Advances in Applied Mathematics 应用数学进展, **2024, 13(8), 4064-4076**
Published Online August 2024 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2024.138388

Hans汉斯

几类射影三重和四重二元线性码及其应用

周 欢

西北师范大学数学与统计学院，甘肃 兰州

收稿日期：2024年7月23日；录用日期：2024年8月16日；发布日期：2024年8月26日

摘 要

本文通过恰当地选择定义集，构造了四类具有较少重量的射影二元线性码，并通过计算指数和确定了它们的重量分布。特别地，根据Grassl 的在线数据库，构造的某些二元线性码是最优的，并且其中某些码的对偶是最优的或几乎最优的。本文还利用Griesmer界刻画了四类线性码的最优性，并得到了一些(几乎)距离最优的线性码或(近) Griesmer码。在实际应用方面，本文得到的一些线性码可以用于构造具有良好访问结构的秘密共享方案。

关键词

射影二元线性码，重量分布，最优线性码，Griesmer码，关联方案

Several Classes of Projective Three-Weight and Four-Weight Binary Linear Codes and Their Applications

Huan Zhou

College of Mathematics and Statistics, Northwest Normal University, Lanzhou Gansu

Received: Jul. 23^{rd}, 2024; accepted: Aug. 16^{th}, 2024; published: Aug. 26^{th}, 2024

文章引用: 周欢. 几类射影三重和四重二元线性码及其应用[J]. 应用数学进展, 2024, 13(8): 4064-4076.
DOI: 10.12677/aam.2024.138388

Abstract

In this paper, we construct four classes of projective binary linear codes with a few weights by selecting defining sets properly and completely determine their weight distributions by calculating the exponential sums. Especially, some of the constructed binary linear codes are optimal according to the online Database of Grassl, and the duals of some of them are optimal or almost optimal. We also characterize the optimality of these four classes of linear codes using the Griesmer bound and obtain some (almost) distance-optimal linear codes or (near) Griesmer codes. As applications, some of the linear codes obtained in this paper can be used to construct secret sharing schemes with interesting access structures.

Keywords

Projective Binary Linear Code, Weight Distribution, Optimal Linear Code, Griesmer Code, Association Scheme

1. 引言

设 m 为正整数, r 为素数, 且使得 2 为模 r^m 本原根, 即 2 为模 r^m 乘法群的生成元. 设 $q=2^{\phi(r^m)}$, 其中 ϕ 为欧拉函数. 方便起见, 我们用 ℓ 来表示 $\phi(r^m)$. 设 $\mathbb{F}_q$ 为具有 q 个元素的有限域, $\mathbb{F}_q^*=\mathbb{F}_q\setminus\{0\}$ 为它的乘法群.

向量空间 $\mathbb{F}_2^n$ 的一个 k 维线性子空间称为二元 $[n,k,d]$ 线性码 C, 其中 d 为最小 (汉明) 距离. 设 $\mathbf{x}=(x_1,x_2,\cdots,x_n)$ 与 $\mathbf{y}=(y_1,y_2,\cdots,y_n)$. C 的对偶码定义为

$$C^{\perp}=\{\mathbf{x}\in\mathbb{F}_2^n:\langle\mathbf{x},\mathbf{y}\rangle=0,\ \text{对所有}\ \mathbf{y}\in C\},$$

其中, $\langle\mathbf{x},\mathbf{y}\rangle=\sum_{i=1}^{n}x_iy_i$. $C^{\perp}$ 的最小距离用 $d^{\perp}$ 表示, 称为 C 的对偶距离. 显然, 对偶码 $C^{\perp}$ 的参数为 $[n,n-k,d^{\perp}]$. 若 $d^{\perp}\geq 3$, 则称线性码 C 为射影码. 若 $C=C^{\perp}$, 则称线性码 C 为自对偶码. 自对偶

码的长度 n 为偶数, 维数为 $\frac{n}{2}$. 对于 $1 \leq i \leq n$, 设 A_i 表示码长 n 的线性码 C 中汉明重量为 i 的码字的个数. 线性码 C 的重量计数器定义为

$$1 + A_1 z + A_2 z^2 + \cdots + A_n z^n,$$

其中 $(1, A_1, \cdots, A_n)$ 为 C 的重量分布. 重量分布包含了估计误差检测和校正概率的基本信息. 因此, 重量分布在编码理论中引起了广泛的关注, 并且许多学者将其研究重点集中于线性码重量分布的确定 [1]. 若序列 $(A_1, A_2, \cdots, A_n)$ 中非零 A_i 的数量等于 t, 则称码 C 为 t 重码. 若二元线性码 C 包含全一向量, 则称其为自补码. 具有较少重量的线性码在秘密共享 [2], 强正则图 [3], 关联方案 [4] 和认证码 [5] 中有不同的应用. 这些线性码的构造是纠错码理论中一个有意义的研究课题.

对任意的正整数 s, Tr_1^s 表示从 $\mathbb{F}_{2^s}$ 到 $\mathbb{F}_2$ 的迹函数 [6]. 对任意的集合 $D = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_q^*$, 定义 $\mathbb{F}_2$ 上长度为 n 的线性码为

$$C_D = \{(\mathrm{Tr}_1^s(xd_1), \mathrm{Tr}_1^s(xd_2), \cdots, \mathrm{Tr}_1^s(xd_n)) : x \in \mathbb{F}_q\}, \tag{1}$$

并称 D 为码 C_D 的定义集 [7]. 这种构造方法具有通用性, 因为许多具有优良性质的码可以通过选择适当的定义集 D 获得 [5, 8–14].

