Pure Mathematics 理论数学, 2023, 13(5), 1389-1402
Published Online May 2023 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2023.135142

几类 p 元线性码的构造

刘文辉

西北师范大学，数学与统计学院，甘肃 兰州

收稿日期：2023年4月21日；录用日期：2023年5月23日；发布日期：2023年5月30日

摘 要

低重线性码因在秘密共享方案、认证码、结合方案、强正则图等方面具有重要的应用，所以被广泛研究。本文通过选取新的定义集，构造了几类新的 p 元线性码，并利用指数和理论确定了码的参数和重量分布，最后说明本文构造的线性码在多数情况下是极小码，可以用来设计具有良好访问结构的秘密共享方案。

关键词

线性码，定义集，指数和，重量分布

Construction of Several Classes of p-Ary Linear Codes

Wenhui Liu

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

Received: Apr. 21^{st}, 2023; accepted: May 23^{rd}, 2023; published: May 30^{th}, 2023

Abstract

Linear codes with a few weights are widely studied due to their important applications

文章引用: 刘文辉. 几类 p 元线性码的构造[J]. 理论数学, 2023, 13(5): 1389-1402.
DOI: 10.12677/pm.2023.135142

in secret sharing schemes, authentication codes, association schemes, strongly regular graphs, etc. In this paper, several classes of p-ary linear codes are constructed by selecting a new definition set, and the parameters and weight distributions of the codes are determined by exponential sums. Finally, it is shown that the linear codes constructed in this paper are minimal linear codes in most cases, which can be used to design secret sharing schemess with good access structures.

Keywords

Linear Code, Defining Set, Exponential Sum, Weight Distribution

1. 引言

设 $\mathbb{F}_q$ 为含有 q 个元素的有限域, 其中 $q = p^m$, p 为奇素数且 m 为正整数, $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$. 有限域 $\mathbb{F}_p$ 上的 n 维向量空间 $\mathbb{F}_p^n$ 的 k 维线性子空间 C 称为码长为 n, 信息位为 k 的 p 元 $[n, k]$ 线性码, 码 C 中的每一个向量称为码字. 令 A_i 表示码 C 中重量为 i 的码字个数, 则码 C 的重量计数器定义为 $1 + A_1z + A_2z^2 + \ldots + A_nz^n$, 序列 $(1, A_1, A_2, \ldots, A_n)$ 称为码 C 的重量分布. 若 $(A_1, A_2, \ldots, A_n)$ 中不为 0 的 A_i 的个数为 t, 则称码 C 为 t 重码. 线性码由于具有良好的代数结构以及易于描述和加解密等特性, 所以在通信、数据存储和信息安全等领域具有重要的应用, 特别地, 具有较低重量的线性码在关联方案 [1], 秘密共享方案 [2], 强正则图 [3] 等领域具有重要的意义, 所以被广泛研究.

Baumert [4] 在 1972 年首次提出利用定义集构造低重线性码的方法. 2007 年, Ding [5] 开始借助指数和理论进一步通过此方法构造具有较低重量的线性码. 这类线性码参数的好坏由定义集决定, 而且很多已知的线性码均可通过此方法选取恰当的定义集得到, 因此很多学者尝试选取不同的定义集进行构造, 相关结果可以参考文献 [6–14] 等, 这些工作都极大丰富了线性码的研究.

近几年, Ding 等人 [15] 和 Li 等人 [16] 研究具有以下形式的线性码

$$C_D = \{(\mathrm{Tr}(\alpha x))_{x \in D} \mid \alpha \in \mathbb{F}_q\}, \tag{1}$$

选取的定义集分别为 $D = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}\left(x^2\right) = 0\right\}$ 和 $D = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}\left(x^2 + x\right) = 0\right\}$, 构造了几类低重线性码. 2021 年, Ouyang 等人 [17] 将以上构造进行推广, 即基于定义集

$$D = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}\left(ax^2 + bx\right) = 0\right\},$$

其中 $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$, 构造了几类线性码. 受以上工作的启发, 本文继续对 (1) 式的线性码进行研究, 选取定义集为

$$D = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}\left(ax^2 + bx\right) = \gamma\right\}, \tag{2}$$

其中 $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$ 且 $\gamma \in \mathbb{F}_p^*$, 构造了几类新参数的 p 元线性码并确定了码的参数及重量分布. 通过 Aschikhmin-Barg 条件说明本文构造的线性码是极小线性码, 可以用来设计具有良好访问结构的秘密共享方案. 显然, 当 (2) 式中的 $(a,b,c) = (1,0,0)$ 且 $\gamma = 0$ 时, 所得结果即为 Ding 等人的结论; 当 (2) 式中的 $(a,b,c) = (1,1,0)$ 且 $\gamma = 0$ 时, 所得结果即为 Li 等人的结论; 当 (2) 式中的 $\gamma = 0$ 时, 所得结果即为 Ouyang 等人的结论.

全文组织结构如下, 第二部分介绍一些预备知识; 第三部分研究了 m 为奇数和 m 为偶数两种情形下码 C_D 的参数及重量分布; 第四部分总结全文.

2. 基础知识

首先介绍有限域中的一些基础知识.

对任意的 $a \in \mathbb{F}_q$, $\mathbb{F}_q$ 上的加法特征 [18] 定义为 $\chi_a(x) = \zeta_p^{\mathrm{Tr}(ax)}$, 其中 $x \in \mathbb{F}_q$, $\zeta_p = e^{2\pi\sqrt{-1}/p}$ 为 $\mathbb{F}_q$ 的一个 p 次本原单位根. 若 $a = 1$, 称 χ_1 为 $\mathbb{F}_q$ 的加法主特征. 加法特征满足正交性 [18]

$$\sum_{x\in\mathbb{F}_q} \chi_1(ax) = \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(ax)} = \begin{cases} q, & a = 0, \\ 0, & a \in \mathbb{F}_q^*. \end{cases} \tag{3}$$

令 ξ 为 $\mathbb{F}_q^*$ 的一个生成元, 对任意的 $0 \le j \le q-2$, $\mathbb{F}_q$ 上的乘法特征 [18]定义为

$$\psi_j\left(\xi^k\right) = e^{2\pi\sqrt{-1}jk/(q-1)},\ k = 0, 1, \ldots, q-2.$$

