有限域上两类新的 2-重量码的构造

管 玥[1],施敏加[1,2],张 欣[1],伍文婷[1]
(1. 安徽大学数学科学学院,安徽合肥 230601;2. 安徽大学计算智能与信号处理教育部重点实验室,安徽合肥 230039)

摘 要: 有限域上二重量码的构造是图论、编码与密码中的重要研究课题. 本文得到了有限域上两类新的 2-重量码并且它们都是最优的,达到了 Griesmer 界. 这些码由有限域的扩域上迹码的 p 元像定义,有阿贝尔码的代数结构,利用特征和和高斯和来计算了它们的重量分布. 我们也计算了这些像码的对偶码的极小距离. 最后对扩域上迹码的像在秘钥共享方案中的应用进行了刻画.

关键词: 2-重量码; 迹码; 循环码; 高斯和; 秘钥共享方案; Griesmer 界
中图分类号: TN911. 22 **文献标识码:** A **文章编号:** 0372-2112 (2019)03-0714-05
电子学报 URL: http://www. ejournal. org. cn **DOI:** 10. 3969/j. issn. 0372-2112. 2019. 03. 028

The Construction of Two New Series of Two-Weight Codes over Finite Fields

GUAN Yue[1], SHI Min-jia[1,2], ZHANG Xin[1], WU Wen-ting[1]
(1. *School of Mathematical Sciences, Anhui University, Hefei, Anhui* 230601, *China*;
2. *Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education, Anhui University, Hefei, Anhui* 230039, *China*)

Abstract: The construction of two-weight codes over finite fields is an important research topic in graph, coding and cryptography fields. We obtain two new series of two-weight codes over finite fields and they are both optimal, which arrive at Griesmer bound. These codes are defined as p-ary images of trace codes over the extended fields. They have the algebraic structure of abelian codes. Their weight distributions are evaluated explicitly by using character sums, Gauss sums in particular. We also calculate the minimum distance of the dual codes of the image codes. Finally, an application of the Gray images of trace codes over the extended fields to secret sharing schemes is described.

Key words: two-weight codes; trace codes; cyclic codes; Gauss sums; secret sharing schemes, Griesmer bound

1 引言

自 1970 年以来,域上的 2-重量码由于其与强正则图、差集和有限几何之间的关联,一直被广泛研究[1]. 2-重量码的已知构造和参数表在文献[2]中给出,一些最近的研究结果见文献[3]. 本文介绍了 F_p 上两类 2-重量码,这些码是 F_{p^2} 上迹码的 p 元像,具有阿贝尔码的性质,但是非循环码. 这些码都满足最优码的条件.

最近,由环上的迹码构造域上的少重量码的研究方面,我们做了一些积极的工作,譬如见文献[4~7]. 但是本文只使用有限域上的算法. 譬如,下文中的 Gray 映射可以看成是一个线性 Gray 映射,域 F_{p^2} 看成是 F_p 的扩环.

值得注意的是,已有文献中大多数二重量码的构造是基于不可约循环码,见文献[8]和分圆法,见文献[3]. 重量计算的要点是二次高斯和以及它们的高斯周期的计算,见文献[9]. 我们计算得到的重量与频数与文献[2~7]中的不同,表明这些码是新的. 我们完全确定了极小码字的结构且给出了对 Massey 秘钥共享方案的一个应用.

2 预备知识

2.1 域

令 F_p 为阶是 p 的有限域,其中 p 是奇素数. 令 u 是 x^2+1 在 F_{p^2} 上的一个根,则 F_{p^2} 可以看作 F_p 由 u 生成的

收稿日期:2018-02-19;修回日期:2018-03-19;责任编辑:覃怀银
基金项目:国家自然科学基金面上项目(No. 61672036);安徽省自然科学基金杰出青年基金(No. 1808085J20)

一个二次扩域. 令 m 是奇数,我们定义 $T_{m/1}(\ )$ 为 F_{p^m} 到 F_p 的迹映射. 因此,对任意的 $x\in F_{p^m}$,有 $T_{m/1}(x)=x+x^p+\cdots+x^{p^{m-1}}$. 对所有的 $\alpha,\beta\in F_{p^m}$ 定义函数 tr( ) 为 $\mathrm{tr}(\alpha+u\beta)=T_{m/1}(\alpha)+uT_{m/1}(\beta)$,下述命题表明该函数就是从 $F_{p^{2m}}$ 到 F_{p^2} 的迹函数.

