一类四重和六重线性码的构造

杜小妮* 吕红霞 王 蓉
(西北师范大学数学与统计学院 兰州 730070)

摘 要：低重线性码在结合方案、认证码以及秘密共享方案等方面有着极其重要的作用，因而低重线性码的设计一直是线性码的重要研究方向。该文通过选取恰当的定义集，构造了有限域F_p(p为奇素数)上的一类四重和六重线性码，利用高斯和确定了码的重量分布，并编写Magma程序进行了验证。结果表明，构造的码中存在关于Singleton界的几乎最佳码。

关键词：线性码；认证码；重量分布；高斯和
中图分类号：TP391 **文献标识码**：A **文章编号**：1009-5896(2019)12-2995-05
DOI: 10.11999/JEIT180939

Construction of a Class of Linear Codes with Four-weight and Six-weight

DU Xiaoni LÜ Hongxia WANG Rong
(*College of Mathematics and Statistics, Northwest Normal University, Lanzhou* 730070, *China*)

Abstract: Due to the wide applications in association schemes, authentication codes and secret sharing schemes etc., construction of the linear codes with a few weights is an important research topic. A class of linear codes with four-weight and six-weight over finite field F_p (p is an odd prime) is constructed by a proper selection of the defining set. The explicit weight distribution is obtained using Gauss sums, and some examples from Magma program to illustrate the validity of the conclusions are provided. The results show that these codes include almost optimal codes with respect to Singleton bound.

Key words: Linear codes; Authentication codes; Weight distribution; Gauss sums

1 引言

线性码由于具有良好的代数结构以及易于描述和加解密的特性，在通信、数据存储和信息安全等领域具有重要的应用。线性码的重量分布问题是编码理论中的一个重要课题，码的重量分布不仅表明了码的纠错能力，还可以用来计算信息在传输过程中产生的错误概率，其中具有较低重量的线性码在结合方案[1]，认证码[2]，组合设计[3]以及秘密共享方案[4]等方面有着极重要的作用。然而确定一般线性码的重量分布是十分困难的，仅有少数线性码可以确定其重量分布。线性码研究的一个重要目标是寻找关于某个给定界的最佳码和几乎最佳码。

继文献[5]首次提出利用定义集来构造线性码的新方法之后，关于线性码的重量分布得到了较为广泛的研究[6–9]。文献[10]中提出通过选择合适的定义集，可以构造具有较低重量的线性码。近年来，文献[11–13]通过选取适当的定义集构造了几类较低重的线性码。这些工作极大地丰富了线性码的研究，但现有工作主要集中于研究定义集为一些特殊函数在迹函数作用下核的线性码的重量分布，而定义集的选取范围较小。本文受文献[11,13]工作的启发，从2次剩余在迹函数下的原像中选取平方函数的核作为定义集构造线性码，并研究了码的重量分布，所构造的码中存在关于Singleton界的几乎最佳码。此外，对于和本文维数相同的线性码，本文所构造的码长度更短，从而信息率更高。

2 基础知识

设m为正整数，p为奇素数，$q=p^m$。F_q是含有q个元素的有限域[14]，记$F_q^*=F_q\backslash\{0\}$。令n为正整数，对任意的向量$\boldsymbol{a}=(a_1,a_2,\cdots,a_n)\in F_q^n$，$\boldsymbol{b}=(b_1,b_2,\cdots,b_n)\in F_q^n$，向量$\boldsymbol{a}$与$\boldsymbol{b}$的(汉明)距离定义为$d(\boldsymbol{a},\boldsymbol{b})=|\{1\le i\le n,\ a_i\ne b_i\}|$。$F_q$上一个$[n,k,d]$线性码$C$是线性空间$F_q^n$的一个$k$维子空间，其最小(汉明)距离为$d$，即$d=\min\limits_{\boldsymbol{a}\ne\boldsymbol{b}\in C} d(\boldsymbol{a},\boldsymbol{b})$。设$A_i$是长度

收稿日期：2018-10-09；改回日期：2019-03-18；网络出版：2019-04-25
*通信作者： 杜小妮 ymldxn@126.com
基金项目：国家自然科学基金(61772022, 61562077)，上海市自然科学基金(16ZR1411200)
Foundation Items: The National Natural Science Foundtion of China (61772022, 61562077), The Shanghai Natural Science Foundation (16ZR1411200)