本文采用指数和的方法来研究 (1) 式中线性码 C_D 的重量分布, 其中

$$D = \{x \in \mathbb{F}_q^* : \mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}}) = t_1, \mathrm{Tr}_1^\ell(x) = t_2\}, \tag{2}$$

对于 $t_1, t_2 \in \mathbb{F}_2$. 我们提出了几类三重和四重线性码并确定了其重量分布, 并且某些二元线性码对于 Grassl 的在线数据库是最优的或几乎最优的, 还确定了它们对偶码的参数. 此外, 本文构造的所有二元线性码都是射影的.

本文的其余部分组织如下. 在第2节中, 介绍了一些与线性码相关的基本概念和结论. 在第3节中, 重点研究了所提出的线性码 C_D 的重量分布, 还提供了一些例子来证明我们的主要结果. 第4节讨论了构造的线性码的某些实际应用. 第5节总结本文工作.

2. 预备知识

本节首先介绍编码理论中的一些基本符号和结果, 这将在本文后面使用.

2.1. 有限域上的特征以及指数和

本文的主要目标是构造有限域上具有较少重量的线性码并研究其性质, 如长度和重量分布, 这需要计算由相关函数推导出的指数和. 本小节给出了一些关于特征以及指数和的已知结论, 用于证明本文的主要结果.

$\mathbb{F}_q$ 的加法特征 χ 是从 $\mathbb{F}_q$ 到绝对值为 1 的复数组成的集合的函数, 使得对所有的 $x, y \in \mathbb{F}_q$,

$\chi(x+y)=\chi(x)\chi(y)$. 对每个 $b\in\mathbb{F}_q$, 定义 $\mathbb{F}_q$ 的一个加法特征为函数

$$\chi_b(x)=(-1)^{\mathrm{Tr}_1^\ell(bx)},\ \text{对所有}\ x\in\mathbb{F}_q, \tag{3}$$

$\mathbb{F}_q$ 的每个加法特征都可以通过这种方式得到. 特别地, 当 $b=1$ 时, (3)式中的特征 χ_1 称为 $\mathbb{F}_q$ 的标准加法特征. 显然 $\chi_b(x)=\chi_1(bx)$. $\mathbb{F}_q$ 的加法特征的正交性 [6, 定理5.4] 如下所示

$$\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell(bx)}=\begin{cases}q, & \text{若 } b=0,\\ 0, & \text{否则.}\end{cases} \tag{4}$$

关于有限域上加法特征的更多内容, 读者可参考专著 [6].

对任意的 $a,b\in\mathbb{F}_q$, 以下指数和的值由 Moisio 在 [15] 中确定, 并且 $S(1,b)$ 的确切值由 [16] 给出

$$S(a,b)=\sum_{x\in\mathbb{F}_q^*}\chi_1\left(ax^{\frac{q-1}{l^m}}+bx\right).$$

以下引理中总结了文献 [16] 中的结论, 可用于计算二元线性码的重量分布.

引理1. 符号定义如上. 则

$$S(1,b)=\begin{cases}\frac{q-1}{r^m}(r^m-2r+2), & \text{若 } b=0,\\ \sqrt{q}-\frac{\sqrt{q}+1}{r^m}(r^m-2r+2), & \text{若 } b=1,\\ \pm\sqrt{q}-\frac{\sqrt{q}+1}{r^m}(r^m-2r+2), & \text{若 } b\neq 0,1.\end{cases}$$

2.2. 极小线性码

对于长度为 n 的线性码 C, 码字 $\mathbf{c}=(c_1,c_2,\cdots,c_n)\in C$ 的支撑定义为

$$\mathrm{Suppt}(\mathbf{c})=\{1\le i\le n: c_i\neq 0\}.$$

对于 $\mathbf{u},\mathbf{v}\in C$, 若 $\mathrm{Suppt}(\mathbf{u})\subseteq\mathrm{Suppt}(\mathbf{v})$, 则称 $\mathbf{v}$ 覆盖了 $\mathbf{u}$, 记为 $\mathbf{u}\preceq\mathbf{v}$. 在二元线性码 C 中, 若一个非零码字 $\mathbf{c}\in C$ 仅覆盖本身, 则称 $\mathbf{c}$ 是极小的. 若 C 中的每个码字都是极小的, 则称线性码 C 是极小线性码. Ashikhmin 和 Barg [17] 给出了判断线性码极小的充分条件: 若 $\frac{w_{\min}}{w_{\max}}>\frac{1}{2}$, 则二元线性码 C 为极小的, 其中 $w_{\min}$ 和 $w_{\max}$ 分别表示码 C 中非零码字的最小和最大重量.

2.3. Pless幂矩公式和Griesmer界

设 C 是 $[n,k,d]$ 二元线性码, 重量分布为 $(1,A_1,\cdots,A_n)$, 其对偶码的重量分布为 $(1,A_1^\perp,\cdots,A_n^\perp)$.

