

奇特特征域上一类二重量线性码

段冰冰, 韩广国, 亓延峰

(杭州电子科技大学 理学院, 浙江杭州 310018)

摘要: 线性码在通信, 数据存储和秘密共享方案等领域都有很好的应用. 基于定义集的构造方法, 选择二变量函数确定有限域上的定义集, 从而构造了奇特特征域上一类二重量线性码, 并利用加法特征, 乘法特征以及高斯和等确定了线性码的具体参数和重量分布. 此外, 大部分线性码是极小码, 这些码可用于构造秘密共享方案.

关键词: 线性码; 重量分布; 加法特征; 乘法特征; 高斯和

中图分类号: O157.04

文献标识码: A **文章编号:** 1000-4424(2023)03-0364-09

§1 引言

设 F_q 表示具有 q 个元素的有限域, 并且 $F_q^* = F_q \setminus \{0\}$, 其中 $q = p^m$, p 是素数, m 是正整数. 定义 F_p^n 为 F_p 上的 n 维向量空间, 则 F_p 上参数为 $[n, k, d]$ 的线性码 C 是 F_p^n 的一个 k 维子空间, 其中 n 为码长, k 为信息位, d 为最小距离. 设 A_i 表示码 C 中汉明重量为 i 的码字个数, 码 C 的重量计数器定义为 $1 + A_1z + A_2z^2 + \cdots + A_nz^n$. 序列 $(1, A_1, A_2, \cdots, A_n)$ 称为码 C 的重量分布. 如果序列 $(A_1, A_2, \cdots, A_n)$ 中非零分量的个数等于 t , 则称码 C 为 t 重量线性码. 如果 t 的值较小, 则称其是少重量线性码. 线性码的重量分布包含了关于码的纠错能力, 检错概率和纠错概率的重要信息. 因此, 线性码的重量分布问题在编码理论中备受关注^[1-6].

少重量线性码在通信, 认证码^[7-8], 结合方案, 强正则图^[9], 秘密共享协议和数据存储系统等方面都有重要的应用. 二重量线性码在秘密共享方案^[10]和强正则图^[9]中有很好的应用. 因此, 构造少重量线性码是线性码研究中一个重要的课题. 2007年, 文献[11]提出了一种基于定义集构造线性码的一般性方法. 设定义集 $D = \{d_1, d_2, \cdots, d_n\} \subseteq F_q$, 则线性码为

$$C_D = \{Tr(\beta d_1), Tr(\beta d_2), \cdots, Tr(\beta d_n) : \beta \in F_q\}.$$

其中 Tr 是从 F_q 到 F_p 的迹映射. 显然, 定义集 D 的选取直接影响所构造的线性码. 通常情况下, 可取 $D = \{x \in F_q^* : f(x) = 0\}$, 其中 $f(x) = Tr(F(x))$. 学者们从 $f(x)$ 和 $F(x)$ 入手, 构造了多类少重量线性码. 文献[12]介绍了利用布尔函数构造线性码的最新成果. 文献[10]利用函数 $F(x) = x^2$ 构造了 F_p 上一类二重量和三重量的线性码, 并且该类线性码适用于秘密共享方案. 文献[13]利用函

数 $F(x) = x^2 + x$ 构造出 F_p 上一类三重量和五重量的线性码. 许多论文在构造少重量线性码时采用了特殊形式的函数^[14-23].

基于定义集的构造方法, 文献[24]将线性码的构造推广到二元形式, 即: 长度为 n 的线性码为

$$C_D = \{c_{a,b} = (Tr(ax + by))_{(x,y) \in D} : a, b \in F_q\}, \quad (1)$$

其中 $D \subseteq F_q^2$ 是线性码 C_D 的定义集. 文献[25]对于构造二元形式的线性码也做了一些工作. 文献[26]选择定义集

$$D = \{(x, y) \in F_{2m}^2 \setminus \{(0, 0)\} : Tr(x^2 + xy) = u\}, \quad u \in F_2,$$

构造形式为(1)式的线性码. 本文推广了文献[27]的结果, 将二元域上的线性码推广到奇特征域上的线性码. 通过选取定义集

$$D = \{(x, y) \in F_q^2 \setminus \{(0, 0)\} : Tr(x^2 + xy) = u\}, \quad u \in F_p, \quad (2)$$

构造形式为(1)式的线性码, 其中 $q = p^m$, m 为正整数, p 为奇素数, Tr 是从 F_q 到 F_p 的迹映射. 并利用指数和的相关结论确定了线性码的码长和重量分布.