有限域上的任何一个乘法特征 ψ 均可以用此形式表示. 若 $j = (q-1)/2$, 则 $\psi_{(q-1)/2}$ 称为 $\mathbb{F}_q$ 的二次乘法特征, 记为 η. 本文中用 η 和 $\bar{\eta}$ 分别表示 $\mathbb{F}_q$ 和 $\mathbb{F}_p$ 上的二次乘法特征, 则任意 $x \in \mathbb{F}_p^*$: 若 m 为偶数, 则 $\eta(x) = 1$; 若 m 为奇数, 则 $\eta(x) = \bar{\eta}(x)$. 这个性质非常重要, 本文正是因为该性质所以才分 m 为奇数和 m 为偶数两种情形分开讨论. $\mathbb{F}_q$ 上二次特征的高斯和定义为 $G(\eta) = \sum_{x\in\mathbb{F}_q^*} \eta(x)\chi(x)$, 其中 η 和 χ 分别为 $\mathbb{F}_q$ 上的二次乘法和加法特征. 关于二次高斯和, 有如下两个重要结论.

引理1. [18] 设 $\mathbb{F}_q$ 为含有 q 个元素的有限域. 则

$$G_m = \sum_{x\in\mathbb{F}_{p^m}^*} \eta(x)\chi(x) = (-1)^{m-1}\sqrt{-1}^{\frac{(p-1)^2 m}{4}}\sqrt{p^m}.$$

由引理 1, 显然有 $G_1 = (-1)^{\frac{p-1}{4}} p^{\frac{1}{2}}$. 则

$$G_{m+1} = G_m G_1 = (-1)^{\frac{(p-1)(m+1)}{4}} p^{\frac{m+1}{2}} \text{ 且 } G_{m+2} = G_m G_1^2 = (-1)^{m-1}(-1)^{\frac{(p-1)^2(m+1)}{4}} p^{\frac{m+2}{2}}.$$

引理2. [18] 若 $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$ 且 $a_2\neq 0$. 则

$$\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}(f(x))}=\zeta_p^{\mathrm{Tr}\left(a_0-a_1^2(4a_2)^{-1}\right)}\eta\left(a_2\right)G(\eta,\chi).$$

下面介绍极小码的相关知识.

线性码 C 中码字 $\mathbf{c}=(c_1,c_2,\ldots,c_n)$ 的支撑定义为

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

若对任意的两个码字 $\mathbf{u},\mathbf{v}\in C$, 有 $\mathrm{Suppt}(\mathbf{v})\subseteq\mathrm{Suppt}(\mathbf{u})$, 则称 $\mathbf{u}$ 覆盖 $\mathbf{v}$. 若码 C 的一个非零码字 $\mathbf{c}$ 只覆盖它的纯量倍数, 则称 $\mathbf{c}$ 是一个极小码字. 若线性码 C 中的所有码字均是极小码字, 则称线性码 C 是极小线性码 [19].

关于极小码的判定, 有如下充分条件.

引理3. [20] (Aschikhmin-Barg 条件) 若 $\mathbb{F}_p$ 上线性码 C 的最大汉明重量 $w_{\max}$ 和最小汉明重量 $w_{\min}$ 满足

$$\frac{w_{\min}}{w_{\max}}>\frac{p-1}{p},$$

则码 C 是极小码.

为了方便, 下文中记 $M=\mathrm{Tr}(\frac{b^2}{a})$, $\omega=-\gamma$.

3. 主要结论及证明

3.1. m 为奇数时码 C_D 的参数及其重量分布

本小节讨论 m 为奇数时, 基于 (2) 式构造的 (1) 式线性码 C_D 的码长, 维数以及重量分布. 首先计算码长.

引理4. 设 C_D 的码长为 n, 则

$$n=\begin{cases}p^{m-1}, & \omega-\frac{M}{4}=0,\\ p^{m-1}+\frac{1}{p}G_{m+1}\eta(a)\overline{\eta}(\omega-\frac{M}{4}), & \omega-\frac{M}{4}\neq 0.\end{cases}$$

证明 由 (3) 式可得

$$\begin{aligned}n&=\frac{1}{p}\sum_{x\in\mathbb{F}_q^*}\left(\sum_{y\in\mathbb{F}_p}\zeta_p^{y(\mathrm{Tr}(ax^2+bx)+\omega)}\right)\\&=\frac{1}{p}\sum_{x\in\mathbb{F}_q}\left(\sum_{y\in\mathbb{F}_p}\zeta_p^{y(\mathrm{Tr}(ax^2+bx)+\omega)}\right)-\frac{1}{p}\sum_{y\in\mathbb{F}_p}\zeta_p^{\omega y}\\&=\frac{1}{p}\sum_{x\in\mathbb{F}_q}\left(1+\sum_{y\in\mathbb{F}_p^*}\zeta_p^{y(\mathrm{Tr}(ax^2+bx)+\omega)}\right)\end{aligned}$$

$$
\begin{aligned}
&= p^{m-1} + \frac{1}{p} G_m \eta(a) \sum_{y\in\mathbb{F}_p^*} \zeta_p^{(\omega-\frac{M}{4})y} \bar{\eta}(y) \\
&= \begin{cases} p^{m-1}, & \omega - \frac{M}{4} = 0, \\ p^{m-1} + \frac{1}{p} G_{m+1} \eta(a) \bar{\eta}(\omega - \frac{M}{4}), & \omega - \frac{M}{4} \neq 0. \end{cases}
\end{aligned} \tag{4}
$$

下面开始确定线性码 C_D 中非零码字的汉明重量. 用 $\sharp A$ 表示集合 A 中元素的个数. 设

$$
N_\rho(a,b) = \sharp \left\{ x \in \mathbb{F}_{p^m}^* \mid \operatorname{Tr}\left(ax^2+bx\right) + \omega = 0, \operatorname{Tr}(\rho x) = 0 \right\}.
$$