命题 1　沿用上述标记,若 T 表示从 $F_{p^{2m}}$ 到 F_{p^2} 的迹映射,则 $T(\gamma)=\mathrm{tr}(\gamma),\gamma\in F_{p^{2m}}$.

证明　记 $\gamma=\alpha+u\beta,\alpha,\beta\in F_{p^m}$. 因为 $u\in F_{p^2}$,由 T 的线性性得到 $T(\gamma)=T(\alpha)+uT(\beta)$. 现在,我们断言对任意 $\alpha\in F_{p^m}$,有 $T(\alpha)=T_{m/1}(\alpha)$. 根据定义 $T(\alpha)=\sum_{j=0}^{m-1}\alpha^{p^{2j}}$,又由 $\alpha\in F_{p^m}$ 得到 $\alpha^{p^m}=\alpha$. 对于 $2j\geq m$,将 $2j$ 用 $2j-m$ 替换,则上式变为 $T(\alpha)=\sum_{j=0}^{m-1}\alpha^{p^j}=T_{m/1}(\alpha)$. 根据tr( )的定义,于是有 $T(\gamma)=\mathrm{tr}(\gamma),\gamma\in F_{p^{2m}}$.

对任意的 $a,b\in F_p$,定义从 F_{p^2} 到 F_p^2 的一个线性映射 $\Psi,\Psi(a+ub)=(a,b)$. 这一映射可自然地扩展到从 $F_{p^2}^n$ 到 F_p^{2n} 的映射:$\Psi(\boldsymbol{a}+u\boldsymbol{b})=(\boldsymbol{a},\boldsymbol{b})$,其中 $\boldsymbol{a},\boldsymbol{b}\in F_p^m$.

2.2　平方数

令 q 是任意奇素数的方幂,F_q 是阶为 q 的有限域. F_q 中的平方数为 $\{z\mid z=y^2,z,y\in F_q,z\neq 0\}$. F_q 中的非平方数为 F_q 中不具有上述形式的元素. 平方数和非平方数构成的集合中元素个数都是 $\frac{1}{2}(q-1)$.

2.3　码

令 q 是任意素数的方幂. F_q 上长度为 n 的线性码 C 是 F_q^n 的一个向量子空间. $\boldsymbol{x}\in F_q^n$ 的汉明重量 $w_H(x)$ 是使得 $x_j\neq 0$ 的下标 j 的个数. 若 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$ 和 $\boldsymbol{y}=(y_1,y_2,\cdots,y_n)$ 是 F_q^n 中的两个元素,则它们在 F_q 上的标准内积定义为 $<\boldsymbol{x},\boldsymbol{y}>=\sum_{i=1}^{n}x_iy_i$. C 的对偶码用 $C^\perp$ 表示且定义为 $C^\perp=\{\boldsymbol{y}\in F_q^n\mid <\boldsymbol{x},\boldsymbol{y}>=0,\forall\boldsymbol{x}\in C\}$. 由定义可知,$C^\perp$ 也是 F_q 上的线性码. 给定一个有限阿贝尔群 A,F_q 上一个码称为阿贝尔的若它是群环 $F_q[A]$ 的一个理想. 换句话说,C 中的坐标由 A 中的元素确定,且 A 通过乘法均匀作用在该集合上,在 A 是循环群的特殊情况下,该码是循环码,见文献[8]. F_{q^n} 上的一个单项变换是指一个线性变换对应的 $n\times n$ 矩阵的每行每列恰好只有一个非零数.