本文的其余部分组织如下. §2介绍了加法特征, 乘法特征以及高斯和的相关结果. §3介绍了一些计算线性码的参数以及重量分布的辅助结果. §4是主要结果及其应用. §5是总结.

§2 预备知识

本节主要介绍加法特征, 乘法特征以及高斯和的一些基本结果.

定义2.1 有限域加法群 F_q 到非零复数乘法群 C^* 的群同态 $\chi: F_q \rightarrow C^*$ 称为有限域 F_q 上的一个加法特征, 即 $\forall (x, y) \in F_q^2$, 有 $\chi(x + y) = \chi(x)\chi(y)$.

对每一个 $a \in F_q$, F_q 上的加法特征可定义为函数 $\chi_a(x) = \zeta_p^{Tr(ax)}$, 其中 $x \in F_q$. 当 $a = 1$ 时, 称 χ_1 为 F_q 上的标准加法特征. 注意: $\chi_a(x) = \chi_1(ax)$.

引理2.1^[28] 设 χ_1 为 F_q 上的标准加法特征, 则加法特征满足正交性, 即

$$\sum_{x \in F_q} \chi_1(ax) = \sum_{x \in F_q} \zeta_p^{Tr(ax)} = \begin{cases} q & \text{若 } a = 0, \\ 0 & \text{若 } a \in F_q^*. \end{cases}$$

下面介绍乘法特征以及高斯和的相关定义和引理.

定义2.2 设 α 是有限域的乘法群 F_q^* 的生成元, 则有限域 F_q 的所有乘法特征定义为函数

$$\psi_j(\alpha^k) = e^{2\pi\sqrt{-1}jk/(q-1)},$$

其中 $k = 0, 1, \dots, q-2$, $0 \leq j \leq q-2$. 当 $j = (q-1)/2$ 时, 称 $\psi_{(q-1)/2}$ 为 F_q 上的二次乘法特征, 记为 η . 当 $j = (p-1)/2$ 时, 称 $\psi_{(p-1)/2}$ 为 F_p 上的二次乘法特征, 记为 η_1 .

若 p 是奇素数, 则对 $c \in F_p^*$, 有

$$\eta(c) = \left(\frac{c}{p}\right) = \pm 1 \equiv c^{\frac{p-1}{2}} \pmod{p},$$

其中 $(\frac{c}{p})$ 称为勒让德符号. 若 $(\frac{c}{p}) = 1$, 则 c 称为二次剩余; 若 $(\frac{c}{p}) = -1$, 则 c 称为二次非剩余.

定义2.3 设 η 是 F_q 上的二次乘法特征, χ_1 是 F_q 上的标准加法特征. 则 F_q 上的高斯和 $G(\eta, \chi_1)$ 定义为

$$G(\eta, \chi_1) = \sum_{c \in F_q^*} \eta(c) \chi_1(c).$$

设 η_1 是 F_p 上的二次乘法特征, χ_1' 是 F_p 上的标准加法特征. 则 F_p 上的高斯和 $G(\eta_1, \chi_1')$ 定义为

$$G(\eta_1, \chi_1') = \sum_{c \in F_p^*} \eta_1(c) \chi_1'(c).$$

下面是关于指数和的引理.

引理2.2^[28] 设 $f(x) = a_2x^2 + a_1x + a_0 \in F_q[x]$ 且 $a_2 \neq 0$, 则

$$\sum_{x \in F_q} \chi(f(x)) = \zeta_p^{\text{Tr}(a_0 - a_1^2(4a_2)^{-1})} \eta(a_2) G(\eta, \chi),$$

其中 η 是 F_q 上的二次乘法特征, χ 是 F_q 上的非平凡加法特征.

