中国科学 : 数学　2014 年　第 44 卷　第 9 期 : 1021 ∼ 1034
link.springer.com　math.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

具有两个非零点循环码的权重分布

胡丽琴*, 岳勤, 朱小萌

南京航空航天大学理学院, 南京 210016
E-mail: huqin0916@126.com, yueqin@nuaa.edu.cn, mooneernanjing@163.com

收稿日期: 2014-02-20; 接受日期: 2014-06-09; * 通信作者
国家自然科学基金 (批准号: 11171150)、信息保障技术重点实验室开放基金 (批准号: KJ-13-001)、江苏省普通高校研究生科研创新计划 (批准号: CXLX13-127) 和南京航空航天大学博士学位论文创新与创优基金 (批准号: BCXJ13-17) 资助项目

摘要　循环码作为一类重要的线性码, 因其有效的编码和译码算法而被广泛应用于通信和存储系统. 令 $\mathbb{F}_r$ 为有限域 $\mathbb{F}_q$ 的一个扩域, 其中 $r=q^m$, α 为有限域 $\mathbb{F}_r$ 的本原元. 设 $n=n_1n_2$ 满足 $\gcd(n_1,n_2)=1$ 为 $r-1$ 的因子. 定义 $\mathbb{F}_q$ 上的一类循环码

$$\mathcal{C}=\{c(a_1,a_2)=(T_{r/q}(a_1g_1^i+a_2(g_1g_2)^i))_{i=0}^{n-1}:a_1,a_2\in\mathbb{F}_r\},$$

其中 $g_1=\alpha^{\frac{r-1}{n_1}}$, $g_2=\alpha^{\frac{r-1}{n_2}}$, 且 g_1 与 g_1g_2 不共轭. 本文将利用 Gauss 周期刻画循环码 $\mathcal{C}$ 的权重分布. 特别地, 这类循环码包含一类二重循环码和一类三重循环码.

关键词　循环码　权重分布　分圆　Gauss 周期
MSC (2010) 主题分类　94B15, 11T22, 11T23

1　引言

令 $\mathbb{F}_q$ 为 q 元有限域, 其中 $q=p^s$, p 为素数, s 为正整数. $\mathbb{F}_q$ 上 $[n,k,d]$ 线性码 $\mathcal{C}$ 定义为 $\mathbb{F}_q^n$ 中具有极小 Hamming 距离 d 的 k 维线性子空间. $\mathbb{F}_q$ 上线性码 $\mathcal{C}$ 称为循环码是指对任意的 $(c_0,c_1,\ldots,c_{n-1})\in\mathcal{C}$, 则循环移位得到的 $(c_{n-1},c_0,c_1,\ldots,c_{n-2})\in\mathcal{C}$. 令 $\gcd(n,q)=1$. 考虑一一对应

$$\pi:\mathbb{F}_q^n\to\mathbb{F}_q[x]/(x^n-1),\quad (c_0,c_1,\ldots,c_{n-1})\mapsto c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1},$$

则 $\mathcal{C}$ 为循环码当且仅当 $\pi(\mathcal{C})$ 为环 $\mathbb{F}_q[x]/(x^n-1)$ 的一个理想. 我们知道, $\mathbb{F}_q[x]/(x^n-1)$ 为主理想环, 因此, 存在唯一的次数最小的首一多项式 $g(x)$ 满足 $g(x)\mid(x^n-1)$ 使得 $\pi(\mathcal{C})=(g(x))$, $g(x)$ 称为码 $\mathcal{C}$ 的生成多项式, $h(x)=(x^n-1)/g(x)$ 称为 $\mathcal{C}$ 的校验多项式.

记 A_i 是码长为 n 的码 $\mathcal{C}$ 中 Hamming 权重为 i 的码字个数, 即非负整数 i 为码字中非零分量的个数. $\mathcal{C}$ 的权重计数多项式定义为

$$1+A_1x+A_2x^2+\cdots+A_nx^n.$$

向量 $(1,A_1,A_2,\ldots,A_n)$ 称为码 $\mathcal{C}$ 的权重分布. 若循环码 $\mathcal{C}$ 中码字非零权重的个数为 t, 则称 $\mathcal{C}$ 为 t 重循环码. 码的权重分布不仅对研究码的结构起了很重要的作用, 而且提供了码用于纠错时不能纠错的

英文引用格式: Hu L Q, Yue Q, Zhu X M. Weight distributions of a class of cyclic codes with two nonzeros (in Chinese). Sci Sin Math, 2014, 44: 1021–1034, doi: 10.1360/012014-36

可能性的信息. 因而, 码的权重分布的研究一直是编码理论研究的热点之一. 当然, 确定一般情形下的循环码的权重是极其困难的. 然而, 获得特殊情况下的循环码的权重分布是相对容易的. 关于不可约循环码的相关研究包括文献 [1–5] 等; 具有两个非零点的可约循环码权重分布的研究包括文献 [6–13] 等. 当然, 还有很多其他类的循环码权重分布的研究, 如文献 [14–20] 等. 具有较少权重的循环码的研究与结合方案和跳频序列等紧密相关, 特别地, 二重循环码与强正则图和 partial 差集等问题的研究等价. 关于二重循环码的研究已有很多, 如文献 [21–23], 而 Schmidt 等人[24] 在 2002 年给出了所有不可约二重循环码的刻画. 在二重码的研究基础上, 近期内, 一些学者给出了很多三重和五重循环码, 特别地, 文献 [25,26] 分别给出了一类三重循环码和七类三重循环码.

在下文中, α 为有限域 $\mathbb{F}_r$ 的本原元, $r=q^m$, $q=p^s$, 其中 s 和 m 均为正整数. 令正整数 $n=\prod_{j=1}^{l}n_j$ 为 $r-1$ 的因子, 满足: 对任意的 $1\leqslant i\neq j\leqslant l$, $\gcd(n_i,n_j)=1$. 对于 $1\leqslant i\leqslant l$, 令 $N_i=\frac{r-1}{n_i}$, $g_i=\alpha^{N_i}$, $g_i'=\prod_{j=1}^{i}g_j$, $1\leqslant j\leqslant l$. 为记号方便, 记 $N_0=\frac{r-1}{q-1}$, $g=g_l'$.

本文将考虑循环码

$$\mathcal{C}_{(n_1,\ldots,\prod_{j=1}^{l}n_j)}=\left\{c(a_1,\ldots,a_l)=\left(T_{r/q}\left(\sum_{j=1}^{l}a_jg_j'^i\right)\right)_{i=0}^{n-1}:a_1,\ldots,a_l\in\mathbb{F}_r\right\},\tag{1.1}$$

其中 $T_{r/q}$ 表示 $\mathbb{F}_r$ 到 $\mathbb{F}_q$ 的迹映射, 且对任意的 $i\neq j$, g_i' 和 g_j' 为非共轭元. 由 Delsarte 定理[27] 知, $\mathcal{C}_{(n_1,\ldots,\prod_{j=1}^{l}n_j)}$ 为 $\mathbb{F}_q$ 上以 $\prod_{i=1}^{l}h_i(x)$ 为校验多项式的一个 $[n,k]$ 循环码, 其中 $h_i(x)$ 是 $g_i'^{-1}$ 在 $\mathbb{F}_q$ 上的极小多项式, $1\leqslant i\leqslant l$, $k=\deg(h_1(x))+\deg(h_2(x))+\cdots+\deg(h_l(x))$. 当 $l=2$ 时, 此结果就是文献 [28] 的一个特殊情况, 我们利用这个结果给出了二重循环码和三重循环码, 其中二重循环码也许是已有的, 但是我们给出了不同的证明方法.