则码字 $c_\rho \in C_D$ $\left(\rho \in \mathbb{F}_q^*\right)$ 的汉明重量可以表示为

$$
\operatorname{wt}\left(c_\rho\right) = n - N_\rho(a,b), \tag{5}
$$

其中 n 为码 C_D 的码长. 显然

$$
\begin{aligned}
N_\rho(a,b) &= \frac{1}{p^2} \sum_{x\in\mathbb{F}_q^*} \left(\sum_{y\in\mathbb{F}_p} \zeta_p^{y(\operatorname{Tr}(ax^2+bx)+\omega)} \right) \left(\sum_{z\in\mathbb{F}_p} \zeta_p^{z\operatorname{Tr}(\rho x)} \right) \\
&= \frac{1}{p^2} \sum_{x\in\mathbb{F}_q} \left(1 + \sum_{y\in\mathbb{F}_p^*} \zeta_p^{y(\operatorname{Tr}(ax^2+bx)+\omega)} \right) \left(1 + \sum_{z\in\mathbb{F}_p^*} \zeta_p^{z\operatorname{Tr}(\rho x)} \right) - \frac{1}{p} \sum_{y\in\mathbb{F}_p} \zeta_p^{\omega y} \\
&= p^{m-2} + \frac{1}{p^2} \left(\Omega_1 + \Omega_2 + \sum_{x\in\mathbb{F}_q} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{z\operatorname{Tr}(\rho x)} \right) \\
&= p^{m-2} + \frac{1}{p^2} \left(\Omega_1 + \Omega_2 \right),
\end{aligned} \tag{6}
$$

其中

$$
\Omega_1 = \sum_{x\in\mathbb{F}_q} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{y\left(\operatorname{Tr}\left(ax^2+bx\right)+\omega\right)} = \begin{cases} 0, & \omega - \frac{M}{4} \neq 0, \\ G_{m+1} \eta(a) \bar{\eta}(\omega - \frac{M}{4}), & \omega - \frac{M}{4} = 0. \end{cases} \tag{7}
$$

$$
\Omega_2 = \sum_{y\in\mathbb{F}_p^*} \sum_{z\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q} \zeta_p^{\operatorname{Tr}\left(ayx^2+(by+z\rho)x\right)+\omega y}.
$$

下面计算 Ω_2 的值。

引理5. 设 $\Omega_2 = \sum\limits_{y\in\mathbb{F}_p^*} \sum\limits_{z\in\mathbb{F}_p^*} \sum\limits_{x\in\mathbb{F}_q} \zeta_p^{\operatorname{Tr}\left(ayx^2+(by+z\rho)x\right)+\omega y}$.

DOI: 10.12677/pm.2023.135142

(1) 若 $\omega-\frac{M}{4}=0$, 则

$$\Omega_2=\begin{cases}0, & \operatorname{Tr}\left(\frac{\rho^2}{a}\right)=0,\\ (p-1)G_{m+1}\eta(a)\bar{\eta}\left(-\operatorname{Tr}\left(\frac{\rho^2}{a}\right)\right), & \operatorname{Tr}\left(\frac{\rho^2}{a}\right)\neq 0 \text{ 且 } \operatorname{Tr}\left(\frac{b\rho}{a}\right)=0,\\ -G_{m+1}\eta(a)\bar{\eta}\left(-\operatorname{Tr}\left(\frac{\rho^2}{a}\right)\right), & \operatorname{Tr}\left(\frac{\rho^2}{a}\right)\cdot\operatorname{Tr}\left(\frac{b\rho}{a}\right)\neq 0.\end{cases}$$

(2) 若 $\omega-\frac{M}{4}\neq 0$, 则

$$\Omega_2=\begin{cases}(p-1)G_{m+1}\eta(a)\bar{\eta}(\omega-\frac{M}{4}), & \operatorname{Tr}\left(\frac{\rho^2}{a}\right)=\operatorname{Tr}\left(\frac{b\rho}{a}\right)=0,\\ -G_{m+1}\eta(a)\bar{\eta}(\omega-\frac{M}{4}), & \operatorname{Tr}\left(\frac{\rho^2}{a}\right)=0 \text{ 且 } \operatorname{Tr}\left(\frac{b\rho}{a}\right)\neq 0,\\ -G_{m+1}\eta(a)\left(\bar{\eta}\left(-\operatorname{Tr}\left(\frac{\rho^2}{a}\right)\right)+\bar{\eta}(\omega-\frac{M}{4})\right), & \left(\operatorname{Tr}\left(\frac{\rho^2}{a}\right)\neq 0 \text{ 且 } \operatorname{Tr}\left(\frac{b\rho}{a}\right)=0\right) \text{ 或者}\\ & \left(\operatorname{Tr}\left(\frac{\rho^2}{a}\right)\cdot\operatorname{Tr}\left(\frac{b\rho}{a}\right)\neq 0 \text{ 且 } 4\omega\operatorname{Tr}(\frac{\rho^2}{a})\right.\\ & \left.+\operatorname{Tr}^2\left(\frac{bp}{a}\right)\neq M\operatorname{Tr}\left(\frac{\rho^2}{a}\right)\right),\\ G_{m+1}\eta(a)\left((p-1)\bar{\eta}\left(-\operatorname{Tr}\left(\frac{\rho^2}{a}\right)\right)-\bar{\eta}(\omega-\frac{M}{4})\right), & \operatorname{Tr}\left(\frac{\rho^2}{a}\right)\cdot\operatorname{Tr}\left(\frac{b\rho}{a}\right)\neq 0 \text{ 且 } 4\omega\operatorname{Tr}(\frac{\rho^2}{a})\\ & +\operatorname{Tr}^2\left(\frac{bp}{a}\right)=M\operatorname{Tr}\left(\frac{\rho^2}{a}\right).\end{cases}$$

证明

$$\begin{aligned}\Omega_2&=\sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\zeta_p^{\operatorname{Tr}\left(ayx^2+(by+z\rho)x\right)+\omega y}\\ &=\sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*}G_m\eta(ay)\zeta_p^{\operatorname{Tr}(-\frac{(by+z\rho)^2}{4ay})+\omega y}\\ &=G_m\eta(a)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}(y)\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-\frac{\operatorname{Tr}\left(\frac{\rho^2}{a}\right)z^2}{4y}-\frac{\operatorname{Tr}\left(\frac{b\rho}{a}\right)z}{2}}.\end{aligned}$$

只证明 $\omega-\frac{M}{4}\neq 0$ 的情形, $\omega-\frac{M}{4}=0$ 证明方法类似. 下面分四种情形计 Ω_2.

