DOI:10.13878/j.cnki.jnuist.2018.06.016

邓岚[1]

一类极小线性码及其应用

摘要

利用由定义集设计线性码的方法,通过选取新的定义集,构造了一类新的且具有2个非零重量的线性码,并以指数和为工具,确定了其重量分布.进一步,判定了所构造这类线性码是极小线性码,并研究了该类线性码在秘密共享方案中的应用.

关键词

线性码;重量分布;秘密共享方案

中图分类号 O157

文献标志码 A

0 引言

在编码领域中,具有较少非零重量的线性码可被应用于秘密共享方案[1]、强正则图[2]、结合方案[3]等领域,因此,构造具有较少非零重量的线性码是一个十分有意义的研究课题.线性码的重量分布是反映其性能的一个重要参数,但是,计算线性码的重量分布并不容易.只有当线性码具有较少个数的重量时,才有可能确定其重量分布.计算线性码的重量分布常常可转化为确定某些指数和的取值分布问题.近年来,已有大量关于线性码的构造及其重量分布的研究成果[4-5].

利用定义集构造线性码是一种常用的构造线性码的方法[5],下面简要回顾一下该方法.设 $\mathbb{F}_q$ 表示含有 q 个元素的有限域,其中 $q=p^m$,p 为一素数,m 为正整数.集合 $D=\{d_1,d_2,\cdots,d_n\}\subseteq\mathbb{F}_q$,$\mathrm{tr}_m$ 为从 $\mathbb{F}_q$ 到 $\mathbb{F}_p$ 的迹函数,$\mathbb{F}_p$ 上长度为 n 的线性码定义为 $C_D=\{(\mathrm{tr}_m(xd_1),\mathrm{tr}_m(xd_2),\cdots,\mathrm{tr}_m(xd_n)):x\in\mathbb{F}_q\}$,并称集合 D 为线性码 C_D 的定义集.根据已有的研究可知只要恰当地选择定义集 D,就可以构造一些具有较少重量的线性码.近年来,研究者通过选择不同的定义集构造了多类具有较少重量的线性码,详见文献[6-7].

当 p 为一素数,$m\geqslant 2$ 为正整数时,Li 等[8] 通过选取定义集 $D=\{(x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n)\}=\{(x,y)\in\mathbb{F}_q^2\setminus\{(0,0)\}:\mathrm{tr}_m(x^{l_1}+y^{l_2})=0\}$,构造了 p 元线性码:$C_D=\{(\mathrm{tr}_m(ax_1+by_1),\cdots,\mathrm{tr}_m(ax_n+by_n)):a,b\in\mathbb{F}_{p^m}\}$,其中$(l_1,l_2)=(1,1),(1,2),(1,p^{\frac{m}{2}}+1),(2,2),(2,p^{\frac{m}{2}}+1)$ 或$(p^{\frac{m}{2}}+1,p^{\frac{m}{2}}+1)$.通过计算,他们证明了这些码是二重量或三重量的.

由此受到启发,本文选取定义集 $D_c=\{(x,y)\in\mathbb{F}_q^2:\mathrm{tr}_m(x^2+y^2)=c\}$ 来构造线性码,其中 $q=p^m$,p 是一个奇素数,$m\geqslant 2$ 为正整数,c 为$\mathbb{F}_p$ 中一给定的非零元素.以有限域上的指数和为工具,计算了这类线性码的重量分布,并证明了所构造的这类线性码是极小线性码.进一步,本文还研究了此类码在秘密共享方案中的应用.

1 预备知识

为了研究所构造的线性码的重量分布情况,接下来给出一些基本的定义和用到的引理.

设 p 为一素数,$\mathbb{F}_p^n$表示有限域$\mathbb{F}_p$ 上的 n 维向量空间,若 C 是向量

收稿日期 2018-06-27

资助项目 国家自然科学基金(11301552)

作者简介

邓岚,女,硕士生,研究方向为代数编码与密码学.753321777@qq.com

1 中南民族大学 数学与统计学学院,武汉,430074

空间 $\mathbb{F}_p^n$的一个线性子空间,则 C 称为 p 元线性码,C 中每一个向量称为一个码字,n 为码长.设 $a=(a_1,a_2,\cdots,a_n)$ 和 $b=(b_1,b_2,\cdots,b_n)$ 是线性码 C 中的两个码字,码字 a 的 Hamming 重量定义为:$W(a)=|\{a_i|a_i\neq 0,1\leqslant i\leqslant n\}|$,码字 a 和 b 的 Hamming 距离定义为:$d(a,b)=W(a-b)$.设 C 为有限域$\mathbb{F}_p$ 上的线性码,若其码长为 n,维数为 k,极小 Hamming 距离为 d,则记 C 为 $[n,k,d;p]$ 线性码.令 A_i 代表码 C 中 Hamming 重量为 i 的码字的数目,则码的重量分布多项式为 $W_C(z)=1+A_1z+A_2z^2+A_nz^n$,并称序列$(A_1,A_2\cdots,A_n)$ 为码的重量分布.

后文始终假设 $q=p^m$,p 为奇素数,$m\geqslant 2$ 为正整数,$\mathbb{F}_q$ 表示含有 q 个元素的有限域,$\mathbb{F}_q^*$ 表示$\mathbb{F}_q$ 中的非零元素的集合.设 $\forall a\in\mathbb{F}_q$,$\mathbb{F}_q$ 上的加法特征定义为 $\chi_a(x)=\xi_p^{\mathrm{tr}_m(ax)}$,$\forall x\in\mathbb{F}_q$,其中 $\xi_p=\mathrm{e}^{\frac{2\pi\sqrt{-1}}{p}}$ 为 p 次本原单位根.显然$\chi_0(x)=1$,$\forall x\in\mathbb{F}_q$,称$\chi_0(x)$ 为$\mathbb{F}_q$ 的平凡加法特征.易知:当 $a=0$ 时,$\sum\limits_{x\in\mathbb{F}_q}\chi_a(x)=q$;当 $a\in\mathbb{F}_q^*$ 时,$\sum\limits_{x\in\mathbb{F}_q}\chi_a(x)=0$.此外,称$\chi_1$ 为$\mathbb{F}_q$ 的加法主特征,任取 $b\in\mathbb{F}_q$,有$\chi_b(x)=\chi_1(bx)$,$\forall x\in\mathbb{F}_q$.