本文主要包含以下几个部分: 第 2 节介绍计算循环码权重分布所需要的群特征、分圆和 Gauss 周期等数学工具; 第 3 节给出计算 (1.1) 定义的码 $\mathcal{C}_{(n_1,\ldots,\prod_{j=1}^{l}n_j)}$ 权重分布的方法, 利用 Gauss 周期给出 $l=2$ 情形码的权重分布; 第 4 节给出 $r=q^2$ 时, 一些循环码的权重分布, 特别地, 我们将得到一类二重循环码和一类三重循环码.

2 分圆、特征和 Gauss 周期

设 r 为素数 p 的幂次, $r-1=nN$, n 和 N 为正整数, $\mathbb{F}_r$ 为 r 元有限域, α 为 $\mathbb{F}_r$ 的一个固定的本原元. 定义

$$C_i^{(N,r)}=\alpha^i\langle\alpha^N\rangle,\quad i=0,1,\ldots,N-1,\tag{2.1}$$

其中 $\langle\alpha^N\rangle$ 表示由 α^N 生成的 $\mathbb{F}_r^*$ 的子群. 陪集 $C_i^{(N,r)}$, $0\leqslant i\leqslant N-1$ 称为 $\mathbb{F}_r$ 的 N 阶分圆类[29].

记 $T_{r/p}$ 为 $\mathbb{F}_r$ 到 $\mathbb{F}_p$ 的迹映射, $\zeta_p=\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}}$ 为复数域中 p 次本原单位根, 对有限域 $\mathbb{F}_r$ 中的任意元素 a, 我们可定义 $\mathbb{F}_r$ 的一个加法特征[30,31] 如下:

$$\psi_a:\mathbb{F}_r\to\mathbb{C}^*,\quad \psi_a(x)=\zeta_p^{T_{r/p}(ax)},$$

当 $a=1$ 时, ψ_1 称为 $\mathbb{F}_r$ 的正规加法特征, 我们简单记为 ψ. 加法特征的正交公式[31] 为

$$\sum_{x\in\mathbb{F}_r}\psi(ax)=\begin{cases}r, & \text{若 } a=0;\\ 0, & \text{若 } a\in\mathbb{F}_r^*.\end{cases}\tag{2.2}$$

$\mathbb{F}_r$ 上的 N 阶 Gauss 周期定义为

$$\eta_i^{(N,r)} = \sum_{x\in C_i^{(N,r)}} \psi(x), \quad 0 \leqslant i \leqslant N-1,$$

若 $i \geqslant N$, 令 $\eta_i^{(N,r)} = \eta_{i \pmod N}^{(N,r)}$. 一般情况下, Gauss 周期的取值是很难计算的. 但是, 可以计算出一些特殊情形. 下面给出部分已知的关于 Gauss 周期的结果.

引理 1 [32] 当 $N=2$ 时, Gauss 周期为

$$\eta_0^{(2,r)} = \begin{cases} \dfrac{-1+(-1)^{sm-1}\sqrt{r}}{2}, & \text{若 } p\equiv 1 \pmod 4, \\ \dfrac{-1+(-1)^{sm-1}(\sqrt{-1})^{sm}\sqrt{r}}{2}, & \text{若 } p\equiv 3 \pmod 4, \end{cases}$$
$$\eta_1^{(2,r)} = -1-\eta_0^{(2,r)}.$$

半本原情形的 Gauss 周期的值如下:

引理 2 [33] 若存在一个正整数 e 满足 $p^e \equiv -1 \pmod N$. 令 $r=p^{2ef}$, f 为正整数.

(1) 若 f, p 和 $\frac{p^e+1}{N}$ 都是奇数, 则

$$\eta_{N/2}^{(N,r)} = \frac{(N-1)\sqrt{r}-1}{N}, \quad \eta_i^{(N,r)} = -\frac{\sqrt{r}+1}{N}, \quad \text{对任意的 } i \neq \frac{N}{2};$$

(2) 对于所有其他情形, 有

$$\eta_0^{(N,r)} = \frac{(-1)^{f+1}(N-1)\sqrt{r}-1}{N}, \quad \eta_i^{(N,r)} = \frac{(-1)^f\sqrt{r}-1}{N}, \quad \text{对任意的 } i \neq 0.$$

3 循环码的权重分布

本节将刻画 (1.1) 定义的循环码 $\mathcal{C}_{(n_1,n_1n_2,\ldots,\prod_{j=1}^l n_j)}$ 的权重分布的计算方法, 并且利用 Gauss 周期刻画 $l=2$ 时码的权重分布. 令 $\chi(x) = \zeta_p^{T_{q/p}(x)}$ 为 $\mathbb{F}_q$ 的正规加法特征, 则 $\psi = \chi \circ T_{r/q}$ 是 $\mathbb{F}_r$ 的正规加法特征. 利用特征的正交关系 (2.2), 可得码字 $c(a_1,a_2,\ldots,a_l)$ 的 Hamming 权重 $w_H(c(a_1,a_2,\ldots,a_l))$ 为

$$\begin{aligned} w_H(c(a_1,a_2,\ldots,a_l)) &= \left|\left\{i : T_{r/q}\Big(\sum_{j=1}^l a_j g_j'^i\Big) \neq 0, 0\leqslant i\leqslant n-1\right\}\right| \\ &= n - \left|\left\{i : T_{r/q}\Big(\sum_{j=1}^l a_j g_j'^i\Big) = 0, 0\leqslant i\leqslant n-1\right\}\right| \\ &= n - \sum_{i=0}^{n-1}\frac{1}{q}\sum_{y\in\mathbb{F}_q}\chi\Big(yT_{r/q}\Big(\sum_{j=1}^l a_j g_j'^i\Big)\Big) \\ &= n - \frac{n}{q} - \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{i=0}^{n-1}\chi\Big(T_{r/q}\Big(y\Big(\sum_{j=1}^l a_j g_j'^i\Big)\Big)\Big) \\ &= \frac{(q-1)n}{q} - \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{i=0}^{n-1}\psi\Big(y\Big(\sum_{j=1}^l a_j g_j'^i\Big)\Big). \end{aligned}$$

因为 $\gcd(n_1, n_j) = 1$, $2 \leqslant j \leqslant l$, 对每个 i, $0 \leqslant i \leqslant n-1$, 有

$$i = s\frac{n}{n_1} + t, \quad 0 \leqslant s \leqslant n_1 - 1, \quad 0 \leqslant t \leqslant \frac{n}{n_1} - 1.$$