为n的码C中汉明重量为i的码字个数。码C的重量枚举定义为$\sum_{i=0}^{n} A_i x^i$，其中，$A_0=1$。序列$(1, A_1, A_2, \cdots, A_n)$称为码$C$的重量分布。若$|\{1 \le i \le n : A_i \ne 0\}| = t$，则称码$C$为$t$–重码。

若$[n, k, d]$线性码满足$d = n-k+1$，则称其为关于Singleton界的最佳码。若满足$d = n-k$，则称其为关于Singleton界的几乎最佳码。

由有限域F_q到F_p的迹函数[14]$\mathrm{Tr}(\cdot)$定义为$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{m-1}}$，$\forall \alpha \in F_q$。设集合$D = \{d_1, d_2, \cdots, d_n\} \subseteq F_q$，则$sF_p$上长度为$n$的线性码定义为

$$C_D = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \cdots, \mathrm{Tr}(xd_n)) : x \in F_q\} \quad (1)$$

称集合D为线性码C_D的定义集。

令Sq表示F_p^*中所有2次剩余元素的集合，选择定义集

$$D = \{x \in F_q : \mathrm{Tr}(x) \in Sq, \mathrm{Tr}(x^2)=0\} \quad (2)$$

构造线性码

$$C_D = \{(\mathrm{Tr}(ax))_{x \in D} : a \in F_q\} \quad (3)$$

下文中将讨论当$p \nmid m$时码C_D的重量分布，而当$p|m$时码的性质已被研究[15]。

对任意的$b \in F_q$，F_q上的加法特征[14]定义为$\chi_b(x) = \zeta_p^{\mathrm{Tr}(bx)}$，其中，$x \in F_q$, $\zeta_p = \exp(2\pi\sqrt{-1}/p)$为一个$p$次本原单位根。显然对任意的$x \in F_q$，$\chi_0(x) = 1$，称$\chi_0$为$F_q$的平凡加法特征。加法特征满足正交性[14]

$$\sum_{x \in F_q} \chi_b(x) = \begin{cases} q, & b = 0 \\ 0, & b \ne 0 \end{cases} \quad (4)$$

令g是F_q^*的一个生成元，则F_q上的乘法特征[14]定义为

$$\lambda_j(g^k) = \zeta_p^{2\pi\sqrt{-1}jk/(q-1)}, \quad k = 0, 1, \cdots, (q-2),\ 0 \le j \le (q-2) \quad (5)$$

补充定义$\lambda_j(0) = 0$。对$j = (q-1)/2$，记乘法特征$\eta := \lambda_{(q-1)/2}$为$F_q$的2次特征，令$\bar{\eta}$为$F_p$的2次特征。$F_q$和$F_p$上的高斯和取分别定义为$G(\lambda) = \sum_{x \in F_q^*} \lambda(x)\chi(x)$和$G(\bar{\lambda}) = \sum_{x \in F_p^*} \bar{\lambda}(x)\bar{\chi}(x)$，其中，$\bar{\lambda}$和$\bar{\chi}$分别为$F_p$上的乘法和加法特征。分别记$G_m := G(\eta)$, $G := G(\bar{\eta})$。

3 辅助引理及其证明

本节将给出证明主要结论所用到的引理。

引理 1[14] 若$f(x) = a_2x^2 + a_1x + a_0 \in F_q[x]$，其中$a_2 \ne 0$，则

$$\sum_{x \in F_q} \zeta_p^{\mathrm{Tr}(f(x))} = \zeta_p^{\mathrm{Tr}(a_0 - a_1^2(4a_2)^{-1})} \eta(a_2) G(\eta) \quad (6)$$

引理 2[7] 对任意的$y \in F_p^*$，m为偶数时，$\eta(y) = 1$；m为奇数时，$\eta(y) = \bar{\eta}(y)$。

引理 3[14] 符号含义如上，$G(\eta) = (-1)^{m-1}\sqrt{(p^*)^m}$，其中$p^* = (-1)^{\frac{p-1}{2}} p$。

引理 4[11] 定义$N(u, v) = |\{x \in F_q : \mathrm{Tr}(x^2) = u, \mathrm{Tr}(x) = v,\ u, v \in F_p\}|$，则有

(1)当$u = 0$, $v = 0$时，

$$N(0,\ 0) = \begin{cases} p^{m-2}, & 2|m \\ p^{m-2} + \bar{\eta}(-m)p^{-2}(p-1)G_m G, & 2 \nmid m \end{cases} \quad (7)$$