3　对称性

Q 和 N 分别表示 F_{p^m} 中的平方数和非平方数构成的集合,在本文中,我们定义两种不同的集合 $L=Q\times F_{p^m}$ 和 $L'=F_{p^m}^*\times F_{p^m}$. 令 G 表示 $(F_{p^m}^*,\times)$ 和 $(F_{p^m},+)$ 相乘得到的乘群. 则 Q 是 $(F_{p^m}^*,\times)$ 中指数为 2 的子群. 令 $n=|L|=\frac{1}{2}(p^{2m}-p^m)$,$n'=|L'|=p^{2m}-p^m$,$N=2n$,$N'=2n'$. 对于 $x=t+ut'\in L$ 和 $a=\alpha+u\beta$,其中 $t\in Q,t'\in F_{p^m}$,$\alpha,\beta\in F_{p^m}$,定义 $ax=(t+ut')(\alpha+u\beta)=t\alpha+u(t\beta+t'\alpha)+t'\beta$. $x\in L'$ 时,也类似地定义 ax. 对于 $a\in F_{p^{2m}}$,定义 $E(a),E'(a)\in F_{p^2}^n$ 分别为 $E(a)=\mathrm{tr}(ax)_{x\in L}$ 和 $E'(a)=\mathrm{tr}(ax)_{x\in L'}$. 定义码 $C_{m,p}$ 和 $C'_{m,p}$ 分别为 $C_{m,p}=\{E(a)\mid a\in F_{p^{2m}}\}$ 和 $C'_{m,p}=\{E'(a)\mid a\in F_{p^{2m}}\}$. 因此 $C_{m,p}(C'_{m,p})$ 是 F_{p^2} 上长度为 $n(n')$ 的码,$\Psi(C_{m,p})(\Psi(C'_{m,p}))$ 是 F_p 上长度为 $2n=p^{2m}-p^m(2n'=2p^{2m}-2p^m)$ 的码.

命题 2　群 $L(L')$ 在 $C_{m,p}(C'_{m,p})$ 中的坐标上均匀作用.

证明　令 $v,w\in L(L')$,则 $v=(v_1,v_2)$,$w=(w_1,w_2)$,其中 $v_1,w_1\in Q(v_1,w_1\in F_{p^m}^*)$,$v_2,w_2\in F_{p^m}$. 对变量 (x,y) 的改变 $(x,y)\longmapsto\left(\frac{w_1x}{v_1},w_2+y-v_2\right)$ 是从 v 映射到 w 上. 注意到,因为 $\frac{w_1}{v_1}\in Q(\frac{w_1}{v_1}\in F_{p^m}^*)$,这定义了一个从 $L(L')$ 到其自身的变换. 对于给定的 v,w,有这种性质的置换是唯一的. 因此该作用是均匀分布在 $C_{m,p}(C'_{m,p})$ 中的坐标上的.

因此码 $C_{m,p}$ 是关于群 L 的阿贝尔码,即码 $C_{m,p}$ 是群环 $F_{p^2}[L]$ 的一个理想. 由其定义可知,L 不是一个循环群,因此 $C_{m,p}$ 不一定是循环的. 码 $C'_{m,p}$ 的这一性质与 $C_{m,p}$ 类似,所以在此省略.

一个码称为是传递的,若它的自同构群对它的坐标作用是传递的.

命题 3　码 $\Psi(C_{m,p})$ 是传递的.

证明　令 $\mathrm{tr}(\boldsymbol{a}x)_{x\in L}=\boldsymbol{a}+\boldsymbol{b}u$,其中 $\boldsymbol{a},\boldsymbol{b}\in F_p^n$. 又令 $x=t+ut'$ 和 $a=\alpha+u\beta$,其中 $t\in Q,t'\in F_{p^m},\alpha,\beta\in F_{p^m}$,由命题 2.1 得到 $a=T_{m/1}(\alpha t-\beta t')_{x\in L}$,$b=T_{m/1}(\alpha t'+\beta t)_{x\in L}$.

由前述命题,通过对 a 和 b 的每一位坐标置换,L 的作用是传递的. 对变量的改变 $\alpha+u\beta\longmapsto\beta-\alpha u$ 把 a 变成 b,把 b 变成 $-a$. 这是一个阶为 4 的单项变换,对每个码字的"两半"进行了交换. 证明完毕.

对于 L' 由类似的结论并由下述命题给出,该命题的证明是类似的,故省略.

命题 4　码 $\Psi(C'_{m,p})$ 是传递的.

4　特征和

首先回顾一些文献[7,9]中已知的事实,令 χ 是 F_q 的任意复值乘法特征,假设 q 是奇数. 用 η 表示二次乘法特征且定义为 $\eta(x)=1$,若 x 是平方数,否则 $\eta(x)=-1$. 令 ψ 为 F_q 的标准加法特征. 经典的高斯和定义为 $G(\chi)=\sum_{x\in F_q^*}\psi(x)\chi(x)$. 我们定义一下特征和,有时称

为高斯周期:$\hat{Q}=\sum_{x\in Q}\psi(x)$,$\hat{N}=\sum_{x\in N}\psi(x)$. 由特征的正交性,容易看出$\hat{Q}+\hat{N}=-1$. 注意到 Q 的特征函数是$\frac{1}{2}(1+\eta)$,则有$\hat{Q}=\frac{1}{2}(G(\eta)-1)$,$\hat{N}=\frac{1}{2}(-G(\eta)-1)$. 文献[9]中指出若 $q=p^m$,则二次高斯和值为

(1)$G(\eta)=(-1)^{m-1}\sqrt{q}$,$p\equiv1(\bmod 4)$,(2)$G(\eta)=(-1)^{m-1}i^m\sqrt{q}$,$p\equiv3(\bmod 4)$.

