Finite Fields and Their Applications 36 (2015) 41–62

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Weight distributions of a class of cyclic codes with arbitrary number of nonzeros in quadratic case

Jing Yang [a,*], Maosheng Xiong [b], Lingli Xia [c]

[a] *Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China*
[b] *Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong*
[c] *Basic Courses Department, Beijing Union University, Beijing, 100101, China*

ARTICLE INFO

Article history:
Received 2 June 2014
Received in revised form 10 July 2015
Accepted 11 July 2015
Available online xxxx
Communicated by Jacques Wolfmann

MSC:
11T71
94B15

Keywords:
Cyclic codes
Weight distribution
Gaussian periods
Jacobi sums

ABSTRACT

Cyclic codes are an important class of linear codes, whose weight distribution have been extensively studied. So far, most of previous results obtained were for cyclic codes with no more than three nonzeros. Recently, the authors of [37] constructed a class of cyclic codes with arbitrary number of nonzeros, and computed the weight distribution for several cases. In this paper, we determine the weight distribution for a new family of such codes. This is achieved by introducing certain new methods, such as the theory of Jacobi sums over finite fields and subtle treatment of some complicated combinatorial identities.

* Corresponding author.
E-mail addresses: jingyang@math.tsinghua.edu.cn (J. Yang), mamsxiong@ust.hk (M. Xiong), lingli@buu.edu.cn (L. Xia).

http://dx.doi.org/10.1016/j.ffa.2015.07.002
1071-5797/

1. Introduction

A linear code $\mathcal{C}$ over the finite field $\mathbb{F}_q$ of length n is a subspace of $\mathbb{F}_q^n$. It is called *cyclic* if it also satisfies that any $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$. By the one-to-one correspondence

$$\sigma : \mathcal{C} \to R := \mathbb{F}_q[x]/(x^n - 1)$$
$$(c_0, c_1, \cdots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1},$$

each cyclic code $\mathcal{C}$ is equivalent to an ideal of R. Since R is a principal ideal ring, there exists a unique monic polynomial $g(x)$ with least degree such that $\sigma(\mathcal{C}) = g(x)R$ and $g(x) \mid (x^n - 1)$. The $g(x)$ is called the *generator polynomial* of $\mathcal{C}$ and $h(x) := (x^n - 1)/g(x)$ is called the *parity-check polynomial* of $\mathcal{C}$. The cyclic code $\mathcal{C}$ is called irreducible (resp. reducible) if $h(x)$ is irreducible (resp. reducible) over $\mathbb{F}_q$. For $\mathcal{C}$ reducible, we say that $\mathcal{C}$ *has* t (≥ 2) *nonzeros* if $h(x)$ has t irreducible factors over $\mathbb{F}_q$. (In the literature some authors call $\mathcal{C}$ as "the dual of a cyclic code with t zeros" instead.)

Denote by A_i the number of codewords of $\mathcal{C}$ with Hamming weight i. The *weight enumerator* of $\mathcal{C}$ with length n is a polynomial in $\mathbb{Z}[Y]$ defined by

$$A_0 + A_1 Y + A_2 Y^2 + \cdots + A_n Y^n.$$

The sequence $(A_0, A_1, \cdots, A_n)$ is called the *weight distribution* of $\mathcal{C}$. The study of the weight distribution of a linear code is important in both theory and application, since it gives the minimum distance and thus the error correcting capability of the code, and the determination of weight distribution of a code allows the computation of the probability of error detection and correction with respect to some algorithms [14]. Moreover, the weight distribution is always related to interesting and challenging problems in number theory [5,27].

For irreducible cyclic codes, an identity due to McEliece [20] shows that the weights of the codes can be expressed via Gauss sums. Because Gauss sums in general are extremely difficult to evaluate, the weight distribution of irreducible cyclic codes is still quite difficult to obtain, however, extensive studies have been carried out with much success by various number theoretic techniques [1–3,12,20,21,25,28,33]. In particular nice characterizations were given in [8,29,30] for irreducible cyclic codes with exactly one nonzero weight; necessary and sufficient conditions were provided and conjectures were also raised by Schmidt and White [26] for irreducible cyclic codes with at most two nonzero weights. Interested readers may consult the survey paper [8] for more updated information on the weight distribution of irreducible cyclic codes.

For reducible cyclic codes, it has been known that the determination of weight distribution involves the evaluation of exponential sums. This may be even more difficult in general. For many special families of reducible cyclic codes where neat expressions are available, various delicate techniques from number theory and algebraic combinatorics

have been developed and utilized, and for some of such families, the weight distribution can been obtained (see for example [7,9–11,13,16–19,22,23,31,32,34–36,38]). However, to our best knowledge, most of these literature works focus on reducible cyclic codes with two or three nonzeros. The exponential sums which have been explicitly evaluated seem to share a common feature that they attain only a few distinct values.

For reducible cyclic codes with more than three nonzeros, not much is known. In a beautiful work [15], the authors obtained the weight distribution of a class of cyclic codes with arbitrary number of nonzeros. Their work built upon an unexpected connection between the corresponding exponential sums and the spectra of Hermitian forms graphs which were known in the literature. In another recent work [37] a general family of reducible cyclic codes with arbitrary number of nonzeros were constructed and under certain conditions the weight distribution was also obtained. The purpose of this paper is to explore the construction of [37] much further and to determine the weight distribution for another new family of reducible cyclic codes with arbitrary number of nonzeros. Compared with [37], we achieve our goal by more advanced theory of Jacobi sums and by more subtle treatment of some complicated combinatorial identities.

The rest of the paper is organized as follows. The codes we consider will be introduced in Section 2, so are the main results (Theorems 1, 2 and 3). Section 3 introduces some mathematical tools such as cyclotomy, Gaussian periods and general Jacobi sums that will be needed later. In Sections 4 and 5 we prove our main theorems. To streamline the proofs of Theorems 1, 2 and 3 we have left out the proof of a complicated combinatorial identity to Section 6. Section 7 concludes this paper.

2. Weight distribution of code $\mathcal{C}_{(a_1,\cdots,a_t)}$

We first fix some notations. Let p be a prime, $q = p^s$, $r = q^m$ for some integers $s, m \geqslant 1$. Let $\mathbb{F}_r$ be a finite field of order r and γ be a generator of the multiplicative group $\mathbb{F}_r^* := \mathbb{F}_r \setminus \{0\}$. For any $t \geq 2$, the family of reducible cyclic codes $\mathcal{C}_{(a_1,\cdots,a_t)}$ with t nonzeros were introduced in [37] as follows.

Let e, t be integers such that $e \geqslant t \geqslant 2$, and assume that

i) $a \not\equiv 0 \pmod{r-1}$ *and* $e|(r-1)$;
ii) $a_i \equiv a + \frac{r-1}{e}\Delta_i \pmod{r-1}$, $1 \leqslant i \leqslant t$, *where* $\Delta_i \not\equiv \Delta_j \pmod{e}$ *for any* $i \neq j$ *and* $\gcd(\Delta_2 - \Delta_1, \ldots, \Delta_t - \Delta_1, e) = 1$;
iii) $\deg h_{a_1}(x) = \cdots = \deg h_{a_t}(x) = m$, *and* $h_{a_i}(x) \neq h_{a_j}(x)$ *for any* $1 \leqslant i \neq j \leqslant t$, *where* $h_{a_i}(x)$ *is the minimal polynomial of* γ^{-a_i} *over* $\mathbb{F}_q$;
iv) $N = \gcd\left(\frac{r-1}{q-1}, ae\right)$;
v) $\delta = \gcd(r-1, a_1, a_2, \cdots, a_t)$, $n = \frac{r-1}{\delta}$.

The cyclic code $\mathcal{C}_{(a_1,\cdots,a_t)}$ with t nonzeros $\gamma^{-a_1}, \cdots, \gamma^{-a_t}$ is given by

$$\mathcal{C}_{(a_1,\cdots,a_t)} = \left\{ c(x_1,x_2,\cdots,x_t) = \left(\mathrm{Tr}_{r/q}\left(\sum_{j=1}^{t} x_j \gamma^{a_j i}\right)\right)_{i=0}^{n-1} \ : \ \forall\, x_1,\cdots,x_t \in \mathbb{F}_r \right\}, \tag{1}$$

where $\mathrm{Tr}_{r/q}$ *denotes the trace map from* $\mathbb{F}_r$ *to* $\mathbb{F}_q$.

It shall be noted that Condition iii) can be easily verified, for example, it holds if $\frac{r-1}{q^\ell-1} \nmid N$ for any proper factor ℓ of m (i.e. $\ell \mid m$ and $\ell < m$, see [37, Lemma 6]). In particular this is always the case if $N = 2$, which is our interest in the paper.

