Vol. 36 (2016)
No. 3

数 学 杂 志
J. of Math. (PRC)

A CLASS OF THREE-WEIGHT CYCLIC CODES

LIANG Hua[1,2], CHEN Wen-bing[2], TANG Yuan-sheng[2]

(*1. School of Mathematical Sciences, Huaiyin Normal University, Huaian 223300, China*)

(*2. School of Mathematical Sciences, Yangzhou University, Yangzhou 225002, China*)

Abstract: In this paper, the value distribution of the exponential sum $S(\alpha,\beta) = \sum\limits_{x\in\mathbb{F}_{p^m}} \chi(\alpha x^{\frac{p^k+1}{2}} + \beta x^{\frac{p^{3k}+1}{2}})$ is investigated. Applying the value distribution of $S(\alpha,\beta)$, the weight distribution of a class of p-ary cyclic codes is determined. It turns out that the proposed cyclic codes has three nonzero weights, here p is an odd prime, m and k are two positive integers such that $m/\gcd(m,k)$ is odd, $k = /\gcd(m,k)$ is even and $m \geq 3$.

Keywords: exponential sum; cyclic code; weight distribution; quadratic form

2010 MR Subject Classification: 94B15; 11T71

Document code: A **Article ID:** 0255-7797(2016)03-0474-07

1 Introduction

Let p be a prime. An $[n,k]$-linear code $\mathcal{C}$ over the finite field $\mathbb{F}_p$ is a k-dimensional linear subspace of $\mathbb{F}_p^n$. Moreover, if $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$ then $\mathcal{C}$ is called a cyclic code. For a cyclic code $\mathcal{C}$ with length n over $\mathbb{F}_p$, let A_i be the number of codewords in $\mathcal{C}$ with Hamming weight i. The sequence $(1, A_1, A_2, \cdots, A_n)$ is called the weight distribution of $\mathcal{C}$. The weight distribution of a code is an important research object in coding theory. If $\mathcal{C}$ is cyclic, the weight of each codeword can be expressed by exponential sums, so the weight distribution of $\mathcal{C}$ can be determined if the corresponding exponential sums (or their certain combinations) can be calculated explicitly (see [1–8]).

The value distribution of the exponential sum $S(\alpha,\beta) = \sum\limits_{x\in\mathbb{F}_{p^m}} \chi(\alpha x^{d_1} + \beta x^{d_2})$ and the weight distribution of the cyclic code

$$\mathcal{C} = \left\{ c(\alpha,\beta) = \left(\mathrm{Tr}_1^m(\alpha x^{d_1} + \beta x^{d_2})\right)_{x\in\mathbb{F}_{p^m}^*} | (\alpha,\beta) \in \mathbb{F}_{p^m}^2 \right\}$$

were extensively studied, where $\chi(\cdot) = \zeta_p^{\mathrm{Tr}_1^m(\cdot)}$ is the canonical additive character on the finite field $\mathbb{F}_{p^m}$, $\mathrm{Tr}_1^m(\cdot)$ is the trace mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$, and $\zeta_p = \exp(2\pi\sqrt{-1}/p)$ is a primitive p-th root of unity. For $d_1 = p^k+1, d_2 = 2$, the exponential sum $S(\alpha,\beta)$ and the associated cyclic code $\mathcal{C}$ were studied in [2]. For $d_1 = (p^k+1)/2, d_2 = 1$, the value distribution of $S(\alpha,\beta)$ and the weight distribution of $\mathcal{C}$ were derived in [3]. When $d_1 = p^k+1, d_2 = p^{3k}+1$,

* **Received date:** 2015-01-07 **Accepted date:** 2015-07-06

Foundation item: Supported by National Natural Science Foundation of China (61379004) and the Postgraduate Innovation Project of Jiangsu Province (KYZZ15_0360).

Biography: Liang Hua (1977–), male, born at Yancheng, Jiangsu, doctor, major in coding theory.

the weight distribution of $\mathcal{C}$ was determined in [5] for $\frac{m}{\gcd(m,k)}$ odd, and in [6, 7] for $\frac{m}{\gcd(m,k)}$ even.