5 迹码的重量分布

令 $\omega=e^{\frac{2\pi i}{p}}$,$y=(y_1,y_2,\cdots,y_N)\in F_p^N$,令 $\Theta(y)=\sum_{j=1}^{N}\omega^{y_j}$. 为表述简便,我们令 $\theta(a)=\Theta(\Psi(E(a)))$ 和 $\theta'(a)=\Theta(\Psi(E'(a)))$. 由映射 Ψ 和赋值映射的线性性可知 $\theta(sa)=\Theta(\Psi(E(sa)))$,对任意的 $s\in F_p^*$ 和 $\theta'(\tau a)=\Theta(\Psi(E'(\tau a)))$,对任意的 $\tau\in F_p^*$.

下面的引理来自参考文献[7]中的 Lemma 5.1.

引理 1 对所有的 $\boldsymbol{y}=(y_1,y_2,\cdots,y_N)\in F_p^N$,有 $\sum_{s=1}^{p-1}\Theta(s\boldsymbol{y})=(p-1)N-pw_{H(\boldsymbol{y})}$.

5.1 $\Psi(C_{m,p})$的重量分布

下面计算 $\theta(\boldsymbol{a})$,$\boldsymbol{a}\in F_p^m$. 假设 $x=t+t'u$,其中 $t\in Q$,$t'\in F_{p^m}$;$\theta(a)=\theta_{A(a)}+\theta_{B(a)}$,其中 $a=\alpha+u\beta$,$\alpha,\beta\in F_{p^m}$且 $\theta_{A(a)}=\sum_{t\in Q,t'\in F_{p^m}}\omega^{T_{m/1}(\alpha t-\beta t')}$,$\theta_{B(a)}=\sum_{t\in Q,t'\in F_{p^m}}\omega^{T_{m/1}(\alpha t'+\beta t)}$.

首先计算 $\theta_{A(a)}$.

引理 2 (1)若 $\beta\neq0$,则 $\theta_{A(a)}=0$;(2)若 $\beta=0$,则(ⅰ)$\theta_{A(a)}=p^m\hat{Q}$,其中 $\alpha\in Q$,(ⅱ)$\theta_{A(a)}=p^m\hat{N}$,其中 $\alpha\in N$.

证明 令 $\theta_{A(a)}=\sum_{t\in Q}\omega^{T_{m/1}(\alpha t)}\sum_{t'\in F_{p^m}}\omega^{T_{m/1}(-\beta t')}$. 由特征的正交性,当 $\beta=0$ 时,$\sum_{t'\in F_{p^m}}\omega^{T_{m/1}((-\beta t'))}=p^m$,否则 $\sum_{t'\in F_{p^m}}\omega^{T_{m/1}(-\beta t')}=0$. 根据$\hat{Q}$和$\hat{N}$的定义即可得到所要证明的结论.

计算 $\theta_{B(a)}$的方法类似,故证明过程省略.

引理 3 假设 $a\neq0$. (1)若 $\alpha\neq0$,则 $\theta_{B(a)}=0$;(2)若 $\alpha=0$,则(ⅰ)$\theta_{B(a)}=p^m\hat{Q}$,其中 $\beta\in Q$,(ⅱ)$\theta_{B(a)}=p^m\hat{N}$,其中 $\beta\in N$.

命题 5 假设 $a\neq0$.

(1)若 $\alpha=0$,则(ⅰ)$\theta(a)=p^m\hat{Q}$,其中 $\beta\in Q$,(ⅱ)$\theta(a)=p^m\hat{N}$,其中 $\beta\in N$;

(2)若 $\alpha\neq0$ 且 $\beta\neq0$,则 $\theta(a)=0$;

(3)若 $\alpha\neq0$ 且 $\beta=0$,则(ⅰ)$\theta(a)=p^mQ$,其中 $\alpha\in Q$,(ⅱ)$\theta(a)=p^m\hat{N}$,其中 $\alpha\in N$.