Delsarte's Theorem [6] states that $\mathcal{C}_{(a_1,\cdots,a_t)}$ is an $[n, tm]$ cyclic code over $\mathbb{F}_q$ with parity-check polynomial $h(x) = h_{a_1}(x)\cdots h_{a_t}(x)$. This class of codes $\mathcal{C}_{(a_1,\cdots,a_t)}$ contains many interesting cyclic codes as special cases which have been extensively studied in the literature [19,7,11,32,34–36], all of which focus on the case $t = 2$.

For any $t \geq 2$, in [37] we obtain the weight distribution of $\mathcal{C}_{(a_1,\cdots,a_t)}$ under either of the following conditions:

- for any $t, e \geq 2$ when $N = 1$; or
- for any $t = e \geq 2$ with $N = 1, 2, 3$; or with $N = (p^j + 1)/k$ for some positive integers j, k; or with N being a prime number such that $N \equiv 3 \pmod 4$, $\left(\frac{p}{N}\right) = 1$ (here $\left(\frac{*}{*}\right)$ denotes the Legendre symbol).

In this paper we obtain the weight distribution of $\mathcal{C}_{(a_1,\cdots,a_t)}$ for any $t \geq 2$ such that $t = e - 1$ and $N = 2$. Note that under these conditions, it is necessary that q is odd, m is even and $2|ae$. Our main results are stated as follows.

Theorem 1. *In the case of* $N = 2$, $t = e - 1 \geqslant 2$, *and we further assume that*

$$e|(q^{m/2} - 1) \ \text{ and } \ 2|a. \tag{2}$$

The code $\mathcal{C}_{(a_1,\ldots,a_t)}$ *is an* $[n, tm]$ *cyclic code over* $\mathbb{F}_q$ *with the minimal Hamming distance* $d = \frac{2(q-1)(r-\sqrt{r})}{(t+1)q\delta}$. *It has (at most)* $\frac{1}{2}(t^2 + 5t - 2)$ *non-zero distinct weights.*

(i). If $q \equiv 1 \pmod 4$, *then the weight distribution is listed in Table 1.*
(ii). If $q \equiv 3 \pmod 4$, *then the weight distribution is listed in Table 2.*

We remark that if $N = 2$ and $t = e - 1$ is even, then the condition (2) will be always satisfied, so this settles the case completely. In particular the special case $N = 2$, $e = 3$, $t = 2$ was already studied in [32]. When $N = 2$ and $t = e - 1$ is odd, there are two cases: if the condition (2) is satisfied, this is again settled by Theorem 1; on the other hand, if the condition (2) is not satisfied, in principle the weight distribution still can be obtained. However, the formulas become quite complicated. To illustrate that, we first present the weight distribution for the simple case $t = 3$ in Theorem 2, and then give a computational formula for the general case in Theorem 3.

Table 1
The weight distribution of $\mathcal{C}$ when $N = 2$ and $t = e - 1 \geqslant 2$: Case (i).

Weight	Frequency $(\forall\, 1 \leqslant k \leqslant t, 0 \leqslant u \leqslant k+1)$
0	once
$\frac{q-1}{(t+1)q\delta} \cdot \left\{(k+1)r - (k+1-2u)\sqrt{r}\right\}$	$\frac{(r-1)}{r2^{k+2}} \cdot \binom{t+1}{k+1}\binom{k+1}{u} \cdot \Big\{2(r-1)^k$ $-(-1)^k \left\{(1+\sqrt{r})^u(1-\sqrt{r})^{k+1-u}\right.$ $\left.+(1-\sqrt{r})^u(1+\sqrt{r})^{k+1-u}\right\}\Big\}$

Table 2
The weight distribution of $\mathcal{C}$ when $N = 2$ and $t = e - 1 \geqslant 2$: Case (ii).

Weight	Frequency $(\forall\, 1 \leqslant k \leqslant t, 0 \leqslant u \leqslant k+1)$
0	once
$\frac{q-1}{(t+1)q\delta} \cdot \Big\{(k+1)r$ $-(-1)^{m/2}(k+1-2u)\sqrt{r}\Big\}$	$\frac{(r-1)}{r2^{k+2}} \cdot \binom{t+1}{k+1}\binom{k+1}{u} \cdot \Big\{2(r-1)^k$ $-(-1)^k \left\{(1+\sqrt{r})^u(1-\sqrt{r})^{k+1-u}\right.$ $\left.+(1-\sqrt{r})^u(1+\sqrt{r})^{k+1-u}\right\}\Big\}$

Theorem 2. *In the case of $N = 2$, $t = e - 1 = 3$, the code $\mathcal{C}_{(a_1,a_2,a_3)}$ is an $[n, 3m]$ cyclic code over $\mathbb{F}_q$ with the minimal Hamming distance $d = \frac{(q-1)(r-\sqrt{r})}{2q\delta}$. It has (at most) 12 non-zero weights.*

(i). If $2|a$, then its weight distribution is listed in Table 3 (or Table 1 with $t = 3$).
(ii). If $2 \nmid a$, then its weight distribution is listed in Table 4.

We now consider the general case for $N = 2$ and $t = e - 1$. Denote $g := \gamma^a$ and $\beta := \gamma^{(r-1)/e}$. And let A be the Vandermonde matrix of size $(t+1) \times (t+1)$, given by

$$A := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta & \cdots & \beta^{e-1} \\ 1 & \beta^2 & \cdots & \beta^{2(e-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{e-1} & \cdots & \beta^{(e-1)^2} \end{pmatrix}. \tag{3}$$

Take B be the $(t+1)\times t$-matrix whose columns consist of the $\{\triangle_1+1, \ldots, \triangle_t+1\} \pmod e$ columns of A, where $\triangle_i$ are the basic parameters of $\mathcal{C}_{(a_1,\cdots,a_t)}$. Let

$$(y_0, \cdots, y_t)^T = B(x_1, \cdots, x_t)^T. \tag{4}$$

Since $\mathrm{rank}B = t$ (see also [37, Lemma 18]), this gives a one-to-one correspondence between $(y_1, \ldots, y_t)$ and $(x_1, \ldots, x_t)$, and there exist some $0 \neq \lambda_i \in \mathbb{F}_q$ for $1 \leqslant i \leqslant t$ such that

Table 3
The weight distribution of $\mathcal{C}_{(a_1,a_2,a_3)}$ when $t = e - 1 = 3$, $N = 2$ and $2 \mid a$.

Weight	Frequency
0	once
$\frac{q-1}{2\delta q}(r + \sqrt{r})$	$3(r-1)$ times
$\frac{q-1}{2\delta q}(r - \sqrt{r})$	$3(r-1)$ times
$\frac{3(q-1)}{4\delta q}(r + \sqrt{r})$	$(r-1)(r-5)/2$ times
$\frac{3(q-1)}{4\delta q}(r - \sqrt{r})$	$(r-1)(r-5)/2$ times
$\frac{(q-1)}{4\delta q}(3r + \sqrt{r})$	$3(r-1)^2/2$ times
$\frac{(q-1)}{4\delta q}(3r - \sqrt{r})$	$3(r-1)^2/2$ times
$\frac{(q-1)}{\delta q}(r + \sqrt{r})$	$(r-1)(r^2-2r+9)/16$ times
$\frac{(q-1)}{\delta q}(r - \sqrt{r})$	$(r-1)(r^2-2r+9)/16$ times
$\frac{(q-1)}{2\delta q}(2r + \sqrt{r})$	$(r-1)(r^2-4r+3)/4$ times
$\frac{(q-1)}{2\delta q}(2r - \sqrt{r})$	$(r-1)(r^2-4r+3)/4$ times
$\frac{(q-1)}{\delta q}r$	$3(r-1)^3/8$ times

Table 4
The weight distribution of $\mathcal{C}_{(a_1,a_2,a_3)}$ when $t = e - 1 = 3$, $N = 2$ and $2 \nmid a$.