下面给出前五个Pless 幂矩公式 [18, p.260] :

$$\sum_{i=0}^{n} A_i = 2^k,$$

$$\sum_{i=0}^{n} iA_i = 2^{k-1}(n - A_1^{\perp}),$$

$$\sum_{i=0}^{n} i^2 A_i = 2^{k-2}[n(n+1) - 2nA_1^{\perp} + 2A_2^{\perp}],$$

$$\sum_{i=0}^{n} i^3 A_i = 2^{k-3}[n^2(n+3) - (3n^2+3n-2)A_1^{\perp} + 6nA_2^{\perp} - 6A_3^{\perp}],$$

$$\sum_{i=0}^{n} i^4 A_i = 2^{k-4}[n(n+1)(n^2+5n-2) - 4n(n^2+3n-2)A_1^{\perp}$$

$$+ 4(3n^2+3n-4)A_2^{\perp} - 24nA_3^{\perp} + 24A_4^{\perp}].$$

最优线性码在编码理论中有重要的作用, 并受到了广泛的关注. 若不存在 $[n, k, d+1]$ 码, 则称 $[n, k, d]$ 线性码 C 为距离最优码, 若存在 $[n, k, d+1]$ 距离最优码, 则称 $[n, k, d]$ 线性码为几乎距离最优码. 若 $[n, k, d]$ 线性码 C 的参数 n, k 和 d (或 $d+1$) 满足线性码中任何的界, 例如 Plotkin 界, Singleton 界, 或者 Griesmer 界, 则称 C 为最优码 (或几乎最优码) [18]. 特别地, 对于 $\mathbb{F}_2$ 上的 $[n, k, d]$ 线性码 C, 其 Griesmer 界由以下式子给出:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil,$$

其中, $\lceil \cdot \rceil$ 为向上取整函数. 若线性码 C 的参数 n (或 $n-1$), k 和 d 达到 Griesmer 界, 则称线性码 C 为 Griesmer 码 (或几乎 Griesmer 码). Griesmer 码由于其最优性和几何应用 [19, 20] 而引起了相当多的关注. 一般来说, 构造最优线性码是一个困难的问题, 读者可以参考 [21–27] 来了解最近的结论.

3. 码C_D的重量分布

本节重点研究 (1) 式中线性码 C_D 的重量分布. 以下引理用于证明本文的主要结论, 其中 $|S|$ 为有限集合 S 的基数.

引理2. 设 $n_0 = |D|$, 其中 D 为 (2) 式中所定义. 则

$$n_0 = \frac{1}{4}q + \frac{1}{4}(-1)^{t_1}(1 + S(1,0)) + \frac{1}{4}(-1)^{t_1+t_2}(1 + S(1,1)).$$

证明 由 (4) 式中加法特征的正交性, 可得

$$\begin{aligned}
n_0 &= \frac{1}{4}\sum_{x\in\mathbb{F}_q}\Big(\sum_{y_1\in\mathbb{F}_2}(-1)^{y_1(\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}})+t_1)}\Big)\Big(\sum_{y_2\in\mathbb{F}_2}(-1)^{y_2(\mathrm{Tr}_1^\ell(x)+t_2)}\Big)\\
&= \frac{1}{4}\sum_{x\in\mathbb{F}_q}\Big(1+(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}})+t_1}\Big)\Big(1+(-1)^{\mathrm{Tr}_1^\ell(x)+t_2}\Big)\\
&= \frac{1}{4}q+\frac{1}{4}\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell(x)+t_2}+\frac{1}{4}\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}})+t_1}\\
&\quad+\frac{1}{4}\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}}+x)+t_1+t_2}\\
&= \frac{1}{4}q+\frac{1}{4}(-1)^{t_1}(1+S(1,0))+\frac{1}{4}(-1)^{t_1+t_2}(1+S(1,1)).
\end{aligned}$$

即得结论. □

引理3. 对任意的 $b\in\mathbb{F}_q^*$, 定义

$$N_b=|\{x\in\mathbb{F}_q:\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}})=t_1,\mathrm{Tr}_1^\ell(x)=t_2,\mathrm{Tr}_1^\ell(bx)=0\}|.$$

则

$$N_b=\begin{cases}\frac{1}{8}(1+(-1)^{t_2})(q+(-1)^{t_1}(2+S(1,0)+S(1,1))), & \text{若 } b=1,\\ \frac{1}{8}q+\frac{1}{8}(-1)^{t_1}(2+S(1,0)+S(1,b))\\ +\frac{1}{8}(-1)^{t_1+t_2}(2+S(1,1)+S(1,b+1)), & \text{若 } b\neq 1.\end{cases}$$