设g是$\mathbb{F}_q$的一个生成元,$0\leqslant j\leqslant q-2$,$\mathbb{F}_q$的乘法特征[9]$\lambda_j(\cdot)$ 定义为 $\lambda_j(g^k)=\xi_p^{2\pi\sqrt{-1}jk/(q-1)}$,$k=0,1,\cdots,q-2$.特别地,乘法特征$\lambda_{(q-1)/2}$为$\mathbb{F}_q$的二次特征,下文中用 η 来表示,约定 $\eta(0)=0$.

下文中令 $\bar{\lambda}$ 和$\bar{\chi}$ 分别为$\mathbb{F}_p$ 的乘法特征和加法特征,$\bar{\eta}$ 为 $\mathbb{F}_p$ 的二次特征.$G(\lambda)=\sum\limits_{x\in\mathbb{F}_{q^*}}\lambda(x)\chi(x)$ 和 $\bar{G}(\bar{\lambda})=\sum\limits_{x\in\mathbb{F}_p^*}\bar{\lambda}(x)\bar{\chi}(x)$ 分别为$\mathbb{F}_q$ 和$\mathbb{F}_p$ 上的高斯和,显然有 $G(\lambda_0)=\bar{G}(\bar{\lambda}_0)=-1$.下面给出本文所需的一些重要结论:

引理 1[8-9]　令 $q=p^m$,p 为奇素数,$m\geqslant 1$ 为整数,η 为$\mathbb{F}_q$ 的二次特征,则有

$$G(\eta)=(-1)^{m-1}\sqrt{(p^*)^m}=\begin{cases}(-1)^{m-1}\sqrt{q}, & \text{若 } p\equiv 1 \bmod 4,\\ (-1)^{m-1}(\sqrt{-1})^m\sqrt{q}, & \text{若 } p\equiv 3 \bmod 4,\end{cases}$$

这里 $p^*=(-1)^{\frac{p-1}{2}}p$.

引理 2[10]　设p 为奇素数,$q=p^m$,η 和 $\bar{\eta}$ 分别表示$\mathbb{F}_q$ 和$\mathbb{F}_p$ 上的二次特征.若 m 为偶数,则对于 $y\in\mathbb{F}_p^*$ 有 $\eta(y)=1$;若 $m\geqslant 2$ 为奇数,则对于 $y\in\mathbb{F}_p^*$ 有$\eta(y)=\bar{\eta}(y)$.

引理 3[9]　符号同前,若q为奇数且$f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$,其中 $a_2\neq 0$,则

$$\sum_{x\in\mathbb{F}_q}\xi_p^{\mathrm{tr}_m(f(x))}=\xi_p^{\mathrm{tr}_m(a_0-a_1^2(4a_2)^{-1})}\eta(a_2)G(\eta).$$

2　线性码的构造及其重量分布

设 c 为$\mathbb{F}_p^*$ 中一给定元素,选取定义集:

$$D_c=\{(x,y)\in\mathbb{F}_q^2:\mathrm{tr}_m(x^2+y^2)=c\}.\tag{1}$$

设 $n_c=|D_c|$,并设 $D_c=\{(x_1,y_1),\cdots,(x_{n_c},y_{n_c})\}$,构造线性码:

$$C_{D_c}=\{(\mathrm{tr}_m(ad_1+bd_1),\cdots,\mathrm{tr}_m(ad_{n_c}+bd_{n_c})):a,b\in\mathbb{F}_q\}.\tag{2}$$

本文的主要任务是研究式(2)中构造的线性码 C_{D_c} 的重量分布.首先,计算码 C_{D_c} 的码长 n_c:

$$\begin{aligned}n_c&=|\{(x,y)\in\mathbb{F}_q^2:\mathrm{tr}_m(x^2+y^2)=c\}|=\\&\sum_{x,y\in\mathbb{F}_q}\frac{1}{p}\sum_{z\in\mathbb{F}_p}\xi_p^{z[\mathrm{tr}_m(x^2+y^2)-c]}=\\&\sum_{x,y\in\mathbb{F}_q}\frac{1}{p}\left(1+\sum_{z\in\mathbb{F}_p^*}\xi_p^{z[\mathrm{tr}_m(x^2+y^2)-c]}\right)=\\&\frac{q^2}{p}+\frac{1}{p}\sum_{z\in\mathbb{F}_p^*}\xi_p^{-zc}\sum_{x\in\mathbb{F}_q}\xi_p^{z\mathrm{tr}_m(x^2)}\sum_{y\in\mathbb{F}_q}\xi_p^{z\mathrm{tr}_m(y^2)}=\\&\frac{q^2}{p}+\frac{1}{p}(-1)G(\eta)^2.\end{aligned}$$

同时,由引理 1 有 $G(\eta)^2=(-1)^{\frac{m(p-1)}{2}}p^m$,则码长为 $n_c=p^{2m-1}-(-1)^{\frac{m(p-1)}{2}}p^{m-1}$.

