基于二次乘法特征的射影线性码

陈辅灵[1,2],衡子灵[1],王鑫然[1],李成举[3,2]
(1. 长安大学理学院,陕西西安 710064;2. 东南大学移动通信国家重点实验室,江苏南京 210096;
3. 华东师范大学高可信计算重点实验室,上海 200062)

摘 要: 基于有限域上的二次乘法特征构造了两类线性码,精确计算出了它们的参数和重量分布. 结果表明,第一类线性码是射影三重码,且对偶码关于球填充界几乎最优;第二类线性码是射影二重码,且对偶码关于球填充界几乎最优. 此外,本文还得到了一些自正交码和极小码,它们可分别用于构造量子码和安全高效访问结构上的密钥共享方案.

关键词: 射影码;增信码;自正交码;极小码
基金项目: 国家自然科学基金(No.11901049,No.12071138);陕西省高校科协青年人才托举计划(No.20200505);东南大学移动通信国家重点实验室开放研究基金(No.2022D05);长安大学中央高校基本科研业务费专项资金(No.300102122202);上海市可信工业互联网软件协同创新中心项目
中图分类号: O236.2 **文献标识码:** A **文章编号:** 0372-2112(2023)01-0032-10
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20211633

Projective Linear Codes Based on the Quadratic Multiplicative Characters

CHEN Fu-ling[1,2], HENG Zi-ling[1], WANG Xin-ran[1], LI Cheng-ju[3,2]
(1. *School of Science*, *Chang' an University*, *Xi' an*, *Shaanxi* 710064, *China*;
2. *State Key Laboratory of Mobile Communication*, *Southeast University*, *Nanjing*, *Jiangsu* 210096, *China*;
3. *Key Laboratory of Highly Trusted Computing*, *East China Normal University*, *Shanghai* 200062, *China*)

Abstract: Two families of linear codes are constructed based on the quadratic multiplicative characters of finite fields. The parameters and weight distributions of the codes are explicitly determined. It turns out that the first family of linear codes are projective three-weight ones whose duals are almost optimal according to the sphere-packing bound. The second family of linear codes are projective two-weight ones whose duals are also almost optimal according to the sphere-packing bound. Besides, some self-orthogonal codes and minimal codes are obtained. The self-orthogonal codes can be used to construct quantum codes and minimal codes can be used to construct secret sharing schemes with safe and sufficient access structures.

Key words: projective code; augmented code; self-orthogonal code; minimal code
Foundation Item(s): National Natural Science Foundation of China (No.11901049, No.12071138); The Young Talent Fund of University Association for Science and Technology in Shaanxi, China (No.20200505); The Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (No.2022D05); The Fundamental Research Funds for the Central Universities, CHD (No.300102122202); Shanghai Trusted Industry Internet Software Collaborative Innovation Center

1 引言

令 $q=p^e$,p 是一个素数,$r=q^m$,$\mathbb{F}_r$ 表示有 r 个元素的有限域. 设集合 $\mathcal{C}\subseteq\mathbb{F}_q^n$,如果 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 上的 $\mathbb{F}_q$-线性子空间,那么称 $\mathcal{C}$ 是 q 元线性码. 若线性码 $\mathcal{C}$ 的维数为 k,最小(Hamming)距离为 d,则记 $\mathcal{C}$ 的参数为 $[n,k,d]$. 这里 n 称为线性码的码长,k 表示码的信息位数,$\frac{k}{n}$ 表示码

收稿日期:2021-12-08;修回日期:2022-05-15;责任编辑:李勇锋

的传输效率,d可用于刻画码的检错能力和纠错能力[1]. 特别地,线性码的最小距离恰好是$\mathcal{C}$中所有非零码字汉明重量的最小值. 线性码$\mathcal{C}$的对偶码定义为

$$\mathcal{C}^{\perp}=\{\boldsymbol{c}^{\perp}\in\mathbb{F}_q^n:\ <\boldsymbol{c}^{\perp},\boldsymbol{c}>=0,\forall\boldsymbol{c}\in\mathcal{C}\},$$

其中$<\boldsymbol{c}^{\perp},\boldsymbol{c}>$表示这两个向量的欧氏内积. 当线性码$\mathcal{C}^{\perp}$的最小距离$d^{\perp}\geqslant 3$时,称$\mathcal{C}$为射影码. 有限域$\mathbb{F}_q$上$[n,k]$射影码生成矩阵的列向量可以看作射影空间$\mathrm{PG}\left(k-1,\mathbb{F}_q\right)$中的点. 在编码理论中,希望构造出的线性码同时具有高的传输效率和良好的检错、纠错能力,即$\frac{k}{n}$大且d大. 然而,n,k,d之间相互制约,它们满足一些界. 参数为$[n,k,d]$的q元线性码满足如下的球填充界[1]:

$q^n\geqslant q^k\left(\sum\limits_{i=0}^{\lfloor(d-1)/2\rfloor}(q-1)^i\binom{n}{i}\right)$. 参数为$[n,k,d]$的$q$元线性码也满足如下的Griesmer界[2]:$n\geqslant\sum\limits_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil$. 此外,如果存在参数为$[n,k,d]$的$q$元线性码,则该线性码满足Singleton界[1]:$n\geqslant k+d-1$. 如果不存在参数为$[n,k,d+1]$的线性码,则称参数为$[n,k,d]$的码为最优码. 如果参数为$[n,k,d]$的码为最优码,则称参数为$[n,k,d-1]$的码为几乎最优码. 特别地,恰好达到Singleton界的码称为MDS码.

线性码的重量分布是编码理论中的重要研究课题. 令A_i表示码长为n的线性码$\mathcal{C}$中所有重量为i的码字个数,序列$(1,A_1,A_2,\cdots,A_n)$称为$\mathcal{C}$的重量分布,$1+A_1z+A_2z^2+\cdots+A_nz^n$称为$\mathcal{C}$的重量计数器. 线性码的重量分布一般很难计算,文献中研究了一些特殊线性码的重量分布[3~20]. Ding等人在文献[21]中构造了线性码

$$\mathcal{C}_D=\left\{\left(\mathrm{Tr}_{r/q}(bd_1),\mathrm{Tr}_{r/q}(bd_2),\cdots,\mathrm{Tr}_{r/q}(bd_n)\right):b\in\mathbb{F}_r\right\},$$

其中集合$D=\{d_1,d_2,\cdots,d_n\}\subseteq\mathbb{F}_r^*$称为线性码$\mathcal{C}_D$的定义集. 通过选取合适的定义集,可以构造一些重量较少并且参数比较好的一些线性码. 文献中已有代表性结果如下:(1) Ding等人利用一些PN函数构造定义集,得到了一些二重码和三重码[21];(2) Tang等人用弱正则bent函数构造定义集,得到了一些二重码和三重码[3];(3) Zhou等人用二次函数构造定义集,得到了一些二重码和三重码[19];(4) Li等人利用一些特殊差集构造定义集,得到了一些重量较少的线性码[22].

线性码的概念还可以推广到有限环上,一些文献研究了环上的线性码[23,24].

构造射影码是编码理论中比较困难的问题之一. 本文基于有限域的二次乘法特征构造定义集,得到了两类线性码. 主要结果如下:(1) 借助于有限域上的指数和分别计算出了这两类线性码的重量分布,结果表明这两类线性码分别是三重和二重射影码;(2) 计算出了这两类线性码对偶码的参数,结果表明对偶码关于球填充界几乎最优.

此外,本文还得到了一些自正交码和极小码,它们可用于构造量子码和密钥共享方案.

2　预备知识

2.1　有限域上特征与指数和

定义1　有限域$\mathbb{F}_r$到$\mathbb{F}_q$的迹函数定义为

$$\mathrm{Tr}_{r/q}(x)=x+x^q+\cdots\cdots+x^{q^{m-1}}.$$

乘法群$\mathbb{F}_r^*$到$\mathbb{F}_q^*$的范函数定义为

$$\mathrm{N}_{q^m/q}(x)=x\cdot x^q\cdot x^{q^2}\cdots x^{q^{m-1}}=x^{\frac{q^m-1}{q-1}}.$$

显然迹函数为$\mathbb{F}_r$上加法满同态,范函数为$\mathbb{F}_r^*$上乘法满同态.