(2)当$u = 0$, $v \ne 0$时，

$$N(0, \bar{0}) = \begin{cases} (p-1)(p^{m-2} + p^{-1}G_m), & 2|m \\ (p-1)(p^{m-2} - p^{-2}\bar{\eta}(-m)G_m G), & 2 \nmid m \end{cases} \quad (8)$$

(3)当$u \ne 0$, $v \ne 0$时，

$$N(\bar{0}, \bar{0}) = \begin{cases} (p-1)^2 p^{m-2} - p^{-1}(p-1)G_m, & 2|m \\ (p-1)^2 p^{m-2} + \bar{\eta}(-m)p^{-2}(p-1)G_m G, & 2 \nmid m \end{cases} \quad (9)$$

(4)当$u \ne 0$, $v = 0$时，

$$N(\bar{0},\ 0) = \begin{cases} (p-1)p^{m-2}, & 2|m \\ (p-1)p^{m-2} - \bar{\eta}(-m)p^{-2}(p-1)G_m G, & 2 \nmid m \end{cases} \quad (10)$$

显然，码C_D的长度为$n = N(0,\ \bar{0})/2$

$$= \begin{cases} (p-1)(p^{m-2} + p^{-1}G_m)/2, & 2|m \\ (p-1)(p^{m-2} - \bar{\eta}(-m)p^{-2}G_m G)/2, & 2 \nmid m \end{cases} \quad (11)$$

引理 5[11] 设$p \nmid m$，令$V = |\{x \in F_q : \mathrm{Tr}(x) \ne 0, \mathrm{Tr}^2(x) = m\mathrm{Tr}(x^2)\}|$，则

$$V = \begin{cases} (p-1)p^{m-2}, & 2|m \\ (p-1)p^{m-2} + \bar{\eta}(-m)\ p^{-2}(p-1)^2 G_m G, & 2 \nmid m \end{cases} \quad (12)$$

下面确定线性码C_D的重量分布。

令$T = |\{x \in F_q : \mathrm{Tr}(x) = b^2, \mathrm{Tr}(x^2) = 0, \mathrm{Tr}(ax) = 0\}|$, $b \in F_p^*$，任意的$a \in F_q$，则码字$\boldsymbol{c}(a)$的重量为

$$W(\boldsymbol{c}(a)) = n - \frac{p-1}{2} T \quad (13)$$

$$T = \sum_{x \in F_q} \left(\frac{1}{p} \sum_{y \in F_p} \zeta_p^{y(\mathrm{Tr}(x) - b^2)} \right) \left(\frac{1}{p} \sum_{z \in F_p} \zeta_p^{z\mathrm{Tr}(x^2)} \right) \cdot \left(\frac{1}{p} \sum_{\delta \in F_p} \zeta_p^{\delta \mathrm{Tr}(ax)} \right) = \frac{2n}{p(p-1)} + \frac{1}{p^3}(\Omega_1 + \Omega_2 + \Omega_3 + \Omega_4) \quad (14)$$

其中，

$$\Omega_1=\sum_{x\in F_q}\sum_{\delta\in F_p^*}\zeta_p^{\delta\mathrm{Tr}(ax)}=\begin{cases}(p-1)p^m, a=0\\ 0, \quad a\neq 0\end{cases},$$

$$\Omega_2=\sum_{x\in F_q}\sum_{y\in F_p^*}\zeta_p^{y(\mathrm{Tr}(x)-b^2)}\sum_{\delta\in F_p^*}\zeta_p^{\delta\mathrm{Tr}(ax)}=\begin{cases}p^m, a\in F_p^*\\ 0, \quad a\notin F_p^*\end{cases},$$

$$\Omega_3=\sum_{x\in F_q}\sum_{z\in F_p^*}\zeta_p^{z\mathrm{Tr}(x^2)}\sum_{\delta\in F_p^*}\zeta_p^{\delta\mathrm{Tr}(ax)},$$

$$\Omega_4=\sum_{x\in F_q}\sum_{y\in F_p^*}\zeta_p^{y(\mathrm{Tr}(x)-b^2)}\sum_{z\in F_p^*}\zeta_p^{z\mathrm{Tr}(x^2)}\sum_{\delta\in F_p^*}\zeta_p^{\delta\mathrm{Tr}(ax)} \tag{15}$$