对于码 C_{D_c} 中的码字 $c(a,b)$,记 $N(a,b)$ 为码字 $(\mathrm{tr}_m(ax_1+by_1),\cdots,\mathrm{tr}_m(ax_{n_c}+by_{n_c}))$ 中分量 0 的个数.即有:

$$\begin{aligned}N(a,b)&=|\{(x_i,y_i)\in D_c:\mathrm{tr}_m(ax_i+by_i)=0,1\leqslant i\leqslant n_c\}|=\\&\sum_{x,y\in\mathbb{F}_q}\left(\frac{1}{p}\sum_{z_1\in\mathbb{F}_p}\xi_p^{z_1[\mathrm{tr}_m(x^2+y^2)-c]}\right)\left(\frac{1}{p}\sum_{z_2\in F_p}\xi_p^{z_2\mathrm{tr}_m(ax+by)}\right)=\\&\frac{1}{p^2}\sum_{x,y\in\mathbb{F}_q}\Big[1+\sum_{z_1\in F_p^*}\xi_p^{z_1[\mathrm{tr}_m(x^2+y^2)-c]}+\sum_{z_2\in\mathbb{F}_p^*}\xi_p^{z_2\mathrm{tr}_m(ax+by)}+\\&\sum_{z_1\in F_p^*}\xi_p^{z_1[\mathrm{tr}_m(x^2+y^2)-c]}\sum_{z_2\in\mathbb{F}_p^*}\xi_p^{z_2\mathrm{tr}_m(ax+by)}\Big]=\\&\frac{q^2}{p^2}+\frac{1}{p^2}(\Omega_1+\Omega_2+\Omega_3).\end{aligned}\tag{3}$$

其中:

$$\Omega_1=\sum_{x,y\in\mathbb{F}_q}\sum_{z_1\in\mathbb{F}_p^*}\xi_p^{z_1[\mathrm{tr}_m(x^2+y^2)-c]},$$

$$\Omega_2=\sum_{x,y\in\mathbb{F}_q}\sum_{z_2\in\mathbb{F}_p^*}\xi_p^{z_2\mathrm{tr}_m(ax+by)},$$

$$\Omega_3=\sum_{x,y\in\mathbb{F}_q}\sum_{z_1\in\mathbb{F}_p^*}\xi_p^{z_1[\mathrm{tr}_m(x^2+y^2)-c]}\sum_{z_2\in\mathbb{F}_p^*}\xi_p^{z_2\mathrm{tr}_m(ax+by)}.$$

下面计算 Ω_1,Ω_2 和 Ω_3.由 n_c 的计算不难求得:

$$\Omega_1=\sum_{x,y\in\mathbf{F}_q}\sum_{z_1\in\mathbf{F}_p^*}\xi_p^{z_1[\mathrm{tr}_m(x^2+y^2)-c]}=$$
$$\sum_{z_1\in\mathbf{F}_p^*}\xi_p^{-z_1c}\sum_{x\in\mathbf{F}_q}\xi_p^{z_1\mathrm{tr}_m(x^2)}\sum_{y\in\mathbf{F}_q}\xi_p^{z_1\mathrm{tr}_m(y^2)}=-G(\eta)^2,$$
$$\Omega_2=\sum_{x,y\in\mathbf{F}_q}\sum_{z_2\in\mathbf{F}_p^*}\xi_p^{z_2\mathrm{tr}_m(ax+by)}=$$
$$\sum_{z_2\in F_p^*}\sum_{x\in\mathbf{F}_q}\xi_p^{\mathrm{tr}_m(z_2ax)}\sum_{y\in\mathbf{F}_q}\xi_p^{\mathrm{tr}_m(z_2by)}=$$
$$\begin{cases}(p-1)q^2, & (a,b)=(0,0),\\ 0, & (a,b)\neq(0,0),\end{cases}$$
$$\Omega_3=\sum_{x,y\in\mathbf{F}_q}\sum_{z_1\in\mathbf{F}_p^*}\xi_p^{z_1[\mathrm{tr}_m(x^2+y^2)-c]}\sum_{z_2\in\mathbf{F}_p^*}\xi_p^{z_2\mathrm{tr}_m(ax+by)}=$$
$$\sum_{z_1,z_2\in\mathbf{F}_p^*}\xi_p^{-z_1c}\sum_{x\in\mathbf{F}_q}\xi_p^{\mathrm{tr}_m(z_1x^2+z_2ax)}\sum_{y\in\mathbf{F}_q}\xi_p^{\mathrm{tr}_m(z_1y^2+z_2by)}=$$
$$\sum_{z_1\in\mathbf{F}_p^*}\xi_p^{-z_1c}\sum_{z_2\in\mathbf{F}_p^*}(\xi_p^{\mathrm{tr}_m\left(-\frac{a^2z_2^2}{4z_1}\right)}\eta(z_1)G(\eta))\times$$
$$\xi_p^{\mathrm{tr}_m\left(-\frac{b^2z_2^2}{4z_1}\right)}\eta(z_1G(\eta))=$$
$$\sum_{z_1\in\mathbf{F}_p^*}\xi_p^{-z_1c}\sum_{z_2\in\mathbf{F}_p^*}\xi_p^{\mathrm{tr}_m\left(-\frac{(a^2+b^2)z_2^2}{4z_1}\right)}G(\eta)^2=$$
$$G(\eta)^2\sum_{z_1\in\mathbf{F}_p^*}\xi_p^{-z_1c}\sum_{z_2\in\mathbf{F}_p^*}\xi_p^{\mathrm{tr}_m((a^2+b^2)(-z_2^2z_1)}=$$
$$G(\eta)^2\sum_{z_2\in\mathbf{F}_p^*}\sum_{z_1\in\mathbf{F}_p^*}\xi_p^{[\mathrm{tr}_m(a^2+b^2)z_2^2+c]z_1}.$$

下面不妨设 c 为 $\mathbb{F}_p^*$ 中的平方元且 $p\equiv1 \bmod 4$，其他情况可类似讨论.分以下几种情况讨论：

（ⅰ）当 $\mathrm{tr}_m(a^2+b^2)=0$ 时，有：

$$\Omega_3=G(\eta)^2\sum_{z_1,z_2\in\mathbf{F}_p^*}\xi_p^{[\mathrm{tr}_m(a^2+b^2)z_2^2+c]z_1}=$$
$$G(\eta)^2(p-1)\sum_{z_1\in\mathbf{F}_p^*}\xi_p^{cz_1}=-(p-1)G(\eta)^2.$$