定义2　令$q=p^e$,p是一个素数且e为正整数. 令ζ_p表示p次本原复单位根,有限域$\mathbb{F}_q$上加法特征定义为$\phi_a(x)=\zeta_p^{\mathrm{Tr}_{q/p}(ax)}$, $x\in\mathbb{F}_q$,其中$\{\phi_a:a\in\mathbb{F}_q\}$构成加法群且包含$\mathbb{F}_q$的全部$q$个不同的加法特征. 特别地,当$a=0$时,称$\phi_0$为$\mathbb{F}_q$的平凡加法特征;当$a=1$时,称$\phi_1$为$\mathbb{F}_q$的典范加法特征. 显然,$\phi_a(x)=\phi_1(ax),x\in\mathbb{F}_q$. 令$\mathbb{F}_q^*=\mathbb{F}_q\backslash\{0\}$. 加法特征满足如下的正交关系[17]:

$$\sum_{x\in\mathbb{F}_q}\phi_1(ax)=\begin{cases}q, & \text{若}a=0,\\ 0, & \text{若}a\in\mathbb{F}_q^*.\end{cases}$$

定义3　有限域$\mathbb{F}_q$的乘法特征ψ定义为乘法群$\mathbb{F}_q^*$到复乘法群$\mathbb{C}^*$的同态映射,即ψ满足$\psi(xy)=\psi(x)\psi(y)$, $x,y\in\mathbb{F}_q^*$. $\mathbb{F}_q$的所有乘法特征可由如下函数给出:

$$\psi_j(\alpha^k)=\zeta_{q-1}^{jk},\ \ k=0,1,\cdots,q-1,$$

其中$0\leqslant j\leqslant q-2$. 特别地,$\psi_0$称为平凡乘法特征,$\eta:=\psi_{(q-1)/2}$称为二次乘法特征. 乘法特征的正交关系如下[17]:

$$\sum_{x\in\mathbb{F}_q^*}\psi_j(x)=\begin{cases}q-1, & \text{若}j=0,\\ 0, & \text{若}j\neq 0.\end{cases}$$

定义4[25]　设ψ,ϕ分别为$\mathbb{F}_q$的乘法特征和加法特征. 定义有限域上高斯和

$$G(\psi,\phi)=\sum_{x\in\mathbb{F}_q^*}\psi(x)\phi(x).$$

对于非平凡特征ϕ,称$G(\eta,\phi)$为$\mathbb{F}_q$上的二次高斯和.

引理1[25]　令η为$\mathbb{F}_q$的二次乘法特征,ϕ_1为$\mathbb{F}_q$的典范加法特征,则

$$G(\eta,\phi_1)=(-1)^{e-1}(\sqrt{-1})^{(\frac{p-1}{2})^2 e}\sqrt{q}$$
$$=\begin{cases}(-1)^{e-1}\sqrt{q}\ , & \text{若}p\equiv 1(\bmod 4),\\ (-1)^{e-1}(\sqrt{-1})^{e}\sqrt{q}\ , & \text{若}p\equiv 3(\bmod 4).\end{cases}$$

定义5 令ϕ为$\mathbb{F}_q$的非平凡加法特征,$f\in\mathbb{F}_q[x]$为正次数多项式. 形如$\sum_{c\in\mathbb{F}_q}\phi(f(c))$的特征和称为Weil和.

引理2[25] 令ϕ为$\mathbb{F}_q$的非平凡加法特征,其中q为奇素数的方幂.

$$f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x],\ a_2\neq 0,$$

则

$$\sum_{c\in\mathbb{F}_q}\phi(f(c))=\phi(a_0-a_1^2(4a_2)^{-1})\eta(a_2)G(\eta,\phi).$$

2.2 Pless幂等式

设$\mathcal{C}$是$\mathbb{F}_q$上参数为$[n,k,d]$的线性码,其重量分布为$(1,A_1,A_2,\cdots,A_n)$. 设对偶码$\mathcal{C}^{\perp}$的重量分布为$(1,A_1^{\perp},A_2^{\perp},\cdots,A_n^{\perp})$. 它们满足如下Pless幂等式[25]:

$$\sum_{j=0}^{n}A_j=q^k,$$
$$\sum_{j=0}^{n}jA_j=q^{k-1}(qn-n-A_1^{\perp}),$$
$$\sum_{j=0}^{n}j^2A_j=q^{k-2}((q-1)n(qn-n+1)-(2qn-q-2n+2)A_1^{\perp}+2A_2^{\perp}),$$
$$\sum_{j=0}^{n}j^3A_j=q^{k-3}[(q-1)n(q^2n^2-2qn^2+3qn-q+n^2-3n+2)-(3q^2n^2-3q^2n-6qn^2+12qn+q^2-6q+3n^2-9n+6)A_1^{\perp}+6(qn-q-n+2)A_2^{\perp}-6A_3^{\perp}].$$

Pless幂等式在编码理论中常用于计算对偶码的重量分布.

3 主要证明及结果

令$r=q^m$,q为奇素数的方幂. 设χ_1和ϕ_1分别为$\mathbb{F}_r$和$\mathbb{F}_q$的典范加法特征. 设η和η'分别为$\mathbb{F}_r$和$\mathbb{F}_q$的二次乘法特征.

3.1 第一类射影线性码

设$\mathcal{C}$是$\mathbb{F}_q$上$[n,k,d]$线性码,$\mathcal{C}$的生成矩阵为$\boldsymbol{G}$,长度为n的向量$\mathbf{1}=(1,1,\cdots,1)\notin\mathcal{C}$. 定义$\mathcal{C}$的增信码为如下矩阵生成的线性码:

$$\begin{bmatrix}\boldsymbol{G}\\ \mathbf{1}\end{bmatrix},$$

则增信码$\overline{\mathcal{C}}$的参数为$[n,k+1]$. 显然$\overline{\mathcal{C}}$的传输效率大于$\mathcal{C}$的传输效率.

设α为$\mathbb{F}_q$的本原元,取定义集

$$D=\{x\in\mathbb{F}_r^*:\eta'(\mathrm{Tr}_{r/q}(x))=-1\}$$
$$=\{x\in\mathbb{F}_r^*:\mathrm{Tr}_{r/q}(x)\in\alpha\langle\alpha^2\rangle\},$$

构造线性码

$$\overline{\mathcal{C}_D}=\{(\mathrm{Tr}_{r/q}(bx)+c)_{x\in D}:b\in\mathbb{F}_r,c\in\mathbb{F}_q\}.$$

显然$\overline{\mathcal{C}_D}$为线性码$\mathcal{C}_D=\{(\mathrm{Tr}_{r/q}(bx))_{x\in D}:b\in\mathbb{F}_r\}$的增信码. 容易看出,$\overline{\mathcal{C}_D}$的码长为$n=\frac{(q-1)q^{m-1}}{2}$. 当$q=3$时,定义集$D=\{x\in\mathbb{F}_r^*:\mathrm{Tr}_{r/q}(x)\in\alpha\langle\alpha^2\rangle\}$等价于$D=\{x\in\mathbb{F}_r^*:\mathrm{Tr}_{r/q}(x)=-1\}$,此时很容易得出$\mathcal{C}_D$是射影二重码. 下面只考虑$q>3$的情况.