情形 1: $\operatorname{Tr}\left(\frac{\rho^2}{a}\right)=0$ 且 $\operatorname{Tr}\left(\frac{b\rho}{a}\right)=0$. 则

$$\begin{aligned}\Omega_2&=(p-1)G_m\eta(a)\sum_{y\in F_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}(y)=(p-1)G_m\eta(a)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}\Big(\Big(\omega-\frac{M}{4}\Big)y\Big)\bar{\eta}\Big(\omega-\frac{M}{4}\Big)\\ &=(p-1)G_{m+1}\eta(a)\bar{\eta}\Big(\omega-\frac{M}{4}\Big).\end{aligned}$$

情形 2: $\operatorname{Tr}\left(\frac{\rho^2}{a}\right)=0$ 且 $\operatorname{Tr}\left(\frac{b\rho}{a}\right)\neq 0$. 则

$$\begin{aligned}\Omega_2&=G_m\eta(a)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}(y)\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-\frac{\mathrm{T}\left(\frac{bp}{a}\right)z}{2}}=-G_m\eta(a)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}(y)\\ &=-G_{m+1}\eta(a)\bar{\eta}\Big(\omega-\frac{M}{4}\Big).\end{aligned}$$

情形 3: $\mathrm{Tr}\left(\frac{\rho^2}{a}\right) \neq 0$ 且 $\mathrm{Tr}\left(\frac{b\rho}{a}\right) \doteq 0$. 则

$$\begin{aligned}\Omega_2 &= G_m\eta(a)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}(y)\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-\frac{\mathrm{Tr}\left(\frac{\rho^2}{a}\right)z^2}{4y}} \\ &= G_m\eta(a)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}(y)\sum_{z\in\mathbb{F}_p}\zeta_p^{-\frac{\mathrm{Tr}\left(\frac{\rho^2}{a}\right)z^2}{4y}} - G_m\eta(a)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}(y).\end{aligned}$$

由引理 2 可得

$$\begin{aligned}\Omega_2 &= G_{m+1}\eta(a)\bar{\eta}\left(-\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y} - G_m\eta(a)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}(y) \\ &= -G_{m+1}\eta(a)\left(\bar{\eta}\left(-\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right) + \bar{\eta}(\omega-\tfrac{M}{4})\right).\end{aligned}$$

情形 4: $\mathrm{Tr}\left(\frac{\rho^2}{a}\right) \neq 0$ 且 $\mathrm{Tr}\left(\frac{b\rho}{a}\right) \neq 0$. 则

$$\Omega_2 = G_m\eta(a)\sum_{y\in\mathbb{F}_p^*}\zeta_p^{(\omega-\frac{M}{4})y}\bar{\eta}(y)\sum_{z\in\mathbb{F}_p}\zeta_p^{-\frac{\mathrm{Tr}\left(\frac{\rho^2}{a}\right)z^2}{4y}-\frac{\mathrm{Tr}\left(\frac{bp}{a}\right)z}{2}} - G_{m+1}\eta(a)\bar{\eta}(\omega-\frac{M}{4}).$$

由引理 2 可得

$$\Omega_2 = G_{m+1}\eta(a)\sum_{y\in F_p^*}\zeta_p^{\frac{\left(4\,\mathrm{Tr}(\frac{\rho^2}{a})\omega+\mathrm{Tr}^2\left(\frac{bp}{a}\right)-M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)y}{4\mathrm{Tr}\left(\frac{\rho^2}{a}\right)}}\bar{\eta}\left(-\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right) - G_{m+1}\eta(a)\bar{\eta}(\omega-\frac{M}{4}).$$

若 $4\,\mathrm{Tr}(\frac{\rho^2}{a})\omega + \mathrm{Tr}^2\left(\frac{bp}{a}\right) = M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right)$, 则

$$\Omega_2 = G_{m+1}\eta(a)\left((p-1)\bar{\eta}\left(-\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right) - \bar{\eta}(\omega-\frac{M}{4})\right).$$

若 $4\,\mathrm{Tr}(\frac{\rho^2}{a})\omega + \mathrm{Tr}^2\left(\frac{bp}{a}\right) \neq M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right)$, 则

$$\begin{aligned}\Omega_2 &= -G_{m+1}\eta(a)\bar{\eta}\left(-\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right) - G_{m+1}\eta(a)\bar{\eta}(\omega-\frac{M}{4}) \\ &= -G_{m+1}\eta(a)\left(\bar{\eta}(\omega-\frac{M}{4}) + \bar{\eta}\left(-\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)\right).\end{aligned}$$

□

注意到任意 $\rho \in \mathbb{F}_{p^m}^*$, $wt\,(c_\rho) \neq 0$, 则 C_D 的维数为 m. 综合以上结果可得如下结论.

命题1. 设 m 为奇数, 定义集为 (2) 式. 则 (1) 式定义的线性码 C_D 码长为 n, 维数为 m. 非零码字的汉明重量为

$$\mathrm{wt}\,(c_\rho) = (p-1)p^{m-2} + N.$$

(1) 若 $\omega - \frac{M}{4} = 0$, 则 $n = p^{m-1}$. 且

$$N=\begin{cases} 0, & \mathrm{Tr}\left(\frac{\rho^2}{a}\right)=0, \\ -\frac{p-1}{p^2}G_{m+1}\eta(a), & \mathrm{Tr}\left(\frac{b\rho}{a}\right)=0 \text{ 且 } \bar{\eta}\left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)=-1, \\ \frac{p-1}{p^2}G_{m+1}\eta(a), & \mathrm{Tr}\left(\frac{b\rho}{a}\right)=0 \text{ 且 } \bar{\eta}\left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)=1, \\ \frac{1}{p^2}G_{m+1}\eta(a), & \mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0 \text{ 且 } \bar{\eta}\left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)=-1, \\ -\frac{1}{p^2}G_{m+1}\eta(a), & \mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0 \text{ 且 } \bar{\eta}\left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)=1. \end{cases}$$