证明 结合上述两个引理即可得到.

在计算重量分布之前,我们需要再次完善引理. 复数 z 的实数部分用 $\mathrm{Re}(z)$ 表示. 下面的引理来自参考文献[7]中的引理 2.

引理 4 若 $p\equiv3(\bmod 4)$,则 $\sum_{s=1}^{p-1}\theta(sa)=(p-1)\mathrm{Re}(\theta(a))$.

下面计算码 $\Psi(C_{m,p})$的重量分布.

定理 1 假设 $a\neq0$,$p\equiv3(\bmod 4)$且 m 是奇数.

(1)当 $\theta(a)=0$ 时,$w_H(\Psi(E(a)))=(p-1)(p^{2m-1}-p^{m-1})$,这样的码字有$(p^m-1)^2$个;

(2)当 $\theta(a)\neq0$ 时,$w_H(\Psi(E(a)))=\frac{1}{2}(p-1)(2p^{2m-1}-p^{m-1})$,这样的码字有 $2(p^m-1)$个.

证明 第一种情况下的重量通过结合引理 1 和引理 4 即可得到. 在第二种情况中,由命题 5,有 $\theta(a)=p^m\hat{Q}$,或者 $\theta(a)=p^m\hat{N}$. 注意到,在对 p 和 m 的假设下,根据第四部分中的等式(2),高斯和 $G(\eta)$ 是虚数且 $\mathrm{Re}(\hat{Q})=\mathrm{Re}(\hat{N})=-\frac{1}{2}$. 结合引理 1 和引理 4 得到第二种情况下的重量. 每种重量的码字个数由命题 5 得到.

因此我们构造出了一个 F_p 上码长为 $p^{2m}-p^m$,维数为 $2m$ 的码,其非零码字重量 w_1,w_2 和对应的频数在表 1 中给出.

表 1 $\Psi(C_{m,p})$的重量分布

重量	频数
0	1
$w_1=(p-1)(p^{2m-1}-p^{m-1})$	$(p^m-1)^2$
$w_2=\frac{1}{2}(p-1)(2p^{2m-1}-p^{m-1})$	$2(p^m-1)$

5.2 $\Psi(C'_{m,p})$的重量分布

接下来计算 $\theta'(a)=\theta'_{A(a)}+\theta'_{B(a)}$,其中 $a=\alpha+u\beta$ 且 $\alpha,\beta\in F_{p^m}$. 令 $x'=t_1+t_1'u$,$t_1\in F_{p^m}^*$,$t_1'\in F_{p^m}$. 显然有 $\theta'_{A(a)}=\sum_{t_1\in F_{p^m}^*,t_1'\in F_{p^m}}\omega^{T_{m/1}(\alpha t_1-\beta t_1')}$,$\theta'_{B(a)}=\sum_{t_1\in F_{p^m}^*,t_1'\in F_{p^m}}\omega^{T_{m/1}(\alpha t_1'+\beta t_1)}$.

下面通过计算 $\theta'_{A(a)}$和 $\theta'_{B(a)}$来得到 $\theta'(a)$的值.

引理 5 假设 $a\neq0$. (1)当 $\beta\neq0$ 时,$\theta'_{A(a)}=0$;(2)当 $\beta=0$ 且 $\alpha\in F_{p^m}^*$时,$\theta'_{A(a)}=-p^m$.

证明 $\theta'_{A(a)}=\sum_{t_1\in F_{p^m}^*}\omega^{T_{m/1}(\alpha t_1)}\sum_{t_1'\in F_{p^m}}\omega^{T_{m/1}(-\beta t_1')}$. 由特征的正交性,当 $\beta=0$ 时,$\sum_{t_1'\in F_{p^m}}\omega^{T_{m/1}(-\beta t_1')}=p^m$,否则等于 0. 当 $\beta=0$,$\alpha\in F_{p^m}^*$时,因为 $a\neq0$,所以 $\sum_{t_1\in F_{p^m}^*}\omega^{T_{m/1}(\alpha t_1)}=-1$.

引理 6 假设 $a\neq0$. (1)若 $\alpha\neq0$,则 $\theta'_{B(a)}=0$;(2)若 $\alpha=0$ 且 $\beta\in F_{p^m}^*$,则 $\theta'_{B(a)}=-p^m$.