证明 由 (4) 式中加法特征的正交性, 可得

$$\begin{aligned}
N_b &= \frac{1}{8}\sum_{x\in\mathbb{F}_q}\Big(\sum_{y_1\in\mathbb{F}_2}(-1)^{y_1(\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}})+t_1)}\sum_{y_2\in\mathbb{F}_2}(-1)^{y_2(\mathrm{Tr}_1^\ell(x)+t_2)}\sum_{y_3\in\mathbb{F}_2}(-1)^{y_3\mathrm{Tr}_1^\ell(bx)}\Big)\\
&= \frac{1}{8}\sum_{x\in\mathbb{F}_q}\Big((1+(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}})+t_1})(1+(-1)^{\mathrm{Tr}_1^\ell(x)+t_2})(1+(-1)^{\mathrm{Tr}_1^\ell(bx)})\Big)\\
&= \frac{1}{8}\sum_{x\in\mathbb{F}_q}\Big(1+(-1)^{\mathrm{Tr}_1^\ell(bx)}+(-1)^{\mathrm{Tr}_1^\ell(x)+t_2}+(-1)^{\mathrm{Tr}_1^\ell(bx+x)+t_2}+(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}})+t_1}\\
&\quad+(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}}+bx)+t_1}+(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}}+x)+t_1+t_2}+(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}}+bx+x)+t_1+t_2}\Big)\\
&= \frac{1}{8}q+\frac{1}{8}\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell(bx+x)+t_2}+\frac{1}{8}\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}})+t_1}\\
&\quad+\frac{1}{8}\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}}+bx)+t_1}+\frac{1}{8}\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}}+x)+t_1+t_2}\\
&\quad+\frac{1}{8}\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}}+bx+x)+t_1+t_2}
\end{aligned}$$

$$= \frac{1}{8}q + \frac{1}{8}(-1)^{t_2}\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}_1^\ell((1+b)x)} + \frac{1}{8}(-1)^{t_1}(1+S(1,0)) + \frac{1}{8}(-1)^{t_1}(1+S(1,b)) + \frac{1}{8}(-1)^{t_1+t_2}(1+S(1,1)) + \frac{1}{8}(-1)^{t_1+t_2}(1+S(1,1+b)).$$

下面根据 b 是否等于 1 分为两种情况讨论.

(1) 若 $b=1$, 有

$$\begin{aligned} N_b &= \frac{1}{8}q + \frac{1}{8}(-1)^{t_2}q + \frac{1}{8}(-1)^{t_1}(1+S(1,0)) + \frac{1}{8}(-1)^{t_1}(1+S(1,1)) \\ &\quad + \frac{1}{8}(-1)^{t_1+t_2}(1+S(1,1)) + \frac{1}{8}(-1)^{t_1+t_2}(1+S(1,0)) \\ &= \frac{1}{8}(1+(-1)^{t_2})(q+(-1)^{t_1}(2+S(1,0)+S(1,1))). \end{aligned}$$

(2) 若 $b\neq 1$, 有

$$\begin{aligned} N_b &= \frac{1}{8}q + \frac{1}{8}(-1)^{t_1}(1+S(1,0)) + \frac{1}{8}(-1)^{t_1}(1+S(1,b)) \\ &\quad + \frac{1}{8}(-1)^{t_1+t_2}(1+S(1,1)) + \frac{1}{8}(-1)^{t_1+t_2}(1+S(1,b+1)) \\ &= \frac{1}{8}q + \frac{1}{8}(-1)^{t_1}(2+S(1,0)+S(1,b)) + \frac{1}{8}(-1)^{t_1+t_2}(2+S(1,1)+S(1,b+1)). \end{aligned}$$

即得结论. □

下面分四种情形研究 C_D 的参数和重量分布.

3.1. 情形 1: $t_1 = t_2 = 1$

定理1. 设 $D=\{x\in\mathbb{F}_q : \mathrm{Tr}_1^\ell(x^{\frac{q-1}{r^m}})=1, \mathrm{Tr}_1^\ell(x)=1\}$. 则 (1) 式中码 C_D 为 $[n,\ell,d]$ 射影四重二元线性码, 重量分布如表 1所示, 其中 $n=\frac{(q+\sqrt{q})(r-1)}{2r^m}$, $d=\frac{(q+\sqrt{q})(r-1)}{4r^m}-\frac{\sqrt{q}}{4}$. 对偶码 $C_D^\perp$ 的参数为 $[n,n-\ell,4]$.

证明 显然码 C_D 的长度 n 等于 n_0, 由引理 2, $n=\frac{(q+\sqrt{q})(r-1)}{2r^m}$.

由引理 1, 对任意的 $b\in\mathbb{F}_q^*\backslash\{1\}$, 可得

$$S(1,1+b)\in\Big\{\pm\sqrt{q}-\frac{\sqrt{q}+1}{r^m}(r^m-2r+2)\Big\}.$$

对任意的 $b\in\mathbb{F}_q^*$, 码 C_D 的码字

$$\mathbf{c}_b=(\mathrm{Tr}(bx))_{x\in D} \tag{5}$$

的汉明重量 $\mathrm{wt}(\mathbf{c}_b)$ 为 $n-N_b$. 因此, 由引理 1, 2 和 3, (5)式中码字 $\mathbf{c}_b$ 的重量 $\mathrm{wt}(\mathbf{c}_b)\in\{\omega_1,\omega_2,\omega_3,\omega_4\}$,

Table 1. Weight distribution of codes in Theorem 1
表 1. 定理 1 中的码的重量分布

重量ω	频数A_ω
0	1
$\frac{(q+\sqrt{q})(r-1)}{2r^m}$	1
$\frac{(q+\sqrt{q})(r-1)}{4r^m}$	$2\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2-\frac{2(q+\sqrt{q})(r-1)}{r^m}+q-2$
$\frac{(q+\sqrt{q})(r-1)}{4r^m}-\frac{\sqrt{q}}{4}$	$\frac{(q+\sqrt{q})(r-1)}{r^m}-\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2$
$\frac{(q+\sqrt{q})(r-1)}{4r^m}+\frac{\sqrt{q}}{4}$	$\frac{(q+\sqrt{q})(r-1)}{r^m}-\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2$