令$b\in\mathbb{F}_r^*$,$c\in\mathbb{F}_q$,记

$$N_0=|\{x\in\mathbb{F}_r:\mathrm{Tr}_{r/q}(x)=0,\mathrm{Tr}_{r/q}(bx)+c=0\}|,$$
$$N_1=|\{x\in\mathbb{F}_r:\mathrm{Tr}_{r/q}(x)\in\alpha\langle\alpha^2\rangle,\mathrm{Tr}_{r/q}(bx)+c=0\}|,$$
$$N_2=|\{x\in\mathbb{F}_r:\mathrm{Tr}_{r/q}(x)\in\langle\alpha^2\rangle,\mathrm{Tr}_{r/q}(bx)+c=0\}|.$$

引理3 令$b\in\mathbb{F}_r^*$,$c\in\mathbb{F}_q$,则

$$N_0=\begin{cases}q^{m-2}, & \text{若}b\notin\mathbb{F}_q^{\ *}\text{且}c\in\mathbb{F}_q,\\ q^{m-1}, & \text{若}b\in\mathbb{F}_q^{\ *}\text{且}c=0,\\ 0, & \text{若}b\in\mathbb{F}_q^{\ *}\text{且}c\in\mathbb{F}_q^*.\end{cases}$$

证明 根据加法特征的正交关系

$$N_0=|\{x\in\mathbb{F}_r:\mathrm{Tr}_{r/q}(x)=0,\mathrm{Tr}_{r/q}(bx)+c=0\}|$$
$$=\frac{1}{q^2}\left(\sum_{x\in\mathbb{F}_r}\sum_{y\in\mathbb{F}_q}\chi_1(yx)\sum_{z\in\mathbb{F}_q}\chi_1(bzx)\phi_1(zc)\right)$$
$$=\frac{1}{q^2}\left(r+\sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_r}\chi_1(yx)+\sum_{z\in\mathbb{F}_q^*}\phi_1(zc)\sum_{x\in\mathbb{F}_r}\chi_1(zbx)+S_1\right),\tag{1}$$

其中

$$S_1=\sum_{z\in\mathbb{F}_q^*}\phi_1(zc)\sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_r}\chi_1((bz+y)x)$$
$$=\begin{cases}0, & \text{若}b\notin\mathbb{F}_q^{\ *}\text{且}c\in\mathbb{F}_q,\\ r(q-1), & \text{若}b\in\mathbb{F}_q^{\ *}\text{且}c=0,\\ -r, & \text{若}b\in\mathbb{F}_q^{\ *}\text{且}c\in\mathbb{F}_q^*.\end{cases}\tag{2}$$

由加法特征的正交关系,

$$\sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_r}\chi_1(yx)=0;\ \sum_{z\in\mathbb{F}_q^*}\phi_1(zc)\sum_{x\in\mathbb{F}_r}\chi_1(bzx)=0.\tag{3}$$

根据式(1),(2),(3)可得到N_0的值. □

引理4 令$r=q^m$且$b\in\mathbb{F}_r^*$,$c\in\mathbb{F}_q$,则

$$N_1+N_2=\begin{cases}q^{m-1}-q^{m-2}, & \text{若}b\notin\mathbb{F}_q^{\ *}\text{且}c\in\mathbb{F}_q,\\ 0, & \text{若}b\in\mathbb{F}_q^{\ *}\text{且}c=0,\\ q^{m-1}, & \text{若}b\in\mathbb{F}_q^{\ *}\text{且}c\in\mathbb{F}_q^{*}.\end{cases}$$

证明　根据N_0,N_1和N_2的关系，

$$N_0+N_1+N_2=\left|\left\{x\in\mathbb{F}_r\colon \mathrm{Tr}_{r/q}(bx)+c=0\right\}\right|=q^{m-1}.$$

从而根据引理3可得N_1+N_2的值. □

引理5　设$r=q^m$且 $b\in\mathbb{F}_r^{*}$, $c\in\mathbb{F}_q$, 则

$$N_2-N_1=\begin{cases}0, & \text{若}b\notin\mathbb{F}_q^{\ *}\text{且}c\in\mathbb{F}_q,\\ 0, & \text{若}b\in\mathbb{F}_q^{\ *}\text{且}c=0,\\ q^{m-1}\eta'(-\dfrac{c}{b}), & \text{若}b\in\mathbb{F}_q^{\ *}\text{且}c\in\mathbb{F}_q^{*}.\end{cases}$$

证明　设 $b\in\mathbb{F}_r^{*}$, $c\in\mathbb{F}_q$,令

$N=\sum\limits_{x\in\mathbb{F}_r}\sum\limits_{y,z\in\mathbb{F}_q}\phi_1(y^2\mathrm{Tr}_{r/q}(x))\phi_1\left(z\left(\mathrm{Tr}_{r/q}(bx)+c\right)\right)$. 根据引理2，

$$\sum_{y\in\mathbb{F}_q}\phi_1(y^2\mathrm{Tr}_{r/q}(x))=\begin{cases}q, & \text{若}\mathrm{Tr}_{r/q}(x)=0,\\ G(\eta',\phi_1), & \text{若}\mathrm{Tr}_{r/q}(x)\in\langle\alpha^2\rangle,\\ -G(\eta',\phi_1), & \text{若}\mathrm{Tr}_{r/q}(x)\in\alpha\langle\alpha^2\rangle.\end{cases}$$

根据加法特征的正交关系，

$$\sum_{z\in\mathbb{F}_q}\phi_1(z(\mathrm{Tr}_{r/q}(bx)+c))=\begin{cases}q, & \text{若}\mathrm{Tr}_{r/q}(bx)+c=0,\\ 0, & \text{若}\mathrm{Tr}_{r/q}(bx)+c\neq 0.\end{cases}$$

故

$$N=N_0q^2+(N_2-N_1)qG(\eta',\phi_1).\tag{4}$$

另一方面，

$$N=r+\sum_{y\in\mathbb{F}_q^{*}}\sum_{x\in\mathbb{F}_r}\chi_1(y^2x)+\sum_{z\in\mathbb{F}_q^{*}}\phi_1(zc)\sum_{x\in\mathbb{F}_r}\chi_1(zbx)+S_2,$$

其中，

$$S_2\colon=\sum_{y\in\mathbb{F}_q^{*}}\sum_{z\in\mathbb{F}_q^{*}}\phi_1(zc)\sum_{x\in\mathbb{F}_r}\chi_1((zb+y^2)x).$$

根据加法特征的正交关系，

$$\sum_{y\in\mathbb{F}_q^{*}}\sum_{x\in\mathbb{F}_r}\chi_1(y^2x)=0,$$

$$\sum_{z\in\mathbb{F}_q^{*}}\phi_1(zc)\sum_{x\in\mathbb{F}_r}\chi_1(zbx)=0.$$

根据加法特征的正交关系和引理2，

$$S_2=\begin{cases}0, & \text{若}b\notin\mathbb{F}_q^{*}\text{且}c\in\mathbb{F}_q,\\ r(q-1), & \text{若}b\in\mathbb{F}_q^{*}\text{且}c=0,\\ r\left(-1+\sum\limits_{y\in\mathbb{F}_q}\phi_1(-\dfrac{c}{b}y^2)\right), & \text{若}b\in\mathbb{F}_q^{*}\text{且}c\in\mathbb{F}_q^{*},\end{cases}$$

$$=\begin{cases}0, & \text{若}b\notin\mathbb{F}_q^{*}\text{且}c\in\mathbb{F}_q,\\ r(q-1), & \text{若}b\in\mathbb{F}_q^{*}\text{且}c=0,\\ -r+rG(\eta',\phi_1)\eta'(-\dfrac{c}{b}), & \text{若}b\in\mathbb{F}_q^{*}\text{且}c\in\mathbb{F}_q^{*}.\end{cases}$$

所以

$$N=\begin{cases}r, & \text{若}b\notin\mathbb{F}_q^{*}\text{且}c\in\mathbb{F}_q,\\ rq, & \text{若}b\in\mathbb{F}_q^{*}\text{且}c=0,\\ rG(\eta',\phi_1)\eta'(-\dfrac{c}{b}), & \text{若}b\in\mathbb{F}_q^{*}\text{且}c\in\mathbb{F}_q^{*}.\end{cases}\tag{5}$$

根据等式(4)和(5)、引理3可得N_2-N_1的值. □

引理6　令$m>1$,则

$$\left|\left\{(b,c)\colon b\in\mathbb{F}_{q^m}^{*}\text{且}\,b\notin\mathbb{F}_q^{*},c\in\mathbb{F}_q\right\}\right|=q^{m+1}-q^2;$$

$$\left|\left\{(b,c)\colon b\in\mathbb{F}_q^{*},c\in\mathbb{F}_q^{*}\text{且}\eta'(-\frac{c}{b})=-1\right\}\right|=\frac{(q-1)^2}{2};$$

$$\left|\left\{(b,c)\colon b\in\mathbb{F}_q^{*}\text{且}c=0\right\}\right|+\left|\left\{(b,c)\colon b=0,c\in\mathbb{F}_q^{*}\right\}\right|+\left|\left\{(b,c)\colon b,c\in\mathbb{F}_q^{*},\ \eta'(-\frac{c}{b})=1\right\}\right|=\frac{q^2+2q-3}{2}.$$

证明　在$\mathbb{F}_q^{*}$中平方元和非平方元的个数均为$\dfrac{q-1}{2}$,从而容易看出引理中三个等式显然成立. □

定理1　令q为奇素数的方幂，且$q>3,m>1$, $r=q^m$, 定义集$D=\left\{x\in\mathbb{F}_r^{*}\colon \mathrm{Tr}_{r/q}(x)\in\alpha\langle\alpha^2\rangle\right\}$. 则增信码$\overline{\mathcal{C}_D}$是参数为$\left[\dfrac{(q-1)q^{m-1}}{2},m+1,\dfrac{(q-3)q^{m-1}}{2}\right]$的射影三重码，其重量分布如表1所示. 此外，$\overline{\mathcal{C}_D}^{\perp}$关于球填充界几乎最优.