（ⅱ）当 $\mathrm{tr}_m(a^2+b^2)\neq0$ 时，有：

情况 1.当 $\mathrm{tr}_m(a^2+b^2)$ 且为 $\mathbb{F}_p^*$ 中的平方元时，$-\dfrac{c}{\mathrm{tr}_m(a^2+b^2)}$ 为 $\mathbb{F}_p^*$ 中的平方元.当 $z_2\in\mathbb{F}_p^*$ 时，$z_2^2=-\dfrac{c}{\mathrm{tr}_m(a^2+b^2)}$ 有两解，即对于给定的 a,b,c，域 $\mathbb{F}_p^*$ 中满足 $\mathrm{tr}_m(a^2+b^2)z_2^2+c=0$ 的 z_2 有 2 个，$\mathbb{F}_p^*$ 中其余 $p-3$ 个 z_2 使得 $\mathrm{tr}_m(a^2+b^2)z_2^2+c\neq0$.从而有：

$$\Omega_3=G(\eta)^2\sum_{z_1,z_2\in\mathbf{F}_p^*}\xi_p^{[\mathrm{tr}_m(a^2+b^2)z_2^2+c]z_1}=$$
$$G(\eta)^2[2(p-1)+(p-3)(-1)]=(p+1)G(\eta)^2.$$

情况 2.当 $\mathrm{tr}_m(a^2+b^2)$ 且为 $\mathbb{F}_p^*$ 中的非平方元时，$-\dfrac{c}{\mathrm{tr}_m(a^2+b^2)}$ 为 $\mathbb{F}_p^*$ 中的非平方元.$z_2\in\mathbb{F}_p^*$ 时，$z_2^2=-\dfrac{c}{\mathrm{tr}_m(a^2+b^2)}$ 无解，即 $\mathbb{F}_p^*$ 中 $p-1$ 个 z_2 均使得 $\mathrm{tr}_m(a^2+b^2)z_2^2+c\neq0$，从而有：

$$\Omega_3=G(\eta)^2\sum_{z_1,z_2\in\mathbf{F}_p^*}\xi_p^{[\mathrm{tr}_m(a^2+b^2)z_2^2+c]z_1}=-(p-1)G(\eta)^2.$$

综上，当 c 为 $\mathbb{F}_p^*$ 中的平方元且 $p\equiv1 \bmod 4$ 时，有

$$\Omega_3=\sum_{x,y\in F_q}\sum_{z_1\in F_p^*}\xi_p^{z_1[\mathrm{tr}_m(x^2+y^2)-c]}\sum_{z_2\in F_p^*}\xi_p^{z_2\mathrm{tr}_m(ax+by)}=$$
$$\begin{cases}-(p-1)G(\eta)^2, & \mathrm{tr}_m(a^2+b^2)=0,\\ (p+1)G(\eta)^2, & \mathrm{tr}_m(a^2+b^2)\text{ 为 }\mathbb{F}_p^*\text{ 中的平方元},\\ -(p-1)G(\eta)^2, & \mathrm{tr}_m(a^2+b^2)\text{ 为 }\mathbb{F}_p^*\text{ 中非平方元}.\end{cases}$$

其他情况可得类似结果，此处不再展开讨论.利用以上分析，可以给出如下结果：

定理 1 由式(1)和式(2)定义的码 C_{D_c} 是一个码长为 $p^{2m-1}-(-1)^{\frac{m(p-1)}{2}}p^{m-1}$，维数为 $2m$ 的二重线性码，其重量分布如表 1 所示.

证明 C_{D_c} 中码字个数为 q^2 个，从而 C_{D_c} 的维数为 $2m$.下面来考察 C_{D_c} 的重量分布.不妨设 c 为 $\mathbb{F}_p^*$ 中的平方元且 $p\equiv1 \bmod 4$，其他情况可类似证明.码字 $c(a,b)$ 的汉明重量为：

$$W_{\mathrm{H}}(c(a,b))=n_c-N(a,b). \tag{4}$$

所以将式(3)和上述 $n_c,\Omega_1,\Omega_2,\Omega_3$ 的计算结果代入式(4)中，有：

（ⅰ）当 $(a,b)=(0,0)$ 时，有

$$W_H(c(a,b))=n_c-N(a,b)=0.$$

（ⅱ）当 $(a,b)\neq(0,0)$ 且 $\mathrm{tr}_m(a^2+b^2)=0$ 时，有

$$W_H(c(a,b))=n_c-N(a,b)=p^{2m-1}-p^{2m-2}.$$

表 1 线性码 C_{D_c} 的重量分布

Table 1 Weight distribution for code C_{D_c}

重量	次数
0	1
$p^{2m-1}-p^{2m-2}$	$\dfrac{p^{2m-1}(p+1)+(-1)^{\frac{m(p-1)}{2}}p^{m-1}(p-1)}{2}-1$
$p^{2m-1}-p^{2m-2}-2(-1)^{\frac{m(p-1)}{2}}p^{m-1}$	$\dfrac{(p-1)[p^{2m-1}-(-1)^{\frac{m(p-1)}{2}}p^{m-1}]}{2}$

这种情况出现的次数为同时满足条件 $(a,b)\in\mathbb{F}_q^2\backslash\{(0,0)\}$ 和条件 $\mathrm{tr}_m(a^2+b^2)=0$ 的 (a,b) 的个数,其等价求解 $|\{(a,b)\in\mathbb{F}_q^2\backslash\{(0,0)\}:\mathrm{tr}_m(a^2+b^2)=0\}|$ 的值.文献[11]中已经给出 $|\{(a,b)\in\mathbb{F}_q^2\backslash\{(0,0)\}:\mathrm{tr}_m(a^2+b^2)=0\}|$ 的求解过程和结果,则从中易得重数为 $p^{2m-1}+(-1)^{\frac{m(p-1)}{2}}(p-1)p^{m-1}-1$.