§3 辅助结果

本节将给出一些引理, 用于确定由(2)式的定义集 D 构造的 F_p 上形式为(1)式的线性码 C_D 的基本参数和重量分布, 其中 p 为奇素数.

下面三个引理将用于计算线性码的码长和线性码中非零码字的重量.

引理3.1 设 $u \in F_p$, 令 $\Omega_1 = \sum_{x, y \in F_{p^m}} \sum_{w_1 \in F_p^*} \zeta_p^{w_1(\text{Tr}(x^2 + xy) - u)}$, 则

$$\Omega_1 = \begin{cases} (p-1)p^m & \text{若 } u = 0, \\ -p^m & \text{若 } u \neq 0. \end{cases}$$

证 由引理2.1, 可得

$$\begin{aligned} \Omega_1 &= \sum_{x, y \in F_{p^m}} \sum_{w_1 \in F_p^*} \zeta_p^{w_1(\text{Tr}(x^2 + xy) - u)} \\ &= \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \sum_{x \in F_{p^m}} \zeta_p^{w_1 \text{Tr}(x^2)} \sum_{y \in F_{p^m}} \zeta_p^{w_1 \text{Tr}(yx)} \\ &= \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} (p^m + \sum_{\substack{x \in F_{p^m} \\ x \neq 0}} \zeta_p^{w_1 \text{Tr}(x^2)} \sum_{y \in F_{p^m}} \zeta_p^{w_1 \text{Tr}(yx)}) \\ &= p^m \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \\ &= \begin{cases} (p-1)p^m & \text{若 } u = 0, \\ -p^m & \text{若 } u \neq 0. \end{cases} \end{aligned}$$

引理3.2 设 $u \in F_p$, 令 $\Omega_2 = \sum_{x, y \in F_{p^m}} \sum_{w_2 \in F_p^*} \zeta_p^{w_2 \text{Tr}(ax + by)}$, 其中 $a, b \in F_q$, 则

$$\Omega_2 = \begin{cases} (p-1)p^{2m} & \text{若 } (a, b) = (0, 0), \\ 0 & \text{若 } (a, b) \neq (0, 0). \end{cases}$$

证 与引理3.1的证明类似.

引理3.3 设 $u \in F_p$, 令 $\Omega_3 = \sum_{x, y \in F_{p^m}} \sum_{w_1 \in F_p^*} \zeta_p^{w_1(\text{Tr}(x^2 + xy) - u)} \sum_{w_2 \in F_p^*} \zeta_p^{w_2 \text{Tr}(ax + by)}$, 其中 $a, b \in$

F_q , 则

(1) 当 $u = 0$ 时有

$$\Omega_3 = \begin{cases} (p-1)^2 p^m & \text{若 } \text{Tr}(b(b-a)) = 0, \\ -(p-1)p^m & \text{若 } \text{Tr}(b(b-a)) \neq 0. \end{cases}$$

(2) 当 $u \neq 0$ 时有

$$\Omega_3 = \begin{cases} -(p-1)p^m & \text{若 } \text{Tr}(b(b-a)) = 0 \text{ 或 } \frac{\text{Tr}(b(b-a))}{u} \text{ 是 } F_p \text{ 上的二次非剩余,} \\ (p+1)p^m & \text{若 } \frac{\text{Tr}(b(b-a))}{u} \text{ 是 } F_p \text{ 上的二次剩余.} \end{cases}$$

证 由加法特征可得

$$\begin{aligned} \Omega_3 &= \sum_{x,y \in F_p^m} \sum_{w_1 \in F_p^*} \zeta_p^{w_1(\text{Tr}(x^2+xy)-u)} \sum_{w_2 \in F_p^*} \zeta_p^{w_2 \text{Tr}(ax+by)} \\ &= \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \sum_{x,y \in F_p^m} \zeta_p^{w_1 \text{Tr}(x^2+xy)} \sum_{w_2 \in F_p^*} \zeta_p^{w_2 \text{Tr}(ax+by)} \\ &= \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \sum_{w_2 \in F_p^*} \sum_{x \in F_p^m} \zeta_p^{\text{Tr}(w_1 x^2 + w_2 ax)} \sum_{y \in F_p^m} \zeta_p^{\text{Tr}(y(w_1 x + w_2 b))} \quad (\text{引理2.1}) \\ &= \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \sum_{w_2 \in F_p^*} \sum_{\substack{x \in F_p^m \\ w_1 x + w_2 b = 0}} \zeta_p^{\text{Tr}(w_1 x^2 + w_2 ax)} \sum_{y \in F_p^m} \zeta_p^{\text{Tr}(y(w_1 x + w_2 b))} \\ &= p^m \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \sum_{w_2 \in F_p^*} \sum_{\substack{x \in F_p^m \\ w_1 x + w_2 b = 0}} \zeta_p^{\text{Tr}(w_2 ax - w_2 bx)}. \end{aligned}$$