Weight	Frequency
0	once
$\frac{q-1}{2\delta q}(r + \sqrt{r})$	$(r-1)$ times
$\frac{q-1}{2\delta q}(r - \sqrt{r})$	$(r-1)$ times
$\frac{q-1}{2\delta q}r$	$4(r-1)$ times
$\frac{3(q-1)}{4\delta q}(r + \sqrt{r})$	$(r-1)^2/2$ times
$\frac{3(q-1)}{4\delta q}(r - \sqrt{r})$	$(r-1)^2/2$ times
$\frac{(q-1)}{4\delta q}(3r + \sqrt{r})$	$(r-1)(3r-7)/2$ times
$\frac{(q-1)}{4\delta q}(3r - \sqrt{r})$	$(r-1)(3r-7)/2$ times
$\frac{(q-1)}{\delta q}(r + \sqrt{r})$	$(r-1)^3/16$ times
$\frac{(q-1)}{\delta q}(r - \sqrt{r})$	$(r-1)^3/16$ times
$\frac{(q-1)}{2\delta q}(2r + \sqrt{r})$	$(r-1)(r^2-4r+3)/4$ times
$\frac{(q-1)}{2\delta q}(2r - \sqrt{r})$	$(r-1)(r^2-4r+3)/4$ times
$\frac{(q-1)}{\delta q}r$	$(r-1)(3r^2-6r+11)/8$ times

$$y_0 + \sum_{i=1}^{t} \lambda_i y_i = 0.$$

We note that $\{\lambda_i\}_{i=1}^{t}$ depend only on the parameters $\{\triangle_i \pmod e\}_{i=1}^{t}$ and β. We further define

$$l_0 = \#\{i \mid \lambda_i g^i \text{ is a square in } \mathbb{F}_r, 1 \leqslant i \leqslant t\};$$
$$l_1 = \#\{i \mid \lambda_i g^i \text{ is a nonsquare in } \mathbb{F}_r, 1 \leqslant i \leqslant t\}. \tag{5}$$

Next, we extend the definition of binomial coefficient to all integers such that

$$\binom{n}{i} = 0, \text{ for } i < 0 \text{ and } i > n.$$

With such preparations, we give our main result for the general case as follows.

Theorem 3. *In the case of $N = 2$ and $t = e-1 \geqslant 2$, the code $\mathcal{C}_{(a_1,\ldots,a_t)}$ is an $[n, tm]$ cyclic code over $\mathbb{F}_q$ with the minimal Hamming distance $d = \frac{2(q-1)(r-\sqrt{r})}{(t+1)q\delta}$, and the Hamming weight of its codewords takes the value 0 once and the value*

$$\frac{(q-1)}{(t+1)q\delta}\left[k(r-1) - 2u\eta_0^{(2,r)} - 2(k-u)\eta_1^{(2,r)}\right],$$

for any $2 \leq k \leq t+1$ and $0 \leqslant u \leq k$, with the frequency

$$\sum_{k_0=0}^{k}\sum_{u_0=0}^{u}\binom{l_0+1}{k_0}\binom{l_1}{k-k_0}\binom{k_0}{u_0}\binom{k-k_0}{u-u_0}\Omega_{\underbrace{0\cdots0}_{2u_0+k-k_0-u},\ \underbrace{1\cdots1}_{k_0+u-2u_0}},$$

where $\eta_0^{(2,r)}, \eta_1^{(2,r)}$ are given by Lemma 5, $\Omega_{\underbrace{0\ldots0}_{u}\underbrace{1\ldots1}_{v}}$ is determined by Lemma 10 and l_0, l_1 are defined by (5).

We remark that Theorem 3 is a general computational formula for the weight distribution of $\mathcal{C}_{(a_1,\cdots,a_t)}$, and the results of Theorem 1 and Theorem 2 can be viewed as its corollaries. However, the frequency formula in Theorem 3 is complicated since it depends on the choice of $\triangle_1, \cdots, \triangle_t$, and there seems no easy way to write them down in a simple closed form as Theorem 1.

In the end of this section, we give several numerical examples to illustrate our main theorems.

Example 4. Let $(q, m, e, t) = (5, 2, 4, 3)$, then $\frac{r-1}{3} = \frac{5^2-1}{4} = 6$. Let γ be the generator of $\mathbb{F}_{25}^*$ with characteristic polynomial $\gamma^2 + 4\gamma + 2 = 0$. Let $(\triangle_1, \triangle_2, \triangle_3) = (1, 2, 3)$.

(1). For $a = 2$ we have $(a_1, a_2, a_3) = (8, 14, 20)$, $(\delta, n) = (2, 12)$ and

$$h_{a_1}(x) = x^2 + x + 1,\ h_{a_2}(x) = x^2 + 3x + 4,\ h_{a_3}(x) = x^2 + 4x + 1.$$

The parity-check polynomial of $\mathcal{C}$ is $h(x) = x^6 + 3x^5 + 3x^3 + 3x + 4$. The code $\mathcal{C}$ is a $[12, 6, 4]$-cyclic code over $\mathbb{F}_5$ with weight enumerator given by

$$1 + 72Y^4 + 312Y^6 + 864Y^7 + 1740Y^8 + 3408Y^9 + 5184Y^{10} + 3168z^{11} + 876Y^{12}.$$

This also follows from Table 3. There are 8 distinct non-zero weights because some of the weights in Table 3 turn out the same. More precisely,

$$\begin{aligned}
&\tfrac{(q-1)}{2\delta q}(r+\sqrt{r}) = \tfrac{3(q-1)}{4\delta q}(r-\sqrt{r}),\\
&\tfrac{(q-1)}{4\delta q}(3r+\sqrt{r}) = \tfrac{(q-1)}{\delta q}(r-\sqrt{r}),\\
&\tfrac{3(q-1)}{4\delta q}(r+\sqrt{r}) = \tfrac{(q-1)}{2\delta q}(2r-\sqrt{r}).
\end{aligned} \tag{6}$$

(2). For $a = 1$ we have $(a_1, a_2, a_3) = (7, 13, 19)$, $(\delta, n) = (1, 24)$ and

$$h_{a_1}(x) = x^2 + x + 2,\ h_{a_2}(x) = x^2 + 2x + 1,\ h_{a_3}(x) = x^2 + 4x + 2.$$

The parity-check polynomial of $\mathcal{C}$ is $h(x) = x^6 + 2x^5 + 4x^4 + x^3 + 2x^2 + 3x + 4$. The code $\mathcal{C}$ is a $[24, 6, 8]$-cyclic code over $\mathbb{F}_5$ with weight enumerator given by

$$\begin{aligned}
&1 + 24Y^8 + 96Y^{10} + 312Y^{12} + 816Y^{14} + 1680Y^{16} + 3456Y^{18} + 5208z^{20}\\
&\quad + 3168Y^{22} + 864Y^{24}.
\end{aligned}$$

This also follows from Table 4. There are 9 distinct non-zero weights because some of the weights in Table 4 turn out the same. More precisely, equations (6) still hold true.

3. Cyclotomy, Gaussian periods and Jacobi sums

An *additive character* of $\mathbb{F}_r$ is a non-zero function ϕ from $\mathbb{F}_r$ to the set of complex numbers such that $\phi(x + y) = \phi(x)\phi(y)$ for any pair $(x, y) \in \mathbb{F}_r^2$. Let $\mathrm{Tr}_{r/p}$ denote the trace function from $\mathbb{F}_r$ to $\mathbb{F}_p$ and $\zeta_p = e^{2\pi\sqrt{-1}/p}$ be the primitive p-th complex root of unit. The additive character ψ given by

$$\psi(c) = \zeta_p^{\mathrm{Tr}_{r/p}(c)} \quad \text{for any } c \in \mathbb{F}_r \tag{7}$$

is called the *canonical additive character* of $\mathbb{F}_r$. For any $x \in \mathbb{F}_r$, one can easily check the orthogonal property

$$\frac{1}{r}\sum_{x\in\mathbb{F}_r} \psi(ax) = \begin{cases} 1, & \text{if } a = 0;\\ 0, & \text{if } a \in \mathbb{F}_r^*. \end{cases} \tag{8}$$

Let $r - 1 = lL$ for two positive integers $l, L \geqslant 1$, and let γ be a fixed primitive element of $\mathbb{F}_r$. Define $C_i^{(L,r)} = \gamma^i\langle\gamma^L\rangle$ for $i = 0, 1, \ldots, L - 1$, where $\langle\gamma^L\rangle$ denotes the subgroup of $\mathbb{F}_r^*$ generated by γ^L. The $C_i^{(L,r)}$ are called the *cyclotomic classes* of order L in $\mathbb{F}_r$. The

Gaussian periods of order L are defined by

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

The values of Gaussian periods are difficult to compute in general. However, they are known in a few cases. We will need the following whose proofs can be found in [4] and [24].

Lemma 5. *When $L = 2$, the Gaussian periods are given by*

$$\eta_0^{(2,r)} = \begin{cases} \frac{-1+(-1)^{s\cdot m-1} r^{1/2}}{2}, & \text{if } p \equiv 1 \pmod 4 \\ \frac{-1+(-1)^{s\cdot m-1} (\sqrt{-1})^{s\cdot m} r^{1/2}}{2}, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

and $\eta_1^{(2,r)} = -1 - \eta_0^{(2,r)}$.