证明过程类似引理 5,故此处省略.

命题6　假设 $a\neq 0$. (1)若 $\alpha=0$,则 $\theta'(a)=-p^m$;(2)若 $\alpha\neq 0$,则(i) $\theta'(a)=0$,若 $\beta\neq 0$,(ii) $\theta'(a)=-p^m$,若 $\beta=0$.

证明　该结果可由 $\theta'_{A(a)}$ 和 $\theta'_{B(a)}$ 的值计算得到.

定理2　假设 $a\neq 0$,对于所有的奇素数 p 和奇数 m,

(1)当 $\theta'(a)=0$ 时,$w_H(\Psi(E'(a)))=2(p-1)(p^{2m-1}-p^{m-1})$,这一重量的码字个数为 $(p^m-1)^2$;

(2)当 $\theta'(a)\neq 0$ 时,$w_H(\Psi(E'(a)))=(p-1)(2p^{2m-1}-p^{m-1})$,这一重量的码字个数为 $2(p^m-1)$.

因此我们构造了 F_p 上一个码长为 $2(p^{2m}-p^m)$,维数为 $2m$ 的码,其中非零码字的重量 w'_1,w'_2 及其对应的频数在表2中给出.

表2　$\Psi(C'_{m,p})$ 的重量分布

重量	频数
0	1
$w'_1=2(p-1)(p^{2m-1}-p^{m-1})$	$(p^m-1)^2$
$w'_2=(p-1)(2p^{2m-1}-p^{m-1})$	$2(p^m-1)$

表1和表2中的参数在文献[2~4,6,10]中没有出现过. 表1和表2中码的参数与文献[2]中的码 SU1 和 SU2 的长度成比例,维数相同,但是重量分布不同,因此我们得到的码是新的. $w'_1=2w_1$,$w'_2=2w_2$,$N'=2N$,且 w'_1,w'_2 分别与 w_1,w_2 的频数相同,维数也相同,因此码 $\Psi(C'_{m,p})$ 可以看作是 $\Psi(C_{m,p})$ 的一个2-重复码.

下面利用 Griesmer 界研究 $\Psi(C_{m,p})$ 和 $\Psi(C'_{m,p})$ 的最优性. 首先回顾一下 Griesmer 界:令 C 是参数为 $[n,k,d]$ 的码,若 $\sum_{j=0}^{k-1}\lceil d/p^j\rceil\leqslant n$,则码 C 是最优的.

定理3　对所有的奇素数 p 和奇数 $m\geqslant 3$,码 $\Psi(C_{m,p})$ 是最优的.

证明　码 $\Psi(C_{m,p})$ 的参数分别为 $N=p^{2m}-p^m$,$k=2m$,$d=(p-1)(p^{2m-1}-p^{m-1})$. 我们断言 $\sum_{j=0}^{k-1}\lceil d/p^j\rceil\leqslant N$,达到 Griesmer 界. 取整函数的值根据 j 的取值有两个不同的值.

(1)当 $0\leqslant j\leqslant m-1$ 时,$\lceil d/p^j\rceil=p^{2m-j}-p^{2m-j-1}-p^{m-j}+p^{m-j-1}$;(2)当 $m\leqslant j\leqslant 2m-1$ 时,$\lceil d/p^j\rceil=p^{2m-j}-p^{2m-j-1}$. 因此,$\sum_{j=0}^{k-1}\lceil d/p^j\rceil=p^{2m}-p^m=N$. 所以这个码是最优的.

例　当 $p=m=3$ 时,我们得到了一个三元码,其参数为 $[702,6]$,且其非零码字的重量分别为 468,677. 由 Griesmer 界可以验证得到的这个码是最优的.

定理4　对奇素数 p 和奇数 $m\geqslant 3$,码 $\Psi(C'_{m,p})$ 是最优的.

证明　码 $4\Psi(C'_{m,p})$ 的参数为 $N'=2(p^{2m}-p^m)$,$d=2(p-1)(p^{2m-1}-p^{m-1})$,$k=2m$. 我们断言 $\sum_{j=0}^{k-1}\lceil d/p^j\rceil<N'$,满足最优码的条件. 取整函数根据 j 的取值有三种不同的值.