(ⅲ) 当 $(a,b)\neq(0,0)$ 且 $\mathrm{tr}_m(a^2+b^2)$ 为 $\mathbb{F}_p^*$ 中的非平方元时,有

$$W_{\mathrm{H}}(c(a,b))=n_c-N(a,b)=p^{2m-1}-p^{2m-2}.$$

这种情况出现的次数为同时满足条件 $(a,b)\in\mathbb{F}_q^2\backslash\{(0,0)\}$ 和条件 $\mathrm{tr}_m(a^2+b^2)=t$ 的 (a,b) 的个数,其中 t 为 $\mathbb{F}_p^*$ 中非平方元.因为 $\mathbb{F}_p^*$ 中平方元与非平方元各占一半,即域 $\mathbb{F}_p^*$ 中平方元和非平方元的个数均为 $\frac{(p-1)}{2}$ 个,结合 n_c 的计算易求得重数为 $\frac{(p-1)[p^{2m-1}-(-1)^{\frac{m(p-1)}{2}}p^{m-1}]}{2}$.

(ⅳ) 当 $(a,b)\neq(0,0)$ 且 $\mathrm{tr}_m(a^2+b^2)$ 为 $\mathbb{F}_p^*$ 中的平方元,有

$$W_{\mathrm{H}}(c(a,b))=n_c-N(a,b)=p^{2m-1}-p^{2m-2}-2(-1)^{\frac{m(p-1)}{2}}p^{m-1}.$$

这种情况出现的次数为同时满足条件 $(a,b)\in\mathbb{F}_q^2\backslash\{(0,0)\}$ 和条件 $\mathrm{tr}_m(a^2+b^2)=t$ 的 (a,b) 的个数,其中 t 为 $\mathbb{F}_p^*$ 中平方元.与(ⅲ)中计算同理易求得此时重数为 $\frac{(p-1)[p^{2m-1}-(-1)^{\frac{m(p-1)}{2}}p^{m-1}]}{2}$.

由(ⅰ)到(ⅳ)可得码 C_{D_c} 重量分布(表1).其中需要注意的是:情况(ⅱ)和情况(ⅲ)计算出的重量均为 $p^{2m-1}-p^{2m-2}$,因此此重量对应的重数应为两种情况的重数之和,经计算可得此重量对应的重数为 $\frac{p^{2m-1}(p+1)+(-1)^{\frac{m(p-1)}{2}}p^{m-1}(p-1)}{2}-1$.证毕.

下面用 Magma 给出两个例子,实验结果与定理1结论吻合.

例1 设 $p=3,m=2$,分别取 $c=1,2$,经 Magma 程序验证可得,C_{D_c} 均为一个[24,4]线性码,重量分布均为 $1+56x^{18}+24x^{12}$,与定理1结论吻合.

例2 设 $p=3,m=3$,分别取 $c=1,2$,经 Magma 程序验证可得,C_{D_c} 均为一个[252,6]线性码,重量分布均为 $1+476x^{162}+252x^{180}$,与定理1结论吻合.

3 线性码上的秘密共享方案

下面介绍的有关秘密共享方案的基本知识,主要来自文献[1,11].秘密共享方案包含一个可信的秘密分发者和 $n-1$ 个参与者所组成的集合 $P=\{P_1,P_2,\cdots,P_{n-1}\}$、存取结构、秘密空间 S、份额空间、份额分发算法以及秘密恢复算法.其中参与者集合包含全体参与秘密共享的人员,秘密空间 S 给出要共享秘密的取值范围.对于主秘密 s,参与者集合中只有那些事先授权的子集中的参与者,利用他们手中的秘密份额才能恢复秘密,这些子集组成的集合称为存取结构,其中子集叫做授权子集.如果一个授权子集的任何真子集均不能恢复秘密,称这个授权子集为极小授权子集.份额空间给出了分发给参与者子秘密的取值范围.利用线性码构造秘密共享方案是一种常用的方法.

一般来说,线性码所构造秘密共享方案的存取结构是难以确定的,但是基于极小线性码的对偶码所构造的秘密存取结构是容易确定的.所以,在这部分先判定本文所构造的线性码是一个极小码,然后再研究其在秘密共享协议中的应用.

在判定本文所构造的线性码是一个极小码前,我们给出一些基本的定义和用到的引理:

定义1[12] 设向量 $\boldsymbol{c}=(c_1,c_2,\cdots,c_n)\in\mathbb{F}_q^n$,指标集 $\{i|\ c_i\neq0,1\leqslant i\leqslant n\}$ 称为向量 $\boldsymbol{c}$ 的支撑.如果码字 c_2 的支撑包含码字 c_1 的支撑就称码字 c_2 覆盖 c_1.

定义2[12] 如果码 C 的第一个码字 c 的第一个分量为1,称这样的码字为正规码字.如果一个正规码字不覆盖码 C 的其他码字,则称这个码字为一个极小码字.

定义3[13] 如果码 C 的一个非零码字只覆盖它的倍,不覆盖别的码字,则称这样的码字是一个极小向量.

定义4[11] 如果线性码 C 的生成矩阵中不含零列,且码 C 的每个非零码字为极小向量,则称码 C 是极小线性码.

由于直接由定义判定线性码是否为极小码较为困难,所以常转化为用以下引理来判定线性码是否为极小码.

引理4[1] 在线性码 C 中,如果码 C 的生成矩阵没有零列,且满足不等式 $\frac{w_{\min}}{w_{\max}}>\frac{p-1}{p}$,此处 $w_{\max}$ 和 $w_{\min}$ 分别代表码 C 的极大重量和极小重量,则线性码 C 是一个极小线性码.

推论1 令定义集 $D_c=\{(x,y)\in\mathbb{F}_q^2:\mathrm{tr}_m(x^2+y^2)=c\}$,其中 $c\in\mathbb{F}_p^*$ 且为 $\mathbb{F}_p^*$ 中的平方元,p 为奇素

数,则定义在此定义集上的码 C_{D_c} 是一个极小线性码.