A *multiplicative character* of $\mathbb{F}_r$ is a non-zero function χ from $\mathbb{F}_r^*$ to the set of complex numbers such that $\chi(xy) = \chi(x)\chi(y)$ for all the pairs $(x, y) \in \mathbb{F}_r^* \times \mathbb{F}_r^*$. For $j = 1, 2, \ldots, r-1$, one can easily check that the functions $\chi^{(j)}$ with

$$\chi^{(j)}(\gamma^k) = \zeta_{r-1}^{jk} \quad \text{for } k = 0, 1, \ldots, r-2$$

give all the multiplicative character of order dividing $r-1$, here ζ_{r-1} denotes the primitive complex $(r-1)$-th root of unit. When $j = r-1$, $\varepsilon(c) := \chi^{(r-1)}(c) = 1$ for all $c \in \mathbb{F}_r^*$, which is called the *trivial multiplicative character* of $\mathbb{F}_r$. One can check the following orthogonal property of multiplicative characters

$$\frac{1}{r-1} \sum_{x \in \mathbb{F}_r^*} \chi(x) = \begin{cases} 1, & \text{if } \chi = \varepsilon; \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

Furthermore, we may extend the definition of any multiplicative character χ to $\mathbb{F}_r$ as follows,

$$\chi(0) = \begin{cases} 0, & \text{if } \chi \neq \varepsilon; \\ 1, & \text{if } \chi = \varepsilon. \end{cases}$$

Let $k \geqslant 2$ and $\chi_1, \cdots, \chi_k$ be multiplicative characters of $\mathbb{F}_r$. The *Jacobi sum* related with $\chi_1, \cdots, \chi_k$ over $\mathbb{F}_r$ is defined by

$$J(\chi_1, \cdots, \chi_k) := \sum_{\substack{z_1, \cdots z_k \in \mathbb{F}_r \\ z_1 + \cdots + z_k = 1}} \chi_1(z_1)\chi_2(z_2)\cdots\chi_k(z_k).$$

The following [4] are elementary properties of Jacobi sums.

Lemma 6.

(a). $J(\underbrace{\varepsilon,\cdots,\varepsilon}_{k}) = r^{k-1}$.

(b). $J(\chi_1,\cdots,\chi_k) = 0$ *if some but not all of* $\chi_1,\cdots,\chi_k$ *are trivial.*

(c). When r *is odd, let* ρ *be the quadratic multiplicative character of* $\mathbb{F}_r$*, then*

$$J(\underbrace{\rho,\cdots,\rho}_{k}) = \begin{cases} -\rho(-1)^{\frac{k}{2}} r^{\frac{k-2}{2}}, & \text{if } k \text{ is even;} \\ \rho(-1)^{\frac{k-1}{2}} r^{\frac{k-1}{2}}, & \text{if } k \text{ is odd.} \end{cases}$$

We now define the *reduced Jacobi sum* below,

$$J^*(\chi_1,\cdots,\chi_k) := \sum_{\substack{z_1,\cdots z_k\in\mathbb{F}_r^* \\ z_1+\cdots+z_k=1}} \chi_1(z_1)\chi_2(z_2)\cdots\chi_k(z_k), \tag{10}$$

which is needed in the next section.

Notice that $J^*(\chi_1,\cdots,\chi_k) = J(\chi_1,\cdots,\chi_k)$ if all of $\chi_1,\cdots,\chi_k$ are non-trivial. The following results give the evaluation of $J^*(\chi_1,\cdots,\chi_k)$ if some of $\chi_1,\cdots,\chi_k$ are trivial. The proof is not difficult but may be of independent interest. It is essential in Section 6 to establish a complicated combinatorial identity, which is needed in the proofs of Theorems 1 and 2.

Lemma 7.

(a). $J^*(\varepsilon,\cdots,\varepsilon) = \left\{(r-1)^k - (-1)^k\right\}/r$.

(b). Define $J(\chi) := 1$ *for any multiplicative character* χ*. Let* u *be an integer such that* $0 \leqslant u \leqslant k-1$*. If* $\chi_1,\cdots,\chi_{k-u}$ *are all nontrivial multiplicative characters, then*

$$J^*(\chi_1,\cdots,\chi_{k-u},\underbrace{\varepsilon,\cdots,\varepsilon}_{u}) = (-1)^u J(\chi_1,\cdots,\chi_{k-u}).$$

Proof. By definition, we have

$$J^*(\varepsilon,\cdots,\varepsilon) = J(\varepsilon,\cdots,\varepsilon) - \sum_{\mathcal{I}} \sum_{\sum\limits_{i\in\mathcal{I}} z_i=1} \varepsilon\Big(\prod_{i\in\mathcal{I}} z_i\Big),$$

where the subscript $\mathcal{I}$ under the $\sum$ symbol means to sum over all subsets $\mathcal{I}$ such that $\mathcal{I} \subsetneqq \{1,2,\cdots,k\}$. Using the inclusion–exclusion principle, Part (a) of Lemma 7 can be easily proved. Now for Part (b), let $\mathcal{I}' \subsetneqq \{k-u+1,\cdots,k\}$, then

$$\begin{aligned} &J^*(\chi_1,\cdots,\chi_{k-u},\underbrace{\varepsilon,\cdots,\varepsilon}_{u}) \\ &= J(\chi_1,\cdots,\chi_{k-u},\underbrace{\varepsilon,\cdots,\varepsilon}_{u}) - \sum_{\mathcal{I}'} \sum_{\sum_{j=1}^{k-u} z_j + \sum\limits_{i\in\mathcal{I}'} z_i=1} \chi_1(z_1)\chi_2(z_2)\cdots\chi_k(z_{k-u})\varepsilon\Big(\prod_{i\in\mathcal{I}'} z_i\Big) \end{aligned}$$

$$= 0 - \binom{u}{1} J^*(\chi_1, \cdots, \chi_{k-u}, \underbrace{\varepsilon, \cdots, \varepsilon}_{u-1}) - \binom{u}{2} J^*(\chi_1, \cdots, \chi_{k-u}, \underbrace{\varepsilon, \cdots, \varepsilon}_{u-2})$$
$$- \cdots - \binom{u}{u} J^*(\chi_1, \cdots, \chi_{k-u}).$$

By induction, Part (b) can be also verified. □

4. Proof of Theorem 1

4.1. The weight distribution of $\mathcal{C}_{(a_1,\cdots,a_t)}$ and summation of Gaussian periods

We now consider the weight distribution of the cyclic code $\mathcal{C}_{(a_1,\cdots,a_t)}$ given in (1). Using the orthogonal relation (8) and some computational techniques, in [37] the authors expressed the Hamming weight of the codeword $c(x_1, \cdots, x_t)$ by

$$w_H(c(x_1, \cdots, x_t)) = \frac{(r-1)(q-1)}{q\delta} - \frac{N(q-1)}{eq\delta} \sum_{h=0}^{e-1} \bar{\eta}^{(N,r)}_{g^h \cdot \sum_{\tau=1}^{t} x_\tau \beta_\tau^h}, \tag{11}$$

where $g = \gamma^a$, $\beta_\tau = \gamma^{\frac{r-1}{e}\Delta_\tau}$ for $1 \leqslant \tau \leqslant t$ and $\bar{\eta}_v^{(N,r)} = \sum_{z \in C_0^{(N,r)}} \psi(vz)$ for any $v \in \mathbb{F}_r$. These $\bar{\eta}_v^{(N,r)}$ are called the *modified Gaussian periods*, given by

$$\begin{cases} \bar{\eta}_0^{(N,r)} = \frac{r-1}{N}, \\ \bar{\eta}_{\gamma^j}^{(N,r)} = \eta_i^{(N,r)}, \quad \text{for } 0 \leqslant j \leqslant r-2, \end{cases}$$

where $0 \leqslant i \leqslant N-1$ such that $i \equiv j \pmod N$, and these $\eta_i^{(N,r)}$ are the ordinary Gaussian periods. Thus, to compute the weight distribution of cyclic code $\mathcal{C}_{(a_1,\cdots,a_t)}$, it suffices to compute the value distribution of the sum

$$T(x_1, \cdots, x_t) := \sum_{h=0}^{e-1} \bar{\eta}^{(N,r)}_{g^h \cdot \sum_{\tau=1}^{t} x_\tau \beta_\tau^h}, \quad (\forall x_1, \cdots, x_t \in \mathbb{F}_r). \tag{12}$$

Now we deal with it under the assumption of $N = 2$ and $t = e - 1 \geq 2$.

