四维最优二元自正交码及其构造

赵全习[1,2]， 郭罗斌[3]， 赵学军[3]， 贺筱军[3]

(1. 空军工程大学 电讯工程学院，陕西 西安 710077；2. 空军工程大学 导弹学院，陕西 三原 713800；3. 空军工程大学 理学院，陕西 西安 710051)

摘 要：研究了四维二元自正交码的码长与距离之间的关系，证明了参数为$[15m+5,4,8m+2]$及$[15m+12,4,8m+6]$自正交码的不存在性，从而对每个$n\geqslant 8$确定了最优自正交码的极小距离，再构造出相应的最优$[n,4]$自正交码的生成阵，计算出它们的重量多项式。

关键词：二元码；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(2007)04-0072-03

自正交码是一类重要的线性码，许多重要的线性码(如Golay码)是自正交码或与自正交码有关。自正交码不仅具有很好的实用性，还与数学中许多分支密切相关。自1972年Pless给出$n\leqslant 20$的自对偶码与极大自正交码分类后[1]，人们开始研究特殊的自正交码-自对偶码的分类与计数，在过去三十多年里，自对偶码一直是人们研究的热点。但是关于一般自正交码的研究却很少，近年来由于量子纠错码研究的推动，人们开始研究非对偶的二元自正交码[2-3]，2006年Bouyukliev[4]等人开始研究一般二元自正交码的分类，他们解决了四维以下最优自正交码问题，给出码长$n\leqslant 25$的最优自正交码的分类与构造，并给出$n\leqslant 40$，$k\leqslant 10$时最优自正交码[5-8]的部分结论。

本文将研究一般码长情况下四维最优自正交码的码长与距离值的关系，并相应构造达到最优和拟最优的自正交码。

设$\boldsymbol{F}_2=\{0,1\}$为二元域，$\boldsymbol{F}_2^n$为$\boldsymbol{F}_2$上n维行线性空间，$\boldsymbol{F}_2^n$的k维子空间$\boldsymbol{C}$叫做码长为n的k维二元码，并记为$\boldsymbol{C}=[n,k]$；如果$\boldsymbol{C}$的Hamming距离为d，则简记为$\boldsymbol{C}=[n,k,d]$。

设$\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$，$\boldsymbol{Y}=(y_1,y_2,\cdots,y_n)\in\boldsymbol{F}_2^n$，$\boldsymbol{X}\cdot\boldsymbol{Y}=x_1y_1+x_2y_2+\cdots+x_ny_n=\boldsymbol{X}\boldsymbol{Y}^{\mathrm{T}}$称为$\boldsymbol{X}$与$\boldsymbol{Y}$的欧氏(Euclid)内积；若$\boldsymbol{X}\cdot\boldsymbol{Y}=0$，称$\boldsymbol{X}$与$\boldsymbol{Y}$正交。$\boldsymbol{C}^{\perp}=\{\boldsymbol{X}:\boldsymbol{X}\times\boldsymbol{Y}=0,\forall\boldsymbol{Y}\in\boldsymbol{C}\}$，称为$\boldsymbol{C}$的对偶码。若$\boldsymbol{C}\subseteq\boldsymbol{C}^{\perp}$，称$\boldsymbol{C}$为自正交码，简记为SO码。若码字的重量全部为偶数，则称为偶码。

自正交码中每个码字的重量为偶数，从而C的极小距离为偶数。如果不存在自正交码$\boldsymbol{C}=[n,k,d+2]$；一个自正交码$\boldsymbol{C}==[n,k,d]$称为最优自正交码(简称最优SO码)，如果不存在自正交码$C=[n,k,d+4]$一个自正交码$\boldsymbol{C}=[n,k,d]$称为拟最优自正交码(简称拟最优SO码)。

依据Griesmer界$n\geqslant\sum_{i=0}^{k-1}\lceil\frac{d}{2^i}\rceil$可知，当维数$k=4$时，$d=8m$时$n\geqslant 15m$，为此将码长设为$n\geqslant 15m+t$，$0\leqslant t\leqslant 14$。

依据下面的引理，利用并置(Justposition)方法，对每个n可构造出最优自正交$[n,4,d_{\mathrm{SO}}]$。

引理1[1]若$\boldsymbol{C}_1=[n_1,k,d_1]$，$\boldsymbol{C}_2=[n_2,k,d_2]$为自正交码，则存在$[n_1+n_2,k,d_1+d_2]$自正交码。

引理2[1]若$\boldsymbol{C}=[n,k,d]$码，则由并置法，可得到$[2n,k,2d]$自正交码。

收稿日期：2006-10-30
基金项目：国家自然科学基金资助项目(60573040)；空军工程大学理学院科研基金资助项目
作者简介：赵全习(1965-)，男，陕西凤翔人，副教授，博士，主要从事代数编码及密码研究.