整理可得

$$\begin{aligned} \Omega_3 &= p^m \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \sum_{w_2 \in F_p^*} \zeta_p^{\text{Tr}((w_2 b - w_2 a)(\frac{w_2}{w_1} b))} \\ &= p^m \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \sum_{w_2 \in F_p^*} \zeta_p^{\frac{w_2^2}{w_1} \text{Tr}(b(b-a))}. \end{aligned}$$

(1) 当 $u = 0$ 时

若 $\text{Tr}(b(b-a)) = 0$, 则 $\Omega_3 = p^m \sum_{w_1, w_2 \in F_p^*} \zeta_p^0 = (p-1)^2 p^m$.

若 $\text{Tr}(b(b-a)) \neq 0$, 则由引理2.2以及文献[28]中定理5.12(iv), 可以得到

$$\begin{aligned} \Omega_3 &= p^m \sum_{w_1, w_2 \in F_p^*} \zeta_p^{\frac{w_2^2}{w_1} \text{Tr}(b(b-a))} \\ &= p^m \sum_{w_1 \in F_p^*} \left(\sum_{w_2 \in F_p} \zeta_p^{\frac{\text{Tr}(b(b-a))}{w_1} w_2^2} - 1 \right) \\ &= p^m \eta_1(\text{Tr}(b(b-a))) \sum_{w_1 \in F_p^*} \eta_1(w_1) G(\eta_1, \chi_1') - (p-1)p^m \\ &= -(p-1)p^m. \end{aligned}$$

因此当 $u = 0$ 时

$$\Omega_3 = \begin{cases} (p-1)^2 p^m & \text{若 } \text{Tr}(b(b-a)) = 0, \\ -(p-1)p^m & \text{若 } \text{Tr}(b(b-a)) \neq 0. \end{cases}$$

(2) 当 $u \neq 0$ 时

若 $\text{Tr}(b(b-a)) = 0$, 则 $\Omega_3 = p^m \sum_{w_1, w_2 \in F_p^*} \zeta_p^{-uw_1} = -(p-1)p^m$.

若 $\text{Tr}(b(b-a)) \neq 0$, 令 $t_1 = \text{Tr}(b(b-a))$, 则由引理2.2, 可以得到

$$\begin{aligned}\Omega_3 &= p^m \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \sum_{w_2 \in F_p^*} \zeta_p^{\frac{t_1 w_2^2}{w_1}} \\ &= p^m \sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \left(\sum_{w_2 \in F_p^*} \zeta_p^{\frac{t_1}{w_1} w_2^2} - 1 \right) \\ &= p^m \left(\sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \eta_1(t_1 w_1) G(\eta_1, \chi_1') + 1 \right).\end{aligned}$$

然后由高斯和的定义以及文献[28]中定理5.12(iv), 可得

$$\begin{aligned}\Omega_3 &= p^m \left(\sum_{w_1 \in F_p^*} \zeta_p^{-uw_1} \eta_1(-uw_1) \eta_1\left(\frac{-t_1}{u}\right) G(\eta_1, \chi_1') + 1 \right) \\ &= p^m \left(\eta_1(-1) \eta_1\left(\frac{t_1}{u}\right) G^2(\eta_1, \chi_1') + 1 \right) \\ &= p^m \left(p \eta_1\left(\frac{t_1}{u}\right) + 1 \right) \\ &= \begin{cases} -(p-1)p^m & \text{若 } \frac{t_1}{u} \text{ 是 } F_p \text{ 上的二次非剩余,} \\ (p+1)p^m & \text{若 } \frac{t_1}{u} \text{ 是 } F_p \text{ 上的二次剩余.} \end{cases}\end{aligned}$$