因此,

$$\begin{aligned}
w_H(c(a_1, a_2, \ldots, a_l)) &= \frac{(q-1)n}{q} - \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{s=0}^{n_1-1}\sum_{t=0}^{\frac{n}{n_1}-1}\psi\Big(y\Big(\sum_{j=1}^{l}a_j\Big(\prod_{k=1}^{j}g_k\Big)^{s\frac{n}{n_1}+t}\Big)\Big)\\
&= \frac{(q-1)n}{q} - \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{s=0}^{n_1-1}\sum_{t=0}^{\frac{n}{n_1}-1}\psi\Big(y\Big(a_1g_1^{s\frac{n}{n_1}+t} + \sum_{j=2}^{l}a_j\Big(\prod_{k=1}^{j}g_k\Big)^{s\frac{n}{n_1}+t}\Big)\Big)\\
&= \frac{(q-1)n}{q} - \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{s=0}^{n_1-1}\sum_{t=0}^{\frac{n}{n_1}-1}\psi\Big(y\Big(a_1g_1^{s\frac{n}{n_1}+t} + \sum_{j=2}^{l}a_j\Big(g_1^{s\frac{n}{n_1}+t}\Big(\prod_{k=2}^{j}g_k\Big)^t\Big)\Big)\Big)\\
&= \frac{(q-1)n}{q} - \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{t=0}^{\frac{n}{n_1}-1}\sum_{s=0}^{n_1-1}\psi\Big(y\Big(a_1g_1^{s\frac{n}{n_1}+t} + \sum_{j=2}^{l}a_j\Big(g_1^{s\frac{n}{n_1}+t}\Big(\prod_{k=2}^{j}g_k\Big)^t\Big)\Big)\Big)\\
&= \frac{(q-1)n}{q} - \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{t=0}^{\frac{n}{n_1}-1}\sum_{s=0}^{n_1-1}\psi\Big(y\Big(a_1g_1^{s} + \sum_{j=2}^{l}a_j\Big(g_1^{s}\Big(\prod_{k=2}^{j}g_k\Big)^t\Big)\Big)\Big).
\end{aligned}$$

反复利用除法算式可得

$$w_H(c(a_1, a_2, \ldots, a_l)) = \frac{(q-1)n}{q} - \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{s_1=0}^{n_1-1}\sum_{s_2=0}^{n_2-1}\cdots\sum_{s_l=0}^{n_l-1}\psi(y(a_1g_1^{s_1} + \cdots + a_lg_1^{s_1}g_2^{s_2}\cdots g_l^{s_l})).$$

因此, 计算循环码 $\mathcal{C}$ 的权重分布, 归结为计算下面和式的值分布:

$$\sum_{y\in\mathbb{F}_q^*}\sum_{s_1=0}^{n_1-1}\cdots\sum_{s_l=0}^{n_l-1}\psi(y(a_1g_1^{s_1} + \cdots + a_lg_1^{s_1}g_2^{s_2}\cdots g_l^{s_l})).$$

一般情形下, 上述和式的值分布也是很难计算的, 因此, 循环码 (1.1) 的权重分布依然很难得到. 然而, 特殊情况下码的权重分布可能相对容易, 因此, 我们将考虑 $l = 2$ 的情形.

设 α 为 $\mathbb{F}_r$ 的本原元, $r = q^m = p^{sm}$, $n = n_1n_2$ 满足 $n \mid r-1$, 其中 n_1 和 n_2 为正整数. 记 $N_0 = \frac{r-1}{q-1}$, $N_1 = \frac{r-1}{n_1}$, $N_2 = \frac{r-1}{n_2}$, $N = \frac{r-1}{n}$. 下面将决定循环码

$$\mathcal{C} := \mathcal{C}_{(n_1,n_1n_2)} = \{c(a,b) = (T_{r/q}(ag_1^i + bg^i))_{i=0}^{n-1} : a, b \in \mathbb{F}_r\} \tag{3.1}$$

的权重分布. 由 Delsarte 定理[34], 码 $\mathcal{C}$ 为 $\mathbb{F}_q$ 上以 $h_1(x)h_2(x)$ 为校验多项式的循环码, 其中 $h_1(x)$ 和 $h_2(x)$ 分别为 g_1^{-1} 和 g^{-1} 在 $\mathbb{F}_q$ 上的极小多项式. 我们很容易得到下面的结论.

引理 3 令 $\deg(h_1(x)) = m_1$, $\deg(h_2(x)) = m_2$, 则

(1) $|\mathcal{C}| = q^{m_1+m_2}$, 即 $\mathcal{C}$ 为 $\mathbb{F}_q$ 上参数为 $[n, m_1+m_2]$ 的循环码;

(2) 存在 $\mathbb{F}_q$ 上线性空间的正合序列:

$$0 \to \ker\mathcal{C} \to \mathbb{F}_r \times \mathbb{F}_r \xrightarrow{\mathcal{C}} \mathcal{C} \to 0,$$

其中 $\mathcal{C}:(a,b)\mapsto c(a,b)$, $\ker\mathcal{C}=\{(a,b)\in\mathbb{F}_r\times\mathbb{F}_r : c(a,b)=0\}$.

证明 参见文献 [35]. □

由引理 3 知, $\mathcal{C}$ 的每个码字在多重集合 $\{c(a,b):(a,b)\in\mathbb{F}_r\times\mathbb{F}_r\}$ 中出现 $q^{2m-m_1-m_2}$ 次, 即

$$\{c(a,b):(a,b)\in\mathbb{F}_r\times\mathbb{F}_r\}=q^{2m-m_1-m_2}*\mathcal{C}.$$

因此, 决定码 $\mathcal{C}$ 的权重分布, 我们只需给出多重集合 $\{c(a,b):(a,b)\in\mathbb{F}_r\times\mathbb{F}_r\}$ 的权重分布.

引理 4 [36] 令 H 和 K 为有限 Abel 群 G 的两个子群, $HK=\{hk:h\in H,k\in K\}$, 则

(1) 对任意的 $h_1,h_2\in H$, $h_1K=h_2K$ 当且仅当 $h_1(H\cap K)=h_2(H\cap K)$. 特别地, 存在群同构 $HK/K\cong H/(H\cap K)$, 因此, $[HK:K]=[H:(H\cap K)]$.

(2) $|H|\cdot|K|=|HK|\cdot|H\cap K|$.

下面给出 $l=2$ 时码的权重分布.

定理 5 令 $d_1=\gcd(N_0,N_1),d_2=\gcd(N_0,N_2)$, $d=\gcd(N_0,N)$. 若 $\gcd(n_1,n_2)=1$, 则由 (3.1) 定义的多重集合 $\{c(a,b):(a,b)\in\mathbb{F}_r\times\mathbb{F}_r\}$ 的权重分布见表 1.

证明 令 χ 为 $\mathbb{F}_q$ 的正规加法特征, 则 $\psi=\chi\circ T_{r/q}$ 为 $\mathbb{F}_r$ 的正规加法特征. 由上面计算的结果可得

$$w_H(c(a,b))=\frac{(q-1)n}{q}-\frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{i=0}^{n_1-1}\sum_{j=0}^{n_2-1}\psi(yag_1^i+ybg_1^ig_2^j).$$

我们分 4 种情形计算 $w_H(c(a,b))$ 的值:

(1) 若 $a=0$ 且 $b=0$, 则

$$w_H(c(a,b))=0.$$

这个值恰好出现一次.