其中

$$\omega_1=\frac{(q+\sqrt{q})(r-1)}{2r^m},\qquad \omega_2=\frac{(q+\sqrt{q})(r-1)}{4r^m},$$
$$\omega_3=\frac{(q+\sqrt{q})(r-1)}{4r^m}-\frac{\sqrt{q}}{4},\ \omega_4=\frac{(q+\sqrt{q})(r-1)}{4r^m}+\frac{\sqrt{q}}{4}.$$

由于对每个 $b\in\mathbb{F}_q^*$, $\mathrm{wt}(\mathbf{c}_b)>0$, 所以码 C_D 的维数为 ℓ.

下面计算 C_D 中重量为 ω_i 的码字个数 A_{ω_i}, 其中 $1\le i\le 4$. 由引理 3 中 N_b 的计算可知: $\mathrm{wt}(\mathbf{c}_b)=\frac{(q+\sqrt{q})(r-1)}{2r^m}$ 当且仅当 $b=1$, i.e., $A_{\omega_1}=1$. 由 D 的定义可知 $0\notin D$. 因此 $A_1^\perp=0$. 由于 D 不是多重集, 所以如果 $i\neq j$, 那么 D 的任意两个元素 d_i 和 d_j 必不相同. 故 $A_2^\perp=0$ 且 $d^\perp>2$. 由前三个 Pless 幂矩公式可得以下方程组:

$$\begin{cases} A_{\omega_1}+A_{\omega_2}+A_{\omega_3}+A_{\omega_4}=q-1,\\ \omega_1A_{\omega_1}+\omega_2A_{\omega_2}+\omega_3A_{\omega_3}+\omega_4A_{\omega_4}=\frac{1}{2}qn,\\ \omega_1^2A_{\omega_1}+\omega_2^2A_{\omega_2}+\omega_3^2A_{\omega_3}+\omega_4^2A_{\omega_4}=\frac{1}{4}q[n(n+1)]. \end{cases}$$

求解后可得码 C_D 的重量分布如表 1所示.

对偶码 $C_D^\perp$ 的结论可由 C_D 的长度和维数得到. 此外, 由第四个和第五个 Pless 幂矩公式可推得 $A_3^\perp=0$, $A_4^\perp>0$, 故 $C_D^\perp$ 的最小距离为 4. □

例1. (1) 设 $r=3$, $m=2$. Magma 程序表明 C_D 为一个 $[8,6,2]$ 线性码, 其重量计数器为 $1+12z^2+38z^4+12z^6+z^8$, 与定理 1 的结论一致. 特别地, 这个码为近 Griesmer 码, 且由文献 [28] 可知, 它还是最优的. 此外, 它的对偶码 $C_D^\perp$ 的参数为 $[8,2,4]$, 关于 Griesmer 界是几乎距离最优码, 且由文献 [28] 可知是几乎最优码.

(2) 设 $r=5$, $m=1$. Magma 程序表明 C_D 为一个 $[8,4,4]$ 线性码, 其重量计数器为 $1+14z^4+z^8$, 与定理 1 的结论一致. 注意到当 $r=5$, $m=1$ 时, C_D 的最后两个重量不存在, 所以它是一个二重码. 特别地, 这个码是 Griesmer 码, 且由文献 [28] 可知, 它还是最优的. 此外, 它的对偶码 $C_D^\perp$ 的参数为 $[8,4,4]$, 所以 C_D 为自对偶码.

(3) 设 $r=11$, $m=1$. Magma 程序表明 C_D 为一个 $[480,10,232]$ 线性码, 其重量计数器

为 $1+60z^{232}+902z^{240}+60z^{248}+z^{480}$, 与定理 1 的结论一致. 此外, 它的对偶码 $C_D^{\perp}$ 的参数为 $[480,470,4]$.

3.2. 情形 2: $t_1=1,\ t_2=0$

定理2. 设 $r^m\geq 11$, $D=\{x\in\mathbb{F}_q:\mathrm{Tr}_1^{\ell}(x^{\frac{q-1}{r^m}})=1,\mathrm{Tr}_1^{\ell}(x)=0\}$. 则 (1) 式中码 C_D 为 $[n,\ell-1,d]$ 射影三重二元线性码, 重量分布如表 2所示, 其中 $n=\frac{(q-\sqrt{q}-2)(r-1)}{2r^m}$, $d=\frac{(q+\sqrt{q})(r-1)}{4r^m}-\frac{\sqrt{q}}{2}$. 对偶码 $C_D^{\perp}$ 的参数为 $[n,n-\ell+1,3]$.

Table 2. Weight distribution of codes in Theorem 2

表 2. 定理 2 中的码的重量分布

重量ω	频数A_ω
0	1
$\frac{(q+\sqrt{q})(r-1)}{4r^m}$	$\frac{1}{2}\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2-\frac{(2q+\sqrt{q}-1)(r-1)}{2r^m}+\frac{q}{2}-1$
$\frac{(q+\sqrt{q})(r-1)}{4r^m}-\frac{\sqrt{q}}{4}$	$\frac{(q+\sqrt{q})(r-1)}{r^m}-\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2$
$\frac{(q+\sqrt{q})(r-1)}{4r^m}-\frac{\sqrt{q}}{2}$	$\frac{1}{2}\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2-\frac{(\sqrt{q}+1)(r-1)}{2r^m}$

证明 显然码 C_D 的长度 n 等于 n_0, 由引理 2, $n=\frac{(q-\sqrt{q}-2)(r-1)}{2r^m}$.