引理 6　符号含义如上，有

(1)m为偶数时，

$$\Omega_3=\begin{cases}(p-1)^2G_m, & \mathrm{Tr}(a^2)=0\\ -(p-1)G_m, & \mathrm{Tr}(a^2)\neq 0\end{cases} \tag{16}$$

(2)m为奇数时，$\Omega_3=\bar{\eta}\left(-\mathrm{Tr}(a^2)\right)(p-1)G_mG$。

证明　由引理1和引理2，结论显然成立。证毕

对任意的$a\in F_q$，令$\Delta=m\mathrm{Tr}(a^2)-\mathrm{Tr}^2(a)$，则有下面的引理。

引理 7　符号含义如上，有

(1)m为偶数时，

$$\Omega_4=\begin{cases}(p-1)G_m, & \mathrm{Tr}(a^2)=0,\mathrm{Tr}(a)=0\\ -G_m, & \mathrm{Tr}(a^2)=0,\mathrm{Tr}(a)\neq 0\\ -\bar{\eta}(\Delta)G_mG^2-G_m, & \mathrm{Tr}(a^2)\neq 0\end{cases} \tag{17}$$

(2)m为奇数时，

$$\Omega_4=\begin{cases}-\bar{\eta}(-m)(p-1)G_mG,\\ \qquad \mathrm{Tr}(a^2)=0,\mathrm{Tr}(a)=0\\ \bar{\eta}(-m)G_mG,\\ \qquad \mathrm{Tr}(a^2)=0,\mathrm{Tr}(a)\neq 0\\ \left(-\bar{\eta}(-\mathrm{Tr}(a^2))(p-1)+\bar{\eta}(-m)\right)G_mG,\\ \qquad \mathrm{Tr}(a^2)\neq 0,\Delta=0\\ \left(\bar{\eta}(-\mathrm{Tr}(a^2))+\bar{\eta}(-m)\right)G_mG,\\ \qquad \mathrm{Tr}(a^2)\neq 0,\Delta\neq 0\end{cases} \tag{18}$$

证明　由引理1，有

$$\Omega_4=G_m\sum_{y\in F_p^*}\zeta_p^{-b^2y}\sum_{z\in F_p^*}\eta_m(z)\sum_{\delta\in F_p^*}\zeta_p^{\mathrm{Tr}\left(\frac{a^2\delta^2+2ay\delta+y^2}{-4z}\right)} \tag{19}$$

(1)若m为偶数时，

$$\Omega_4=G_m\sum_{y\in F_p^*}\zeta_p^{-b^2y}\sum_{z\in F_p^*}\zeta_p^{-\frac{m}{4z}y^2}\sum_{\delta\in F_p^*}\zeta_p^{\frac{\mathrm{Tr}(a^2)}{-4z}\delta^2-\frac{\mathrm{Tr}(a)y}{2z}\delta} \tag{20}$$

则当$\mathrm{Tr}(a^2)=0$时，

$$\Omega_4=\begin{cases}(p-1)G_m, & \mathrm{Tr}(a)=0\\ -G_m, & \mathrm{Tr}(a)\neq 0\end{cases} \tag{21}$$

而当$\mathrm{Tr}(a^2)\neq 0$时，

$$\Omega_4=G_mG\sum_{y\in F_p^*}\zeta_p^{-b^2y}\sum_{z\in F_p^*}\zeta_p^{\frac{\mathrm{Tr}(a^2)-m\mathrm{Tr}^2(a)}{4\mathrm{Tr}(a^2)z}y^2}\bar{\eta}(-\mathrm{Tr}(a^2)z)$$
$$-G_m=-\bar{\eta}(\Delta)G_mG^2-G_m \tag{22}$$

(2)若m为奇数时，

$$\Omega_4=G_m\sum_{y\in F_p^*}\zeta_p^{-b^2y}\sum_{z\in F_p^*}\zeta_p^{-\frac{m}{4z}y^2}\bar{\eta}(z)\sum_{\delta\in F_p^*}\zeta_p^{\frac{\mathrm{Tr}(a^2)}{-4z}\delta^2-\frac{2\mathrm{Tr}(a)y}{4z}\delta} \tag{23}$$

因而当$\mathrm{Tr}(a^2)=0$时，

$$\Omega_4=\begin{cases}-\bar{\eta}(-m)(p-1)G_mG, & \mathrm{Tr}(a)=0\\ \bar{\eta}(-m)G_mG, & \mathrm{Tr}(a)\neq 0\end{cases} \tag{24}$$