In this paper, we will study the exponential sum

$$S(\alpha,\beta)=\sum_{x\in\mathbb{F}_{p^m}}\chi(\alpha x^{\frac{p^k+1}{2}}+\beta x^{\frac{p^{3k}+1}{2}}),$$

and determine the weight distibution of the cyclic code $\mathcal{C}=\{c=c(\alpha,\beta)\mid(\alpha,\beta)\in\mathbb{F}_{p^m}\}$, where

$$c(\alpha,\beta)=\left(\mathrm{Tr}_1^m(\alpha x^{\frac{p^k+1}{2}}+\beta x^{\frac{p^{3k}+1}{2}})\right)_{x\in\mathbb{F}_{p^m}^*},$$

$m/\gcd(m,k)$ is odd and $k/\gcd(m,k)$ is even.

This paper is presented as follows. In Section 2, we introduce some definitions and auxiliary results that will be needed later in this paper. In Section 3, we determine the value distribution of $S(\alpha,\beta)$ and the weight distribution of the cyclic code $\mathcal{C}$.

2 Preliminaries

The following notations are fixed throughout this paper.

(a) Let m and k be positive integers such that $s=m/e$ is odd, k/e is even and $m\geq 3$, where $e=\gcd(m,k)$. Let p be an odd prime, $q=p^m$, $q_0=p^e$, $q_0^*=(-1)^{\frac{q_0-1}{2}}q_0$.

(b) Let $\mathbb{F}_{p^i}$ be the finite field with p^i elements, and $\mathbb{F}_{p^i}^*=\mathbb{F}_{p^i}\backslash\{0\}$.

(c) Let $\mathrm{Tr}_i^j:\mathbb{F}_{p^j}\rightarrow\mathbb{F}_{p^i}$ be the trace mapping defined by $\mathrm{Tr}_i^j(x)=\sum\limits_{l=0}^{j/i-1}x^{p^{il}}$ for $i|j$. For $x\in\mathbb{F}_q$, define $\chi(x)=\zeta_p^{\mathrm{Tr}_1^m(x)}$ to be the canonical additive character of $\mathbb{F}_q$, where $\zeta_p=\exp(2\pi\sqrt{-1}/p)$ is a p-th root of unity.

From now on, we assume that λ is a fixed nonsquare in $\mathbb{F}_{q_0}$. Note that s is odd and k/e is even. It is easy to get that λ is also a nonsquare in $\mathbb{F}_q$ and $\lambda^{(p^{3k}+1)/2}=\lambda^{(p^k+1)/2}=\lambda$. Since the union of the images of maps $x\mapsto x^2$ and $x\mapsto\lambda x^2$ covers each element of $\mathbb{F}_q$ exactly two times, then we have

$$\begin{aligned}S(\alpha,\beta)&=\sum_{x\in\mathbb{F}_q}\chi\left(\alpha x^{\frac{p^k+1}{2}}+\beta x^{\frac{p^{3k}+1}{2}}\right)\\&=\frac{1}{2}\left(T(\alpha,\beta)+T(\lambda\alpha,\lambda\beta)\right),\end{aligned}\tag{2.1}$$

where

$$T(\alpha,\beta)=\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^k+1}+\beta x^{p^{3k}+1})}.\tag{2.2}$$

The exponential sum $T(\alpha,\beta)$ have been extensively studied in [4–6]. This is an important tool we will use.

Definition 2.1 [9] The quadratic character of $\mathbb{F}_{q_0}$ is defined as

$$\eta_0(x)=\begin{cases}1, & \text{if } x \text{ is a nonzero square in } \mathbb{F}_{q_0},\\-1, & \text{if } x \text{ is a nonsquare in } \mathbb{F}_{q_0},\\0, & \text{if } x=0.\end{cases}$$

Definition 2.2 [9] A quadratic form in s indeterminates over $\mathbb{F}_{q_0}$ is a homogeneous polynomial in $\mathbb{F}_{q_0}[x_1, x_2, \cdots, x_s]$ of degree 2 and can be uniquely expressed as

$$f(x_1, x_2, \cdots, x_s) = \sum_{i,j=1}^{s} h_{ij} x_i x_j \quad \text{with} \quad h_{ij} = h_{ji} \in \mathbb{F}_{q_0}.$$