由引理 1, 对任意的 $b\in\mathbb{F}_q^*\backslash\{1\}$, 可得

$$S(1,1+b)\in\left\{\pm\sqrt{q}-\frac{\sqrt{q}+1}{r^m}(r^m-2r+2)\right\}.$$

对任意的 $b\in\mathbb{F}_q^*$, 码 C_D 的码字

$$\mathbf{c}_b=(\mathrm{Tr}(bx))_{x\in D} \tag{6}$$

的汉明重量 $\mathrm{wt}(\mathbf{c}_b)$ 为 $n-N_b$. 因此, 由引理 1, 2 和 3, (6)式中码字 $\mathbf{c}_b$ 的重量 $\mathrm{wt}(\mathbf{c}_b)\in\{0,\omega_1,\omega_2,\omega_3\}$, 其中

$$\omega_1=\frac{(q+\sqrt{q})(r-1)}{4r^m},\omega_2=\frac{(q+\sqrt{q})(r-1)}{4r^m}-\frac{\sqrt{q}}{4},\omega_3=\frac{(q+\sqrt{q})(r-1)}{4r^m}-\frac{\sqrt{q}}{2}.$$

当 $r^m\geq 11$ 时, 对每个 $b\in\mathbb{F}_q^*\backslash\{1\}$, 都有 $\mathrm{wt}(\mathbf{c}_b)>0$, 所以码 C_D 的维数为 $\ell-1$.

下面计算 C_D 中重量为 ω_i 的码字个数 A_{ω_i}, 其中 $1\leq i\leq 3$. 与定理 1 的证明论述一致, 由前三个 Pless 幂矩公式可推得以下方程组:

$$\begin{cases}A_{\omega_1}+A_{\omega_2}+A_{\omega_3}=\frac{1}{2}q-1,\\ \omega_1A_{\omega_1}+\omega_2A_{\omega_2}+\omega_3A_{\omega_3}=\frac{1}{4}qn,\\ \omega_1^2A_{\omega_1}+\omega_2^2A_{\omega_2}+\omega_3^2A_{\omega_3}=\frac{1}{8}q[n(n+1)].\end{cases}$$

求解后可得码 C_D 的重量分布如表 2所示.

对偶码 $C_D^{\perp}$ 的结论可由 C_D 的长度和维数得到. 由第四个 Pless 幂矩公式可推得 $A_3^{\perp}>0$. □

例2. 设 $r=11, m=1$. Magma 程序表明 C_D 为一个 $[450,9,224]$ 线性码, 其重量计数器为 $1+435z^{224}+60z^{232}+16z^{240}$, 与定理 2 的结论一致. 特别地, 这个码关于 Griesmer 界是距离最优码. 此外, 它的对偶码 $C_D^{\perp}$ 的参数为 $[450,441,3]$.

3.3. 情形 3: $t_1=0,\ t_2=1$

下面定理的证明与定理 1 相似, 所以这里省略了证明.

定理3. 设 $r^m\geq 9, D=\{x\in\mathbb{F}_q:\mathrm{Tr}_1^{\ell}(x^{\frac{q-1}{r^m}})=0,\mathrm{Tr}_1^{\ell}(x)=1\}$. 则 (1) 式中码 C_D 为 $[n,\ell,d]$ 射影四重二元线性码, 重量分布如表 3所示, 其中 $n=\frac{(q+\sqrt{q})(r^m-r+1)}{2r^m}-\frac{\sqrt{q}}{2}$, $d=\frac{(q+\sqrt{q})(r^m-r+1)}{4r^m}-\frac{\sqrt{q}}{2}$. 对偶码 $C_D^{\perp}$ 的参数为 $[n,n-\ell,4]$.

Table 3. Weight distribution of codes in Theorem 3

表 3. 定理 3 中的码的重量分布

重量ω	频数A_ω
0	1
$\frac{(q+\sqrt{q})(r^m-r+1)}{2r^m}-\frac{\sqrt{q}}{2}$	1
$\frac{(q+\sqrt{q})(r^m-r+1)}{4r^m}-\frac{\sqrt{q}}{4}$	$2\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2-\frac{2(q+\sqrt{q})(r-1)}{r^m}+q-2$
$\frac{(q+\sqrt{q})(r^m-r+1)}{4r^m}-\frac{\sqrt{q}}{2}$	$\frac{(q+\sqrt{q})(r-1)}{r^m}-\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2$
$\frac{(q+\sqrt{q})(r^m-r+1)}{4r^m}$	$\frac{(q+\sqrt{q})(r-1)}{r^m}-\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2$

例3. (1) 设 $r=3, m=2$. Magma 程序表明 C_D 为一个 $[24,6,10]$ 线性码, 其重量计数器为 $1+12z^{10}+38z^{12}+12z^{14}+z^{24}$, 与定理 3 的结论一致. 特别地, 这个码关于 Griesmer 界是几乎距离最优码, 且由文献 [28] 可知, 它还是最优的. 此外, 它的对偶码 $C_D^{\perp}$ 的参数为 $[24,18,4]$, 关于 Griesmer 界是距离最优码, 且由文献 [28] 可知是最优码.