(2) 若 $a\neq0$, $b=0$, 则

$$w_H(c(a,b))=\frac{(q-1)n}{q}-\frac{n_2}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{i=0}^{n_1-1}\psi(yag_1^i)=\frac{(q-1)n}{q}-\frac{n_2}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{x\in C_0^{(N_1,r)}}\psi(ayx).$$

由 α 为 $\mathbb{F}_r$ 的本原元, 我们有 $\mathbb{F}_q^*=\langle\alpha^{\frac{r-1}{q-1}}\rangle=\langle\alpha^{N_0}\rangle$. 因此,

$$\mathbb{F}_q^*\cdot C_0^{(N_1,r)}=\langle\alpha^{d_1}\rangle,\quad \mathbb{F}_q^*\cap C_0^{(N_1,r)}=\langle\alpha^{N_0\cdot\frac{N_1}{d_1}}\rangle,$$

表 1 多重集 $\{c(a,b):(a,b)\in\mathbb{F}_r\times\mathbb{F}_r\}$ 的权重分布

权重	频率
0	1
$\frac{(q-1)n}{q}-\frac{(q-1)d_1}{qN}\eta_j^{(d_1,r)}$	$\frac{r-1}{d_1}\ (0\leqslant j\leqslant d_1-1)$
$\frac{(q-1)n}{q}-\frac{(q-1)d}{qN}\eta_k^{(d,r)}$	$\frac{r-1}{d}\ (0\leqslant k\leqslant d-1)$
$\frac{(q-1)n}{q}-\frac{(q-1)d_1}{qN_1}\sum_{i=0}^{\frac{N_2}{d}-1}\eta_{d_1i+k}^{(N_2,r)}\eta_{d_1i+j}^{(\frac{N_2d_1}{d},r)}$	$\frac{n_2^2d}{d_1}\begin{pmatrix}0\leqslant j\leqslant\frac{N_2d_1}{d}-1\\ 0\leqslant k\leqslant N_2-1\end{pmatrix}$

其中 $d_1=\gcd(N_0,N_1)$. 由引理 4, 我们得到, 若 $a\in C_j^{(d_1,r)}$,

$$w_H(c(a,b))=\frac{(q-1)n}{q}-\frac{n_2}{q}\cdot\frac{(q-1)d_1}{N_1}\sum_{x\in C_0^{(d_1,r)}}\psi(ax)=\frac{(q-1)n}{q}-\frac{(q-1)d_1}{qN}\eta_j^{(d_1,r)}.$$

每个值出现 $\frac{r-1}{d_1}$ 次.

(3) 若 $a=0$, $b\neq 0$, 则

$$w_H(c(a,b))=\frac{(q-1)n}{q}-\frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{i=0}^{n-1}\psi(ybg^i)=\frac{(q-1)n}{q}-\frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{x\in C_0^{(N,r)}}\psi(byx).$$

设 $\gcd(N_0,N)=d$. 我们可类似得到, 若 $b\in C_k^{(d,r)}$,

$$w_H(c(a,b))=\frac{(q-1)n}{q}-\frac{1}{q}\cdot\frac{(q-1)d}{N}\sum_{x\in C_0^{(d,r)}}\psi(bx)=\frac{(q-1)n}{q}-\frac{(q-1)d}{qN}\eta_k^{(d,r)}.$$

每个值出现 $\frac{r-1}{d}$ 次.

(4) 考虑 $a\neq 0, b\neq 0$ 情形. 由上面的结果, 我们得到

$$\begin{aligned}w_H(c(a,b))&=\frac{(q-1)n}{q}-\frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{i=0}^{n_1-1}\sum_{j=0}^{n_2-1}\psi(yag_1^i+ybg_1^ig_2^j)\\&=\frac{(q-1)n}{q}-\frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{x\in C_0^{(N_1,r)}}\sum_{z\in C_0^{(N_2,r)}}\psi(ayx+byxz).\end{aligned}$$

类似地, 由引理 4, 有

$$\begin{aligned}w_H(c(a,b))&=\frac{(q-1)n}{q}-\frac{1}{q}\sum_{z\in C_0^{(N_2,r)}}\sum_{y\in\mathbb{F}_q^*}\sum_{x\in C_0^{(N_1,r)}}\psi(ayx+byxz)\\&=\frac{(q-1)n}{q}-\frac{(q-1)d_1}{qN_1}\sum_{z\in C_0^{(N_2,r)}}\sum_{y\in C_0^{(d_1,r)}}\psi(ay+byz)\\&=\frac{(q-1)n}{q}-\frac{(q-1)d_1}{qN_1}\sum_{y\in C_0^{(d_1,r)}}\psi(ay)\sum_{z\in C_0^{(N_2,r)}}\psi(byz).\end{aligned}$$

若 $d=\gcd(N,N_0)$, 利用循环群的性质可得

$$C_0^{(d_1,r)}\cap C_0^{(N_2,r)}=\langle\alpha^{\frac{N_2d_1}{d}}\rangle,\quad C_0^{(d_1,r)}=\bigcup_{i=0}^{\frac{N_2}{d}-1}\alpha^{d_1\cdot i}C_0^{(\frac{N_2d_1}{d},r)}=\bigcup_{i=0}^{\frac{N_2}{d}-1}C_{d_1\cdot i}^{(\frac{N_2d_1}{d},r)}.$$

再次利用引理 4, 有

$$C_0^{(d_1,r)}\cdot C_0^{(N_2,r)}=\bigcup_{i=0}^{\frac{N_2}{d}-1}\alpha^{d_1i}C_0^{(N_2,r)}=\bigcup_{i=0}^{\frac{N_2}{d}-1}C_{d_1\cdot i}^{(N_2,r)}.$$

因此, 对任意的 $a\in C_j^{(\frac{N_2d_1}{d},r)}$, $b\in C_k^{(N_2,r)}$,

$$w_H(c(a,b))=\frac{(q-1)n}{q}-\frac{(q-1)d_1}{qN_1}\sum_{i=0}^{\frac{N_2}{d}-1}\sum_{y\in C_{d_1\cdot i}^{(\frac{N_2d_1}{d},r)}}\psi(ay)\sum_{z\in C_0^{(N_2,r)}}\psi(byz)$$

$$= \frac{(q-1)n}{q} - \frac{(q-1)d_1}{qN_1} \sum_{i=0}^{\frac{N_2}{d}-1} \sum_{y \in C_{d_1 \cdot i}^{(\frac{N_2 d_1}{d}, r)}} \psi(ay) \sum_{z \in C_{d_1 \cdot i}^{(N_2, r)}} \psi(bz)$$

$$= \frac{(q-1)n}{q} - \frac{(q-1)d_1}{qN_1} \sum_{i=0}^{\frac{N_2}{d}-1} \sum_{z \in C_{d_1 \cdot i}^{(N_2, r)}} \psi(bz) \sum_{y \in C_{d_1 \cdot i}^{(\frac{N_2 d_1}{d}, r)}} \psi(ay)$$

$$= \frac{(q-1)n}{q} - \frac{(q-1)d_1}{qN_1} \sum_{i=0}^{\frac{N_2}{d}-1} \eta_{d_1 i+k}^{(N_2, r)} \eta_{d_1 i+j}^{(\frac{N_2 d_1}{d}, r)}.$$

每个值出现 $\frac{n_2^2 d}{d_1}$ 次.

综上所述, 我们得到表 1. □

例 1 若 $p=3$, $s=m=2$, $n_1=5$, $n_2=16$, 则由 (3.1) 定义的循环码的权重计数多项式为

$$1 + 680x^{64} + 3200x^{71} + 80x^{72} + 2560x^{73} + 40x^{80}.$$

事实上, 我们有 $q=9$, $r=81$, $N_1=16$, $N_2=5$, $d_1=2$, $d_2=5$, $d=1$. 由引理 1 可知,

$$\eta_0^{(2,81)} = -5, \quad \eta_1^{(2,81)} = 4.$$

由引理 2 可得

$$\eta_0^{(5,81)} = 7, \quad \eta_i^{(5,81)} = -2, \quad i = 1,2,3,4,$$
$$\eta_5^{(10,81)} = 8, \quad \eta_i^{(10,81)} = -1 \quad \text{对任意的 } 0 \leqslant i \leqslant 9, \quad i \neq 5.$$

由表 1 可得 $\mathcal{C}$ 是 $\mathbb{F}_9$ 上参数为 $[80, 4, 64]$ 的循环码, 权重计数多项式为

$$1 + 680x^{64} + 3200x^{71} + 80x^{72} + 2560x^{73} + 40x^{80}.$$

4 几类循环码的权重分布

第 3 节用 Gauss 周期刻画了 (3.1) 定义的循环码的权重分布. 但是, Gauss 周期的值只是在 $N=2$, $3, 4$、半本原和指数 2 等很少的情况下已知. 因此, 循环码的确切的权重分布在很多情况下依然很难得到. 作为第 3 节的应用, 我们将在这部分给出特殊情形下 (3.1) 定义的循环码权重的值分布, 特别地, 我们将得到一类二重循环码和一类三重循环码, 即 (3.1) 定义的循环码包含很多性质很好的循环码.