4.2. The case of $N = 2$ and $t = e - 1 \geq 2$

Since $N = 2$, it is easy to see that q is odd, m is even and $-1 = \gamma^{\frac{q^m-1}{2}}$ is a square. For simplicity, let us write

$$\bar{\eta}_x := \bar{\eta}_x^{(2,r)}, \quad \forall x \in \mathbb{F}_r.$$

Make a change of variables

$$y_h = \sum_{\tau=1}^{t} x_\tau \beta_\tau^h, \quad 0 \le h \le t = e-1,$$

which can be written as

$$(y_0, \cdots, y_t)^T = B(x_1, \cdots, x_t)^T \tag{13}$$

for some $(t+1) \times t$ matrix B. Recall that $\beta = \gamma^{(r-1)/e}$ is an e-th root of unity in $\mathbb{F}_r$. Since $\beta_\tau = \beta^{\triangle_\tau}$, the matrix B consists of t columns of the Vandermonde matrix A, defined by (3). By [37, Lemma 18], any t rows of B are linearly independent over $\mathbb{F}_q$. This gives a one-to-one correspondence between $(y_1, \ldots, y_t)$ and $(x_1, \ldots, x_t)$ and there exist $\lambda_1, \cdots, \lambda_t \in \mathbb{F}_{q^m}^*$ such that

$$y_0 + \sum_{h=1}^{t} \lambda_h y_h = 0. \tag{14}$$

We define $\tilde{\lambda}_h$ $(1 \leqslant h \leqslant t)$ as

$$\tilde{\lambda}_h = \begin{cases} 1, & \text{if } \lambda_h g^h \text{ is a square in } \mathbb{F}_r; \\ \gamma, & \text{if } \lambda_h g^h \text{ is a nonsquare in } \mathbb{F}_r, \end{cases} \tag{15}$$

and we change variables again $\lambda_h y_h \to y_h$, then we see that to compute the weight distribution of the cyclic code $\mathcal{C}_{(a_1,\cdots,a_t)}$, it suffices to compute the value distribution of the sum

$$\widetilde{T}(y_0, \cdots, y_t) := \bar{\eta}_{y_0} + \sum_{h=1}^{t} \bar{\eta}_{\tilde{\lambda}_h y_h}, \quad \forall\, (y_1, \cdots, y_t) \in \mathbb{F}_r^t, \tag{16}$$

where $y_0 := y_0(y_1, \ldots, y_t)$ satisfies

$$y_0 + \sum_{h=1}^{t} y_h = 0 \tag{17}$$

4.3. Proof of Theorem 1

When $2|a$, then $g = \gamma^a$ is a square. Moreover, $e|(q^{m/2}-1)$ means that $\beta = \gamma^{(q^{m/2}+1)(q^{m/2}-1)/e} \in \mathbb{F}_{q^{m/2}}$, hence the matrix A is defined over $\mathbb{F}_{q^{m/2}}$, so are all the λ_h in (14), thus λ_h are all squares in $\mathbb{F}_{q^m}$, that is, $\tilde{\lambda}_h = 1$ $(\forall h)$.

To study the value distribution of $\widetilde{T} := \widetilde{T}(y_0, \ldots, y_t)$, we will divide the space of $(y_1, \ldots, y_t) \in \mathbb{F}_r^t$ according to the integer κ, which counts the number of i $(0 \le i \le t)$ such that $y_i = 0$. Obviously $0 \le \kappa \le t+1$.

If $\kappa \ge t$, i.e., at least t terms of $y_0, y_1, \ldots, y_t$ equal to 0, then all of them equal to 0, $\widetilde{T} = (t+1)\bar{\eta}_0$ and the frequency is 1.

If $\kappa = t-1$, i.e., exactly $(t-1)$ terms of $y_0, y_1, \ldots, y_t$ equal to 0, say for example the two terms which are not 0 are y_i, y_j for some $0 \le i < j \le t$, the number of choices of such i, j is $\binom{t+1}{2}$, and the constraint (17) becomes $y_i + y_j = 0$, or $y_i = -y_j$. Hence for this i, j we find that

$$\widetilde{T} = (t-1)\bar{\eta}_0 + \bar{\eta}_{y_j} + \bar{\eta}_{-y_j} = (t-1)\bar{\eta}_0 + 2\bar{\eta}_{y_j}.$$

So the value distribution of $\widetilde{T}$ for $\kappa = t-1$ is as follows:

Value $\widetilde{T}$	Frequency
$(t-1)\bar{\eta}_0 + 2\eta_0$,	$\frac{r-1}{2} \cdot \binom{t+1}{2}$
$(t-1)\bar{\eta}_0 + 2\eta_1$,	$\frac{r-1}{2} \cdot \binom{t+1}{2}$

Now suppose in general $\kappa = t-k$ for some k with $1 \le k \le t$. Say the $(k+1)$ terms which are not 0 are $y_{i_0}, y_{i_1}, \ldots, y_{i_k}$ for some $0 \le i_0 < i_1 < \cdots < i_k \le t$. The number of ways to choose such i_j's is $\binom{t+1}{k+1}$, and for such i_j's, the constraint (17) becomes

$$y_{i_0} + y_{i_1} + \cdots + y_{i_k} = 0,$$

and we find that

$$\widetilde{T} = (t-k)\bar{\eta}_0 + \bar{\eta}_{y_{i_0}} + \bar{\eta}_{y_{i_1}} + \cdots + \bar{\eta}_{y_{i_k}}.$$

In order to compute the value distribution of $\widetilde{T}$ for these cases, it suffices to compute for any positive integer u and any sequence $i_1, \cdots, i_u, i_{u+1} \in \{0,1\}$ the value $\Omega_{i_1 \cdots i_u i_{u+1}}$ given by

$$\Omega_{i_1 \cdots i_u i_{u+1}} := \# \left\{ (x_1, \cdots, x_u) \in (\mathbb{F}_r^*)^u \;\middle|\; x_1 \in C_{i_1}^{(2,r)}, \cdots, x_u \in C_{i_u}^{(2,r)}, \sum_{j=1}^{u} x_j \in C_{i_{u+1}}^{(2,r)} \right\}. \tag{18}$$

We will prove in Section 6 that the value $\Omega_{i_1 \cdots i_u i_{u+1}}$ depends only on the number of 0's and 1's in the sequence $i_1, \ldots, i_{u+1}$. More precisely for any $u + v \ge 1$ we have (see Lemma 10 in Section 6)

$$\Omega_{\underbrace{0\cdots0}_{u}\underbrace{1\cdots1}_{v}} = \frac{r-1}{r2^{u+v+1}} \left\{ 2(r-1)^{u+v-1} + (-1)^{u+v} \left\{ (1+\sqrt{r})^u (1-\sqrt{r})^v + (1-\sqrt{r})^u (1+\sqrt{r})^v \right\} \right\}.$$

Note that the number of ways to choose a fixed $u \ge 0$ is $\binom{k+1}{u}$. So, for the case that $\kappa = t-k$, $1 \le k \le t$, the value distribution of $\widetilde{T}$ is given as follows

Value $\widetilde{T}$	Frequency $(\forall u, v \geq 0, u+v=k+1)$
$(t-k)\bar{\eta}_0 + u\eta_0 + v\eta_1,$	$\binom{t+1}{k+1}\binom{k+1}{u}\Omega_{\underbrace{0\cdots 0}_{u}\underbrace{1\cdots 1}_{v}}$

As for the values $\bar{\eta}_0, \eta_0, \eta_1$, we have $\bar{\eta}_0 = \frac{r-1}{2}$ and from Lemma 5

$$\begin{cases} \eta_0 = \frac{-1-\sqrt{r}}{2}, & \eta_1 = \frac{-1+\sqrt{r}}{2}, & \text{if } q \equiv 1 \pmod 4, \\ \eta_0 = \frac{-1-(-1)^{ms/2}\sqrt{r}}{2}, & \eta_1 = \frac{-1+(-1)^{ms/2}\sqrt{r}}{2}, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Now we have obtained the value distribution of $\widetilde{T}$. Returning to (12) and (11) gives us the weight distribution of the cyclic code $\mathcal{C}_{(a_1,\cdots,a_t)}$, which is summarized in Tables 1 and 2 in Theorem 1. This completes the proof of Theorem 1.

5. Proof of Theorem 2 and Theorem 3

5.1. Proof of Theorem 3

Recall from (16) and (17) that to compute the weight distribution of the cyclic code $\mathcal{C}_{(a_1,\cdots,a_t)}$, it suffices to compute the value distribution of the sum, $\forall (y_1, \cdots, y_{l_0}, z_1, \ldots, z_{l_1}) \in \mathbb{F}_r^{l_0+l_1}$,

$$\widetilde{T}(y_0, y_1, \cdots, y_{l_0}, \gamma z_1, \cdots, \gamma z_{l_1}) := \sum_{h=0}^{l_0} \bar{\eta}_{y_h} + \sum_{h=1}^{l_1} \bar{\eta}_{\gamma z_h}, \tag{19}$$

where l_0, l_1 are defined by (5) so that $l_0 + l_1 = t$ and $y_0 := y_0(y_1, \ldots, y_{l_0}, z_1, \ldots, z_{l_1})$ satisfies

$$y_0 + y_1 + \cdots + y_{l_0} + z_1 + \cdots + z_{l_1} = 0. \tag{20}$$

To study the value distribution of $\widetilde{T}$ in (19), we consider the different subcases according to different (k_0, k_1), where k_0, k_1 are defined by

$$k_0 := \#\{i \mid 0 \leqslant i \leqslant l_0, y_i \neq 0\};$$
$$k_1 := \#\{i \mid 1 \leqslant i \leqslant l_1, z_i \neq 0\}.$$

If $k_0 + k_1 \leq 1$, by (20), all of $y_0, y_1, \ldots, y_{l_0}, z_1, \ldots, z_{l_1}$ are 0, the frequency is 1 and $\widetilde{T} = (t+1)\bar{\eta}_0$.