The $s \times s$ symmetric matrix H whose (i, j) entry is h_{ij} is called the coefficient matrix of f. Let r be the rank of H. Then, there exists $M \in GL_s(\mathbb{F}_{q_0})$ such that $H' = MHM^T = \operatorname{diag}(a_1, \cdots, a_r, 0, \cdots, 0)$ is a diagonal matrix where $a_i \in \mathbb{F}_{q_0}^*(1 \le i \le r)$. Let $X = (x_1, x_2, \cdots, x_s)$, making a nonsingular linear substitution $X = YM$ with $Y = (y_1, y_2, \cdots, y_s) \in \mathbb{F}_{q_0}^s$, then we have

$$f(X) = XHX^T = YMHM^TY^T = \sum_{i=1}^{r} a_i y_i^2. \tag{2.3}$$

Let $\Delta = a_1 a_2 \cdots a_r$ (we assume $\Delta = 1$ when $r = 0$), and η_0 be the quadratic (multiplicative) character of $\mathbb{F}_{q_0}$. Then $\eta_0(\Delta)$ is an invariant of H under the conjugate action of $M \in GL_s(\mathbb{F}_{q_0})$.

If we regard $\mathbb{F}_q$ as an $\mathbb{F}_{q_0}$-linear space of dimension s, then

$$Q_{\alpha,\beta}(x) := \operatorname{Tr}_e^m(\alpha x^{p^k+1} + \beta x^{p^{3k}+1})$$

is a quadratic form over $\mathbb{F}_{q_0}$. Let $H_{\alpha,\beta}$ be the coefficient matrix of $Q_{\alpha,\beta}(x)$, $r_{\alpha,\beta}$ be the rank of $H_{\alpha,\beta}$, we have

$$T(\alpha, \beta) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\operatorname{Tr}_1^e(Q_{\alpha,\beta}(x))} = \sum_{x \in \mathbb{F}_q} \zeta_p^{\operatorname{Tr}_1^e(XH_{\alpha,\beta}X^T)} \tag{2.4}$$

and

$$T(\lambda\alpha, \lambda\beta) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\operatorname{Tr}_1^e(XH_{\lambda\alpha,\lambda\beta}X^T)} = \sum_{x \in \mathbb{F}_q} \zeta_p^{\operatorname{Tr}_1^e(\lambda XH_{\alpha,\beta}X^T)}, \tag{2.5}$$

where $H_{\lambda\alpha,\lambda\beta} = \lambda H_{\alpha,\beta}$ and $r_{\lambda\alpha,\lambda\beta} = r_{\alpha,\beta}$.

Now we give the following lemmas, which will be used in the next section.

Lemma 2.1 (see Theorems 5.15 and 5.33 of [9]) For $a \in \mathbb{F}_{q_0}^*$, let η_0 be the quadratic (multiplicative) character of $\mathbb{F}_{q_0}$. Then we have

$$\sum_{x \in \mathbb{F}_{q_0}} \zeta_p^{\operatorname{Tr}_1^e(ax^2)} = \begin{cases} \eta_0(a)(-1)^{e-1} q_0^{\frac{1}{2}}, & \text{if } p \equiv 1 \pmod 4, \\ \eta_0(a)(-1)^{e-1} \left(\sqrt{-1}\right)^e q_0^{\frac{1}{2}}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

From Lemma 2.1 and (2.3), it is easy to get the following lemmas.

Lemma 2.2 With the notations as above, we have

$$\begin{aligned} T(\alpha, \beta) &= \sum_{x \in \mathbb{F}_q} \zeta_p^{\operatorname{Tr}_1^e(Q_{\alpha,\beta}(x))} \\ &= \begin{cases} \eta_0(\Delta)(-1)^{(e-1)r_{\alpha,\beta}} q_0^{s - \frac{r_{\alpha,\beta}}{2}}, & \text{if } p \equiv 1 \pmod 4, \\ \eta_0(\Delta)(-1)^{(e-1)r_{\alpha,\beta}} \left(\sqrt{-1}\right)^{e \cdot r_{\alpha,\beta}} q_0^{s - \frac{r_{\alpha,\beta}}{2}}, & \text{if } p \equiv 3 \pmod 4. \end{cases} \end{aligned}$$

Lemma 2.3 (see [4]) For $(\alpha, \beta) \in \mathbb{F}_q^2 \backslash \{(0,0)\}$, we have $r_{\alpha,\beta} = s - i$, $0 \le i \le 2$.