因此

$$\Omega_3 = \begin{cases} -(p-1)p^m & \text{若 } \text{Tr}(b(b-a)) = 0 \text{ 或 } \frac{\text{Tr}(b(b-a))}{u} \text{ 是 } F_p \text{ 上的二次非剩余,} \\ (p+1)p^m & \text{若 } \frac{\text{Tr}(b(b-a))}{u} \text{ 是 } F_p \text{ 上的二次剩余.} \end{cases}$$

综上所述, 该引理得证.

下面的引理用于确定形式为(1)式的线性码 C_D 的码长.

引理3.4 设 $n_0 = \#\{(x, y) \in F_{p^m}^2 : \text{Tr}(x^2 + xy) = u\}$, 其中 $u \in F_p$, 则

$$n_0 = \begin{cases} p^{2m-1} + (p-1)p^{m-1} & \text{若 } u = 0, \\ p^{2m-1} - p^{m-1} & \text{若 } u \neq 0. \end{cases}$$

证 将 n_0 表示为指数和的形式计算, 有

$$\begin{aligned}n_0 &= \#\{(x, y) \in F_{p^m}^2 : \text{Tr}(x^2 + xy) = u\} \\ &= \frac{1}{p} \sum_{x, y \in F_{p^m}} \sum_{w_1 \in F_p} \zeta_p^{w_1(\text{Tr}(x^2 + xy) - u)} \\ &= \frac{1}{p} \sum_{x, y \in F_{p^m}} \left(1 + \sum_{w_1 \in F_p^*} \zeta_p^{w_1(\text{Tr}(x^2 + xy) - u)} \right) \\ &= p^{2m-1} + \frac{1}{p} \Omega_1.\end{aligned}$$

根据 n_0 的定义以及引理3.1, 该引理得证.

下面将给出线性码中非零码字的重量.

对于 $(a, b) \neq (0, 0)$, 码字 $c_{a,b}$ 的汉明重量 $w(c_{a,b}) = n_0 - N_0$, 其中

$$\begin{aligned} N_0 &= \#\{(x, y) \in F_{p^m}^2 : \text{Tr}(x^2 + xy) = u, \text{Tr}(ax + by) = 0\} \\ &= \frac{1}{p^2} \sum_{x, y \in F_{p^m}} \sum_{w_1 \in F_p} \zeta_p^{w_1(\text{Tr}(x^2 + xy) - u)} \sum_{w_2 \in F_p} \zeta_p^{w_2 \text{Tr}(ax + by)} \\ &= \frac{1}{p^2} \sum_{x, y \in F_{p^m}} (1 + \sum_{w_1 \in F_p^*} \zeta_p^{w_1(\text{Tr}(x^2 + xy) - u)}) (1 + \sum_{w_2 \in F_p^*} \zeta_p^{w_2 \text{Tr}(ax + by)}) \\ &= p^{2m-2} + \frac{1}{p^2} (\Omega_1 + \Omega_2 + \Omega_3). \end{aligned}$$

则

$$w(c_{a,b}) = (p-1)p^{2m-2} + \frac{1}{p} \Omega_1 - \frac{1}{p^2} (\Omega_1 + \Omega_2 + \Omega_3). \quad (3)$$

§3 主要结果

在本节中, 研究由(2)式中的定义集 D 构造的形式为(1)式的线性码. 按照定义集中 u 的取值进行分类, 然后分别计算相应的线性码的码长和重量分布.

定理4.1 设 p 为奇素数, $D = \{(x, y) \in F_{p^m}^2 \setminus \{(0, 0)\} : \text{Tr}(x^2 + xy) = 0\}$, 此时形式为(1)式的线性码 C_D 是一个二重量的线性码, 参数为 $[p^{2m-1} + (p-1)p^{m-1} - 1, 2m, (p-1)p^{2m-2}]$, 重量分布见表1.