If $k_0 + k_1 \geq 2$, the number of ways to choose exactly k_0 non-zero terms in $y_0, \ldots, y_{l_0}$ and exactly k_1 non-zero terms in $z_1, \ldots, z_{l_1}$ is $\binom{l_0+1}{k_0}\binom{l_1}{k_1}$. Once they are chosen, without loss of generality we may assume that they are $y_1, \ldots, y_{k_0}$ and $z_1, \ldots, z_{k_1}$. Then in this case we have

$$\widetilde{T} = (t+1-k_0-k_1)\bar{\eta}_0 + \sum_{i=1}^{k_0} \bar{\eta}_{y_i} + \sum_{i=1}^{k_1} \bar{\eta}_{\gamma z_i},$$

and the constraint (20) becomes

$$y_1 + \cdots + y_{k_0} + z_1 + \cdots + z_{k_1} = 0.$$

In order to compute the value distribution of $\widetilde{T}$ for these cases, let us consider for any $i_1, \ldots, i_{k_0}, j_1, \ldots, j_{k_1} \in \{0,1\}$ the value $\Omega'_{i_1\cdots i_{k_0}; j_1\cdots j_{k_1}}$, given by

$$\Omega'_{i_1\cdots i_{k_0}; j_1\cdots j_{k_1}} := \#\left\{ (y_1, \cdots, y_{k_0}; z_1, \cdots, z_{k_1}) \in (\mathbb{F}_r^*)^{k_0+k_1} \;\middle|\; \begin{array}{c} y_u \in C_{i_u}^{(2,r)}, \gamma z_v \in C_{j_v}^{(2,r)}, 1 \le u \le k_0, 1 \le v \le k_1 \\ y_1 + \cdots + y_{k_0} + z_1 + \cdots + z_{k_1} = 0 \end{array} \right\}.$$

For any $i \in \{0,1\}$, define $\bar{i} \in \{0,1\}$ by $\bar{i} \equiv i+1 \pmod 2$. Clearly

$$\Omega'_{i_1\cdots i_{k_0}; j_1\cdots j_{k_1}} = \Omega_{i_1\cdots i_{k_0}\bar{j}_1\cdots\bar{j}_{k_1}},$$

which is defined in (18) and is evaluated in Section 6. In $\{i_1, \ldots, i_{k_0}\}$, let u_0 be the number of 0's and u_1 be the number of 1's; similarly, in $\{j_1, \ldots, j_{k_1}\}$, let v_0 be the number of 0's and v_1 be the number of 1's. Given such u_0, u_1, v_0, v_1, we have

$$\widetilde{T} = (t+1-k_0-k_1)\bar{\eta}_0 + (u_0+v_0)\eta_0 + (u_1+v_1)\eta_1,$$

and the frequency is

$$\binom{l_0+1}{k_0}\binom{l_1}{k_1}\binom{k_0}{u_0}\binom{k_1}{v_0}\Omega_{\underbrace{0\cdots0}_{u_0+v_1}\underbrace{1\cdots1}_{u_1+v_0}}.$$

Now let k and u be fixed such that $k_0+k_1 = k$ and $u_0+v_0 = u$, where $0 \le u \le k_0+k_1 = k$ and $2 \le k \le l_0+l_1+1 = t+1$, we conclude that $\widetilde{T}$ takes the value

$$\widetilde{T} = (t+1-k)\bar{\eta}_0 + u\eta_0 + (k-u)\eta_1, \tag{21}$$

and the frequency is

$$\sum_{k_0=0}^{k}\sum_{u_0=0}^{u}\binom{l_0+1}{k_0}\binom{l_1}{k-k_0}\binom{k_0}{u_0}\binom{k-k_0}{u-u_0}\Omega_{\underbrace{0\cdots0}_{2u_0+k-k_0-u,}\ \underbrace{1\cdots1}_{k_0+u-2u_0}}. \tag{22}$$

This, after returning to (11), provides the weight distribution of the cyclic code $\mathcal{C}_{(a_1,\ldots,a_t)}$ for the general case $N = 2, t = e-1 \geqslant 2$.

5.2. Proof of Theorem 2

From $N = 2 = \gcd((q^m-1)/(q-1), 4a)$ and $t = e-1 = 3$, it is easy to see that $q \equiv 1 \pmod 4$, $m \equiv 2 \pmod 4$ and $e = 4 \mid (q^{m/2}-1)$. If $2|a$, the weight distribution has been obtained from (i) of Theorem 1 with $t = 3$. Thus Table 3 can be worked out. If $2 \nmid a$, we use Theorem 3 to calculate the weight distribution. In this case $l_0 = 1, l_1 = 2$, from (21) and (22), for any k, u with $2 \le k \le 4$, $0 \le u \le k$, the sum $\widetilde{T}$ takes the value

$$\widetilde{T} = (4-k)\bar{\eta}_0 + u\eta_0 + (k-u)\eta_1,$$

with frequency

$$\sum_{k_0=0}^{k}\sum_{u_0=0}^{u}\binom{2}{k_0}\binom{2}{k-k_0}\binom{k_0}{u_0}\binom{k-k_0}{u-u_0}\Omega_{\underbrace{0\cdots0}_{2u_0+k-k_0-u},\ \underbrace{1\cdots1}_{k_0+u-2u_0}}.$$

Using the values

$$\begin{cases} \Omega_{00} = \Omega_{11} = \frac{r-1}{2}; \quad \Omega_{01} = 0; \\ \Omega_{000} = \Omega_{111} = \frac{r-1}{8}(r-5); \\ \Omega_{001} = \Omega_{011} = \frac{(r-1)^2}{8}; \\ \Omega_{0000} = \Omega_{1111} = \frac{r-1}{16}(r^2-2r+9); \\ \Omega_{0001} = \Omega_{0111} = \frac{r-1}{16}(r^2-4r+3); \\ \Omega_{0011} = \frac{(r-1)^3}{16}, \end{cases}$$

which we can obtain from Lemma 10 in Section 6, we find that for $k = 2$,

Value	Frequency
$2\bar{\eta}_0 + 2\eta_0$,	$\Omega_{00} + 4\Omega_{01} + \Omega_{11} = r-1$
$2\bar{\eta}_0 + 2\eta_1$,	$\Omega_{00} + 4\Omega_{01} + \Omega_{11} = r-1$
$2\bar{\eta}_0 + \eta_0 + \eta_1$,	$4\Omega_{00} + 4\Omega_{01} + 4\Omega_{11} = 4(r-1)$

and for $k = 3$,

Value	Frequency
$\bar{\eta}_0 + 3\eta_0$,	$2\Omega_{001} + 2\Omega_{011} = \frac{(r-1)^2}{2}$
$\bar{\eta}_0 + 3\eta_1$,	$2\Omega_{001} + 2\Omega_{011} = \frac{(r-1)^2}{2}$
$\bar{\eta}_0 + 2\eta_0 + \eta_1$,	$4\Omega_{011} + 2\Omega_{000} + 2\Omega_{111} + 4\Omega_{001} = \frac{(r-1)}{2}(3r-7)$
$\bar{\eta}_0 + \eta_0 + 2\eta_1$,	$4\Omega_{011} + 2\Omega_{000} + 2\Omega_{111} + 4\Omega_{001} = \frac{(r-1)}{2}(3r-7)$

and for $k = 4$,

Value	Frequency
$4\eta_0$,	$\Omega_{0011} = \frac{(r-1)^3}{16}$
$4\eta_1$,	$\Omega_{0011} = \frac{(r-1)^3}{16}$
$3\eta_0 + \eta_1$,	$2\Omega_{0111} + 2\Omega_{0001} = \frac{(r-1)}{4}(r^2 - 4r + 3)$
$\eta_0 + 3\eta_1$,	$2\Omega_{0111} + 2\Omega_{0001} = \frac{(r-1)}{4}(r^2 - 4r + 3)$
$2(\eta_0 + \eta_1)$,	$\Omega_{1111} + 4\Omega_{0011} + \Omega_{0000} = \frac{(r-1)}{8}(3r^2 - 6r + 11)$.