证明 这里任设 $p \equiv 1 \bmod 4$,其他情况类似可证.因为当 $p \equiv 1 \bmod 4$ 时,$(-1)^{\frac{m(p-1)}{2}} = 1$,所以有 $\frac{w_{\min}}{w_{\max}} = \frac{p^{2m-1} - p^{2m-2} - 2p^{m-1}}{p^{2m-1} - p^{2m-2}}$,且满足不等式 $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$.则本文中的线性码的极小重量和极大重量无论 p 和 m 取何值时,均满足不等式 $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$,因此本文中的线性码是一个极小线性码.证毕.

由上述命题可知本文构造的线性码是极小码,可被应用于秘密共享方案中.接下来,我们先回顾文献[1]中提到的基于线性码来构造秘密共享方案的方法,然后再研究基于本文中的极小线性码的对偶码上的秘密共享方案的存取结构.

设 C 是 $\mathbb{F}_p$ 上一个参数为 $[n,k,d;p]$ 的线性码,其生成矩阵为 $\boldsymbol{G} = [g_0, g_1, \cdots, g_{n-1}]$,用 $\boldsymbol{H} = [h_0, h_1, \cdots, h_{n-1}]$ 表示其对偶码 $C^{\perp}$ 的生成矩阵.在基于线性码 C 的秘密共享协议中,秘密 s 是 $\mathbb{F}_p$ 中的一个元素,为了共享秘密 s,秘密分发者随机选取向量 $\boldsymbol{u} = [u_0, u_1, \cdots, u_{n-k-1}]$,使得 $s = \boldsymbol{u}h_0$.分发者将 $\boldsymbol{u}$ 作为一个信息向量,计算对应的码字 $t = (t_0, t_1, \cdots, t_{n-1}) = \boldsymbol{u}H$,且将份额 t_i 发送给参与者 P_i,作为他们的秘密份额 $i \geqslant 1$.

注意到 $t_0 = \boldsymbol{u}h_0 = s$,则可知份额集 $\{t_{i_1}, t_{i_2}, \cdots, t_{i_m}\}$ 能重构主秘密 s 当且仅当 h_0 为 $h_{i_1}, h_{i_2}, \cdots, h_{i_m}$ 的线性组合.这个结论等价如下引理:

引理 5[14] 设 C 是 $\mathbb{F}_p$ 上一个参数为 $[n,k;p]$ 的线性码,其生成矩阵为 $G = [g_0, g_1, \cdots, g_{n-1}]$.若其对偶码 $C^{\perp}$ 中存在一个形如

$$(1,0,\cdots,0,c_{i_j},0,\cdots,0,c_{i_m},0,\cdots,0)$$

的极小码字,其中至少对某一个 j 满足 $c_j \neq 0 (1 \leqslant i_1 < \cdots < i_m \leqslant n-1, 1 \leqslant m \leqslant n-1)$,则份额 $\{t_{i_1}, t_{i_2}, \cdots, t_{i_m}\}$ 能重构出主秘密 s.

由引理 5 可知,如果在对偶码 $C^{\perp}$ 中有形如 $(1,0,\cdots,0,c_{i_j},0,\cdots,0,c_{i_m},0,\cdots,0)$ 的极小码字,那么 h_0 则是 $h_{i_1}, h_{i_2}, \cdots, h_{i_m}$ 的一个线性组合,即 $h_0 = \sum_{j=1}^{m} x_j h_{i_j}$.那么主秘密 s 则能通过计算 $s = \sum_{j=1}^{m} x_j s_{i_j}$ 得到,其中 $x_j \in \mathbb{F}_p (1 \leqslant j \leqslant m)$.同时,易知所有极小授权子集所组成的集合与线性码的对偶码中的极小码字所组成的集合存在对应关系.一般来说,秘密共享方案中的存取结构很难确定,通常由以下引理给出:

引理 6[12] 令 C 为有限域 $\mathbb{F}_p$ 上参数为 $[n,k;p]$ 的线性码,$\boldsymbol{G} = [g_0, g_1, \cdots, g_{n-1}]$ 为其生成矩阵.令 $d^{\perp}$ 为对偶码 $C^{\perp}$ 的极小距离.如果 C 的每个非零码字都是极小码字,则基于 $C^{\perp}$ 的秘密共享方案中,一共有 $n-1$ 个参与者,存在 p^{k-1} 个极小授权子集.此外有:

1) 当 $d^{\perp} = 2$ 时:

a.如果 g_i 是 g_0 的倍数,$1 \leqslant i \leqslant n-1$,则参与者 P_i 在每一个授权子集中;

b.如果 g_i 不是 g_0 的倍数,$1 \leqslant i \leqslant n-1$,则参与者 P_i 一定出现在 p^{k-1} 个授权子集中的 $(p-1)p^{k-2}$ 个中.

2) 当 $d^{\perp} = 3$ 时,对任意参与者集合中的 t 个参与者一定出现在 p^{k-1} 个授权子集中的 $(p-1)^t p^{k-(t+1)}$ 个中,其中 $1 \leqslant t \leqslant \min\{k-1, d^{\perp}-2\}$.

为了得到基于本文极小线性码 C_{D_c} 的秘密共享方案的存取结构,确定其对偶码 $C_{D_c}^{\perp}$ 的极小距离是必不可少的一步,可由以下引理确定线性码 C_{D_c} 的对偶码 $C_{D_c}^{\perp}$ 的极小距离:

引理 7 由式(1)和式(2)定义的极小线性码 C_{D_c} 的对偶码 $C_{D_c}^{\perp}$ 的极小距离 $d^{\perp}$ 为 2.