表1 $u = 0$ 时线性码 C_D 的重量分布

w	A_w
0	1
$(p-1)p^{2m-2}$	$p^{2m-1} + (p-1)p^{m-1} - 1$
$(p-1)p^{2m-2} + (p-1)p^{m-1}$	$(p-1)p^{2m-1} - (p-1)p^{m-1}$

证 当 $u = 0$ 时, 线性码的定义集合为 $D = \{(x, y) \in F_{p^m}^2 \setminus \{(0, 0)\} : \text{Tr}(x^2 + xy) = 0\}$, 由引理3.1和引理3.4, 可以得到线性码 C_D 的码长为 $n = n_0 - 1 = p^{2m-1} + (p-1)p^{m-1} - 1$. 由(3)式可知, 线性码中非零码字的重量是由 Ω_1 , Ω_2 和 Ω_3 的取值决定的. 因此由引理3.1, 引理3.2和引理3.3可得

$$w(c_{a,b}) = \begin{cases} (p-1)p^{2m-2} & \text{若 } \text{Tr}(b(b-a)) = 0, \\ (p-1)p^{2m-2} + (p-1)p^{m-1} & \text{若 } \text{Tr}(b(b-a)) \neq 0. \end{cases}$$

显然, 码字重量为0的频数为1. 令 $w_1 = (p-1)p^{2m-2}$, $w_2 = (p-1)p^{2m-2} + (p-1)p^{m-1}$, 然后由Pless Power Moments^[29]有

$$\begin{cases} A_{w_1} + A_{w_2} = p^{2m} - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} = (p-1)np^{2m-1}. \end{cases}$$

计算可得

$$A_{w_1} = p^{2m-1} + (p-1)p^{m-1} - 1, \quad A_{w_2} = (p-1)p^{2m-1} - (p-1)p^{m-1}.$$

该定理得证.

下面利用Magma程序验证了定理4.1中结果的正确性.

例1 令 $p = 3$, $m = 2$, 则 C_D 是参数为 $[32, 4, 18]$ 的线性码, 其重量计数器为 $1 + 32z^{18} + 48z^{24}$.

例2 令 $p = 5, m = 2$, 则 C_D 是参数为 $[144, 4, 100]$ 的线性码, 其重量计数器为 $1 + 144z^{100} + 480z^{120}$.

定理4.2 设 p 为奇素数, $D = \{(x, y) \in F_p^2 \setminus \{(0, 0)\} : \text{Tr}(x^2 + xy) = u\}$, 其中 $u \neq 0$, 此时形式为(1)式的线性码 C_D 是二重量线性码, 参数为 $[p^{2m-1} - p^{m-1}, 2m, (p-1)p^{2m-2} - 2p^{m-1}]$, 重量分布见表2.

表2 $u \neq 0$ 时线性码 C_D 的重量分布

w	A_w
0	1
$(p-1)p^{2m-2} - 2p^{m-1}$	$\frac{1}{2}(p-1)p^{2m-1} - \frac{1}{2}(p-1)p^{m-1}$
$(p-1)p^{2m-2}$	$\frac{1}{2}(p+1)p^{2m-1} + \frac{1}{2}(p-1)p^{m-1} - 1$

证 当 $u \neq 0$ 时, 线性码的定义集合为 $D = \{(x, y) \in F_q^2 \setminus \{(0, 0)\} : \text{Tr}(x^2 + xy) = u\}$. 由引理3.1和引理3.4, 可以得到线性码 C_D 的码长为 $n = n_0 = p^{2m-1} - p^{m-1}$. 由(3)式, 引理3.1, 引理3.2和引理3.3可得, 线性码中非零码字的重量

$$w(c_{a,b}) = \begin{cases} (p-1)p^{2m-2} - 2p^{m-1} & \text{若 } \frac{\text{Tr}(b(b-a))}{u} \text{ 是 } F_p \text{ 上的二次剩余,} \\ (p-1)p^{2m-2} & \text{若 } \text{Tr}(b(b-a)) = 0 \text{ 或 } \frac{\text{Tr}(b(b-a))}{u} \text{ 是 } F_p \text{ 上的二次非剩余.} \end{cases}$$

令 $w_1 = (p-1)p^{2m-2} - 2p^{m-1}$, $w_2 = (p-1)p^{2m-2}$, 然后由 Pless Power Moments^[29] 可得

$$A_{w_1} = \frac{1}{2}(p-1)p^{2m-1} - \frac{1}{2}(p-1)p^{m-1}, \quad A_{w_2} = \frac{1}{2}(p+1)p^{2m-1} + \frac{1}{2}(p-1)p^{m-1} - 1.$$

该定理得证.