而当$\mathrm{Tr}(a^2)\neq 0$时，

$$\Omega_4=\bar{\eta}(-\mathrm{Tr}(a^2))G_mG\sum_{y\in F_p^*}\zeta_p^{-b^2y}\sum_{z\in F_p^*}\zeta_p^{\frac{m\mathrm{Tr}^2(a)-\mathrm{Tr}(a^2)}{4\mathrm{Tr}(a^2)z}y^2}$$
$$+\bar{\eta}(-m)G_mG$$
$$=\begin{cases}-\bar{\eta}(-\mathrm{Tr}(a^2))(p-1)G_mG+\bar{\eta}(-m)G_mG,\\ \qquad \Delta=0\\ \bar{\eta}(-\mathrm{Tr}(a^2))G_mG+\bar{\eta}(-m)G_mG,\\ \qquad \Delta\neq 0\end{cases} \tag{25}$$

证毕

引理8 符号含义如上，则

(1)当$a=0$时，$T=p^{m-2}+p^{-1}G_m$，若m为奇数，$T=p^{m-2}-p^{-2}\bar{\eta}(-m)G_mG$；

(2)当$a\in F_p^*$时，$T=0$；

(3)当$a\in F_q{}^*\backslash F_p^*$时，若$m$为偶数，

$$T=\begin{cases}p^{m-3}+p^{-1}G_m, & \mathrm{Tr}(a^2)=0,\mathrm{Tr}(a)=0\\ p^{m-3}+p^{-2}(p-1)G_m, & \mathrm{Tr}(a^2)=0,\mathrm{Tr}(a)\neq 0\\ p^{m-3}-\bar{\eta}(\Delta)p^{-3}G_mG^2, & \mathrm{Tr}(a)\neq 0\end{cases} \tag{26}$$

若m为奇数，

$$T=\begin{cases}p^{m-3}-\bar{\eta}(-m)p^{-2}G_mG, & \mathrm{Tr}(a^2)=0,\mathrm{Tr}(a)=0\\ p^{m-3}+\bar{\eta}(-\mathrm{Tr}(a^2))p^{-2}G_mG, & \mathrm{Tr}(a^2)\neq 0,\Delta\neq 0\\ p^{m-3}, & \text{其它}\end{cases} \tag{27}$$

证明　由式(14)，Ω_1和Ω_2的取值以及引理6和引理7，简单计算可得结论。　证毕

4　主要结论

定理1和定理2将给出式(3)中线性码的重量分布。定理1表明，当m为偶数时，码C_D为六重码，定理2表明，当m为奇数时，码C_D为四重码。

定理 1　m为偶数时，码C_D的长度和维数为$[(p-1)(p^{m-2}+p^{-1}G_m)/2,m]$，其重量分布见表1。其中，

表 1 m为偶数时码C_D的重量分布

重量	频数
0	1
$(p-1)(p^{m-2}+p^{-1}G_m)/2$	$p-1$
$(p-1)(p^{m-2}-p^{m-3})/2$	$p^{m-2}-1$
$(p-1)(p^{m-2}-p^{m-3}+p^{-2}G_m)/2$	$(p-1)(p^{m-2}+p^{-1}G_m)$
$(p-1)(p^{m-2}-p^{m-3}+p^{-1}G_m)/2$	$(p-1)(p^{m-2}-1)$
$(p-1)(p^{m-2}-p^{m-3}+p^{-1}G_m+p^{-3}G_mG^2)/2$	A_5
$(p-1)(p^{m-2}-p^{m-3}+p^{-1}G_m-p^{-3}G_mG^2)/2$	A_6

$$A_5=(p-1)^2(p^{m-2}+p^{-2}G_mG^2)/2 -(p-1)(p^{m-3}G^2+p^{-1}G_m)/2 \tag{28}$$

$$A_6=(p-1)^2(p^{m-2}-p^{-2}G_mG^2)/2 +(p-1)(p^{m-3}G^2-p^{-1}G_m)/2 \tag{29}$$

证明 码C_D的重量分布由引理8和式(13)可得。将表1中的非零重量从上到下依次记为W_i，其对应的频数分别为A_i，$1\le i\le 6$。显然，$A_1=p-1$；由引理4，

$$A_2=N(0,\ 0)-1=p^{m-2}-1 \tag{30}$$

$$A_3=N(0,\ \bar{0})=(p-1)(p^{m-2}+p^{-1}G_m) \tag{31}$$

由引理5，$A_4=(p-1)(p^{m-2}-1)$；再根据MacWilliams方程[16]，有

$$\left.\begin{aligned}&\sum_{i=1}^{6}A_i=p^m-1\\&\sum_{i=1}^{6}W_iA_i=(p-1)^2p^{m-1}(p^{m-2}+p^{-1}G_m)/2\end{aligned}\right\} \tag{32}$$