(2) 若 $\omega-\frac{M}{4}\neq 0$, 则 $n=p^{m-1}+\frac{1}{p}G_{m+1}\eta(a)\bar{\eta}(\omega-\frac{M}{4})$. 且

$$N=\begin{cases} 0, & \mathrm{Tr}\left(\frac{\rho^2}{a}\right)=\mathrm{Tr}\left(\frac{b\rho}{a}\right)=0, \\ \frac{1}{p}G_{m+1}\eta(a)\bar{\eta}(\omega-\frac{M}{4}), & \mathrm{Tr}\left(\frac{\rho^2}{a}\right)=0 \text{ 且 } \mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0, \\ \frac{1}{p^2}G_{m+1}\eta(a)\left(p\bar{\eta}\left(\omega-\frac{M}{4}\right)+1\right), & \left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\neq 0,\ \mathrm{Tr}\left(\frac{b\rho}{a}\right)=0 \text{ 且 } \bar{\eta}\left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)=-1\right) \text{ 或者} \\ & \left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\neq 0,\ \mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0,\ 4\,\mathrm{Tr}(\frac{\rho^2}{a})\omega+\mathrm{Tr}^2\left(\frac{bp}{a}\right)\neq\right. \\ & \left. M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right) \text{ 且 } \bar{\eta}\left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)=-1\right), \\ \frac{1}{p^2}G_{m+1}\eta(a)(p\bar{\eta}(\omega-\frac{M}{4})-1), & \left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\neq 0,\ \mathrm{Tr}\left(\frac{b\rho}{a}\right)=0 \text{ 且 } \bar{\eta}\left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)=1\right) \text{ 或者} \\ & \left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\neq 0,\ \mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0,\ 4\,\mathrm{Tr}(\frac{\rho^2}{a})\omega+\mathrm{Tr}^2\left(\frac{bp}{a}\right)\neq\right. \\ & \left. M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right) \text{ 且 } \bar{\eta}\left(\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)=1\right), \\ \frac{1}{p^2}G_{m+1}\eta(a)\bar{\eta}(\omega-\frac{M}{4}), & \mathrm{Tr}\left(\frac{\rho^2}{a}\right)\neq 0,\ \mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0 \text{ 且 } 4\,\mathrm{Tr}(\frac{\rho^2}{a})\omega+\mathrm{Tr}^2\left(\frac{bp}{a}\right)= \\ & M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right). \end{cases}$$

证明 由 (4), (5) 和 (6) 式可得

$$\begin{aligned} \mathrm{wt}\left(c_\rho\right) &= p^{m-1}+\frac{1}{p}\Omega_1-\left(p^{m-2}+\frac{1}{p^2}\left(\Omega_1+\Omega_2\right)\right) \\ &= (p-1)p^{m-2}+\frac{p-1}{p^2}\Omega_1-\frac{1}{p^2}\Omega_2, \end{aligned}$$

则

$$N=\frac{p-1}{p^2}\Omega_1-\frac{1}{p^2}\Omega_2.$$

再结合 (7) 式和引理 5 显然可得结论. □

注记1. 对于命题 1 (1) 中的码 C_D, 当 $m\geq 5$ 时:

若 $G_{m+1}\eta(a)=(-1)^{\frac{(p-1)(m+1)}{4}}p^{\frac{m+1}{2}}\eta(a)=\pm p^{\frac{m+1}{2}}$, 则

$$\frac{w_{\min}}{w_{\max}}=\frac{(p-1)(p^{m-2}-p^{\frac{m-3}{2}})}{(p-1)(p^{m-2}+p^{\frac{m-3}{2}})}>\frac{p-1}{p}.$$

对于命题 1 (2) 中的码 C_D, 当 $m\geq 5$ 时:

若 $G_m\eta(a)=(-1)^{m-1}\sqrt{-1}^{\frac{(p-1)^2m}{4}}\sqrt{p^m}\eta(a)\cdot\bar{\eta}(\omega-\frac{M}{4})=p^{\frac{m}{2}}$, 则

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

若 $G_m\eta(a) = (-1)^{m-1}\sqrt{-1}^{\frac{(p-1)^2m}{4}}\sqrt{p^m}\eta(a)\cdot\bar{\eta}(\omega-\frac{M}{4}) = -p^{\frac{m}{2}}$, 则

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

由引理 3 可知, 本节构造的线性码在多数情况下是极小码.

下面开始计算重量分布. 首先, 给出两个计算频率需要的引理, 其中 m 均为奇数.

引理6. [17] 设 $t\in\mathbb{F}_p$. 若 $N(t)=\sharp\left\{x\in\mathbb{F}_{p^m}\mid \mathrm{Tr}\left(\frac{x^2}{a}\right)=t\right\}$. 则

$$N(t)=\begin{cases} p^{m-1}, & t=0,\\ p^{m-1}+\frac{1}{p}G_{m+1}\eta(a)\bar{\eta}(-t), & t\neq 0.\end{cases}$$

引理7. [17] 设 $t\in\mathbb{F}_p$, 且 $a,b\in\mathbb{F}_{p^m}^*$. 则 $N(t,0)=\sharp\left\{x\in\mathbb{F}_{p^m}\mid \mathrm{Tr}\left(\frac{x^2}{a}\right)=t, \mathrm{Tr}\left(\frac{bx}{a}\right)=0\right\}$.

若 $t=0$, 则

$$N(0,0)=\begin{cases} p^{m-2}, & p\mid M,\\ p^{m-2}+\frac{p-1}{p^2}G_{m+1}\eta(a)\bar{\eta}(-M), & p\nmid M.\end{cases}$$

若 $t\neq 0$, 则

$$N(t,0)=\begin{cases} p^{m-2}+\frac{1}{p}G_{m+1}\eta(a)\bar{\eta}(-t), & p\mid M,\\ p^{m-2}-\frac{1}{p^2}G_{m+1}\eta(a)\bar{\eta}(-M), & p\nmid M.\end{cases}$$

以上结果得到之后, 则有下面结论.