下面利用 Magma 程序验证了定理4.2中结果的正确性.

例3 令 $p = 3, m = 2$, 则 C_D 是参数为 $[24, 4, 12]$ 的线性码, 其重量计数器为 $1 + 24z^{12} + 56z^{18}$.

例4 令 $p = 5, m = 2$, 则 C_D 是参数为 $[120, 4, 90]$ 的线性码, 其重量计数器为 $1 + 240z^{90} + 384z^{100}$.

极小码在秘密共享方案^[10,30]和安全两方计算^[26]中有很好的应用. 下面引理给出线性码为极小码的一个充分条件^[31].

引理4.1^[31] 设 C 是参数为 $[n, k, d]$ 的线性码, 记 $w_{\max}$ 为 C 中非零码字汉明重量的最大值, $w_{\min}$ 为 C 中非零码字汉明重量的最小值. 若 $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$, 则 C 中每个非零码字都是极小码字.

由引理4.1, 当 $u = 0, m \geq 2$ 时, 定理4.1中的线性码 C_D 满足

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

当 $u \neq 0, m \geq 3$ 时, 定理4.2中的线性码 C_D 满足

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

因此, 当 $m \geq 3$ 时, 线性码 C_D 中的非零码字都是极小码字. 此时, 线性码是极小码, 可用于构造秘密共享方案.

§5 小结

本文推广了文献[27]的结果, 运用定义集构造线性码的方法, 将线性码的构造从二元域推广到更一般的奇特征域, 得到了奇特征域上一类二重量的线性码, 并确定了线性码的参数以及重量分布. 此外, 本文得到的线性码中大部分码是极小码, 可用于构造秘密共享方案. 如何使用一般的函数来构造新的更好的线性码是以后的研究方向.

参考文献:

- [1] Ding Cunsheng, Yin Jianxing. Algebraic constructions of constant composition codes[J]. IEEE Trans Inform Theory, 2005, 51: 1585-1589.
- [2] Ma Changli, Zeng Liwei, Liu Yang, et al. The weight enumerator of a class of cyclic codes[J]. IEEE Trans Inform Theory, 2011, 57: 397-402.
- [3] Zeng Xiangyong, Hu Lei, Jiang Wenfeng, et al. The weight distribution of a class of p-ary cyclic codes[J]. Finite Fields Appl, 2010, 16: 56-73.
- [4] Ding Cunsheng, Yang Jing. Hamming weights in irreducible cyclic codes[J]. Discrete Math, 2013, 313: 434-446.
- [5] Vega G. The weight distribution of an extended class of reducible cyclic codes[J]. IEEE Trans Inform Theory, 2012, 58: 4862-4869.
- [6] Li Shuxing, Feng Tao, Ge Gennian. On the weight distribution of cyclic codes with Niho exponents[J]. IEEE Trans Inform Theory, 2014, 60: 3903-3912.
- [7] Calderbank A, Goethals J. Three-weight codes and association schemes[J]. Phil J Res, 1984, 39(4): 143-152.
- [8] Stinson D. Some constructions and bounds for authentication codes[J]. J Crypt, 1987, 1(1): 37-51.
- [9] Calderbank R, Kantor W. The geometry of two-weight codes[J]. Bull London Math Soc, 1986, 18(2): 97-122.
- [10] Ding Kelan, Ding Cunsheng. A class of two-weight and three-weight codes and their applications in secret sharing[J]. IEEE Trans Inform Theory, 2015, 61(11): 5835-5842.
- [11] Ding Cunsheng, Niederreiter H. Cyclotomic linear codes of order 3[J]. IEEE Trans Inform Theory, 2007, 53(6): 2274-2277.
- [12] Ding Cunsheng. A construction of binary linear codes from Boolean functions[J]. Discrete Math, 2016, 339: 2288-2303.
- [13] Li Fei, Wang Qiuyan, Lin Dongdai. A class of three-weight and five-weight linear codes[J]. Discrete Appl Math, 2018, 241(6): 25-38.
- [14] Ding Cunsheng. Linear codes from some 2-designs[J]. IEEE Trans Inform Theory, 2015, 61: 3265-3275.
- [15] Ding Cunsheng. Codes from difference sets[M]. Hackensack, NJ: World Scientific Publishing Co. Pte. Ltd, 2015.
- [16] Ding Kelan, Ding Cunsheng. Binary linear codes with three weights[J]. IEEE Comm Lett, 2014, 18: 1879-1882.
- [17] Tang Chunming, Qi Yanfeng, Huang Dongmei. Two-weight and three-weight linear codes from square functions[J]. IEEE Commun Lett, 2015, 20(1): 29-32.
- [18] Li Chengju, Bae S, Ahn J, et al. Complete weight enumerators of some linear codes and their applications[J]. Designs, Codes Crypt, 2016, 81(1): 153-168.