(1)当 $0\leqslant j\leqslant m-1$ 时,则有 $\lceil d/p^j\rceil=2(p^{2m-j}-p^{2m-j-1}-p^{m-j}+p^{m-j-1})$;(2)当 $j=m$ 时,则有 $\lceil d/p^j\rceil=2p^m-2p^{m-1}-1$;(3)当 $m+1\leqslant j\leqslant 2m-1$ 时,则有 $\lceil d/p^j\rceil=2p^{2m-j}-2p^{2m-j-1}$. 因此 $\sum_{j=0}^{k-1}\lceil d/p^j\rceil=2p^{2m}-2p^m-1$,注意到 $\sum_{j=0}^{k-1}\lceil d/p^j\rceil<N'$,得证.

6　迹码的对偶码

首先计算 $\Psi(C_{m,p})$ 和 $\Psi(C'_{m,p})$ 的对偶距离.

定理5　对奇素数 p 和奇数 $m\geqslant 3$,$\Psi(C_{m,p})$ 的对偶距离 d' 为2.

证明　首先通过证明 $\Psi(C_{m,p})^{\perp}$ 中不包含重量为1的码字来证明 $d'\geqslant 2$. 假设存在这样一个非零码字 $x=t+ut'\in L$. 因此,对 $\forall a\in F_{p^{2m}}$,有 $T_{m/1}(\alpha t-\beta t')=0$ 或 $T_{m/1}(\alpha t'+\beta t)=0$. 由 $\beta=\pm\alpha$ 和迹函数是非退化的得到 t,t' 的唯一解为 $t=t'=0$,这与 $t\in Q$ 矛盾. 下面用 Hamming 球包界证明 $d'<3$. 若 $d'\geqslant 3$,则有不等式 $p^{2m}\geqslant 1+N(p-1)>N(p-1)>p^{2m+1}-p^{2m}-p^{m+1}$,即有 $2p^{2m}>p^{m+1}(p^m-1)$,对其两边同时除以 p^{m+1},得到 $1>(p-2)p^{m-1}$,而当 $p\geqslant 3$ 且 $m\geqslant 3$ 时该不等式不可能成立. 综上,$\Psi(C_{m,p})$ 的对偶距离为2.

定理6　对奇素数 p 和奇数 m,$\Psi(C'_{m,p})$ 的对偶距离 d'' 为2.

证明　证明 $d''\geqslant 2$ 的方法与定理5中的类似,故此处省略. 基于 Hamming 球包界定理,经过化简后得到 $2>p^{m-1}(2p-3)$,而该不等式对于任意的 p 和 m 都不成立,因此证明了 $d''<3$.

7　在秘钥共享方案中的应用

7.1　支撑结构

F_p^N 中的一个向量 $\boldsymbol{x}$ 的支撑 $\boldsymbol{s}(\boldsymbol{x})$ 定义为非零元所在位置组成的集合. 我们称向量 $\boldsymbol{x}$ 比向量 $\boldsymbol{y}$ 大,当 $\boldsymbol{s}(\boldsymbol{x})$ 包含 $\boldsymbol{s}(\boldsymbol{y})$. 线性码 C 的极小码字定义为非零码字中最小的码字. 总的来说,确定一个给定的线性码中的极小码字是困难的. 但是,文献[11]中给出了可以通过码的重量较容易的确定极小码字的一种情况.

引理7　(Ashikhmin-Barg)一个 p-元码 C 中的最小和最大重量分别用 w_0 和 w_∞ 表示,若 $\frac{w_0}{w_\infty}>\frac{p-1}{p}$,则 C 中每个码字都是极小的.

命题7　当 $p\equiv 3(\bmod 4)$ 时,$\Psi(C_{m,p})$ 中的所有非零

码字都是极小的.

证明 由上述引理 $w_0 = w_1$ 且 $w_\infty = w_2$. 将上述引理中的不等式改写成 $pw_1 > (p-1)w_2$,化简后得到 $p^m - \frac{p}{2} - \frac{1}{2} > 0$,该不等式对 $p \geq 3$ 成立.

命题 8 当 p 是奇素数时,$\Psi(C'_{m,p})$ 中的所有非零码字都是极小的.

证明 类似上述命题的证明,我们有 $2p^m > p+1$ 显然成立,当 p 是奇素数.