证明 令 $W_{C_{D_c}^{\perp}}(z) = 1 + A_1^{\perp} z + A_2^{\perp} z^2 + \cdots + A_n^{\perp} z^n$ 为对偶码 $C_{D_c}^{\perp}$ 的重量分布多项式,其中 n 为码 $C_{D_c}^{\perp}$ 的码长,序列 $(A_1^{\perp}, A_2^{\perp} \cdots, A_n^{\perp})$ 称为码 $C_{D_c}^{\perp}$ 的重量分布.由 MacWilliams 恒等式[9] 得:

$$W_{C_{D_c}^{\perp}}(z) = \frac{1}{p^{2m}}(1 + (p-1)z)^{p^{2m-1} - (-1)^{\frac{m(p-1)}{2}} p^{m-1}} \left\{ \frac{(1-z)^{p^{2m-1} - p^{2m-2}} [p^{2m-1}(p+1) + (-1)^{\frac{m(p-1)}{2}} p^{m-1}(p-1) - 2]}{2(1+pz-z)^{p^{2m-1} - p^{2m-2}}} + 1 + \right.$$

$$\left. \frac{(1-z)^{p^{2m-1} - p^{2m-2} - 2(-1)^{\frac{m(p-1)}{2}} p^{m-1}} (p-1)[p^{2m-1} - (-1)^{\frac{m(p-1)}{2}} p^{m-1}]}{2(1+pz-z)^{p^{2m-1} - p^{2m-2} - 2(-1)^{\frac{m(p-1)}{2}} p^{m-1}}} \right\},$$

$W_{C^{\perp}}(z)$ 的展开式中 z^i 的系数即为 $A_i^{\perp}$.$i = 1$ 时 z^i 的系数为零,即 $A_1^{\perp} = 0$;而当 $i = 2$ 时,$A_2^{\perp} \neq 0$,即由极小距离的定义得码 $C_{D_c}^{\perp}$ 的极小距离 $d^{\perp}$ 为 2.证毕.

由引理 6 和引理 7 可得基于本文的极小线性码

C_{D_c} 的秘密共享方案的存取结构如推论 2 所示:

推论 2 线性码 C_{D_c} 是一个参数为 $[p^{2m-1}-(-1)^{\frac{m(p-1)}{2}}p^{m-1},2m;p]$ 的极小线性码,则基于对偶码 $C_{D_c}^{\perp}$ 的秘密共享方案中,一共有 $p^{2m-1}-(-1)^{\frac{m(p-1)}{2}}p^{m-1}-1$ 个参与者,存在 p^{2m-1} 个极小授权子集.此外有:

1) 如果 g_i 是 g_0 的倍数,$1\leqslant i\leqslant n-1$,则参与者 P_i 在每一个授权子集中;

2) 如果 g_i 不是 g_0 的倍数,$1\leqslant i\leqslant n-1$,则参与者 P_i 一定出现在 p^{2m-1} 个授权子集中的 $(p-1)p^{2m-2}$ 个中.

证明 只需证明基于 $C_{D_c}^{\perp}$ 的秘密共享方案中有独裁者,即证对偶码 $C_{D_c}^{\perp}$ 的极小距离 $d^{\perp}$ 为 2,由引理 7 即证得.证毕.

下面给出了一个本文构造的极小线性码 C_{D_c} 在秘密共享方案中应用的具体例子:

例 3 设 $p=3,m=2$,分别取 $c=1,2$,经 Magma 程序可得,码 C_{D_c} 均为一个[24,4]线性码,重量分布均为 $1+56x^{18}+24x^{12}$,其对偶码 $C_{D_c}^{\perp}$ 的重量分布均为 $1+24x^2+256x^3+\cdots+208\,384x^{24}$,且对偶码 $C_{D_c}^{\perp}$ 的生成矩阵 $\boldsymbol{H}=[h_0,h_1,\cdots,h_{n-1}]$ 均为:

$$\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&2&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&2&2\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&1&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&1&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&2\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&2&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&2&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&2&2&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&2&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&2&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1
\end{bmatrix}.$$

则基于线性码 C_{D_c} 的对偶码 $C_{D_c}^{\perp}$ 上的秘密共享方案中有 23 个参与者和一个秘密分发者,这位可信的秘密分发者给每个参与秘密共享的参与者一个公开的身份信息 $j_i=i$,其中 $23\geqslant i\geqslant 0$,同时秘密分发者随机选取向量 $\boldsymbol{u}=[u_0,u_1,\cdots,u_{19}]$.秘密分发者先将主秘密划分:

$$S=\boldsymbol{uH}=(s,s_1,\cdots,s_{23})=(u_0,u_1,\cdots,2u_0+2u_1+\cdots+2u_{18},2u_1+u_3+\cdots+u_{19}).$$

然后,秘密分发者将秘密份额 s_i 发送给参与者 P_i,作为他们的秘密份额,其中 $23\geqslant i\geqslant 0$.需要注意的是在共享秘密的过程中,参与者数目和参与者身份以及对偶码的生成矩阵是公开的,参与者没有修改权限只能读取.

注意到 $s=\boldsymbol{u}h_0=u_0$,子秘密集合 $\{s_{i_1},s_{i_2},\cdots,s_{i_m}\}$ 可以重构主秘密 s 当且仅当 h_0 是 $h_{i_1},h_{i_2},\cdots,h_{i_m}$ 的线性组合.从对偶码 $C_{D_c}^{\perp}$ 的重量分布知对偶码 $C_{D_c}^{\perp}$ 的极小距离 $d^{\perp}$ 为 2,而从对偶码 $C_{D_c}^{\perp}$ 的生成矩阵中可知当参与者 1 号、4 号、5 号、6 号、7 号、11 号、12 号、15 号、16 号、17 号、18 号给出他们手中的子秘密后,可以利用这些子秘密重构主秘密 s:

$$s=u_0=s_{18}+2s_1+2s_4+2s_5+s_6+s_7+s_{11}+2s_{12}+2s_{15}+2s_{16}+s_{17}.$$

同理,一共有 $p^{k-1}=3^3=27$ 个极小授权子集,这 27 个极小授权子集如下列出:

{18,1,4,5,6,7,11,12,15,16,17},
{21,1,2,3,9,10,11,12,13,14,20},
{21,23,2,4,6,9,12,14,15,17,22},
{18,19,23,1,2,4,5,6,8,10,11,12,14,17,20,22},
{18,21,2,3,4,5,6,7,9,10,12,13,14,15,16,17,20},
{18,19,2,3,4,5,8,12,13,14,17},
{18,23,3,5,7,10,12,13,16,20,22},
{21,19,6,7,8,9,10,12,15,16,20},
{21,23,1,2,3,4,6,9,10,11,12,13,14,15,17,20,22},
{18,19,1,2,3,4,5,6,7,8,11,12,13,14,15,16,17,20},
{18,19,23,1,2,5,6,7,8,10,11,12,14,15,16,20,22},
{21,19,23,1,3,4,7,8,9,10,11,12,13,16,17,20,22},
{18,19,21,23,5,6,7,8,9,10,12,13,15,16,20,22},
{18,21,19,1,4,5,6,7,8,9,10,11,12,15,16,17,20},
{18,21,23,1,2,3,5,7,9,10,11,12,13,14,16,20,22},
{18,19,21,23,1,2,5,6,8,9,10,11,12,14,15,20,22},
{18,19,21,23,1,3,4,5,7,8,9,11,12,13,16,17,22},
{18,19,21,23,2,3,4,5,6,8,9,12,13,14,15,17,22},
{18,23,1,3,4,5,6,7,10,11,12,13,15,16,17,20,22},
{21,19,1,2,3,6,7,9,10,11,12,13,14,15,16,20},
{18,19,23,2,3,4,5,7,8,10,12,13,14,16,17,20,22},
{18,19,23,1,2,3,5,6,8,10,11,12,13,14,15,20,22},

{19,21,23,2,4,6,7,8,9,10,12,14,15,16,17,20,22},
{19,21,23,1,3,4,6,7,8,9,11,12,13,15,16,17,22},
{19,21,23,1,3,4,6,7,8,9,11,12,13,14,16,17,22},
{18,21,19,1,2,3,4,5,8,9,10,11,12,13,14,17,20},
{18,21,23,1,2,4,5,6,7,9,11,12,14,15,16,17,22}.

同时,参与者集合{1,2,3,4,5,6,7,8,9,10,11,13,14,15,16,17,18,19,20,21,22,23} 中的每一个参与者均出现在 $18=(p-1)p^{k-2}$ 个极小授权子集中.其中,参与者 12 号在每一个极小授权子集中,因此,能够重构主秘密的参与者集合中必须包含此参与者.如果一个参与者集合想要重构主秘密,则至少包含 11 个成员 (占总参与者个数的 47.8%).

4 结束语

与文献[11]定理 5 中定义的线性码 C_D 相比,本文的不同之处在于通过选取不同的定义集 $D_c=\{(x,y)\in\mathbb{F}_q^2:\mathrm{tr}_m(x^2+y^2)=c\}$,其中 c 为 $\mathbb{F}_p^*$ 中一给定元素,从而构造出了一类线性码 C_{D_c}.首先,本文确定了线性码 C_{D_c} 的重量分布.同时,发现这类线性码的重量分布与非零 c 的选取无关.然后,证明了这类线性码是一类极小线性码,且证明了其对偶码 $C_{D_c}^{\perp}$ 的极小距离 $d^{\perp}$ 为 2.最后,本文还给出了此类极小线性码在秘密共享方案中的简单应用.此外,用文献[15]中构造的定义集可将此线性码推广为更宽泛的形式.

参考文献

References

[1] Yuan J,Ding C S.Secret sharing schemes from three classes of linear codes[J].IEEE Trans Inf Theory,2006,52(1):206-212
[2] Ding C S,Wang X S.A coding theory construction of new systematic authentication codes[J].Theoretical Computer Science,2005,330(1):81-99
[3] Calderbank A R,Goethals J M.Three-weight codes and association schemes[J].Philips Journal of Research,1984,39(4):143-152
[4] Li S,Feng T,Ge G.On the weight distribution of cyclic codes with Niho exponents[J].IEEE Trans Inf Theory,2014,60(7):3903-3912
[5] Ding C S,Li C,Li N,et al.Three-weight cyclic codes and their weight distributions[J].Discrete Mathematics,2016,339(2):415-427
[6] Li F,Wang Q Y,Lin D D.Complete weight enumerators of a class of three-weight linear codes[J].Journal of Applied Mathematics & Computing,2017,55(1/2):733-747
[7] Liu H B,Liao Q Y.Several classes of linear codes with a few weights from defining sets over $\mathbb{F}_p+u\mathbb{F}_p$[J].Designs,Codes and Cryptography,2018,DOI:10.1007/s10623-018-0478-1
[8] Li C J,Yue Q,Fu F W.A construction of several classes of two-weight and three-weight linear codes[J].Applicable Algebra in Engineering,Communication & Computing,2017,28(1):11-30
[9] Lidl R,Niederreiter H.Finite fields[M].Cambridge,1993
[10] Li F,Wang Q Y,Lin D D.A class of three-weight and five-weight linear codes[J].Mathematics,2015,241(31):25-38
[11] Song Y,Li Z H,Li Y M.Secret sharing schemes in minimal linear code[J].Acta Electronica Sinica,2013,41(2):220-226
[12] Ding C S,Yuan J.Covering and secret sharing with linear codes[J].Discrete Mathematics,2003,2731:11-25
[13] Li Z H,Xue T,Lai H.Secret sharing schemes from binary linear codes[J].Information Sciences,2011,180(22):4412-4419
[14] Massey J L.Minimal codewords and secret sharing[C]// The 6th Joint Swedish-Russian Workshop on Information theory.Netherlands:Veldhoven,1993:276-279
[15] Du X N,Wan Y Q.Linear codes from quadratic forms[J].Applicable Algebra in Engineering,Communication and Computing,2017,28(6):535-547

A class of minimum linear codes and their applications

DENG Lan[1]

1 College of Mathematics and Statistics,South-Central University for Nationalities,Wuhan 430074

Abstract Based a generic method,a class of linear codes with two nonzero weights wasconstructed by choosing a new definition set.Utilizing the exponential sums,the weight distribution of the proposed linear code was derived.Furthermore,it was shown that the constructed linear codes were minimum linear codes,and their application in secret sharing schemes was demonstrated.

Key words linear code;weight distribution;secret sharing scheme