Combining (2.3), (2.4) and (2.5), by repeatedly using Lemma 2.1 wo obtain the following conclusion.

Lemma 2.4 With the notations introduced above, we have

$$S(\alpha, \beta) = \frac{1}{2}\left(1 + (\eta_0(\lambda))^{r_{\alpha,\beta}}\right) T(\alpha, \beta) = \frac{1}{2}\left(1 + (-1)^{r_{\alpha,\beta}}\right) T(\alpha, \beta).$$

In order to determine the frequency of each value of $S(\alpha, \beta)$ for $\alpha, \beta \in \mathbb{F}_q$, we also need some preliminary identities of $S(\alpha, \beta)$.

Lemma 2.5 Let s be odd and k/e be even. Then the following identities hold.

(i) $\sum\limits_{\alpha,\beta \in \mathbb{F}_q} S(\alpha, \beta) = p^{2m}$;

(ii) $\sum\limits_{\alpha,\beta \in \mathbb{F}_q} S(\alpha, \beta)^2 = p^{3m}$.

Proof (i) We observe that

$$\begin{aligned}
\sum_{\alpha,\beta \in \mathbb{F}_q} S(\alpha, \beta) &= \sum_{\alpha,\beta \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q} \chi\big(\alpha x^{\frac{p^k+1}{2}} + \beta x^{\frac{p^{3k}+1}{2}}\big) \\
&= \sum_{x \in \mathbb{F}_q} \sum_{\alpha \in \mathbb{F}_q} \chi\big(\alpha x^{\frac{p^k+1}{2}}\big) \times \sum_{\beta \in \mathbb{F}_q} \chi\big(\beta x^{\frac{p^{3k}+1}{2}}\big) \\
&= p^{2m}.
\end{aligned}$$

(ii) We can calculate

$$\begin{aligned}
\sum_{\alpha,\beta \in \mathbb{F}_q} S(\alpha, \beta)^2 &= \sum_{\alpha,\beta \in \mathbb{F}_q} \sum_{x,y \in \mathbb{F}_q} \chi\big(\alpha x^{\frac{p^k+1}{2}} + \beta x^{\frac{p^{3k}+1}{2}}\big) \times \chi\big(\alpha y^{\frac{p^k+1}{2}} + \beta y^{\frac{p^{3k}+1}{2}}\big) \\
&= \sum_{x,y \in \mathbb{F}_q} \sum_{\alpha \in \mathbb{F}_q} \chi\left(\alpha\big(x^{\frac{p^k+1}{2}} + y^{\frac{p^k+1}{2}}\big)\right) \times \sum_{\beta \in \mathbb{F}_q} \chi\left(\beta\big(x^{\frac{p^{3k}+1}{2}} + y^{\frac{p^{3k}+1}{2}}\big)\right) \\
&= p^{2m} \cdot M,
\end{aligned}$$

where

$$\begin{aligned}
M &= \#\left\{(x, y) \in \mathbb{F}_q^2 \middle| x^{\frac{p^k+1}{2}} + y^{\frac{p^k+1}{2}} = 0, x^{\frac{p^{3k}+1}{2}} + y^{\frac{p^{3k}+1}{2}} = 0\right\} \\
&= \#\left\{(x, y) \in \mathbb{F}_q^2 \middle| x^{\frac{p^k+1}{2}} + y^{\frac{p^k+1}{2}} = 0\right\} \\
&= \#\left\{(x, y) \in \mathbb{F}_q^2 \middle| y = -x\right\} \\
&= p^m.
\end{aligned}$$

Here the third equality follows from $\gcd\big((p^k + 1)/2, p^m - 1\big) = 1$.

Hence, the result follows.