7.2 Massey 方案

为确定一个秘钥共享方案中包含所有极小访问集,极小码字的概念被提出了. Massey 方案是一个应用 F_p 上长度为 N 的码 C 的秘钥共享方案结构. 文献[12]是一篇著名的关于线性码在秘钥共享方案中的应用的文章. 另一方面,值得注意的是,文献[13]表明在一些特殊情况下,也就是当所有非零码字都是极小码字的情况,根据 d' 的值不同,秘钥共享方案有以下一些选择:

(1)若 $d' \geq 3$,则秘钥共享方案是"democratic":每个用户属于相同个数联盟.

(2)若 $d' = 2$,则存在属于每个联盟的用户,称为"dictators".

由命题 7 和定理 6,我们可以看出基于 $\Psi(C_{m,p})$ 和 $\Psi(C'_{m,p})$ 构建的秘钥共享方案都是"dictatorial".

8 总结

本文主要是构造了两类新的 2-重量码,并且这两个都是最优码. 这些码被定义为 F_{p^2} 上迹码的 p-元像,具有阿贝尔码的代数结构. 通过高斯和以及特征和给出了这两类码重量分布的具体的计算过程. 最后刻画了 F_{p^2} 上迹码的 Gray 像在秘钥共享方案中的应用. 基于 F_{p^m} 的乘群上的一些其他的定义集是值得考虑的. 特别的,将本文中的高斯周期 $\hat{Q}$,$\hat{N}$ 用其他的特征和替换,类似文献[8,9]中研究不可约循环码时用到的特征和,这可能可以得到一些其他的少重量码.

参考文献

[1] P Delsarte. Weights of linear codes and strongly regular normed spaces[J]. Discrete Mathematics,1972,3(1):47-64.

[2] R Calderbank, W M Kantor. The geometry of two-weight codes[J]. Bulletin of London Mathematical Society,1986,18(2):97-122.

[3] A E Brouwer, W H Haemers. Spectra of Graphs[M]. New York:Springer,2012.

[4] M J Shi, Y Liu, P Solé. Optimal two weight codes from trace codes over $F_2 + uF_2$[J]. IEEE Communications Letters,2016,20(12):2346-2349.

[5] M J Shi, Y Liu, P Solé. Optimal two weight codes from trace codes over a non-chain ring[J]. Discrete Applied Mathematics,2017,219:176-181.

[6] Y Liu, M J Shi, P Solé. Two-weight and three-weight codes from trace codes over $F_p + uF_p + vF_p + uvF_p$[J]. Discrete Mathematics,2018,341(2):350-357.

[7] M J Shi, R S Wu, Y Liu, P Solé. Two and three weight codes over $F_p + uF_p$[J]. Cryptography and Communications-Discrete-Structures Boolean Functions and Sequences,2017,9(5):637-646.

[8] R J McEliece, H Rumsey Jr. Euler products, cyclotomy, and coding[J]. Journal of Number Theory, 1972, 4(3):302-311.

[9] C S Ding, J Yuan. Hamming weights in irreducible cyclic codes[J]. Discrete Mathematics,2011,313(4):434-446.

[10] M J Shi, Y Guan, P Solé. Two new families of two-weight codes[J]. IEEE Transactions on Information Theory, 2017,63(10):6240-6246.

[11] A Ashikhmin, A Barg. Minimal vectors in linear codes [J]. IEEE Transactions on Informations Theory,1998,44(5):2010-2017.

[12] J Yuan, C S Ding. Secret sharing schemes from three classes of linear codes[J]. IEEE Transactions on Information Theory,2006,52(1):206-212.

[13] C S Ding, J Yang. Covering and secret sharing with linear codes[A]. International Conference on Discrete Mathematics and Theoretical Computer Science[C]. Berlin Heidelberg:Springer-Verlag,2003. 11-25.

作者简介

管 玥 女,1994 年 11 月出生于江苏省常州市. 安徽大学数学科学学院硕士研究生,主要研究方向为代数编码.
E-mail:guanyueeee@163.com

施敏加 男,1980 年 2 月出生于安徽省枞阳县. 安徽大学数学科学学院教授、博士生导师,基础数学系主任. 主持国家自然科学基金 3 项,安徽省自然科学基金杰出青年基金等省部级重点项目 5 项,在 Elsevier 出版社出版英文学术专著 1 本,发表学术论文 80 余篇,其中 SCI/EI 收录 50 余篇.
E-mail:smjwcl.good@163.com