表1　定理1中射影码的重量分布

重量	频次
0	1
$\dfrac{(q-3)q^{m-1}}{2}$	$\dfrac{(q-1)^2}{2}$
$\dfrac{(q-2)q^{m-1}+q^{m-2}}{2}$	$q^{m+1}-q^2$
$\dfrac{(q-1)q^{m-1}}{2}$	$\dfrac{q^2+2q-3}{2}$

证明　根据引理4和引理5可得

$$N_1=\begin{cases}\dfrac{q^{m-1}-q^{m-2}}{2}, & 若b\notin\mathbb{F}_q{}^*,\ c\in\mathbb{F}_q,\\ 0, & 若b\in\mathbb{F}_q{}^*,c=0,\\ & 或b,c\in\mathbb{F}_q^*且\eta'(-\dfrac{c}{b})=1,\\ q^{m-1}, & 若b\in\mathbb{F}_q{}^*,c\in\mathbb{F}_q^*且\eta'(-\dfrac{c}{b})=-1.\end{cases}$$

设$\mathrm{wt}(\boldsymbol{c})$表示码字$\boldsymbol{c}\in\overline{\mathcal{C}_D}$的汉明重量,则

$$\begin{aligned}\mathrm{wt}(\boldsymbol{c})&=n-N_1\\&=\begin{cases}\dfrac{(q-3)q^{m-1}}{2}, & 若b\in\mathbb{F}_q^*,c\in\mathbb{F}_q^*\\ & 且\eta'(-\dfrac{c}{b})=-1.\\ \dfrac{(q-2)q^{m-1}+q^{m-2}}{2}, & 若b\notin\mathbb{F}_q^*,c\in\mathbb{F}_q,\\ \dfrac{(q-1)q^{m-1}}{2}, & 若b\in\mathbb{F}_q^*且c=0\\ & 或b=0且c\in\mathbb{F}_q^*\\ & 或b,c\in\mathbb{F}_q^*,\eta'(-\dfrac{c}{b})=-1.\end{cases}\end{aligned}$$

从而根据引理6即可得到表1中重量分布. 下面证明该线性码为射影码. 令

$$w_1=\frac{(q-3)q^{m-1}}{2},\ w_2=\frac{(q-2)q^{m-1}+q^{m-2}}{2},$$

$$w_3=\frac{(q-1)q^{m-1}}{2},A_{w_1}=\frac{(q-1)^2}{2},$$

$$A_{w_2}=q^{m+1}-q^2,\ A_{w_3}=\frac{q^2+2q-3}{2}.$$

根据Pless幂等式可以得到

$$\begin{cases}w_1A_{w_1}+w_2A_{w_2}+w_3A_{w_3}=q^m(qn-n-A_1^\perp),\\ w_1{}^2A_{w_1}+w_2{}^2A_{w_2}+w_3{}^2A_{w_3}\\ \qquad=q^{m-1}((q-1)n(qn-n+1)+2A_2^\perp),\\ w_1{}^3A_{w_1}+w_2{}^3A_{w_2}+w_3{}^3A_{w_3}=q^{m-2}[(q-1)n(q^2n^2\\ \qquad-2qn^2+3qn-q+n^2-3n+2)-6A_3^\perp].\end{cases}$$

解方程组得

$$A_1^\perp=0,A_2^\perp=0,A_3^\perp=q^{m-2}(q-1)^2t>0,$$

其中,

$$t=\frac{8q-4q^{m+1}+7q^m+q^{m+2}-4q^2}{48}\ (q>3).$$

因此,对偶码的参数为

$$\left[\frac{(q-1)q^{m-1}}{2},\ \frac{(q-1)q^{m-1}}{2}-m-1,3\right],$$

故线性码$\overline{\mathcal{C}_D}$为射影码.

若$q>3$,根据球填充界[1],

$$q^{\frac{(q-1)q^{m-1}}{2}}\geqslant q^{\frac{(q-1)q^{m-1}}{2}-m-1}\left(\sum_{i=0}^{\left\lfloor\frac{\tilde{d}^\perp-1}{2}\right\rfloor}(q-1)^i\binom{\frac{(q-1)q^{m-1}}{2}}{i}\right).$$

易得出$\tilde{d}^\perp\leqslant4$. 从而$\overline{\mathcal{C}_D}^\perp$关于球填充界几乎最优. □

推论1 $\mathcal{C}_D$是参数为

$$\left[\frac{(q-1)q^{m-1}}{2},m,\frac{(q-2)q^{m-1}+q^{m-2}}{2}\right]$$

的二重码,其重量分布如表2所示.

表2 推论1中线性码的重量分布

重量	频次
0	1
$\frac{(q-2)q^{m-1}+q^{m-2}}{2}$	q^m-q
$\frac{(q-1)q^{m-1}}{2}$	$q-1$

证明 当$c=0$时,根据定理1

$$N_1=\begin{cases}\dfrac{q^{m-1}-q^{m-2}}{2}, & 若b\notin\mathbb{F}_q{}^*,\\ 0, & 若b\in\mathbb{F}_q{}^*.\end{cases}$$

设$\mathrm{wt}(\boldsymbol{c})$表示码字$\boldsymbol{c}\in\mathcal{C}$的汉明重量,则

$$\begin{aligned}\mathrm{wt}(\boldsymbol{c})&=n-N_1\\&=\begin{cases}\dfrac{(q-2)q^{m-1}+q^{m-2}}{2}, & 若b\notin\mathbb{F}_q^*,\\ \dfrac{(q-1)q^{m-1}}{2}, & 若b\in\mathbb{F}_q^*.\end{cases}\end{aligned}$$

□

备注:当$q>3$情况下,可以用Magma验证线性码$\overline{\mathcal{C}_D}$在很多情形下都是自正交码,表3给出了一些例子. 我们猜测这类码在$q>3$的情况下是自正交码,证明留给读者.

表3 定理1中自正交码的例子

m	q	参数	备注
2	5	[10, 3, 5]	自正交
3	5	[50, 4, 25]	自正交
4	5	[250, 5, 125]	自正交
2	7	[21, 3, 14]	自正交
3	7	[147, 4, 98]	自正交
2	9	[36, 3, 27]	自正交

下面给出由Magma生成的一些例子,它们与定理1的结果一致.

例1 令$q=5$且$m=2$. 则$\overline{\mathcal{C}_D}$为$\mathbb{F}_5$上的[10, 3, 5]射影线性码且其重量计数器为

$$1+8z^5+100z^8+16z^{10}.$$

其对偶码$\overline{\mathcal{C}_D}^\perp$为[10, 7, 3]线性码. 此外,$\mathcal{C}_D$为$\mathbb{F}_5$上的[10, 2, 8]线性码且其重量计数器为

$$1+20z^8+4z^{10}.$$

其对偶码的参数为[10, 8, 2]. 根据http://codetables.de/中的Code Table可知,$\overline{\mathcal{C}_D}^\perp$,$\mathcal{C}_D$,$\mathcal{C}_D{}^\perp$均为最优码.