3 Main Results

Now we give the value distribution of $S(\alpha, \beta)$ and the weight distribution of the cyclic code $\mathcal{C}$.

Theorem 3.1 The value distribution of the multiset

$$\left\{ S(\alpha,\beta) = \sum_{x\in\mathbb{F}_q} \chi\left(\alpha x^{\frac{p^k+1}{2}} + \beta x^{\frac{p^{3k}+1}{2}}\right) \Big| \alpha,\beta\in\mathbb{F}_q \right\}$$

is described as shown in Table I.

Table I

value	multiplicity
p^m	1
0	$(p^m - p^{m-e}+1)(p^m-1)$
$p^{\frac{m+e}{2}}$	$\frac{1}{2}p^{\frac{m-e}{2}}(p^{\frac{m-e}{2}}+1)(p^m-1)$
$-p^{\frac{m+e}{2}}$	$\frac{1}{2}p^{\frac{m-e}{2}}(p^{\frac{m-e}{2}}-1)(p^m-1)$

Proof It is clear that $S(\alpha,\beta)=p^m$ if $(\alpha,\beta)=(0,0)$. For $(\alpha,\beta)\in\mathbb{F}_q^2\backslash\{(0,0)\}$, by Lemmas 2.2, 2.3 and 2.4, we have

$$S(\alpha,\beta)\in\left\{0,\pm p^{\frac{m+e}{2}}\right\}.$$

To determined the distribution of these values, we define

$$n_i = \#\left\{(\alpha,\beta)\in\mathbb{F}_q^2\backslash\{(0,0)\}\big|(\alpha,\beta)=(-1)^i p^{\frac{m+e}{2}}\right\},$$

where $i=0,1$. By Lemma 2.5, we immediately have

$$\begin{cases} (n_0-n_1)p^{\frac{m+e}{2}}+p^m=p^{2m}, \\ (n_0+n_1)p^{m+e}+p^{2m}=p^{3m}. \end{cases}$$

Solving the system of equations, we get the result.

Theorem 3.2 Let p be an odd prime, m and k be two positive integers with $e=\gcd(m,k)$, $m\geq 3$. If m/e is odd and k/e is even, then the weight distribution of the code

$$\mathcal{C}=\left\{c(\alpha,\beta)=\left(\mathrm{Tr}_1^m(\alpha x^{\frac{p^k+1}{2}}+\beta x^{\frac{p^{3k}+1}{2}})\right)_{i=0}^{p^m-2}\right\}$$

is described as shown in Table II.

Table II

i	A_i
0	1
$p^{m-1}(p-1)$	$(p^m-p^{m-e}+1)(p^m-1)$
$(p-1)(p^{m-1}-p^{\frac{m+e}{2}-1})$	$\frac{1}{2}p^{\frac{m-e}{2}}(p^{\frac{m-e}{2}}+1)(p^m-1)$
$(p-1)(p^{m-1}+p^{\frac{m+e}{2}-1})$	$\frac{1}{2}p^{\frac{m-e}{2}}(p^{\frac{m-e}{2}}-1)(p^m-1)$

Proof The Hamming weight of the codeword $c = c(\alpha, \beta)$ in $\mathcal{C}$ is given by