可得

$$A_5=(p-1)^2(p^{m-2}+p^{-2}G_mG^2)/2 -(p-1)(p^{m-3}G^2+p^{-1}G_m)/2 \tag{33}$$

$$A_6=(p-1)^2(p^{m-2}-p^{-2}G_mG^2)/2 +(p-1)(p^{m-3}G^2-p^{-1}G_m)/2 \tag{34}$$

证毕

例1 设$p=3$，$m=4$，由Magma程序表明，码C_D的参数为$[6,4,2]$，其重量枚举为$1+6x^2+16x^3+36x^4+12x^5+10x^6$，与定理1的结论一致，是满足Singleton界的几乎最佳码。由式(2)可得$D=\{\alpha^{11},\alpha^{19},\alpha^{33},\alpha^{50},\alpha^{57},\alpha^{70}\}$，其中$\alpha$为$F_q^*$的生成元，且式(3)中码$C_D$的生成矩阵为

$$G=\begin{pmatrix}1&0&0&0&0&2\\0&1&0&0&1&1\\0&0&1&0&1&1\\0&0&0&1&2&0\end{pmatrix}$$

表 2 m为奇数时码C_D的重量分布

重量	频数
0	1
$(p-1)(p^{m-2}-\bar{\eta}(-m)\cdot p^{-2}G_mG)/2$	$p-1$
$(p-1)(p^{m-2}-p^{m-3})/2$	$(p-1)(p^{m-2}-(p-2)\bar{\eta}(-m)\cdot p^{-2}G_mG)/2-1$
$(p-1)(p^{m-2}-p^{m-3}-\bar{\eta}(-m)p^{-2}G_mG)/2$	$(p-1)(2p^{m-2}+\bar{\eta}(-m)\cdot p^{-2}(p-2)G_mG-1)$
$(p-1)(p^{m-2}-p^{m-3}-2\bar{\eta}(-m)p^{-2}G_mG)/2$	$(p-1)(p-2)(p^{m-2}-\bar{\eta}(-m)\cdot p^{-2}G_mG)/2$

例2 设$p=5$，$m=6$，由Magma程序表明，码C_D的参数为$[1200,6,960]$，其重量枚举为$1+3600x^{940}+2496x^{950}+6500x^{960}+2400x^{990}+624x^{1000}+4x^{1200}$，与定理1的结论一致。

定理 2 m为奇数时，码C_D的长度和维数为$[(p-1)(p^{m-2}-\bar{\eta}(-m)p^{-2}G_mG)/2,m]$，其重量分布见表2。

证明 码C_D的重量分布由引理8和式(13)可得。将表2中的非零重量从上到下依次记为$\bar{W}_i$，其对应的频数分别为$\bar{A}_i$, $1\le i\le 4$。显然，$\bar{A}_1=p-1$；由引理4和引理5，得$\bar{A}_3=(p-1)(2p^{m-2}+\bar{\eta}(-m)p^{-2}(p-2)G_mG-1)$；再根据MacWilliams方程，有

$$\left.\begin{aligned}&\sum_{i=1}^{4}\bar{A}_i=p^m-1\\&\sum_{i=1}^{4}\bar{W}_i\bar{A}_i=(p-1)^2p^{m-1}\\&\quad\cdot(p^{m-2}-\bar{\eta}(-m)p^{-2}G_mG)/2\end{aligned}\right\} \tag{35}$$

证毕

例3 设$p=5$，$m=3$，由Magma程序表明，码C_D的参数为$[12,3,8]$，其重量枚举为$1+60x^8+24x^2+40x^{12}$，与定理2的结论一致。

例4 设$p=3$，$m=5$，由Magma程序表明，码C_D的参数为$[30,5,18]$，其重量枚举为$1+110x^{18}+100x^{21}+30x^{24}+2x^{30}$，与定理2的结论一致。

5 结束语

本文应用有限域上的迹函数和2次剩余理论构造了一类四重和六重的线性码，并利用特征和理论给出了其重量分布的精确值。最后，编写Magma程序验证了结论的正确性。结果表明，所构造的码中存在关于Singleton界的几乎最佳码。此外，对于和本文维数k相同的线性码，本文所构造的长度n更短，从而信息率k/n更高。

参 考 文 献

[1] CALDERBANK A R and GOETHALS J M. Three-weight codes and association schemes[J]. *Philips Journal of Research*, 1984, 39(4/5): 143–152.