例2　设$q=7$且$m=2$,则$\overline{\mathcal{C}_D}$为$\mathbb{F}_7$上的[21,3,14]射影线性码且其重量计数器为

$$1+18z^{14}+294z^{18}+30z^{21}.$$

其对偶码$\overline{\mathcal{C}_D}^{\perp}$为[21,18,3]线性码. 此外,$\mathcal{C}_D$为$\mathbb{F}_7$上的[21,2,18]线性码且其重量计数器为

$$1+42z^{18}+6z^{21}.$$

其对偶码的参数为[21,19,2]. 根据http://codetables.de/中的Code Table可知,$\overline{\mathcal{C}_D}^{\perp}$,$\mathcal{C}_D$,$\mathcal{C}_D{}^{\perp}$均为最优码.

3.1　第二类射影线性码

设$\mathcal{C}$为线性码,如果在$\mathcal{C}$中所有码字在相同的坐标处删除一部分对应的坐标分量,那么所得长度变短的线性码称为$\mathcal{C}$的收缩码.

在本部分中,利用一类线性码的收缩码构造线性码.

令$r=q^m$,$\mathbb{F}_{r^2}^*=\langle\gamma\rangle$,$\mathbb{F}_q^*=\langle\alpha\rangle$.作$\mathbb{F}_{r^2}^*$的陪集分解

$$\mathbb{F}_{r^2}^*=\bigcup_{i=0}^{\frac{r^2-1}{q-1}-1}\gamma^i\mathbb{F}_q^*.$$

令$S=\{\gamma^0,\gamma^1,\cdots,\gamma^{\frac{r^2-1}{q-1}-1}\}$,$T=q^m+1$. 取定义集

$$\begin{aligned}D&=\left\{x\in S:\eta'\left(\mathrm{Tr}_{r/q}(x^T)\right)=-1\right\}\\&=\left\{x\in S:\mathrm{Tr}_{r/q}(x^T)\in\alpha\langle\alpha^2\rangle\right\}.\end{aligned}$$

定义$\mathbb{F}_q$上的线性码

$$\mathcal{C}_D=\left\{\left(\mathrm{Tr}_{r^2/q}(bx)\right)_{x\in D}:b\in\mathbb{F}_{r^2}\right\}.$$

令$E=\left\{x\in\mathbb{F}_{r^2}^*:\mathrm{Tr}_{r/q}(x^T)\in\alpha\langle\alpha^2\rangle\right\}$,定义$\mathbb{F}_q$上的线性码$\mathcal{C}_E=\left\{\left(\mathrm{Tr}_{r^2/q}(bx)\right)_{x\in E}:b\in\mathbb{F}_{r^2}\right\}$. 由于$\mathrm{Tr}_{r/q}(x^T)=\mathrm{Tr}_{r/q}\left(\mathrm{N}_{r^2/r}(x)\right)$,从而$\mathcal{C}_E$的码长

$$\begin{aligned}n_E&=|E|\\&=\frac{(q-1)q^{m-1}(q^m+1)}{2}=\frac{(q-1)(r^2q+rq)}{2q^2}.\end{aligned}$$

引理7　设$\mathcal{C}_E$是上文参数为$[n,k,d]$的线性码,其重量计数器为

$$1+A_dz^d+A_{d+1}z^{d+1}+\cdots+A_nz^n,$$

那么线性码$\mathcal{C}_D$的参数为$\left[\frac{n}{q-1},k,\frac{d}{q-1}\right]$,并且其重量计数器为

$$1+A_dz^{\frac{d}{q-1}}+A_{d+1}z^{\frac{d+1}{q-1}}+\cdots+A_nz^{\frac{n}{q-1}}.$$

证明　根据$\mathbb{F}_{r^2}^*$的陪集分解$\mathbb{F}_{r^2}^*=\bigcup_{i=0}^{\frac{r^2-1}{q-1}-1}\gamma^i\mathbb{F}_q^*$,易知$E=D\mathbb{F}_q^*$,从而结论显然成立. □

设$b\in\mathbb{F}_{r^2}^*$,考虑集合

$$K_0=\left|\left\{x\in\mathbb{F}_{r^2}:\mathrm{Tr}_{r/q}(x^T)=0,\ \mathrm{Tr}_{r^2/q}(bx)=0\right\}\right|,$$

$$K_1=\left|\left\{x\in\mathbb{F}_{r^2}:\mathrm{Tr}_{r/q}(x^T)\in\alpha\langle\alpha^2\rangle,\ \mathrm{Tr}_{r^2/q}(bx)=0\right\}\right|,$$

$$K_2=\left|\left\{x\in\mathbb{F}_{r^2}:\mathrm{Tr}_{r/q}(x^T)\in\langle\alpha^2\rangle,\ \mathrm{Tr}_{r^2/q}(bx)=0\right\}\right|.$$

引理8　设$b\in\mathbb{F}_{r^2}^*$,η'是$\mathbb{F}_q^*$上的二次乘法特征,则

$$K_0=\begin{cases}\dfrac{1}{q^2}(r^2-r(q-1)q), & \text{若}\mathrm{Tr}_{r/q}(b^T)=0,\\[2mm]\dfrac{r^2}{q^2}, & \text{若}\mathrm{Tr}_{r/q}(b^T)\neq0.\end{cases}$$

证明　令ϕ_1,χ_1,λ_1分为$\mathbb{F}_q$,$\mathbb{F}_r$和$\mathbb{F}_{r^2}$的典范加法特征. 根据加法特征的正交关系,

$$\begin{aligned}K_0&=\frac{1}{q^2}\sum_{x\in\mathbb{F}_{r^2},y,z\in\mathbb{F}_q}\phi_1(y\,\mathrm{Tr}_{r/q}(x^T))\phi_1(z\mathrm{Tr}_{r^2/q}(bx))\\&=\frac{1}{q^2}\left(r^2+\sum_{x\in\mathbb{F}_{r^2}}\sum_{z\in\mathbb{F}_q^*}\phi_1(z\mathrm{Tr}_{r^2/q}(bx))\right)\\&\quad+\frac{1}{q^2}\left(\sum_{x\in\mathbb{F}_{r^2}}\sum_{y\in\mathbb{F}_q^*}\phi_1(y(\mathrm{Tr}_{r/q}(x^T)))\right.\\&\quad\left.+\sum_{x\in\mathbb{F}_{r^2}}\sum_{y\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\phi_1\left(z\mathrm{Tr}_{r^2/q}(bx)+y\mathrm{Tr}_{r/q}(x^T)\right)\right)\\&=\frac{1}{q^2}\left(r^2+\sum_{z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\lambda_1(zbx)+\sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\chi_1(yx^T)\right)\\&\quad+\frac{1}{q^2}\left(S_0(b)+(q-1)^2\right),\end{aligned}$$

其中

$$S_0(b)=\sum_{x\in\mathbb{F}_{r^2}^*,y,z\in\mathbb{F}_q^*}\phi_1\left(z\mathrm{Tr}_{r^2/q}(bx)+y\mathrm{Tr}_{r/q}(x^T)\right).$$

由文献[4]中引理6可知

$$S_0(b)=\begin{cases}-(q-1)^2(r+1), & \text{若}\mathrm{Tr}_{r/q}(b^T)=0,\\(q-1)(r-q+1), & \text{若}\mathrm{Tr}_{r/q}(b^T)\neq0.\end{cases}$$

根据加法特征的正交关系

$$\sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\chi_1(yx^T)$$

$$=\sum_{y\in\mathbb{F}_q^*}\left(1+T\sum_{x_1\in\mathbb{F}_r^*}\chi_1(yx_1)\right)=-r(q-1),\ \sum_{z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\lambda_1(zbx)=0.$$

从而可得K_0的值. □

引理9　设$q=p^e$,p是一个奇素数,$b\in\mathbb{F}_{r^2}^*$,则

$$K_1+K_2=\begin{cases}\dfrac{(q-1)(r^2+rq)}{q^2}, & \text{若}\mathrm{Tr}_{r/q}(b^T)=0,\\[2mm]\dfrac{r^2(q-1)}{q^2}, & \text{若}\mathrm{Tr}_{r/q}(b^T)\neq0.\end{cases}$$