1　不存在性定理

引理 3　设 $C=[n,k,4m+2]$ 是自正交码,若 C 有生成阵 $C=\begin{bmatrix}1_{4m+2} & 0_m\\ X & Y\end{bmatrix}$,其中 1_{4m+2} 表示 $4m+2$ 维全一向量,0_m 表示全零向量。令 $C_0=<X|Y>$,$C_1=<X>$,$C_2=<Y>$,则 C_1、C_2 是偶码,且 $d_2=d(C_2)\geqslant 2m+2$ 。

证明 若 $d_2\leqslant 2m$,取 $v\in C_2,\omega(v)=d_2$,取 $u\in C_1$ 使 $(u|v)\in C_0$

若 $\omega(u)\leqslant 2m$,则 $\omega(u|v)\leqslant 4m$,矛盾。

若 $\omega(u)\geqslant 2m+2$,则 $\omega((1_{4m+2}|0)+(u|v))=4m$,而 $(1_{4m+2}|0)+(u|v)\in C_0$,矛盾。

推论 1)设 $n=15m+5$,则不存在 $[15m+5,4,8s+2]$ 自正交码。

2) 设 $n=15m+12$,则不存在 $[15m+5,4,8s+6]$ 自正交码。

证明　设 $G_{15m+5}=\begin{bmatrix}1_{8m+2} & 0_{7m+3}\\ X & Y\end{bmatrix}$ 生成自正交码 $[15m+5,4,8s+2]$,令 $C_0=<X|Y>$,$C_1=<X>$,$C_2=<Y>$,则 $C_2=<Y>$ 是偶码,且 $d(C_2)\geqslant 4m+2$,但由 Griesmer 界可知 $(4m+2)+\lceil\frac{4m+2}{2}\rceil+\lceil\frac{4m+2}{4}\rceil>7m+3$,矛盾,故得证。

同理可证 $[15m+12,4,8s+6]$ 自正交码不存在。

2　最优自正交码的构造

当维数 $k=4$ 时,$[n,k]$ 自正交码存在当且仅当 $n\geqslant 8$ 。给定 n 值和 $k=4$,利用 Griesmer 界可求出最优自正交码的距离可能达到的最大值,用 d_{gso} 表示;d_{gso} 等于 Griesmer 界 d_g 或 d_{gso} 比 Griesmer 界 d_g 小。但由文[1]可知,对某些 n 值并不存在达到 d_{gso} 的自正交码,最优自正交码的距离值仅达到 $d_{gso}-2$,推论 1 说明 $[15m+5,4]$ 最优自正交码的距离是 $8s$,$[15m+12,4]$ 最优自正交码的距离是 $8s+4$ 。此时,最优自正交码的距离比 d_{gso} 小 2。我们用表一给出由 Griesmer 界确定的最优自正交码的距离可能值 d_{gso} 以及最优自正交码的距离实际值 d_{so}。

由[1]可知, $n=8,9,\cdots,15$ 时,四维最优自正交码的距离依次为 $d_{so}=4,4,4,\cdots,4,6,8$ 。

表 1　$k=4,m\geqslant 1$ 时 n 与 d_{gso}、d_{so} 的值

$n=15m+t$	d_{gso}	d_{so}	$n=15m+t$	d_{gso}	d_{so}
$t=0,1,2,3,4$	$8m$	$8m$	$t=8,9,10,11$	$8m+4$	$8m+4$
$t=5$	$8m+2$	$8m$	$t=12$	$8m+6$	$8m+4$
$t=6,7$	$8m+2$	$8m+2$	$t=13,14$	$8m+6$	$8m+6$

以下用 $G_{n,4,d}$ 表示自正交码 $[n,4,d]$ 的生成矩阵(有时简记为 $G_{n,4}$),以下给出了 $8\leqslant n\leqslant 29$ 时最优自正交码 $[n,4,d_{so}]$ 的部分生成阵。

$$G_{8,4,4}\begin{bmatrix}11111111\\00001111\\00110011\\01010101\end{bmatrix}\quad G_{14,4,6}\begin{bmatrix}11111111111111\\00011110001111\\01100110110011\\10101011010101\end{bmatrix}\quad G_{15,4,8}\begin{bmatrix}000000001111111\\00011110001111\\01100110110011\\10101011010101\end{bmatrix}\quad G_{21,4,10}\begin{bmatrix}111111111000000001000\\111100000111110000100\\100011100111001100010\\111011010110101010001\end{bmatrix}$$

$$G_{23,4,12}\begin{bmatrix}00000001111111111111111\\00011110000111100001111\\01100110011001100110011\\10101010101010101010101\end{bmatrix}\quad G_{28,4,14}\begin{bmatrix}00000011111111000000111111111\\00111100001111001111000011111\\11001100110011111001100110011\\01010101010101010101010101010\end{bmatrix}$$

设 $G_{sim,4}\begin{bmatrix}0&0&0&\cdots&1\\0&0&0&\cdots&1\\0&1&1&\cdots&1\\1&0&1&\cdots&1\end{bmatrix}$,$G_{sim,4}$ 生成 $[15,4,8]$ Simplex 码,Simplex 码是最优自正交码,且达到 Gries-

mer 界,它的重量多项式是 $1+15y^8$。对于 $16\leqslant n_1\leqslant 29$ 的码长 n_1,我们构造出$[n_1,4,d_{so}]$ 自正交码。若 $n\geqslant 30$ 可设码长 $n=15m+t=15(m-1)+(15+t)$,其中 $m\geqslant 2$,$0\leqslant t\leqslant 14$,则可构造$[n,4,d_{so}]$ 自正交码的生成阵 $G_n=((m-1)G_{sim,4},|G_{n_1,4})$