(2) 设 $r=11, m=1$. Magma 程序表明 C_D 为一个 $[32,10,8]$ 线性码, 其重量计数器为 $1+60z^8+902z^{16}+60z^{24}+z^{32}$, 与定理 3 的结论一致. 此外, 它的对偶码 $C_D^{\perp}$ 的参数为 $[32,22,4]$, 由文献 [28] 可知是几乎最优码.

3.4. 情形 4: $t_1=t_2=0$

下面定理的证明与定理 2 相似, 所以这里省略了证明.

定理4. 设 $r^m\geq 9, D=\{x\in\mathbb{F}_q:\mathrm{Tr}_1^{\ell}(x^{\frac{q-1}{r^m}})=0,\mathrm{Tr}_1^{\ell}(x)=0\}$. 则 (1) 式中码 C_D 为 $[n,\ell-1,d]$ 射影三重二元线性码, 重量分布如表 4所示, 其中 $n=\frac{(r-1)(\sqrt{q}-q+2)}{2r^m}+\frac{q}{2}-1$, $d=\frac{q}{4}-\frac{(q+\sqrt{q})(r-1)}{4r^m}$. 对偶码 $C_D^{\perp}$ 的参数为 $[n,n-\ell+1,3]$.

例4. (1) 设 $r=3, m=2$. Magma 程序表明 C_D 为一个 $[25,5,12]$ 线性码, 其重量计数器为 $1+18z^{12}+12z^{14}+z^{16}$, 与定理 4 的结论一致. 特别地, 这个码为近 Griesmer 码, 且由文献 [28] 可知, 它还是最优的. 此外, 它的对偶码 $C_D^{\perp}$ 的参数为 $[25,20,3]$, 关于 Griesmer 界是几乎距离最优码, 且由文献 [28] 可知是最优码.

Table 4. Weight distribution of codes in Theorem 4
表 4. 定理 4 中的码的重量分布

重量ω	频数A_ω
0	1
$\frac{q}{4}-\frac{(q+\sqrt{q})(r-1)}{4r^m}$	$\frac{1}{2}\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2-\frac{(2q+\sqrt{q}-1)(r-1)}{2r^m}+\frac{q}{2}-1$
$\frac{(q+\sqrt{q})(r^m-r+1)}{4r^m}$	$\frac{(q+\sqrt{q})(r-1)}{r^m}-\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)^2$
$\frac{q+2\sqrt{q}}{4}-\frac{(q+\sqrt{q})(r-1)}{4r^m}$	$\frac{1}{2}\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}\right)\left(\frac{(\sqrt{q}+1)(r-1)}{r^m}-1\right)$

(2) 设 $r=11, m=1$. Magma 程序表明 C_D 为一个 $[61,9,16]$ 线性码, 其重量计数器为 $1+16z^{16}+60z^{24}+435z^{32}$, 与定理 4 的结论一致. 此外, 它的对偶码 $C_D^{\perp}$ 的参数为 $[61,52,3]$, 由文献 [28] 可知是几乎最优码.

4. 码 C_D 的应用

在实际应用方面, 本文得到的一些二元线性码可以用于构造具有良好访问结构的秘密共享方案.

设 $r^m\geq 11$. 则对于定理 2 中的线性码, 有

$$\frac{w_{\min}}{w_{\max}}=\frac{\frac{(q+\sqrt{q})(r-1)}{4r^m}-\frac{\sqrt{q}}{2}}{\frac{(q+\sqrt{q})(r-1)}{4r^m}}>\frac{1}{2}.$$

因此, 根据 Ashikhmin 和 Barg 给出的线性码极小的充分条件, 这个码是极小的, 可以用于构造具有访问结构的秘密共享方案 [2].

5. 总结

本文构造了几类射影三重和四重线性码, 并利用指数和给出了它们的重量计数器. 所提出的一些线性码是最优的, 并且它们的对偶码也是最优或几乎是最优的. 利用 Griesmer 界, 刻画了四类线性码的最优性, 并得到了几类 (几乎) 距离最优的线性码或 (近) Griesmer 码. 此外, 还研究了这些线性码的自补性和极小性, 并得到一些码是自补的或极小的.

参考文献

[1] Qi, Y.F., Tang, C.M. and Huang, D.M. (2016) Binary Linear Codes with Few Weights. *Finite Fields and Their Applications*, **20**, 208-211. https://doi.org/10.1109/LCOMM.2015.2506576

[2] Yuan, J. and Ding, C. (2006) Secret Sharing Schemes from Three Classes of Linear Codes. *IEEE Transactions on Information Theory*, **52**, 206-212. https://doi.org/10.1109/TIT.2005.860412

[3] Calderbank, A.R. and Kantor, W.M. (1986) The Geometry of Two-Weight Codes. *Bulletin of the London Mathematical Society*, **18**, 97-122. https://doi.org/10.1112/blms/18.2.97

[4] Calderbank, A.R. and Goethals, J.M. (1984) Three-Weight Codes and Association Schemes. *Philips Journal of Research*, **39**, 143-152.