证明　根据K_0,K_1和K_2的关系以及$\mathrm{Tr}_{r/q}$的性

质,有

$$K_0+K_1+K_2=\left|\left\{x\in\mathbb{F}_{r^2}:\mathrm{Tr}_{r^2/q}(bx)=0\right\}\right|=q^{2m-1}.\quad(6)$$

从而K_1+K_2的值可根据式(6)和引理8得到. □

引理10 设$q=p^e$,p是一个奇素数,$b\in\mathbb{F}_{r^2}^*$,η'是$\mathbb{F}_q^*$上的二次乘法特征,则

$$K_2-K_1=\begin{cases}0, & \text{若}\mathrm{Tr}_{r/q}(b^T)=0,\\ -q^{m-1}(q-1)\eta'(-\mathrm{Tr}_{r/q}(b^T)), & \text{若}\mathrm{Tr}_{r/q}(b^T)\neq 0.\end{cases}$$

证明

令$K=\sum_{x\in\mathbb{F}_r}\sum_{y,z\in\mathbb{F}_q}\phi_1\left(y^2\mathrm{Tr}_{r/q}(x^T)\right)\phi_1\left(z\mathrm{Tr}_{r^2/q}(bx)\right)$,

根据引理2,

$$\sum_{y\in\mathbb{F}_q}\phi_1(y^2\mathrm{Tr}_{r/q}(x^T))=\begin{cases}q, & \text{若}\mathrm{Tr}_{r/q}(x^T)=0,\\ G(\eta',\phi_1), & \text{若}\mathrm{Tr}_{r/q}(x^T)\in\langle\alpha^2\rangle,\\ -G(\eta',\phi_1), & \text{若}\mathrm{Tr}_{r/q}(x^T)\in\langle\alpha^2\rangle.\end{cases}$$

根据加法特征的正交关系,

$$\sum_{z\in\mathbb{F}_q}\phi_1\left(z\left(\mathrm{Tr}_{r^2/q}(bx)\right)\right)=\begin{cases}q, & \text{若}\mathrm{Tr}_{r^2/q}(bx)=0,\\ 0, & \text{若}\mathrm{Tr}_{r^2/q}(bx)\neq 0.\end{cases}$$

所以,

$$K=K_0q^2+(K_2-K_1)qG(\eta',\phi_1),\quad(7)$$

另一方面,

$$K=r^2+\sum_{z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\lambda_1(zbx)+\Omega_1+\Omega_2,$$

其中

$$\Omega_1:=\sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\chi_1(y^2x^T),$$

$$\Omega_2:=\sum_{x\in\mathbb{F}_{r^2}}\sum_{y,z\in\mathbb{F}_q^*}\phi_1\left(y^2\mathrm{Tr}_{r/q}(x^T)\right)\phi_1\left(z\mathrm{Tr}_{r^2/q}(bx)\right).$$

根据加法特征的正交关系和范函数的性质,

$$\sum_{z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\lambda_1(zbx)=0,$$

$$\begin{aligned}\Omega_1&=(q-1)+T\sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_r}\chi_1(y^2x)\\&=(q-1)-T(q-1)\\&=-r(q-1).\end{aligned}$$

下面计算Ω_2,根据迹函数的传递性,

$$\begin{aligned}&\Omega_2\\&=\sum_{x\in\mathbb{F}_{r^2}}\sum_{y,z\in\mathbb{F}_q^*}\phi_1\left(y^2\mathrm{Tr}_{r/q}(x^T)\right)\phi_1\left(z\mathrm{Tr}_{r/q}\left(\mathrm{Tr}_{r^2/r}(bx)\right)\right)\\&=\sum_{y,z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\phi_1\left(y^2\mathrm{Tr}_{r/q}(x^T)+z\mathrm{Tr}_{r/q}\left(\mathrm{Tr}_{r^2/r}(bx)\right)\right)\\&=\sum_{z,y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\phi_1\left(y^2\mathrm{Tr}_{r/q}\left(x^{q^m+1}+\frac{bzx}{y^2}+\frac{zb^{q^m}x^{q^m}}{y^2}\right)\right).\end{aligned}$$

由于

$$\begin{aligned}&x^{q^m+1}+\frac{bzx}{y^2}+\frac{zb^{q^m}x^{q^m}}{y^2}\\&=\left(x+\frac{zb^{q^m}}{y^2}\right)^{q^m+1}-\frac{z^2b^{q^m+1}}{y^4},\end{aligned}$$

从而

$$\begin{aligned}\Omega_2&=\sum_{y\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\phi_1\left(y^2\mathrm{Tr}_{r/q}\left(x+\frac{zb^{q^m}}{y^2}\right)^{q^m+1}-\frac{z^2b^{q^m+1}}{y^4}\right)\\&=\sum_{y\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\phi_1\left(-\mathrm{Tr}_{r/q}\left(\frac{z^2b^{q^m+1}}{y^2}\right)\right)\sum_{x\in\mathbb{F}_{r^2}}\chi_1(y^2x_1^{q^m+1}),\end{aligned}$$

其中$x_1:=x+\frac{zb^{q^m}}{y^2}$. 根据范函数的性质和加法特征的正交关系,$\sum_{x_1\in\mathbb{F}_{r^2}}\chi_1(y^2x_1^{q^m+1})=1+\left(q^m+1\right)\sum_{x'\in\mathbb{F}_r^*}\chi_1(y^2x')=-r$.

从而可根据引理2得

$$\begin{aligned}\Omega_2&=-r\sum_{y\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\phi_1\left(-\mathrm{Tr}_{r/q}\left(\frac{z^2b^T}{y^2}\right)\right)\\&=-r\sum_{y\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\phi_1\left(-\frac{z^2}{y^2}\mathrm{Tr}_{r/q}(b^T)\right)\\&=\begin{cases}-r(q-1)^2, & \text{若}\mathrm{Tr}_{r/q}(b^T)=0,\\ -r\sum_{y\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q}\phi_1\left(-\frac{z^2}{y^4}\mathrm{Tr}_{r/q}(b^T)\right)+(q-1)r, & \text{若}\mathrm{Tr}_{r/q}(b^T)\neq 0.\end{cases}\\&=\begin{cases}-r(q-1)^2, & \text{若}\mathrm{Tr}_{r/q}(b^T)=0,\\ -r(q-1)\left(G(\eta',\phi_1)\eta'(-\mathrm{Tr}_{r/q}(b^T))-1\right), & \text{若}\mathrm{Tr}_{r/q}(b^T)=0.\end{cases}\end{aligned}$$

因此,

$$\begin{aligned}K&=r^2+\sum_{z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{r^2}}\lambda_1(zbx)+\Omega_1+\Omega_2\\&=\begin{cases}r^2-r(q-1)q, & \text{若}\mathrm{Tr}_{r/q}(b^T)=0,\\ r^2-r(q-1)G(\eta',\phi_1)\eta'(-\mathrm{Tr}_{r/q}(b^T)), & \text{若}\mathrm{Tr}_{r/q}(b^T)\neq 0.\end{cases}\end{aligned}\quad(8)$$

根据等式(7),(8)以及引理1、引理8可得K_2-K_1的值. □

定理2 令q为奇素数p的方幂,$r=q^m$且$m\geqslant 1$,$T=q^m+1$,$D=\left\{x\in S:\mathrm{Tr}_{r/q}(x^T)\in\alpha\langle\alpha^2\rangle\right\}$,其中

$$S=\{\gamma^0,\gamma^1,\cdots,\gamma^{\frac{r^2-1}{q-1}-1}\}.$$

则当$(q,m)\neq(3,1)$时,$\mathcal{C}_D$是参数为

$$\left[\frac{q^{2m-1}+q^{m-1}}{2},2m,\frac{q^{2m-1}-q^{2m-2}}{2}\right]$$

的射影二重码,其重量分布如表4所示;$\mathcal{C}_D^{\perp}$的最小距

离为3且关于球填充界几乎最优. 特别地,

(1) 当$m=1$且$q>3$时,

$\mathcal{C}_D$ 为 $\left[\frac{q+1}{2}, 2, \frac{q-1}{2}\right]$MDS 码; $\mathcal{C}_D{}^{\perp}$ 为 $\left[\frac{q+1}{2}, \frac{q-3}{2}, 3\right]$MDS码;

(2) 当$m>1$且$q=3$时,$\mathcal{C}_D$为 $\left[\frac{3^{2m-1}+3^{m-1}}{2}, 2m, \frac{3^{2m-1}-3^{2m-2}}{2}\right]$自正交线性码.