[2] DING Cunsheng, HELLESETH T, KLOVE T, *et al*. A generic construction of Cartesian authentication codes[J]. *IEEE Transactions on Information Theory*, 2007, 53(6): 2229–2235. doi: 10.1109/tit.2007.896872.

[3] CALDERBANK A R and KANTOR W M. The geometry of two-weight codes[J]. *Bulletin of the London Mathematical Society*, 1986, 18(2): 97–122. doi: 10.1112/blms/18.2.97.

[4] YUAN Jin and DING Cunsheng. Secret sharing schemes from three classes of linear codes[J]. *IEEE Transactions on Information Theory*, 2006, 52(1): 206–212. doi: 10.1109/TIT.2005.860412.

[5] BAUMERT L D and MCELIECE R J. Weights of irreducible cyclic codes[J]. *Information and Control*, 1972, 20(2): 158–175. doi: 10.1016/S0019-9958(72)90354-3.

[6] DING Cunsheng. Linear codes from some 2-designs[J]. *IEEE Transactions on Information Theory*, 2015, 61(6): 3265–3275. doi: 10.1109/TIT.2015.2420118.

[7] DING Kelan and DING Cunsheng. Binary linear codes with three weights[J]. *IEEE Communications Letters*, 2014, 18(11): 1879–1882. doi: 10.1109/LCOMM.2014.2361516.

[8] DING Cunsheng, LI Chunlei, LI Nian, *et al*. Three-weight cyclic codes and their weight distributions[J]. *Discrete Mathematics*, 2016, 339(2): 415–427. doi: 10.1016/j.disc.2015.09.001.

[9] XIANG Can, TANG Chunming, and FENG Keqin. A class of linear codes with a few weights[J]. *Cryptography and Communications*, 2017, 9(1): 93–116. doi: 10.1007/s12095-016-0200-y.

[10] DING Cunsheng and NIEDERREITER H. Cyclotomic linear codes of order 3[J]. *IEEE Transactions on Information Theory*, 2007, 53(6): 2274–2277. doi: 10.1109/TIT.2007.896886.

[11] LI Fei, WANG Qiuyan, and LIN Dongdai. A class of three-weight and five-weight linear codes[J]. *Discrete Applied Mathematics*, 2018, 241: 25–38. doi: 10.1016/j.dam.2016.11.005.

[12] LI Chengju, YUE Qin, and FU Fangwei. Complete weight enumerators of some cyclic codes[J]. *Designs, Codes and Cryptography*, 2016, 80(2): 295–315. doi: 10.1007/s10623-015-0091-5.

[13] YANG Shudi, YAO Zhengan, and ZHAO Changan. A class of three-weight linear codes and their complete weight enumerators[J]. *Cryptography and Communications*, 2017, 9(1): 133–149. doi: 10.1007/s12095-016-0187-4.

[14] LIDL R and NIEDERREITER H. Finite Fields[M]. Reading, Mass: Addison-Wesley, 1983, 54–240.

[15] 杜小妮, 吕红霞, 王蓉, 等. 两类四重线性码的构造[J]. 西北师范大学学报: 自然科学版, 2018, 54(6): 1–4.
DU Xiaoni, LÜ Hongxia, WANG Rong, *et al*. A construction of two classes of linear codes with four-weights[J]. *Journal of Northwest Normal University*: *Natural Science*, 2018, 54(6): 1–4.

[16] MACWILLIAMS F J and SLOANE N J A. The Theory of Error-Correcting Codes[M]. Amsterdam: North-Holland Publishing Co., 1977, 126–144.

杜小妮：女，1972年生，教授，博士生导师，研究方向为密码学与信息安全.

吕红霞：女，1993年生，硕士生，研究方向为密码学与信息安全.

王　蓉：女，1993年生，硕士生，研究方向为密码学与信息安全.