在定理 5 中, 若 $d=d_1$, 则 $n_2 \mid (q-1)$. 事实上, 因为

$$d = \gcd\left(\frac{r-1}{q-1}, \frac{r-1}{n_1 n_2}\right), \quad d = d_1 = \gcd\left(\frac{r-1}{q-1}, \frac{r-1}{n_1}\right),$$

我们可以得到 $r-1 = (q-1)ds = n_1 n_2 dt$, $r-1 = (q-1)d_1 s_1 = n_1 d_1 t_1$, 其中 $s, t, t_1 \in \mathbb{Z}$, $\gcd(s,t)=1$ 且 $\gcd(s_1, t_1)=1$. 所以, $t_1 = n_2 t$, $t_1 \mid (q-1)$, 因此, $n_2 \mid (q-1)$.

定理 6 设记号与定理 5 相同. 若 $d = d_1 \geqslant 1$, $r = q^2$, $n_2 = q-1$, 则 (3.1) 定义的多重集 $\{c(a,b) : (a,b) \in \mathbb{F}_r \times \mathbb{F}_r\}$ 的权重分布见表 2.

表 2　$r=q^2$, $d=d_1>1$, $n_2=q-1$ 时, 多重集 $\{c(a,b):(a,b)\in\mathbb{F}_r\times\mathbb{F}_r\}$ 的权重分布

权重	频率
0	1
$\frac{(q-1)n}{q}-\frac{(q-1)d}{qN}\eta_j^{(d,r)}$	$\frac{2(r-1)}{d}(0\leqslant j\leqslant d-1)$
$\frac{(q-1)n}{q}-\frac{(q-1)d}{qN_1}\left((q-1)^2+\left(\frac{N_0}{d}-1\right)\right)$	$\frac{(q-1)(r-1)}{d}$
$\frac{(q-1)n}{q}-\frac{(q-1)d}{qN_1}\left(-2q+\frac{N_0}{d}\right)$	$\frac{(r-1)^2}{d^2}-\frac{(q-1)(r-1)}{d}$
$\frac{(q-1)n}{q}-\frac{(q-1)d}{qN_1}\left(-q+\frac{N_0}{d}\right)$	$\frac{2(r-1)^2(d-1)}{d^2}$
$(q-2)n_1$	$\frac{(r-1)^2(d-1)^2}{d^2}$

证明　因为 $n_2=q-1$, $r=q^2$, 所以, $N_0=N_2=q+1$, 且存在 f, $0\leqslant f\leqslant N_0-1$, 使得 $\ker(T_{r/q})=\{a\in\mathbb{F}_r:T_{r/q}(a)=0\}=\alpha^f\mathbb{F}_q$. 固定 i, $0\leqslant i\leqslant\frac{N_0}{d_1}-1$, 则存在唯一的 j, $0\leqslant j\leqslant N_0-1$, 使得 $d_1i+j\equiv f\pmod{N_0}$. 因此, $\eta_{d_1i+j}^{(N_0,r)}=q-1$, 且对所有满足 $0\leqslant k\leqslant N_0-1$, $k\neq j$ 的 k, $\eta_{d_1i+k}^{(N_0,r)}=-1$.

假设 $d=d_1\geqslant 1$, $n_2=q-1$. 由定理 5, 我们主要决定 $a\in C_j^{(N_0,r)}$, $b\in C_k^{(N_0,r)}$, $0\leqslant j,k\leqslant N_0-1$ 时 $w_H(c(a,b))$ 的值.

(1) 若 $j=k$ 满足: 存在 i, $0\leqslant i\leqslant N_0/d-1$, 使得 $di+j\equiv di+k\equiv f\pmod{N_0}$, 则

$$\begin{aligned}w_H(c(a,b))&=\frac{(q-1)n}{q}-\frac{(q-1)d}{qN_1}\sum_{i=0}^{\frac{N_0}{d}-1}\eta_{di+k}^{(N_0,r)}\eta_{di+j}^{(N_0,r)}\\&=\frac{(q-1)n}{q}-\frac{(q-1)d}{qN_1}\left((q-1)^2+\left(\frac{N_0}{d}-1\right)\right).\end{aligned}$$

此值出现 $\frac{n_2^2N_0}{d}=\frac{(q-1)(r-1)}{d}$ 次.

(2) 若 $j\neq k$ 均满足: 存在 $i\neq i'$, $0\leqslant i,i'\leqslant N_0/d-1$, 使得 $di+j\equiv di'+k\equiv f\pmod{N_0}$, 则

$$\begin{aligned}w_H(c(a,b))&=\frac{(q-1)n}{q}-\frac{(q-1)d}{qN_1}\left(-2(q-1)+\left(\frac{N_0}{d}-2\right)\right)\\&=\frac{(q-1)n}{q}-\frac{(q-1)d}{qN_1}\left(-2q+\frac{N_0}{d}\right).\end{aligned}$$

此值出现 $n_2^2((N_0/d)^2-(N_0/d))=\frac{(r-1)^2}{d^2}-\frac{(q-1)(r-1)}{d}$ 次.

(3) 若 j 满足: 存在 i 使得 $di+j\equiv f\pmod{N_0}$, 但 k 不满足; 或者 k 满足: 存在 i 使得 $di+k\equiv f\pmod{N_0}$ 但 j 不满足, 则

$$\begin{aligned}w_H(c(a,b))&=\frac{(q-1)n}{q}-\frac{(q-1)d}{qN_1}\left(-(q-1)+\left(\frac{N_0}{d}-1\right)\right)\\&=\frac{(q-1)n}{q}-\frac{(q-1)d}{qN_1}\left(-q+\frac{N_0}{d}\right).\end{aligned}$$

此值出现 $2n_2^2\frac{N_0}{d}(N_0-\frac{N_0}{d})=\frac{2(r-1)^2(d-1)}{d^2}$ 次.

(4) 若对任意的 i, j 和 k 都不满足 $di+j\equiv f\pmod{N_0}$, $di+k\equiv f\pmod{N_0}$, 则

$$w_H(c(a,b))=\frac{(q-1)n}{q}-\frac{(q-1)N_0}{qN_1}=\frac{(q-1)^2n_1}{q}-\frac{r-1}{qN_1}=(q-2)n_1.$$

此值出现 $n_2^2(N_0-\frac{N_0}{d})^2=\frac{(r-1)^2(d-1)^2}{d^2}$ 次.

综合以上结果, 定理得证. □

推论 7 设记号与定理 5 相同. 令 $q=2^s$, $r=q^2$, $n_1=q+1$, $n_2=q-1$, 则由 (3.1) 定义的循环码 $\mathcal{C}$ 的权重分布见表 3.