[5] Ding, C., Helleseth, T., Klove, T. and Wang, X. (2007) A Generic Construction of Cartesian Authentication Codes. *IEEE Transactions on Information Theory*, **53**, 2229-2235. https://doi.org/10.1109/TIT.2007.896872

[6] Lidl, R. and Niederreiter, H. (1997) Finite Fields. Cambridge University Press. https://doi.org/10.1017/CBO9780511525926

[7] Ding, K. and Ding, C. (2014) Binary Linear Codes with Three Weights. *IEEE Communications Letters*, **18**, 1879-1882. https://doi.org/10.1109/LCOMM.2014.2361516

[8] Ding, C. (2015) Linear Codes from Some 2-Designs. *IEEE Transactions on Information Theory*, **61**, 3265-3275. https://doi.org/10.1109/TIT.2015.2420118

[9] Ding, K. and Ding, C. (2015) A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing. *IEEE Transactions on Information Theory*, **61**, 5835-5842. https://doi.org/10.1109/TIT.2015.2473861

[10] Ding, C., Li, C., Li, N. and Zhou, Z. (2016) Three-Weight Cyclic Codes and Their Weight Distributions. *Discrete Mathematics*, **339**, 415-427. https://doi.org/10.1016/j.disc.2015.09.001

[11] Jian, G., Feng, R. and Wu, H. (2017) Generalized Hamming Weights of Three Classes of Linear Codes. *Finite Fields and Their Applications*, **45**, 341-354. https://doi.org/10.1016/j.ffa.2017.01.001

[12] Li, F. (2018) A Class of Cyclotomic Linear Codes and Their Generalized Hamming Weights. *Applicable Algebra in Engineering, Communication and Computing*, **29**, 501-511. https://doi.org/10.1007/s00200-018-0355-1

[13] Li, F. and Li, X. (2021) Weight Distributions and Weight Hierarchies of Two Classes of Binary Linear Codes. *Finite Fields and Their Applications*, **73**, Article 101865. https://doi.org/10.1016/j.ffa.2021.101865

[14] Liu, Z.H. and Wang, J.L. (2020) Notes on Generalized Hamming Weights of Some Classes of Binary Codes. *Cryptography and Communications*, **12**, 645-657. https://doi.org/10.1007/s12095-019-00404-3

[15] Moisio, M. (2009) Explicit Evaluation of Some Exponential Sums. *Finite Fields and Their Applications*, **15**, 644-651. https://doi.org/10.1016/j.ffa.2009.05.005

[16] Wang, Q.Y., Ding, K.L. and Xue, R. (2015) Binary Linear Codes with Two Weights. *IEEE Communications Letters*, **19**, 1097-1100. https://doi.org/10.1109/LCOMM.2015.2431253

[17] Ashikhmin, A. and Barg, A. (1998) Minimal Vectors in Linear Codes. *IEEE Transactions on Information Theory*, **44**, 2010-2017. https://doi.org/10.1109/18.705584

[18] Huffman, W.C. and Pless, V. (2003) Fundamentals of Error-Correcting Codes. Cambridge University Press. https://doi.org/10.1017/CBO9780511807077

[19] Ding, C. (2015) Codes from Difference Sets. World Scientific. https://doi.org/10.1142/9283

[20] Ding, C. (2018) Designs from Linear Codes. World Scientific. https://doi.org/10.1142/11101

[21] Heng, Z., Ding, C. and Wang, W. (2020) Optimal Binary Linear Codes from Maximal Arcs. *IEEE Transactions on Information Theory*, **66**, 5387-5394. https://doi.org/10.1109/TIT.2020.2970405

[22] Heng, Z., Wang, Q. and Ding, C. (2020) Two Families of Optimal Linear Codes and Their Subfield Codes. *IEEE Transactions on Information Theory*, **66**, 6872-6883. https://doi.org/10.1109/TIT.2020.3006846

[23] Hyun, J.Y., Kim, H.K., Wu, Y. and Yue, Q. (2020) Optimal Minimal Linear Codes from Posets. *Designs, Codes and Cryptography*, **88**, 2475-2492. https://doi.org/10.1007/s10623-020-00793-0

[24] Hyun, J.Y., Lee, J. and Lee, Y. (2020) Infinite Families of Optimal Linear Codes Constructed from Simplicial Complexes. *IEEE Transactions on Information Theory*, **66**, 6762-6773. https://doi.org/10.1109/TIT.2020.2993179

[25] Wang, X., Zheng, D. and Ding, C. (2021) Some Punctured Codes of Several Families of Binary Linear Codes. *IEEE Transactions on Information Theory*, **67**, 5133-5148. https://doi.org/10.1109/TIT.2021.3088146

[26] Hu, Z., Li, N., Zeng, X., Wang, L. and Tang, X. (2022) A Subfield-Based Construction of Optimal Linear Codes over Finite Fields. *IEEE Transactions on Information Theory*, **68**, 4408-4421. https://doi.org/10.1109/TIT.2022.3163651

[27] Zhu, C.Z. and Liao, Q.Y. (2022) Several Classes of Projective Few-Weight Linear Codes and Their Applications. arXiv:2211.04519

[28] Grassl M. (2024) Bounds on the Minimum Distance of Linear Codes and Quantum Codes. http://www.codetables.de