表4　定理2中射影码的重量分布

重量	频次
0	1
$\frac{q^{2m-1}-q^{2m-2}}{2}$	$\frac{(q^m+1)(q^m+q^{m-1}-2)}{2}$
$\frac{q^{2m-1}-q^{2m-2}+2q^{m-1}}{2}$	$\frac{(q-1)(q^{2m-1}+q^{m-1})}{2}$

证明　根据引理9和引理10可得

$$K_1=\begin{cases}\dfrac{(q-1)(r^2+rq)}{2q^2}, & \text{若}\mathrm{Tr}_{r/q}(b^T)=0,\text{或}\\ & \mathrm{Tr}_{r/q}(b^T)\neq 0\text{且}\\ & \eta'(-\mathrm{Tr}_{r/q}(b^T))=1,\\ \dfrac{(q-1)(r^2-rq)}{2q^2}, & \text{若}\mathrm{Tr}_{r/q}(b^T)\neq 0,\\ & \text{且}\eta'(-\mathrm{Tr}_{r/q}(b^T))=-1.\end{cases}$$

设$\mathrm{wt}(\boldsymbol{c})$表示码字$\boldsymbol{c}\in\mathcal{C}_E$的汉明重量,则根据$\mathcal{C}_E$的定义可知

$$\begin{aligned}\mathrm{wt}(\boldsymbol{c})&=n-K_1\\&=\begin{cases}\dfrac{(q-1)(q^{2m-1}-q^{2m-2})}{2}, & \text{若}\mathrm{Tr}_{r/q}(b^T)=0,\\ & \text{或}\mathrm{Tr}_{r/q}(b^T)\neq 0\\ & \text{且}\eta'(-\mathrm{Tr}_{r/q}(b^T))=1,\\ \dfrac{(q-1)q^{m-1}(q^m-q^{m-1}+2)}{2} & \text{若}\mathrm{Tr}_{r/q}(b^T)\neq 0\text{且}\\ & \eta'(-\mathrm{Tr}_{r/q}(b^T))=-1,\end{cases}\end{aligned}$$

根据迹函数、范函数和二次特征的性质易得

$$\begin{aligned}&\left|\left\{b: b\in\mathbb{F}_{r^2}^{*},\ \mathrm{Tr}_{r/q}(b^T)\neq 0,\ \eta'(-\mathrm{Tr}_{r/q}(b^T))=-1\right\}\right|\\&=\frac{(q-1)(q^{2m-1}+q^{m-1})}{2};\\&\left|\left\{b: b\in\mathbb{F}_{r^2}^{*}\text{且}\ \mathrm{Tr}_{r/q}(b^T)=0\right\}\right|\\&+\left|\left\{b: b\in\mathbb{F}_{r^2}^{*},\ \mathrm{Tr}_{r/q}(b^T)\neq 0,\ \eta'(-\mathrm{Tr}_{r/q}(b^T))=1\right\}\right|\\&=\frac{(q^m+1)(q^m+q^{m-1}-2)}{2}.\end{aligned}$$

从而可得$\mathcal{C}_E$的重量分布. 再根据引理7即可得到表4中$\mathcal{C}_D$的重量分布. 令$(q,m)\neq(3,1)$. 下面证明$\mathcal{C}_D$为射影码,记

$$\begin{aligned}w_1&=\frac{q^{2m-1}-q^{2m-2}}{2},\\w_2&=\frac{q^{2m-1}-q^{2m-2}+2q^{m-1}}{2},\\A_{w_1}&=\frac{(q^m+1)(q^m+q^{m-1}-2)}{2},\\A_{w_2}&=\frac{(q-1)(q^{2m-1}+q^{m-1})}{2}.\end{aligned}$$

根据Pless幂等式,

$$\begin{cases}w_1A_{w_1}+w_2A_{w_2}=q^{2m-1}(qn-n-A_1^{\perp}),\\ {w_1}^2A_{w_1}+{w_2}^2A_{w_2}=q^{2m-2}((q-1)n(qn-n+1)\\ \qquad\qquad +2A_2^{\perp}),\\ {w_1}^3A_{w_1}+w_2^3A_{w_2}=q^{2m-3}((q-1)n(q^2n^2-2qn^2\\ \qquad\qquad +3qn-q+n^2-3n+2)\\ \qquad\qquad -6A_3^{\perp}).\end{cases}$$

解得

$$A_1^{\perp}=0,\ A_2^{\perp}=0,\ A_3^{\perp}=(q-1)(q^{2m}+q^m)t,$$

其中

$$\begin{aligned}t=\frac{1}{48q^3}&\left(q^{2m}(1+q^2)+4q^2(2-q)\right.\\&\left.-2q^{m+1}(q^m-q+3)\right)>0.\end{aligned}$$

因此,对偶码$\mathcal{C}_D{}^{\perp}$最小距离为3. 根据球填充界[1]

$$q^n\geqslant q^{n-2m}\left(\sum_{i=0}^{\left\lfloor\frac{d^{\perp}-1}{2}\right\rfloor}(q-1)^i\binom{n}{i}\right),$$

其中$n=\frac{q^{2m-1}+q^{m-1}}{2}$,容易得出$\mathcal{C}_D{}^{\perp}$的最小距离满足$d^{\perp}\leqslant 4$. 从而$\mathcal{C}_D{}^{\perp}$的参数为

$$\left[\frac{q^{2m-1}+q^{m-1}}{2}, \frac{q^{2m-1}+q^{m-1}}{2}-2m, 3\right]$$

且$\mathcal{C}_D{}^{\perp}$关于球填充界几乎最优. 特别地,当$m=1, q>3$时,容易看出$\mathcal{C}_D$和$\mathcal{C}_D{}^{\perp}$均为MDS码. 当$m>1, q=3$时,容易验证$\mathcal{C}_D$的两个非零重量均可以被3整除. 根据文献[24]中定理1.4.10可知,三元线性码是自正交码当且仅当它的码字重量都可以被3整除. 故当$m>1, q=3$时,$\mathcal{C}_D$为自正交码. □

下面给出由Magma生成的一些例子,它们与定理2的结果完全一致.

例3　设$q=3$且$m=2$. 则$\mathcal{C}_D$为参数是[15,4,9]的3元射影自正交线性码且其重量计数器为

$$1+50z^9+30z^{12}$$

其对偶码$\mathcal{C}_D{}^{\perp}$为[15,11,3]射影线性码. 根据http://codetables.de/中的Code Table可知,$\mathcal{C}_D$和$\mathcal{C}_D^{\perp}$均为最优码.

4 总结

本文基于二次乘法特征构造了两类线性码，计算出了它们的参数和重量分布．主要结果及应用如下．

（1）定理1中构造的增信码$\overline{\mathcal{C}_D}$是射影三重码且其对偶码关于球填充界几乎最优；利用Magma验证了当$q>3$时$\overline{\mathcal{C}_D}$在很多情形下都是自正交码，从而可以猜测$\overline{\mathcal{C}_D}$在$q>3$的条件下是自正交码．

（2）定理2中构造的线性码$\mathcal{C}_D$是射影二重码且其对偶码关于球填充界几乎最优．特别地，当$m=1,q>3$时，$\mathcal{C}_D$为MDS码．当$m>1,q=3$时，$\mathcal{C}_D$为自正交码．根据量子码的CSS构造，$\mathcal{C}_D^{\perp}$可用于构造极小距离$\geqslant 3$的三元量子码[26]．令$w_{\min},w_{\max}$分别表示定理2中射影码$\mathcal{C}_D$的最小非零汉明重量和最大汉明重量．根据定理2和Ashikhmin-Barg定理[27]，当$m\geqslant 2$时，容易验证$\mathcal{C}_D$是极小码．极小码可用于构造安全访问结构上的密钥共享方案[27]．

（3）定理2所得的射影二重码可用于构造强正则图．对于一个有N个顶点且度数为K的正则连通图，若任意相邻两顶点的公共相邻顶点数为λ，任意不相邻两顶点的公共相邻顶点数为μ，则称该正则连通图是参数为(N,K,λ,μ)的强正则图．文献[28]研究了射影二重量线性码和强正则图之间的关系．从而根据文献[28]，定理2中射影码$\mathcal{C}_D$可用于构造强正则图．

（4）文献[29]将射影三重码和结合方案建立联系．根据文献[29]，定理1中的射影三重码$\overline{\mathcal{C}_D}$可用于构造类数为3的结合方案．

参考文献

[1] 冯克勤, 刘凤梅. 代数与通信[M]. 北京: 高等教育出版社, 2005.