证明 设 $q=2^s$, $r=q^2$, $n_1=q+1$, $n_2=q-1$, 则 $n=q^2-1=r-1$, $N=1$, $\gcd(n_1,n_2)=1$, $d=\gcd(N_0,N)=1=\gcd(N_0,N_1)=d_1$, $N_0=N_2=q+1$. 由定理 6, 推论得证. □

例 2 令 $p=2$, $s=m=2$, , $n_1=5$, $n_2=3$, 则 (3.1) 定义的循环码的权重计数多项式为

$$1+45x^8+210x^{12}.$$

由推论 7 的表 3, 我们同样可得到 $\mathcal{C}$ 是 $\mathbb{F}_4$ 上一个参数为 $[15,4,8]$ 的循环码, 且权重计数多项式为

$$1+45x^8+210x^{12}.$$

例 3 令 $p=2$, $s=3$, $m=2$, $n_1=9$, $n_2=7$, 则 (3.1) 定义的循环码的权重计数多项式为

$$1+441x^{48}+3654x^{56}.$$

由推论 7 的表 3, 我们同样可得到 $\mathcal{C}$ 是 $\mathbb{F}_8$ 上一个参数为 $[63,4,48]$ 的循环码, 且权重计数多项式为

$$1+441x^{48}+3654x^{56}.$$

推论 8 设记号与定理 5 相同. 令 $q=p^s\equiv 1 \pmod 4$, $r=q^2$, $n_1=\frac{q+1}{2}$, $n_2=q-1$, 则由 (3.1) 定义的循环码 $\mathcal{C}$ 的权重分布见表 4.

表 3 $p=2$, $r=q^2$, $n_1=q+1$, $n_2=q-1$ 时 $\mathcal{C}$ 的权重分布

权重	频率
0	1
$q(q-1)$	$(r-1)(r-q+2)$
$q(q-2)$	$(q-1)(r-1)$

表 4 $r=q^2$, $q\equiv 1 \pmod 4$, $n_1=\frac{q+1}{2}$, $n_2=q-1$ 时, $\mathcal{C}$ 的权重分布

权重	频率
0	1
$\frac{q^2-1}{2}$	$r-1$
$\frac{(q-1)^2}{2}$	$r-1$
$\frac{(q-1)(q-2)}{2}$	$\frac{(q-1)(r-1)}{2}$
$\frac{q^2-q+2}{2}$	$\frac{(r-1)(q-1)^2}{4}$
$\frac{q^2-q}{2}$	$\frac{(r-1)^2}{2}$
$\frac{(q-2)(q+1)}{2}$	$\frac{(r-1)^2}{4}$

证明 由 $r=q^2$, $q\equiv 1 \pmod 4$, $n_1=\frac{q+1}{2}$, $n_2=q-1$, 我们得到

$$\gcd(n_1,n_2)=1, \quad n=n_1n_2=\frac{r-1}{2}, \quad N=2,$$

所以,

$$d_1=\gcd(N_0,N_1)=\gcd(q+1,2(q-1))=2=\gcd(q+1,2)=d.$$

由引理 1 有

$$\eta_0^{(2,r)}=\begin{cases}\dfrac{-1-q}{2}, & \text{若 } p\equiv 1 \pmod 4,\\ \dfrac{-1-(-1)^s q}{2}, & \text{若 } p\equiv 3 \pmod 4.\end{cases}$$

因为 $q\equiv 1 \pmod 4$, 所以, 若 $p\equiv 3 \pmod 4$ 则 $2\mid s$. 因此, $\eta_0^{(2,r)}=\frac{-1-q}{2}$. 由定理 6, 推论得证. □

定理 9 设记号与定理 5 相同. 令 $r=q^2$, $q=p^s\equiv 1 \pmod 4$, $n_2=\frac{q+1}{2}$, $1<n_1=\frac{q-1}{e}$, 其中 $e\mid(q-1)$, 则由 (3.1) 定义的循环码 $\mathcal{C}$ 的权重分布见表 5.

证明 由 $q\equiv 1 \pmod 4$ 可得 $\gcd(\frac{q+1}{2},q-1)=1$. 因此, $\gcd(\frac{q+1}{2},e)=1$, 其中 $e\mid(q-1)$. 因为 $r=q^2$, $n_1=\frac{q-1}{e}$, $n_2=\frac{q+1}{2}$, 我们很容易得到

$$n=n_1n_2=\frac{r-1}{2e}, \quad N_1=e(q+1), \quad N_2=2(q-1), \quad d_1=q+1,$$
$$d=\gcd(N_0,N)=\gcd(q+1,2e)=2\times\gcd\left(\frac{q+1}{2},e\right)=2.$$

由引理 1 可得

$$\eta_0^{(2,r)}=\begin{cases}\dfrac{-1-q}{2}, & \text{若 } p\equiv 1 \pmod 4,\\ \dfrac{-1-(-1)^s q}{2}, & \text{若 } p\equiv 3 \pmod 4.\end{cases}$$

因为 $q\equiv 1 \pmod 4$, 若 $p\equiv 3 \pmod 4$, 则 $2\mid s$. 所以, $\eta_0^{(2,r)}=\frac{-1-q}{2}$. 由 $g_1=\alpha^{N_1}=\alpha^{e(q+1)}\in\mathbb{F}_q^*$ 可得若 $T_{r/q}(a_1)=T_{r/q}(a_2)$, 则 $c(a_1,b)=c(a_2,b)$. 因此, 由引理 3, $\mathcal{C}=\{c(a,b):(T_{r/q}(a),b)\in\mathbb{F}_q\times\mathbb{F}_r\}$. 最后, 由定理 5, 我们需要分以下几种情形决定 $T_{r/q}(a)\in\mathbb{F}_q$, $b\in\mathbb{F}_r$ 时 $w_H(c(a,b))$ 的值:

(1) 若 $T_{r/q}(a)=0$, $b=0$, 则 $w_H(c(a,b))=0$.

(2) 若 $T_{r/q}(a)\neq 0$, $b=0$, 则由 $d_1=q+1$ 和表 1 可得

$$w_H(c(a,b))=\frac{(q-1)n}{q}-\frac{(q-1)d_1}{qN}\eta_0^{(d_1,r)}=\frac{(q-1)(r-1)}{2eq}+\frac{r-1}{2eq}=\frac{r-1}{2e}.$$

这个值出现 $q-1$ 次.

表 5 $r=q^2$, $q\equiv 1 \pmod 4$, $1<n_1=\frac{q-1}{e}$, $n_2=\frac{q+1}{2}$ 时, $\mathcal{C}$ 的权重分布

权重	频率
0	1
$\dfrac{r-1}{2e}$	$\dfrac{(q-1)(5r+3)}{8}$
$\dfrac{(q-1)^2}{2e}$	$\dfrac{(r-1)(q+3)}{4}$
$\dfrac{(q-1)(q-3)}{2e}$	$\dfrac{(q-1)(r-1)}{8}$

(3) 若 $T_{r/q}(a)=0$, $b\neq 0$, 则由表 1, 我们得到

$$w_H(c(a,b))=\frac{(q-1)n}{q}-\frac{(q-1)d}{qN}\eta_j^{(d,r)}=\frac{(q-1)(r-1)}{2eq}+\frac{q-1}{eq}\eta_j^{(2,r)}.$$

已知 $\eta_0^{(2,r)}=\frac{-1-q}{2}$, 所以,

$$w_H(c(a,b))=\begin{cases}\dfrac{(q-1)^2}{2e}, & \text{若 } j=0,\\ \dfrac{r-1}{2e}, & \text{若 } j=1.\end{cases}$$

这两个值分别出现 $\frac{r-1}{2}$ 次.