定理1. 设 p 为奇素数, m 为奇数, 定义集如 (2) 式所示且 $\omega-\frac{M}{4}=0$. 则 (1) 式定义的码 C_D 为 $[p^{m-1},m]$ 线性码, 其重量分布如 表 1 所示.

Table 1. The weight distribution of code C_D in Theorem 1

表 1. 定理 1 中码 C_D 的重量分布

重量	频数
0	1
$(p-1)p^{m-2}$	A_{ω_1}
$(p-1)\left(p^{m-2}+\frac{1}{p^2}G_{m+1}\eta(a)\right)$	A_{ω_2}
$(p-1)\left(p^{m-2}-\frac{1}{p^2}G_{m+1}\eta(a)\right)$	A_{ω_3}
$(p-1)p^{m-2}+\frac{1}{p^2}G_{m+1}\eta(a)$	A_{ω_4}
$(p-1)p^{m-2}-\frac{1}{p^2}G_{m+1}\eta(a)$	A_{ω_5}

其中, $A_{\omega_1}=p^{m-1}-1$.

若 $\bar{\eta}(-M) = -1$, 则 $A_{\omega_2} = A_{\omega_3} = \frac{1}{2}(p-1)(p^{m-2} + \frac{1}{p^2}G_{m+1}\eta(a))$.

$$A_{\omega_4} = \frac{1}{2}\frac{1}{p^2G_{m+1}\eta(a)}((1-p)G_{m+1}^2\eta^2(a) + (p^m + p^{m+2} - 2p^{m+1})G_{m+1}\eta(a) + (p^{m+3} - p^{m+2})),$$
$$A_{\omega_5} = \frac{1}{2}\frac{1}{p^2G_{m+1}\eta(a)}((1-p)G_{m+1}^2\eta^2(a) + (p^m + p^{m+2} - 2p^{m+1})G_{m+1}\eta(a) + (p^{m+2} - p^{m+3})).$$

若 $\bar{\eta}(-M) = 1$, 则 $A_{\omega_2} = A_{\omega_3} = \frac{1}{2}(p-1)(p^{m-2} - \frac{1}{p^2}G_{m+1}\eta(a))$.

$$A_{\omega_4} = \frac{1}{2}\frac{1}{p^2G_{m+1}\eta(a)}((p-1)G_{m+1}^2\eta^2(a) + (p^m + p^{m+2} - 2p^{m+1})G_{m+1}\eta(a) + (p^{m+3} - p^{m+2})),$$
$$A_{\omega_5} = \frac{1}{2}\frac{1}{p^2G_{m+1}\eta(a)}((p-1)G_{m+1}^2\eta^2(a) + (p^m + p^{m+2} - 2p^{m+1})G_{m+1}\eta(a) + (p^{m+2} - p^{m+3})).$$

证明 由命题 1 (1) 可知, C_D 中非零码字的汉明重量为 表 1 中第 1 列所示. 将 表 1 中第 1 列的值从上至下依次记为 w_1, w_2, w_3, w_4, w_5, 则对应的频数记为 A_{w_1}, A_{w_2}, A_{w_3}, A_{w_4}, A_{w_5}.

由命题 1 和引理 6 可得

$$A_{w_1} = N(0) - 1 = p^{m-1} - 1.$$

因为 $\omega - \frac{M}{4} = 0$, 所以 $M \neq 0$, 即 $p \nmid M$. 由命题 1 和引理 7 可得 $A_{\omega_2} = A_{\omega_3} = \frac{1}{2}(p-1)(p^{m-2} - \frac{1}{p^2}G_{m+1}\eta(a)\bar{\eta}(-M))$.

由 Pless 幂矩公式 [19] 可得

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} + A_{w_4} + A_{w_5} = p^m - 1, \\ w_1A_{w_1} + w_2A_{w_2} + w_3A_{w_3} + w_4A_{w_5} + w_5A_{w_5} = (p-1)np^{m-1}. \end{cases} \tag{8}$$

因此, 若 $\bar{\eta}(-M)) = -1$, 则 $A_{\omega_2} = A_{\omega_3} = \frac{1}{2}(p-1)(p^{m-2} + \frac{1}{p^2}G_{m+1}\eta(a))$. 再结合 (8) 式可得

$$A_{\omega_4} = \frac{1}{2}\frac{1}{p^2G_{m+1}\eta(a)}((1-p)G_{m+1}^2\eta^2(a) + (p^m + p^{m+2} - 2p^{m-1})G_{m+1}\eta(a) + (p^{m+3} - p^{m+2})),$$
$$A_{\omega_5} = \frac{1}{2}\frac{1}{p^2G_{m+1}\eta(a)}((1-p)G_{m+1}^2\eta^2(a) + (p^m + p^{m+2} - 2p^{m-1})G_{m+1}\eta(a) + (p^{m+2} - p^{m+3})).$$

若 $\bar{\eta}(-M) = 1$, 则 $A_{\omega_2} = A_{\omega_3} = \frac{1}{2}(p-1)(p^{m-2} - \frac{1}{p^2}G_{m+1}\eta(a))$. 再结合 (8) 式可得

$$A_{\omega_4} = \frac{1}{2}\frac{1}{p^2G_{m+1}\eta(a)}((p-1)G_{m+1}^2\eta^2(a) + (p^m + p^{m+2} - 2p^{m-1})G_{m+1}\eta(a) + (p^{m+3} - p^{m+2})),$$
$$A_{\omega_5} = \frac{1}{2}\frac{1}{p^2G_{m+1}\eta(a)}((p-1)G_{m+1}^2\eta^2(a) + (p^m + p^{m+2} - 2p^{m-1})G_{m+1}\eta(a) + (p^{m+2} - p^{m+3})).$$

因此得到码 C_D 的重量分布. □

下面的例子可由 Magma 程序验证.

例1. 设定义集如 (2) 式所示, 且 $p = 5$, $m = 3$, $a = 2$, $b = 4$, $\omega = \mathrm{Tr}(2)$. 则 C_D 为 $[25, 3]$ 线性

码, 其重量计数器为 $1+24z^{20}+12z^{24}+12z^{16}+48z^{21}+28z^{19}$, 与定理 1 的结论一致.