Now we have obtained the value distribution of $\widetilde{T}$. Returning to (12) and (11) gives us the weight distribution of the cyclic code $\mathcal{C}_{(a_1,a_2,a_3)}$ with $2 \nmid a$, which is summarized in Table 4 in Theorem 2. This completes the proof of Theorem 2.

6. Appendix: Calculation of $\Omega_{i_1\cdots i_u i_{u+1}}$

Recall that for positive integer u and any sequence $i_1, \cdots, i_u, i_{u+1} \in \{0, 1\}$, $\Omega_{i_1\cdots i_u i_{u+1}}$ is defined by

$$\Omega_{i_1\cdots i_u i_{u+1}} := \#\left\{(x_1, \cdots, x_u) \in (\mathbb{F}_r^*)^u \;\middle|\; x_1 \in C_{i_1}^{(2,r)}, \cdots, x_u \in C_{i_u}^{(2,r)}, \sum_{j=1}^{u} x_j \in C_{i_{u+1}}^{(2,r)}\right\}.$$

We first prove that the value of $\Omega_{i_1\cdots i_u i_{u+1}}$ is related to reduced quadratic Jacobi sums which were introduced in Section 3 before.

Lemma 8. *The number $\Omega_{i_1\cdots i_u i_{u+1}}$ defined above equals to*

$$\frac{r-1}{2^{u+1}} \sum_{0\le v_2,\cdots,v_{u+1}\le 1} (-1)^{\sum_{j=2}^{u+1}(i_1+i_j)v_j} \rho\left((-1)^{\sum_{j=2}^{u} v_j}\right) J^*(\rho^{v_2}, \cdots, \rho^{v_{u+1}}),$$

where ρ is the quadratic multiplicative character of $\mathbb{F}_r$.

Proof. For $x \in \mathbb{F}_r^*$, let χ denote a multiplicative character of $\mathbb{F}_r$. It is easy to check that

$$\frac{1}{2}\sum_{\chi^2=\varepsilon} \chi(x\gamma^i) = \begin{cases} 1, & \text{if } x \in C_i^{(2,r)}; \\ 0, & \text{otherwise.} \end{cases} \tag{23}$$

Suppose $\chi_1, \chi_2, \cdots, \chi_{u+1}$ denote multiplicative characters of $\mathbb{F}_r$. By the relation (23), we have

$$\Omega_{i_1\cdots i_u i_{u+1}}$$
$$= \sum_{x_1,\cdots x_u\in\mathbb{F}_r^*} \left[\frac{1}{2}\sum_{\chi_1^2=\varepsilon}\chi_1(x_1\gamma^{i_1})\right]\cdots\left[\frac{1}{2}\sum_{\chi_u^2=\varepsilon}\chi_u(x_u\gamma^{i_u})\right]\left[\frac{1}{2}\sum_{\chi_{u+1}^2=\varepsilon}\chi_{u+1}(\gamma^{i_{u+1}}\sum_{j=1}^{u}x_j)\right].$$

Expanding the right hand side and changing the order of summation we obtain

$$\frac{1}{2^{u+1}}\sum_{\substack{\chi_j^2=\varepsilon\\ j=1,\cdots,u+1}}\chi_1(\gamma^{i_1})\cdots\chi_u(\gamma^{i_u})\chi_{u+1}(\gamma^{i_{u+1}})$$
$$\cdot\sum_{x_1,\ldots,x_u\in\mathbb{F}_r^*}\chi_1(x_1)\cdots\chi_u(x_u)\chi_{u+1}(x_1+x_2+\cdots+x_u),$$

which gives

$$\frac{1}{2^{u+1}}\sum_{\substack{\chi_j^2=\varepsilon\\ j=1,\cdots,u+1}}\chi_1(\gamma^{i_1})\chi_2(-\gamma^{i_2})\cdots\chi_u(-\gamma^{i_u})\chi_{u+1}(\gamma^{i_{u+1}})$$
$$\cdot\sum_{x_1,\ldots,x_u\in\mathbb{F}_r^*}\chi_1\chi_2\cdots\chi_{u+1}(x_1)\chi_2(x_2)\cdots\chi_u(x_u)\chi_{u+1}(1-x_2-\cdots-x_u).$$

This is

$$\frac{r-1}{2^{u+1}}\sum_{\substack{\chi_j^2=\varepsilon\\ j=2,\cdots,u+1}}\chi_2(-\gamma^{i_1+i_2})\cdots\chi_u(-\gamma^{i_1+i_u})\chi_{u+1}(\gamma^{i_1+i_{u+1}})$$
$$\cdot\sum_{x_2,\cdots,x_u\in\mathbb{F}_r^*}\chi_2(x_2)\cdots\chi_u(x_u)\chi_{u+1}(1-x_1-\cdots-x_u).$$

So we obtain

$$\Omega_{i_1\cdots i_u i_{u+1}}=\frac{r-1}{2^{u+1}}\sum_{0\le v_2,\cdots,v_{u+1}\le 1}(-1)^{\sum_{j=2}^{u}(i_1+i_j)v_j}\rho\left((-1)^{\sum_{j=2}^{u}v_j}\right)J^*(\rho^{v_2},\cdots,\rho^{v_{u+1}}).$$

This completes the proof of Lemma 8. □

Lemma 9. *Suppose that -1 is a square in $\mathbb{F}_r$, then*

$$\Omega_{i_1\cdots i_u i_{u+1}}=$$
$$\frac{r-1}{2^{u+1}}\left\{\frac{1}{r}\left((r-1)^u-(-1)^u\right)-(-1)^u\sum_{1\le l\le\frac{u+1}{2}}r^{l-1}\sum_{1\le j_1<j_2<\cdots<j_{2l}\le u+1}(-1)^{\sum_{k=1}^{2l}i_{j_k}}\right\}.$$

Proof. Since $N=\gcd(\frac{q^m-1}{q-1},ea)=2$ implies $2|m$, $-1=\gamma^{\frac{q^m-1}{2}}$ is always a square in this paper. From Lemma 8 we have

$$\Omega_{i_1\cdots i_u i_{u+1}} = \tfrac{r-1}{2^{u+1}} \sum_{0\le v_2,\cdots,v_{u+1}\le 1} (-1)^{\sum_{j=2}^{u}(i_1+i_j)v_j} J^*(\rho^{v_2},\cdots,\rho^{v_{u+1}}).$$

Note that $J^*(\rho_1,,\cdots,\rho_u)$ does not depend on the order of the characters $\rho_1,\ldots,\rho_u$, so we have

$$\Omega_{i_1\cdots i_u i_{u+1}} = \tfrac{r-1}{2^{u+1}} \sum_{I\subset\{2,\ldots,u+1\}} (-1)^{\sum_{j\in I}(i_1+i_j)} J^*(\underbrace{\varepsilon,\ldots,\varepsilon}_{u-\#I},\underbrace{\rho,\cdots,\rho}_{\#I}).$$

Separating the cases that $I=\emptyset$, $\#I>0$ is even and $\#I$ is odd and applying Lemmas 6 and 7, we can obtain

$$\Omega_{i_1\cdots i_u i_{u+1}} = \tfrac{r-1}{2^{u+1}} \{A+B+C\},$$

where

$$A = J^*(\underbrace{\varepsilon,\cdots,\varepsilon}_{u}) = \frac{1}{r}\Big((r-1)^u-(-1)^u\Big),$$

$$B = (-1)^{u+1} \sum_{\substack{\emptyset\neq I\subset\{2,\ldots,u+1\}\\ \#I \text{ is even}}} (-1)^{\sum_{j\in I} i_j} r^{(\#I-2)/2},$$

and

$$C = (-1)^{u+1} \sum_{\substack{I\subset\{2,\ldots,u+1\}\\ \#I \text{ is odd}}} (-1)^{i_1+\sum_{j\in I} i_j} r^{(\#I-1)/2}.$$

Set $\#I=2l$ if $\#I$ is even and $\#I=2l-1$ if $\#I$ is odd, then we complete the proof of Lemma 9. □

It is easy to see from Lemma 9 that the value $\Omega_{i_1\cdots i_u i_{u+1}}$ does not depend on the order of the sequence $i_1,\ldots,i_u,i_{u+1}$. Now we can prove

Lemma 10. *Suppose that -1 is a square in $\mathbb{F}_r$, then*

$$\Omega_{\underbrace{0\cdots0}_{u}\underbrace{1\cdots1}_{v}} =$$

$$\tfrac{r-1}{r2^{u+v+1}}\Big\{2(r-1)^{u+v-1}+(-1)^{u+v}\left\{(1+\sqrt{r})^u(1-\sqrt{r})^v+(1-\sqrt{r})^u(1+\sqrt{r})^v\right\}\Big\}.$$

Proof. From Lemma 9, it suffices to compute

$$P = \sum_{1\le l\le \frac{u+v}{2}} r^{l-1} \sum_{1\le j_1<j_2<\cdots<j_{2l}\le u+v} (-1)^{\sum_{k=1}^{2l} i_{j_k}}.$$