(4) 若 $T_{r/q}(a)\neq 0$, $b\neq 0$, 则由定理 5 可得

$$\begin{aligned}w_H(c(a,b))&=\frac{(q-1)n}{q}-\frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{x\in C_0^{(N_1,r)}}\sum_{z\in C_0^{(N_2,r)}}\psi(ayx+byxz)\\&=\frac{(q-1)n}{q}-\frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{x\in C_0^{(e(q+1),r)}}\sum_{z\in C_0^{(N_2,r)}}\psi(ayx+byxz)\\&=\frac{(q-1)(r-1)}{2eq}-\frac{q-1}{eq}\sum_{x\in\mathbb{F}_q^*}\sum_{z\in C_0^{(N_2,r)}}\psi(ax+bxz)\\&=\frac{(q-1)(r-1)}{2eq}-\frac{q-1}{eq}\sum_{z\in C_0^{(N_2,r)}}\sum_{x\in\mathbb{F}_q^*}\zeta_p^{T_{q/p}(xT_{r/q}(a+bz))}.\end{aligned}$$

固定 $T_{r/q}(a)\in\mathbb{F}_q^*$, 我们计算满足 $z\in C_0^{(N_2,r)}$ 时 $T_{r/q}(a+bz)=0$ 的 $b\in\mathbb{F}_r^*$ 的个数. 令

$$S=\{(b,z)\in\mathbb{F}_r^*\times C_0^{(N_2,r)}:T_{r/q}(a+bz)=0\}. \tag{4.1}$$

因为

$$|\{x\in\mathbb{F}_r^*:T_{r/q}(x)=-T_{r/q}(a)\}|=q,$$

即对任意的 $z\in C_0^{(N_2,r)}$,

$$|\{b\in\mathbb{F}_r^*:T_{r/q}(bz)=-T_{r/q}(a)\}|=q.$$

所以, 我们有 $|S|=q\times\frac{q+1}{2}=\frac{q(q+1)}{2}$.

令 $z_1,z_2\in C_0^{(N_2,r)}$, 其中 $z_1\neq z_2$. 假设存在 $b\in\mathbb{F}_r^*$ 满足 $T_{r/q}(bz_1)=-T_{r/q}(a)=T_{r/q}(bz_2)$, 即

$$\begin{cases}bz_1+(bz_1)^q=-T_{r/q}(a),\\ bz_2+(bz_2)^q=-T_{r/q}(a),\end{cases} \tag{4.2}$$

则我们得到 (4.2) 的唯一解

$$\begin{cases}b=\dfrac{-T_{r/q}(a)}{z_1+z_2},\\ b^q=\dfrac{-T_{r/q}(a)z_1z_2}{z_1+z_2}.\end{cases}$$

注意到 $z^q = \alpha^{2q(q-1)t} = z^{-1}$, 其中 $z = \alpha^{2(q-1)t} \in C_0^{(N_2,r)}$, $(\frac{-T_{r/q}(a)}{z_1+z_2})^q = \frac{-T_{r/q}(a)z_1z_2}{z_1+z_2}$. 另外, 假设 $z_1, z_2, z_3 \in C_0^{(N_2,r)}$ 为三个不同的元素, 则不存在 $b \in \mathbb{F}_r^*$ 满足

$$T_{r/q}(z_1b) = T_{r/q}(z_2b) = T_{r/q}(z_3b) = -T_{r/q}(a).$$

因此, 我们得到 S 的一个分割 S_1 和 S_2:

$$S_1 = \{(b,z) \in S: \text{ 存在唯一的 } z \in C_0^{(N_2,r)}\},$$
$$S_2 = \{(b,z),(b,z') \in S : z, z' \in C_0^{(N_2,r)}, z' \neq z\}.$$

由 (4.2) 可得 $|S_2| = 2 \times \frac{((q+1)/2)((q+1)/2-1)}{2} = \frac{q^2-1}{4}$, 所以, $|S_1| = |S| - |S_2| = \frac{(q+1)^2}{4}$.

总之, 固定 $T_{r/q}(a) \in \mathbb{F}_q^*$, 我们将集合 $\{b : b \in \mathbb{F}_r^*\}$ 分成 T_0, T_1 和 T_2 三部分, 即

$$T_1 = \{b \in \mathbb{F}_r^* : (b,z) \in S_1\}, \quad T_2 = \{b \in \mathbb{F}_r^* : (b,z) \in S_2\}, \quad T_0 = \mathbb{F}_r^* \backslash (T_1 \cup T_2).$$

则 $|T_2| = |S_2|/2 = \frac{q^2-1}{8}$, $|T_1| = |S_1| = \frac{(q+1)^2}{4}$, $|T_0| = r - 1 - |T_1| - |T_2| = \frac{5q^2-4q-9}{8}$.

从上边的结果我们得到:

(1) 若 $(T_{r/q}(a), b) \in \mathbb{F}_q^* \times \mathbb{F}_r^*$ 满足存在 $z_1 \neq z_2 \in C_0^{(N_2,r)}$ 使得 $T_{r/q}(bz_1) = T_{r/q}(bz_2) = -T_{r/q}(a)$, 则

$$\begin{aligned} w_H(c(a,b)) &= \frac{(q-1)(q^2-1)}{2eq} - \frac{q-1}{eq} \sum_{z \in C_0^{(N_2,r)}} \sum_{x \in \mathbb{F}_q^*} \zeta_p^{T_{q/p}(xT_{r/q}(a+bz))} \\ &= \frac{(q-1)(q^2-1)}{2eq} - \frac{q-1}{eq}[2(q-1) + (\frac{q+1}{2} - 2) \times (-1)] \\ &= \frac{(q-1)(q^2-1)}{2eq} - \frac{(q-1)(3q-1)}{2eq} \\ &= \frac{(q-1)(q-3)}{2e}. \end{aligned}$$

这个值出现 $(q-1) \times \frac{q^2-1}{8} = \frac{(q-1)^2(q+1)}{8}$ 次.

(2) 若 $(T_{r/q}(a), b) \in \mathbb{F}_q^* \times \mathbb{F}_r^*$ 满足存在唯一的 $z \in C_0^{(N_2,r)}$ 使得 $T_{r/q}(bz) = -T_{r/q}(a)$, 则

$$\begin{aligned} w_H(c(a,b)) &= \frac{(q-1)(q^2-1)}{2eq} - \frac{q-1}{eq} \sum_{z \in C_0^{(N_2,r)}} \sum_{x \in \mathbb{F}_q^*} \zeta_p^{T_{q/p}(xT_{r/q}(a+bz))} \\ &= \frac{(q-1)(q^2-1)}{2eq} - \frac{q-1}{eq}\left[q - 1 + \left(\frac{q+1}{2} - 1\right) \times (-1)\right] \\ &= \frac{(q-1)(q^2-1)}{2eq} - \frac{(q-1)^2}{2eq} \\ &= \frac{(q-1)^2}{2e}. \end{aligned}$$

此值出现 $(q-1) \times \frac{(q+1)^2}{4} = \frac{(q^2-1)(q+1)}{4}$ 次.

(3) 若 $(T_{r/q}(a), b) \in \mathbb{F}_q^* \times \mathbb{F}_r^*$ 满足对任意的 $z \in C_0^{(N_2,r)}$, $T_{r/q}(bz) \neq -T_{r/q}(a)$, 则

$$w_H(c(a,b)) = \frac{(q-1)(q^2-1)}{2eq} - \frac{q-1}{eq} \sum_{z \in C_0^{(N_2,r)}} \sum_{x \in \mathbb{F}_q^*} \zeta_p^{T_{q/p}(xT_{r/q}(a+bz))}$$

$$
\begin{aligned}
&= \frac{(q-1)(q^2-1)}{2eq} - \frac{q-1}{eq}\left(\frac{q+1}{2} \times (-1)\right) \\
&= \frac{(q-1)(q^2-1)}{2eq} + \frac{q^2-1}{2eq} \\
&= \frac{q^2-1}{2e} = \frac{r-1}{2e}.
\end{aligned}
$$

这个值出现 $(q-1) \times \frac{5q^2-4q-9}{8} = \frac{(q-1)(5q^2-4q-9)}{8}$ 次.