$$\begin{aligned}
w_H(c) &= \#\left\{x \in \mathbb{F}_q^* \middle| \mathrm{Tr}_1^m\left(\alpha x^{\frac{p^k+1}{2}} + \beta x^{\frac{p^{3k}+1}{2}}\right) \neq 0\right\} \\
&= q - 1 - \#\left\{x \in \mathbb{F}_q^* \middle| \mathrm{Tr}_1^m\left(\alpha x^{\frac{p^k+1}{2}} + \beta x^{\frac{p^{3k}+1}{2}}\right) = 0\right\} \\
&= q - 1 - \frac{1}{p}\sum_{x\in\mathbb{F}_q^*}\sum_{a\in\mathbb{F}_p}\zeta_p^{a\mathrm{Tr}_1^m\left(\alpha x^{\frac{p^k+1}{2}} + \beta x^{\frac{p^{3k}+1}{2}}\right)} \\
&= q - 1 - \frac{q-1}{p} - \frac{1}{p}\sum_{a\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q^*}\zeta_p^{a\mathrm{Tr}_1^m\left(\alpha x^{\frac{p^k+1}{2}} + \beta x^{\frac{p^{3k}+1}{2}}\right)} \\
&= q - 1 - \frac{q-1}{p} + \frac{p-1}{p} - \frac{1}{p}\sum_{a\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m\left(\alpha a x^{\frac{p^k+1}{2}} + \beta a x^{\frac{p^{3k}+1}{2}}\right)} \\
&= p^{m-1}(p-1) - \frac{1}{p}\sum_{a\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m\left(\alpha (ax)^{\frac{p^k+1}{2}} + \beta (ax)^{\frac{p^{3k}+1}{2}}\right)} \\
&= p^{m-1}(p-1) - \frac{1}{p}\sum_{a\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m\left(\alpha x^{\frac{p^k+1}{2}} + \beta x^{\frac{p^{3k}+1}{2}}\right)} \\
&= p^{m-1}(p-1) - \frac{p-1}{p}S(\alpha, \beta),
\end{aligned}$$

where for the sixth equality we use the fact that $a^{\frac{p^k+1}{2}} = a^{\frac{p^{3k}+1}{2}} = a$ for any $a \in \mathbb{F}_p (k/e$ is even). By Theorem 3.1, we get the weight distribution of the code $\mathcal{C}$.

References

[1] Ding C, Liu Y, Ma C, Zeng L. The weight distributions of the duals of cyclic codes with two zeroes[J]. IEEE Trans. Inf. The., 2011, 57(12): 8000–8006.

[2] Luo J, Feng K. On the weight distribution of two classes of cyclic codes[J]. IEEE Trans. Inf. The., 2008, 54(12): 5345–5353.

[3] Luo J, Feng K. Cyclic codes and sequences from generalized Coulter-Matthews function[J]. IEEE Trans. Inf. The., 2008, 54(12): 5345–5353.

[4] Zeng X, Hu L, Jiang W, Yue Q, Cao X. The weight distribution of a class of p-ary cyclic codes[J]. Finite Fields Appl., 2010, 16: 56–73.

[5] Luo J, Tang Y, Wang H, Cyclic codes and sequences: the generalized Kasami case[J]. IEEE Trans. Inf. The., 2010, 56(5): 2130–2142.

[6] Zhang B, Wang X, Hu L, Zeng X. The weight distribution of two classes of p-ary cyclic codes[J]. Finite Fields Appl., 2014, 29: 202–224.

[7] Feng K, Luo J. Value distribution of exponential sums from perfect nonlinear functions and their applications[J]. IEEE Trans. Inf. The., 2007, 53(9): 3035–3041.

[8] Feng K, Luo J. Weight distribution of some reducible cyclic codes[J]. Finite Fields Appl., 2008, 14: 390–409.

[9] Lidl R, Niederreiter H. Finite fields[M]. New Jersey: Addison-Wesley, 1983.

[10] Liu Hualu. A class of constacyclic codes over $\mathbb{F}_{p^n}[u]/\langle u^a\rangle$[J]. J. Math., 2015, 35(2): 412–418.

一类具有三重量的循环码

梁 华[1,2], 陈文兵[2], 唐元生[2]

(1.淮阴师范学院数学科学学院, 江苏 淮安 223300)

(2.扬州大学数学科学学院, 江苏 扬州 225002)

摘 要: 本文研究了指数和$S(\alpha,\beta)=\sum\limits_{x\in\mathbb{F}_{p^m}}\chi(\alpha x^{\frac{p^k+1}{2}}+\beta x^{\frac{p^{3k}+1}{2}})$的值分布. 应用$S(\alpha,\beta)$的值分布, 确定了一类$p$元循环码的重量分布, 证明了所提出的循环码具有三个非零重量, 这里p是奇素数, m和k是两个正整数, 满足$m/\gcd(m,k)$是奇数, $k/\gcd(m,k)$是偶数以及$m\geq 3$.

关键词: 指数和; 循环码; 重量分布; 二次型

MR(2010)**主题分类号**: 94B15; 11T71 **中图分类号**: O157.4