Since $i_j = 0$ for $1 \le j \le u$ and $i_k = 1$ for $u+1 \le j \le u+v$, we have

$$\sum_{1\le j_1<j_2<\cdots<j_{2l}\le u+v} (-1)^{\sum_{k=1}^{2l} i_{j_k}} = \sum_{s=0}^{2l} \binom{u}{2l-s}\binom{v}{s}(-1)^s,$$

and the right hand side is the coefficient of x^{2l} in the expansion of the polynomial $f(x) := (1+x)^u(1-x)^v$. Hence letting

$$f(x) = 1 + \sum_{n=1}^{u+v} a_n x^n, \quad a_n \in \mathbb{R},$$

then

$$P = \frac{1}{r} \sum_{1\le l\le \frac{u+v}{2}} a_{2l}(\sqrt{r})^{2l}.$$

Clearly the right hand side is

$$\frac{1}{r}\left\{\frac{f(\sqrt{r}) + f(-\sqrt{r})}{2} - 1\right\}.$$

This completes the proof of Lemma 10. □

7. Conclusions

In this paper, we determine the weight distributions of a new family of cyclic codes with arbitrary number of nonzeros, more precisely the cyclic codes $\mathcal{C}_{(a_1,\cdots,a_t)}$ given by (1) with any $t \ge 2$ nonzeros under the conditions that $t = e-1$ and $N = 2$. Our main results are as follows:

- For $N = 2$, $t = e-1 \geqslant 2$, $2|a$ and $e|(q^{m/2}-1)$, we obtain the weight distribution of $\mathcal{C}_{(a_1,\cdots,a_t)}$.
- For $N = 2$ and $t = e-1 = 3$, we obtain the weight distribution of $\mathcal{C}_{(a_1,\cdots,a_t)}$.
- For the general case of $N = 2$ and $t = e-1 \geqslant 2$, we present a computational formula to determine the weight distribution of $\mathcal{C}_{(a_1,\cdots,a_t)}$.

Except for these cases (in [37] and this paper), the weight distribution of the code $\mathcal{C}_{(a_1,\cdots,a_t)}$ is open in most cases when $t < e$. It would be good if some of these open cases can be settled.

Acknowledgments

Jing Yang's research is partly supported by the National Natural Science Foundation of China (Nos. 11371011 and 11471178) and Beijing Higher Education Young Elite Teacher Project. Maosheng Xiong's research is supported by the Research Grants Council, University Grants Committee, Hong Kong (Nos. 609513 and 606211). Lingli Xia's research is partly supported by Beijing Natural Science Foundation (No. 1144012), the Science Research Common Program of Beijing Municipal Commission of Education (No. SQKM201411417009) and Science and Technology on Information Assurance Laboratory (No. KJ-13-005).

References

[1] Y. Aubry, P. Langevin, On the weights of binary irreducible cyclic codes, in: Proceedings of the 2005 International Conference on Coding and Cryptography, in: Lect. Notes Comput. Sci., vol. 3969, Springer-Verlag, 2006, pp. 46–54.
[2] L.D. Baumert, R.J. McEliece, Weights of irreducible cyclic codes, Inf. Control 20 (1972) 158–175.
[3] L.D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, DSN Prog. Rep. 16 (1973) 128–131.
[4] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, J. Wiley and Sons Company, New York, 1997.
[5] R. Calderbankand, W.M. Kantor, The geometry of two-weight codes, Bull. Lond. Math. Soc. 18 (1986) 97–122.
[6] P. Delsarte, On subfield subcodes of modified Reed–Solomon codes, IEEE Trans. Inf. Theory 21 (1975) 575–576.
[7] C. Ding, Y. Liu, C. Ma, L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, IEEE Trans. Inf. Theory 57 (2011) 8000–8006.
[8] C. Ding, J. Yang, Hamming weights in irreducible cyclic codes, Discrete Math. 313 (2013) 434–446.
[9] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes, Finite Fields Appl. 14 (2008) 390–409.
[10] T. Feng, On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights, Des. Codes Cryptogr. 62 (2012) 253–258.
[11] T. Feng, K. Momihara, Evaluation of the weight distribution of a class of cyclic codes based on index 2 Gauss sums, IEEE Trans. Inf. Theory 59 (2013) 5980–5984.
[12] R. Fitzgerald, J. Yucas, Sums of Gauss sums and weights of irreducible codes, Finite Fields Appl. 11 (2005) 89–110.
[13] H.D.L. Hollmann, Q. Xiang, On binary cyclic codes with few weights, in: Proc. Finite Fields Appl. (Augsburg), Berline, Germany, 1999, pp. 251–275.
[14] T. Kløve, Codes for Error Detection, World Scientific, Singapore, 2007.
[15] S. Li, S. Hu, T. Feng, G. Ge, The weight distribution of a class of cyclic codes related to Hermitian forms graphs, IEEE Trans. Inf. Theory 59 (2013) 3064–3067.
[16] J. Luo, K. Feng, On the weight distribution of two classes of cyclic codes, IEEE Trans. Inf. Theory 54 (2008) 5332–5344.
[17] J. Luo, K. Feng, Cyclic codes and sequences from generalized Coulter–Matthews function, IEEE Trans. Inf. Theory 54 (2008) 5345–5353.
[18] J. Luo, Y. Tang, H. Wang, Cyclic codes and sequences: the generalized Kasami case, IEEE Trans. Inf. Theory 56 (2010) 2130–2142.
[19] C. Ma, L. Zeng, Y. Liu, D. Feng, C. Ding, The weight enumerator of a class of cyclic codes, IEEE Trans. Inf. Theory 57 (2011) 397–402.
[20] R.J. McEliece, Irreducible cyclic codes and Gauss sums, in: Combinatorics: Proc. NATO Advanced Study Inst., Part 1: Theory of Designs, Finite Geometry and Coding Theory, Breukelen, 1974, in: Math. Centre Tracts, vol. 55, Math. Centrum, Amsterdam, 1974, pp. 179–196.
[21] R.J. McEliece, J.H. Rumsey, Euler products, cyclotomy and coding, J. Number Theory 4 (1972) 302–311.

[22] M. Moisio, Explicit evaluation of some exponential sums, Finite Fields Appl. 15 (2009) 644–651.
[23] M. Moisio, K. Ranto, M. Rintaaho, K. Väänänen, On the weight distribution of the duals of irreducible cyclic codes, cyclic codes with two zeros and hyper-Kloosterman codes, Adv. Appl. Discrete Math. 3 (2009) 155–164.
[24] G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith. 39 (1981) 251–264.
[25] A. Rao, N. Pinnawala, A family of two-weight irreducible cyclic codes, IEEE Trans. Inf. Theory 56 (2010) 2568–2570.
[26] B. Schmidt, C. White, All two-weight irreducible cyclic codes?, Finite Fields Appl. 8 (2002) 1–17.
[27] R. Schroof, Families of curves and weight distribution of codes, Bull. Am. Math. Soc. 32 (1995) 171–183.
[28] M. van der Vlugt, Hasse–Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes, J. Number Theory 55 (1995) 145–159.
[29] G. Vega, Determining the number of one-weight cyclic codes when length and dimension are given, in: Arithmetic of Finite Fields, in: Lect. Notes Comput. Sci., vol. 4547, Springer, Berlin, Germany, 2007, pp. 284–293.
[30] G. Vega, J. Wolfmann, New classes of 2-weight cyclic codes, Des. Codes Cryptogr. 42 (2007) 327–334.
[31] G. Vega, The weight distribution of an extended class of reducible cyclic codes, IEEE Trans. Inf. Theory 58 (2012) 4862–4869.
[32] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, The weight distributions of cyclic codes and elliptic curves, IEEE Trans. Inf. Theory 58 (2012) 7253–7259.
[33] J. Wolfmann, Weight distributions of some binary primitive cyclic codes, IEEE Trans. Inf. Theory 40 (1994) 2068–2071.
[34] M. Xiong, The weight distributions of a class of cyclic codes, Finite Fields Appl. 18 (2012) 933–945.
[35] M. Xiong, The weight distributions of a class of cyclic codes II, Des. Codes Cryptogr. (2012), http://dx.doi.org/10.1007/s10623-012-9785-0.
[36] M. Xiong, The weight distributions of a class of cyclic codes III, Finite Fields Appl. 21 (2012) 84–96.
[37] J. Yang, M. Xiong, C. Ding, J. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, IEEE Trans. Inf. Theory 59 (2013) 5985–5993.
[38] X. Zeng, L. Hu, W. Jiang, Q. Yue, X. Cao, Weight distribution of a p-ary cyclic code, Finite Fields Appl. 16 (2010) 56–73.