综合以上结果, 定理得证. □

注 1 利用已知的 Gauss 的值, 一些其他类的循环码的权重分布也可确定, 其中可能包含具有少权重的循环码.

5 总结

本文利用 Gauss 刻画了循环码 $\mathcal{C}_{(n_1,n_1n_2)}$ 的权重分布, 并计算了一些特殊情形下该循环码的权重分布. 特别地, 我们得到一类二重循环码和三重循环码.

参考文献

1 Baumert L D, McEliece R J. Weights of irreducible cyclic codes. Inform Control, 1972, 20: 158–175
2 Boston N, McGuire G. The weight distributions of cyclic codes with two zeros and zeta functions. J Symbolic Comput, 2010, 45: 723–733
3 Ding C. The weight distribution of some irreducible cyclic codes. IEEE Trans Inform Theory, 2009, 55: 955–960
4 Ding C, Yang J. Hamming weights in irreducible cyclic codes. Discrete Math, 2013, 313: 434–446
5 Rao A, Pinnawala N. A family of two-weight irreducible cyclic codes. IEEE Trans Inform Theory, 2010, 56: 2568–2570
6 Luo J, Feng K. On the weight distributions of two classes of cyclic codes. IEEE Trans Inform Theory, 2008, 54: 5332–5344
7 Ma C, Zeng L, Liu Y, et al. The weight enumerator of a class of cyclic codes. IEEE Trans Inform Theory, 2011, 57: 397–402
8 Vega G. Two-weight cyclic codes constructed as the direct sum of two one-weight cyclic codes. Finite Fields Appl, 2008, 14: 785–797
9 Wang B, Tang C, Qi W, et al. The weight distributions of cyclic codes and elliptic curves. IEEE Trans Inform Theory, 2012, 58: 7253–7259
10 Xiong M. The weight distributions of a class of cyclic codes. Finite Fields Appl, 2012, 18: 933–945
11 Xiong M. The weight distributions of a class of cyclic codes, II. Des Codes Cryptogr, doi: 10.1007/s10623-012-9875-0, 2012
12 Xiong M. The weight distributions of a class of cyclic codes, III. Finite Fields Appl, 2013, 21: 84–96
13 Ding C, Liu Y, Ma C, et al. The weight distributions of the duals of cyclic codes with two zeros. IEEE Trans Inform Theory, 2011, 57: 8000–8006
14 Feng T, Momihara K. Evaluation of the weight distribution of a class of cyclic codes based on index 2 Gauss sums. IEEE Trans Inform Theory, 2013, 59: 5980–5984
15 Luo J, Tang Y, Wang H. On the weight distribution of a class of cyclic codes. In: Proceeding of IEEE International Symposium on Internation Theory. Seoul: IEEE, 2009, 1726–1729
16 Li S, Hu S, Feng T, et al. The weight distribution of a class of cyclic codes related to Hermitian forms graphs. IEEE Trans Inform Theory, 2013, 59: 3064–3067
17 Yang J, Xiong M, Ding C. Weight distribution of a class of cyclic codes with arbitrary number of zeros. IEEE Trans Inform Theory, 2013, 59: 5985–5993
18 Zeng X, Hu L, Jiang W, et al. The weight distribution of a class of pary cyclic codes. Finite Fields Appl, 2010, 16: 56–73
19 Ding C. Cyclic codes from cyclotomic sequences of order four. Finite Fields Appl, 2013, 23: 8–34

20 Yuan J, Carlet C, Ding C. The weight distribution of a class of linear codes from perfect nonlinear functions. IEEE Trans Inform Theory, 2006, 52: 712–717
21 Brouwer A E. Some new two-weight codes and strongly regular graphs. Discrete Appl Math, 1985, 10: 111–114
22 Calderbank R, Kantor W M. The geometry of two-weight codes. Bull Lond Math Soc, 1986, 18: 97–122
23 Langevin P. A new class of two weight codes. In: Finite Fields and Their Applications. Cambridge: Cambridge University Press, 1996, 181–187
24 Schmidt B, White C. All two-weight irreducible cyclic codes? Finite Fields Appl, 2002, 8: 1–17
25 Zhou Z, Ding C. A class of three-weight cyclic codes. Finite Fields Appl, 2014, 25: 79–93
26 Zhou Z, Ding C. Seven classes of three-weight cyclic codes. IEEE Trans Commun, 2013, 61: 4120–4126
27 Delsarte P. On subfield subcodes of modified Reed-Solomon codes. IEEE Trans Inform Theory, 1975, 21: 575–576
28 Li C, Yue Q, Li F. Hamming weights of duals of cyclic codes with two zeros. IEEE Trans Inform Theory, doi: 10.1109/TIT.2014.2317785, 2014
29 Storer T. Cyclotomy and Difference Sets. Chicago: Markham, 1967
30 Ireland K, Rosen M. A Classical Introduction to Modern Number Theory, 2nd ed. Berlin: Springer-Verlag, 1990
31 Lidl L, Niederreiter H. Finite Fields. Cambridge: Cambridge University Press, 1997
32 Myerson G. Period polynomials and Gauss sums for finite fields. Acta Arith, 1981, 39: 251–264
33 Berndt B C, Evans R J, Williams K S. Gauss and Jacobi Sums. New York: John Wiley and Sons Company, 1997
34 Ding C. Cyclic codes from the two-prime sequences. IEEE Trans Inform Theory, 2012, 58: 3881–3891
35 Li C, Yue Q, Li F. Weight distribution of cyclic codes with respect to two pairwise coprime order elements. Finite Fields Appl, 2014, 28: 94–144
36 Jacoboson N. Basic Algebra I. San Francisco: W H Freeman and Company, 1974

Weight distributions of a class of cyclic codes with two nonzeros

HU LiQin, Yue Qin & ZHU XiaoMeng

Abstract Cyclic codes are an important type of linear codes and have wide applications in communication and storage systems because of their efficient encoding and decoding algorithms.

In this paper, let $\mathbb{F}_r$ be an extension of a finite field $\mathbb{F}_q$ with $r = q^m$, and α be a generator of $\mathbb{F}_r^*$. Let $n = n_1 n_2$ be a positive divisor of $r-1$ such that $\gcd(n_1, n_2) = 1$. We define a class of cyclic codes over $\mathbb{F}_q$ by

$$\mathcal{C} = \{c(a_1, a_2) = (T_{r/q}(a_1 g_1^i + a_2 (g_1 g_2)^i))_{i=0}^{n-1} : a_1, a_2 \in \mathbb{F}_r\},$$

where $g_1 = \alpha^{\frac{r-1}{n_1}}$, $g_2 = \alpha^{\frac{r-1}{n_2}}$, and g_1 and $g_1 g_2$ are not conjugate. In this paper, we determine the weight distribution of the cyclic codes $\mathcal{C}$ using Gauss periods. As applications, we obtain a class of 2-weight cyclic codes and a class of 3-weight cyclic codes.

Keywords cyclic code, weight distribution, cyclotomy, Gauss period

MSC(2010) 94B15, 11T22, 11T23

doi: 10.1360/012014-36