例2. 设定义集如 (2) 式所示, 且 $p=7,\ m=5,\ a=1,\ b=2,\ \omega=\mathrm{Tr}(1)$. 则 C_D 为 $[2401,5]$ 线性码, 其重量计数器为 $1+2400z^{2058}+1050z^{2016}+1050z^{2100}+6006z^{2051}+6300z^{2065}$, 与定理 1 的结论一致.

3.2. m 为偶数时码 C_D 的参数及其重量分布

本小节讨论 m 为偶数时, 基于 (2) 式构造的 (1) 式线性码 C_D 的码长, 维数以及重量分布. 由于证明方法和 m 为奇数的情形类似, 所以不再赘述.

引理8. 设 C_D 的码长为 n, 则

$$n=\begin{cases} p^{m-1}+\frac{p-1}{p}G_m\eta(a), & \omega-\frac{M}{4}=0,\\ p^{m-1}-\frac{1}{p}G_m\eta(a), & \omega-\frac{M}{4}\neq 0.\end{cases}$$

命题2. 设 m 为偶数, 定义集为 (2) 式. 则 (1) 式定义的线性码 C_D 码长为 n, 维数为 m. 非零码字的汉明重量为

$$\mathrm{wt}\,(c_\rho)=(p-1)p^{m-2}+N.$$

(1) 若 $\omega-\frac{M}{4}=0$, 则 $n=p^{m-1}+\frac{p-1}{p}G_m\eta(a)$. 且

$$N=\begin{cases} 0, & \mathrm{Tr}\left(\frac{\rho^2}{a}\right)=\mathrm{Tr}(\frac{b\rho}{a})=0,\\ \frac{p-1}{p}G_m\eta(a), & \mathrm{Tr}\left(\frac{\rho^2}{a}\right)\cdot\mathrm{Tr}(\frac{b\rho}{a})=0 \text{ 且 } \mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq\mathrm{Tr}\left(\frac{\rho^2}{a}\right),\\ \frac{p-2}{p}G_m\eta(a), & \mathrm{Tr}\left(\frac{\rho^2}{a}\right)\cdot\mathrm{Tr}(\frac{b\rho}{a})\neq 0.\end{cases}$$

(1) 若 $\omega-\frac{M}{4}\neq 0$, 则 $n=p^{m-1}-\frac{1}{p}G_m\eta(a))$. 且

$$N=\begin{cases} 0, & (\mathrm{Tr}\left(\frac{\rho^2}{a}\right)=\mathrm{Tr}\left(\frac{b\rho}{a}\right)=0) \text{ 或者 } (\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\neq 0,\ \mathrm{Tr}\left(\frac{b\rho}{a}\right)=0 \text{ 且}\\ & \bar{\eta}(-(\omega-\frac{M}{4})\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right))=-1)) \text{ 或者 } (\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\cdot\mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0,\\ & 4\,\mathrm{Tr}(\frac{\rho^2}{a})\omega+\mathrm{Tr}^2\left(\frac{bp}{a}\right)\neq M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right) \text{ 且 } \bar{\eta}(4\omega\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right)+\mathrm{Tr}^2\left(\frac{b\rho}{a}\right)\\ & -M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right))=-1),\\ \frac{-1}{p}G_m\eta(a), & (\mathrm{Tr}\left(\frac{\rho^2}{a}\right)=0,\mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0) \text{ 或者 } (\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\cdot\mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0 \text{ 且}\\ & 4\,\mathrm{Tr}(\frac{\rho^2}{a})\omega+\mathrm{Tr}^2\left(\frac{bp}{a}\right)=M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right)),\\ \frac{-2}{p}G_m\eta(a), & (\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\neq 0,\mathrm{Tr}\left(\frac{b\rho}{a}\right)=0,\bar{\eta}(-(\omega-\frac{M}{4})\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right))=1)) \text{ 或者}\\ & (\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\cdot\mathrm{Tr}\left(\frac{b\rho}{a}\right)\neq 0,4\omega\,\mathrm{Tr}(\frac{\rho^2}{a})+\mathrm{Tr}^2\left(\frac{bp}{a}\right)\neq M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right),\\ & \bar{\eta}\left(4\omega\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right)+\mathrm{Tr}^2\left(\frac{b\rho}{a}\right)-M\,\mathrm{Tr}\left(\frac{\rho^2}{a}\right)\right)=1).\end{cases}$$

注记2. 对于命题 2 两种情形下的码 C_D, 当 $m\geq 6$ 时, C_D 是极小线性码. 证明方法与注记 1 一样, 这里再不赘述.

下面给出计算频率分布需要的两个引理, 其中 m 均为偶数.

引理9. [17] 设 $t \in \mathbb{F}_p$, 若 $N(t) = \sharp\left\{x \in \mathbb{F}_{p^m} \mid \mathrm{Tr}\left(\frac{x^2}{a}\right) = t\right\}$. 则

$$N(t) = \begin{cases} p^{m-1} + \frac{p-1}{p} G_m \eta(a), & t = 0, \\ p^{m-1} - \frac{1}{p} G_m \eta(a), & t \neq 0. \end{cases}$$

引理10. [17] 设 $t \in \mathbb{F}_p$, 且 $a, b \in \mathbb{F}_{p^m}^*$. $N(0,t) = \sharp\left\{x \in \mathbb{F}_{p^m} \mid \mathrm{Tr}\left(\frac{x^2}{a}\right) = 0, \mathrm{Tr}\left(\frac{bx}{a}\right) = t\right\}$.

若 $t = 0$, 则

$$N(0,0) = \begin{cases} p^{m-2} + \frac{p-1}{p} G_m \eta(a), & p \mid M, \\ p^{m-2}, & p \nmid M. \end{cases}$$

若 $t \neq 0$, 则

$$N(t,0) = \begin{cases} p^{m-2}, & p \mid M, \\ p^{m-2} + \frac{1}{p} G_m \eta(a), & p \nmid M. \end{cases}$$

综合以上结果显然可得如下定理.

