自然科学版,2007,8(4):72 - 74.
ZHAO Quanxi,GUO Luobin,ZHAO Xuejun,et al. Four Dimension Optimal Binary Self - orthogonal Codes and Their Construction[J]. Journal of Air Force Engineering University:Natural Science Edition ,2007,8(4):72 - 74. (in Chinese)

[2] Pless V. A Classification of Self - Orthogonal Codes over GF(2)[J]. Discrete Mathematics,1972, 3:209 - 246.

[3] Rains E M,Sloane N J A. Self - dual Codes Handbook of Coding Theory[M]. Amsterdam:Elsevier Press ,1998.

[4] Huffman W C. On the Classification and Enumeration of Self - dual Codes[J]. Finite Fields Appl. 2005,11:451 - 490.

[5] Bouyuklieva S. Some Optimal Self - Orthogonal Codes and Self - dual Codes[J]. Discrete Mathematics,2004,287:1 - 10.

[6] 李瑞虎. 加性量子纠错码研究[D]. 西安:西北工业大学,2004.
LI Ruihu. Research on Additive Guantccm Codes[D]. Xi'an:Northwestern Polytechnocial University,2004. (in Chinese)

[7] Ruihu Li, Xueliang Li. Binary Construction of Quantum Codes of Minimum Distance Five and Six[J]. Discrete Mathematics, 2008,308:1603 - 1611..

[8] Bouyukliev I,Ostergard P. Classification of Self - Orthogonal Codes Over F_3 and F_4[J]. SIAM J Discrete Mathematics, 2005, 19(2):363 - 370.

[9] Bouyukliev I,Bouyuklieva S,Gulliver T A. Classification of Optimal Binary Self - orthogonal Codes[EB/OL]. [2007 - 10 - 11]http://users. tkk. fi/ ~ pat/patric - pub. html.

[10] Li Rui hu . Rinhil Research on Quantum Codes and Self - orthogonal Codes[D]. Xi'an:Xi'an Jiaotong University,2008.

[11] Huffman W C,Pless V. Fundmentals of Error - correcting Codes[M]. Cambridge:Cambridge University Press,2003.

[12] Macwilliams F J,Sloane N J A. The Theory of Error - correcting Codes[M]. Amsterdam:North - Holland Press,1998.

[13] 王新梅,肖国镇. 纠错码:原理与方法[M]. 西安:西安电子科技大学出版,2001.
WANG Xinmei,XIAO Guozhen. Error - correcting Codes:Theory and Method[M]. Xi'an:Xidian University Press,2001. (in Chinese)

(编辑:田新华)

Classification of Binary Optimal Self - orthogonal Codes

ZHAO Xue - jun[1,2], LEI Ying - jie[1], FENG You - qian[2], GUO Luo - bin[2]
(1. Missile Institute, Air Force Engineering University,Sanyuan 713800,Shaanxi, China;2. Science Institute, Air Force Engineering University, Xi'an 710051, China)

Abstract:The complete classification of 4 - dimensional optimal self - orthogonal codes of code length is presented. The establishment of the optimal orthogonal code matrix and the formation of linear equations between the two links will determine the problem of optimal orthogonal code transforming into that of solving linear equations. Results identify all generator matrixes of the optimal orthogonal code, and further are not equivalent to the optimal orthogonal codes since the integrity of classification, and the generator matrices and weight polynomials of these 4 - dimensional optimal self - orthogonal codes are also given. Therefore, the optimal orthogonal code parameters, structural characteristics and equivalence problem have been completely solved.

Key Words:binary linear code;self - orthogonal code;optimal code