- [19] Tang Chunming, Li Nian, Qi Yanfeng, et al. Linear codes with two or three weights from weakly regular bent functions[J]. IEEE Trans Inform Theory, 2016, 62: 1166-1176.
- [20] Xiang Can, Tang Chunming, Feng Keqin. A class of linear codes with a few weights[J]. Crypt Commun, 2017, 9(1): 93-116.
- [21] Zhou Zhengchun, Li Nian, Fan Cuiling, et al. Linear codes with two or three weights from quadratic bent functions[J]. Designs, Codes Crypt, 2016, 81: 283-295.
- [22] Yang Shudi, Yao Zheng-An. Complete weight enumerators of a family of three-weight linear codes[J]. Designs, Codes Crypt, 2017, 82(3): 663-674.
- [23] Zhou Zhengchun, Li Xia, Tang Chunming, et al. Binary LCD codes and self-orthogonal codes from a generic construction[J]. IEEE Trans Inform Theory, 2019, 65: 16-27.
- [24] Li Chengju, Yue Qin, Fu Fangwei. A construction of several classes of two-weight and three-weight linear codes[J]. Appl Algebra Engineer Commun, 2017, 28: 11-30.
- [25] Jian Gaopeng, Lin Zhouchen, Feng Rongquan. Two-weight and three-weight linear codes based on Weil sums[J]. Finite Fields Appl, 2019, 57: 92-107.
- [26] Cohen G, Mesnager S, Patey A. On minimal and quasi-minimal linear codes[A], In: Cryptography and Coding, Lecture Notes in Comput. Sci, 8308[C]. Heidelberg: Springer, 2013, 85-98.
- [27] Hu Zhao, Wang Lisha, Li Nian, et al. Several classes of linear codes with few weights from the closed butterfly structure[J]. Finite Fields Appl, 2021, 76: 101926.
- [28] Lidl R, Niederreiter H, Cohn P. Finite fields[M]. Cambridge, UK: Cambridge University Press, 1997.
- [29] Huffman W, Pless V. Fundamentals of error-correcting codes[M]. Cambridge, UK: Cambridge University Press, 1997.
- [30] Yuan Jin, Ding Cunsheng. Secret sharing schemes from three classes of linear codes[J]. IEEE Trans Inform Theory, 2006, 52: 206-212.
- [31] Heng Ziling, Ding Cunsheng, Zhou Zhengchun. Minimal linear codes over finite fields[J]. Finite Fields Appl, 2018, 54: 176-196.

A class of two-weight linear codes over finite fields of odd characteristic

DUAN Bing-bing, HAN Guang-guo, QI Yan-feng

(School of Science, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China)

Abstract: Linear codes have applications in communication, data storage systems and secret sharing schemes. A class of two-weight linear codes is obtained by the defining sets determined by the bivariate functions over finite fields of odd characteristic. The parameters and weight distributions of linear codes are determined by the additive characters, multiplicative characters and Gauss sums. Additionally, most of linear codes are minimal and thus they are suitable for secret sharing schemes.

Keywords: linear code; weight distribution; additive character; multiplicative character; Gauss sum

MR Subject Classification: 94B05; 11T23