其中$(m-1)G_{sim,4}$表示$(m-1)$ 个 $G_{sim,4}$的并置,$G_{n_1,4}$是$[15+t,4,d_{so}(15+t)]$ 自正交码的生成阵。由文献[2]对所有 $n\geqslant 16$ 可构造出最优自正交码,即得下面的定理。

定理 1 设 $n=15m+t,m\geqslant 1$,$0\leqslant t\leqslant 14$

(1)当 $m\geqslant 1$ 时存在达到 Griesmer 界的$[15m,4,8m]$ 和$[15m+8,4,8m+4]$。

(2)$m\geqslant 2$ 时存在达到 d_{gso}的自正交码$[15m+t,4,d_{gso}]$ 的最优自正交码。

(3)$m\geqslant 2$ 时存在达到 $d_{gso}-2$ 的自正交码 $[15m+t,4,d_{gso}-2]$的最优自正交码。

文献[1]给出了 $8\leqslant n\leqslant 30$ 时最优自正交码的重量多项式$[n,4]$,我们所构造的最优自正交码的部分重量多项式是:$G_{8,4,4}$、$G_{9,4,4}$的重量多项式是 $1+14y^4+y^8$;$G_{14,4,6}$的重量多项式是 $1+7y^6+7y^8+y^{14}$;$G_{15,4,8}$的重量多项式是 $1+15y^8$;$G_{16,4,8}$、$G_{17,4,8}$的重量多项式是 $1+15y^8+y^{16}$;$G_{20,4,8}$的重量多项式是 $1+14y^{12}+y^{16}$;$G_{21,4,10}$、$G_{22,4,10}$的重量多项式是 $1+7y^{10}+7y^{12}+y^{14}$;$G_{23,4,12}$的重量多项式是 $1+14y^{12}+y^{16}$;$G_{26,4,12}$的重量多项式是 $1+7y^{12}+7y^{14}+y^{26}$;$G_{28,4,14}$、$G_{29,4,14}$的重量多项式是 $1+8y^{14}+7y^{16}$。

定理 2 当 $n=15m+t=15(m-1)+(15+t)$ 时,如$[15+t,4]$ 的重量多项式为 $1+a_1y^{n_1}+a_2y^{n_2}+\cdots+a_sy^{n_s}$,则 $1+a_1y^{n_1+8(m-1)}+a_2y^{n_1+8(m-1)}+\cdots+a_sy^{n_s+8(m-1)}$是 $<G_n>$ 的重量多项式。

参考文献:

[1] Pless V, A classification of self - orthogonal codes over GF(2)[J]. Discrete Math. 1972(3):209 - 246.

[2] 马月娜,赵学军,冯有前. 上 2 维和 3 维最优的自正交码 [J]. 空军工程大学学报:自然科学版, 2005,6(5):63 - 66.

[3] Iliya Bouklliеve Patric R. J . Classification of self - orthogonal codes over and [J]. Discrete Math, 2005,19(2):363 - 370.

[4] Bouyukliev I, Bouyuklieva S, Gulliver T,et al. Classification of Optimal Binary Self - Orthogonal Codes. [EB/OL]. Http://users. tkk. fi/ ~ pat/patric - pub - html.

[5] 李瑞虎. 用四元循环码构造的线性量子码[J]. 空军工程大学学报:自然科学版,2007,8(1):85 - 87.

[6] Stene A M. Simple Quantum Error Correcting Codes[J]. Phys. Rev,1996,7:793 - 797.

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

[8] Macwilliams F J,Sloane N J A. The Theory of Error - Correcting Codes Amsterdam[J]. The Netherlands:North - Holland,1977

(编辑:田新华,徐楠楠)

Four Dimensional Optimal Binary Self - orthogonal Codes and Their Construction

ZHAO Quan - xi[1,2], GUO Luo - bin[3], ZHAO Xue - jun[3], HE Xiao - jun[3]

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 710077, China; 2. The Missile Institute, Air Force Engineering University, Sanyuan 713800, Shaanxi, China; 3. The Science Institute, Air Force Engineering University, Xi'an 710051, China)

Abstract: The relation between the length and the minimum distance of four dimensional binary self - orthogonal codes are discussed. The nonexistence of self - orthogonal codes with parameters [$15m+5$, 4, $8m+2$] and that with parameters [$15m+12$, 4, $8m+6$] are proved, thus for each $n\geqslant 8$, the minimum distance dso of optimal [n, 4] self - orthogonal is determined. At last, for each $n\geqslant 8$ a generator matrix that generates a [n, 4, dso (n)] self - orthogonal code is presented, and their weight polynomials are determined.

Key words: binary code; self - orthogonal code; optimal code