[2] GRIESMER J H. A bound for error-correcting codes[J]. IBM Journal of Research and Development, 1960, 4: 532-542.

[3] TANG Chun-ming, LI Nian, QI Yan-feng, ZHOU Zheng-chun, HELLESETH Tor. Linear codes with two or three weights from weakly regular bent functions[J]. IEEE Transactions on Information Theory, 2016, 62(3): 1166-1176.

[4] HENG Zi-ling, LI De-xiang, DU Jiao, CHEN Fu-ling. A family of projective two-weight linear codes[J]. Designs, Codes and Cryptography, 2021, 89: 1993-2007.

[5] YANG Shu-di, YAO Zheng-an, ZHAO Chang-an. A class of three-weight linear codes and their complete weight enumerators[J]. Cryptography and Communications, 2017, 9: 133-149.

[6] YANG Shu-di, YAO Zheng-an. Complete weight enumerators of a family of three-weight linear codes[J]. Designs, Codes and Cryptography, 2017, 82: 663-674.

[7] YANG Shu-di, YAO Zheng-an, ZHAO Chang-an. The weight distributions of two classes of p ary cyclic codes with few weights[J]. Finite Fields and Their Applications, 2017, 44: 76-91.

[8] 杨淑娣, 唐春明. 循环码的完全重量分布[J]. 江苏师范大学学报(自然科学版), 2018, 36(2): 64-68.
YANG Shu-di, TANG Chun-ming. The complete weight enumerator of cyclic codes[J]. Journal of Jiangsu Normal University, 2018, 36 (2): 64-68. (in Chinese)

[9] 杨淑娣, 岳勤. 一类线性码的完全重量分布[J]. 计算机工程与科学, 2019, 41(2): 281-285.
YANG Shu-di, YUE Qin. Complete weight enumerators of a class of linear codes[J]. Computer Engineering and Science, 2019, 41(2): 281-285. (in Chinese)

[10] HENG Zi-ling, WANG Qiu-yan, DING Cun-sheng. Two families of optimal linear codes and their subfield codes [J]. IEEE Transactions on Information Theory, 2020, 66 (11): 6872-6883.

[11] HENG Zi-ling, DING Cun-sheng, WANG Wei-qiong. Optimal binary linear codes from maximal arcs[J]. IEEE Transactions on Information Theory, 2020, 66(9): 5387-5394.

[12] 杜小妮, 吕红霞, 王蓉, 李丽. 两类四重线性码的构造[J]. 西北师范大学学报(自然科学版), 2018, 54(6): 1-4.
DU Xiao-ni, LV Hong-xia, WANG Rong, LI Li. A construction of two classes of linear codes with four-weights [J]. Journal of Northwestern Normal University (Natural Science Edition), 2018, 54(6): 1-4. (in Chinese)

[13] 杜小妮, 吕红霞, 王蓉. 一类四重和六重线性码的构造[J]. 电子与信息学报, 2019, 41(12): 2995-2999.
DU Xiao-ni, LV Hong-xia, Wang Rong. Construction of a class of linear codes with four-weight and six-weight[J]. Journal of Electronics and Information Technology, 2019, 41(12): 2995-2999. (in Chinese)

[14] DU Xiao-ni, WANG Rong, TANG Chun-ming, WANG Qi. Infinite families of 2-designs from linear codes[J]. Applicable Algebra in Engineering Communication and Computing, 2022, 33: 193-211.

[15] DU Xiao-ni, LI Xiao-dan, WAN Yun-qi. A class of linear codes with three and five weights[J]. Chinese Journal of Electronics, 2019, 28(03): 457-461.

[16] 胡丽琴, 岳勤, 朱小萌. 具有两个非零点循环码的权重分布[J]. 中国科学: 数学, 2014, 44(9): 1021-1034.

HU Li-qin, YUE Qin, ZHU Xiao-meng. Weight distributions of a class of cyclic codes with two non-zeros[J]. Science in China: Mathematics, 2014, 44(9): 1021-1034. (in Chinese)

[17] FENG Tao. On cyclic codes of length 2^{2r} -1 with two zeros whose dual codes have three weights[J]. Designs, Codes and Cryptography, 2012, 62(3): 253-258.

[18] XIANG Can, WANG Xian-Fang, TANG Chun-ming, FU Fang-wei. Two classes of linear codes and their weight distributions[J]. Applicable Algebra in Engineering Communication and Computing, 2018, 29(3): 209-225.

[19] ZHOU Zheng-chun, LI Nian, FAN Cui-ling, HELLESETH Tor. Linear codes with two or three weights from quadratic Bent functions[J]. Designs, Codes and Cryptography, 2016, 81(2): 283-295.

[20] DING Cun-sheng, NIEDERREITER H. Cyclotomic linear codes of order 3[J]. IEEE Transactions on Information Theory, 2007, 53(6): 2274-2277.

[21] DING Ke-lan, DING Cun-sheng. A class of two-weight and three-weight codes and their applications in secret sharing[J]. IEEE Transactions on Information Theory, 2015, 61: 5835-5842.

[22] LI Cheng-ju, BAE S, AHN J, Yang Shu-di, YAO Zheng-an. Complete weight enumerators of some linear codes and their applications[J]. Designs Codes Cryptography, 2016, 81: 153-168.

[23] 高健, 吕京杰. $\mathbb{Z}_4\times(\mathbb{F}_2+u\mathbb{F}_2)$上的一类循环码[J]. 电子学报, 2018, 46(7): 1768-1773.
GAO Jian, LÜ Jing-jie. A class of cyclic codes on $\mathbb{Z}_4\times(\mathbb{F}_2+u\mathbb{F}_2)$[J]. Acta Electronica Sinica, 2018, 46(7): 1768-1773. (in Chinese)

[24] HUFFMAN W C, PLESS V. Fundamentals of Error-Correcting Codes[M]. Cambridge: Cambridge University Press, 2003.

[25] LIDL R, NIEDERREITER H. Finite Fields[M]. Boston: Addison-Wesley, 1983.

[26] KETKAR A, KLAPPENECKER A, KUMAR S. Nonbinary stabilizer codes over finite fields[J]. IEEE Trans Inf Theory, 2006, 52: 4892-4914.

[27] ASHIKHMIN A, BARG A. Minimal vectors in linear codes[J]. IEEE Trans Inf Theory, 1998, 44: 2010-2017.

[28] CALDERBANK R, KANTER W M. The geometry of two-weight codes[J]. Bull Lond Math Soc, 1986, 18: 97-122.

[29] CALDERBANK R, GOETHAL J M. Three-weight codes and association schemes[J]. Philips J Res, 1984, 39: 143-152.

作者简介

陈辅灵　女,996年9月出生于青海省西宁市. 现为长安大学理学院硕士研究生. 主要研究方向为代数编码.
E-mail: chenfuling1109@163.com

衡子灵(通讯作者)　男,1990年出生,河南南阳人. 现为长安大学理学院副教授,硕士生导师. 主要研究方向为编码与密码、序列设计等.
E-mail: zilingheng@chd.edu.cn

王鑫然　男,1999年2月出生于山东省聊城市. 现为长安大学理学院硕士研究生. 主要研究方向为代数编码.
E-mail: WXR782751966@163.com

李成举　男,1988年6月出生,山东鱼台人. 现为华东师范大学教授,博士生导师. 主要研究方向为代数编码和信息安全.
E-mail: cjli@sei.ecnu.edu.cn