定理2. 设 p 为奇素数, m 为偶数, 定义集如 (2) 式所示且 $\omega - \frac{M}{4} = 0$. 则 (1) 式定义的码 C_D 为 $\left[p^{m-1} + \frac{p-1}{p} G_m \eta(a), m\right]$ 线性码, 其重量分布如表 2所示.

Table 2. The weight distribution of code C_D in Theorem 2

表 2. 定理 2 中码 C_D 的重量分布

重量	频数
0	1
$(p-1)p^{m-2}$	$p^{m-2} - 1$
$(p-1)p^{m-2} + \frac{p-1}{p} G_m \eta(a)$	$2(p^{m-1} - p^{m-2}) + \frac{1}{G_m \eta(a)}(p^m - p^{m-1})$
$(p-1)p^{m-2} + \frac{p-2}{p} G_m \eta(a)$	$(p^m + p^{m-2} - 2p^{m-1}) - \frac{1}{G_m \eta(a)}(p^m - p^{m-1})$

注记3. 由表 2 显然可得, 当 $m = 2$ 时, 重量为 $(p-1)p^{m-2}$ 的码字出现的次数为 $p^{m-2} - 1 = 0$ 次. 此时 C_D 为二重线性码.

下面的例子可由 Magma 程序验证.

例3. 设定义集如 (2) 式所示, 且 $p = 5,\ m = 4,\ a = 1,\ b = 2,\ \omega = \mathrm{Tr}(1)$. 则 C_D 为 $[105, 4]$ 线性码, 其重量计数器为 $1 + 24z^{100} + 180z^{80} + 420z^{85}$, 与定理 2 结论一致.

例4. 设定义集如 (2) 式所示, 且 $p = 7,\ m = 2,\ a = 2,\ b = 4,\ \omega = \mathrm{Tr}(2)$. 则 C_D 为 $[13, 2]$ 线性码, 其重量计数器为 $1 + 18z^{12} + 30z^{11}$, 与定理 2 结论一致.

4. 总结

本文推广了文献 [15–17] 中线性码的构造, 基于 (2) 式且分 m 为奇数和 m 为偶数两种情形对 (1) 式的线性码进行研究, 构造了几类新参数的 p 元线性码. 码的长度, 维数以及重量分布等参数与已有

结果均不同. 并用 Magma 程序验证了结论的正确性. 最后, 通过 Aschikhmin-Barg 条件说明, 本文构造的线性码多数情况下是极小线性码, 可以用来设计具有良好访问结构的秘密共享方案. $\omega - \frac{M}{4} \neq 0$ 时 C_D 的频率分布留给感兴趣的读者.

参考文献

[1] See, K. and Song, S.Y. (1998) Association Schemes of Small Order. *Journal of Statistical Planning and Inference*, **73**, 225-271. https://doi.org/10.1016/S0378-3758(98)00064-0

[2] Yuan, J. and Ding, C. (2005) 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, 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] Baumert, L.D. and McEliece, R.J. (1972) Weights of Irreducible Cyclic Codes. *Information and Control*, **20**, 158-175. https://doi.org/10.1016/S0019-9958(72)90354-3

[5] Ding, C. and Niederreiter, H. (2007) Cyclotomic Linear Codes of Order 3. *IEEE Transactions on Information Theory*, **53**, 2274-2277. https://doi.org/10.1109/TIT.2007.896886

[6] Tang, C., Qi, Y. and Huang, D. (2015) Two-Weight and Three-Weight Linear Codes from Square Functions. *IEEE Communications Letters*, **20**, 29-32. https://doi.org/10.1109/LCOMM.2015.2497344

[7] Yang, S. and Yao, Z.A. (2017) Complete Weight Enumerators of a Family of Three-Weight Linear Codes. *Designs, Codes and Cryptography*, **82**, 663-674. https://doi.org/10.1007/s10623-016-0191-x

[8] Heng, Z., Ding, C. and Zhou, Z. (2018) Minimal Linear Codes over Finite Fields. *Finite Fields and Their Applications*, **54**, 176-196. https://doi.org/10.1016/j.ffa.2018.08.010

[9] Jian, G., Lin, Z. and Feng, R. (2019) Two-Weight and Three-Weight Linear Codes Based on Weil Sums. *Finite Fields and Their Applications*, **57**, 92-107. https://doi.org/10.1016/j.ffa.2019.02.001

[10] Lu, H. and Yang, S. (2020) Two Classes of Linear Codes from Weil Sums. *IEEE Access*, **8**, 180471-180480. https://doi.org/10.1109/ACCESS.2020.3028141

[11] Li, C., Yue, Q. and Fu, F.W. (2017) A Construction of Several Classes of Two-Weight and Three-Weight Linear Codes. *Applicable Algebra in Engineering, Communication and Computing*, **28**, 11-30. https://doi.org/10.1007/s00200-016-0297-4

[12] Hu, Z., Wang, L., Li, N., *et al.* (2021) Several Classes of Linear Codes with Few Weights from the Closed Butterfly Structure. *Finite Fields and Their Applications*, **76**, Article 101926. https://doi.org/10.1016/j.ffa.2021.101926

[13] Duan, B., Han, G. and Qi, Y. (2022) A Class of Three-Weight Linear Codes over Finite Fields of Odd Characteristic. *Applicable Algebra in Engineering, Communication and Computing*, 1-17.

[14] Zhu, C. and Liao, Q. (2023) Two New Classes of Projective Two-Weight Linear Codes. *Finite Fields and Their Applications*, **88**, Article 102186. https://doi.org/10.1016/j.ffa.2023.102186

[15] 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

[16] Li, F., Wang, Q. and Lin, D. (2018) A Class of Three-Weight and Five-Weight Linear Codes. *Discrete Applied Mathematics*, **241**, 25-38. https://doi.org/10.1016/j.dam.2016.11.005

[17] Ouyang, J., Liu, H. and Wang, X. (2021) Several Classes of p-ary Linear Codes with Few Weights. *Applicable Algebra in Engineering, Communication and Computing.*

[18] Lidl, R. and Niederreiter, H. (1997) Finite Fields. Cambridge University Press, Cambridge.

[19] Huffman, W. and Pless, V. (2010) Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge.

[20] 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