THE VALUES OF TWO CLASSES OF GAUSSIAN PERIODS IN INDEX 2 CASE AND WEIGHT DISTRIBUTIONS OF LINEAR CODES

FENGWEI LI
School of Mathematics and Statistics, Zaozhuang University
Zaozhuang, Shandong, 277160, China
State Key Laboratory of Cryptology, P. O. Box 5159
Beijing, 100878, China

QIN YUE
Department of Mathematics, Nanjing University of Aeronautics and Astronautics
Nanjing, Jiangsu, 211100, China

XIAOMING SUN
School of Mathematics and Statistics, Zaozhuang University
Zaozhuang, 277160, China

(Communicated by Ferruh özbudak)

Abstract. Let \( l \) be a prime with \( l \equiv 3 \pmod{4} \) and \( l \neq 3 \), \( N = l^m \) for \( m \) a positive integer, \( f = \phi(N)/2 \) the multiplicative order of a prime \( p \) modulo \( N \), and \( q = p^f \), where \( \phi(\cdot) \) is the Euler-function. Let \( \alpha \) be a primitive element of a finite field \( \mathbb{F}_q \), \( C_0^{(N,q)} = \langle \alpha^N \rangle \) a cyclic subgroup of the multiplicative group \( \mathbb{F}_q^* \), and \( C_i^{(N,q)} = \alpha^i(\alpha^N) \) the cosets, \( i = 0, \ldots, N - 1 \). In this paper, we use Gaussian sums to obtain the explicit values of \( \eta_i^{(N,q)} = \sum_{x \in C_i^{(N,q)}} \psi(x) \), \( i = 0, 1, \ldots, N - 1 \), where \( \psi \) is the canonical additive character of \( \mathbb{F}_q \). Moreover, we also compute the explicit values of \( \eta_i^{(2N,q)} \), \( i = 0, 1, \ldots, 2N - 1 \), if \( q \) is a power of an odd prime \( p \).

As an application, we investigate the weight distribution of a \( p \)-ary linear code:

Let \( C \) be a \( (n, k, d) \) \( p \)-ary linear code:

\[
C_D = \{ C = (\text{Tr}_{q/p}(cx_1), \text{Tr}_{q/p}(cx_2), \ldots, \text{Tr}_{q/p}(cx_n)) : c \in \mathbb{F}_q \}.
\]

where its defining set \( D \) is given by

\[
D = \{ x \in \mathbb{F}_q^* : \text{Tr}_{q/p}(x^{\frac{q^i-1}{p-1}}) = 0 \}
\]

and \( \text{Tr}_{q/p} \) denotes the trace function from \( \mathbb{F}_q \) to \( \mathbb{F}_p \).

1. Introduction

Let \( \mathbb{F}_q \) be the finite field with \( q \) elements, where \( q = p^f \), \( p \) is a prime, and \( f \) is a positive integer. An \( \{n, k, d\} \) \( p \)-ary linear code \( C \) is a \( k \)-dimensional subspace of \( \mathbb{F}_p^n \)

2010 Mathematics Subject Classification: Primary: 11T23, 94B05; Secondary: 11L05.

Key words and phrases: Gaussian period, Gaussian sum, cyclotomic polynomial, weight distribution, Linear code.

The paper was supported by National Natural Science Foundation of China under Grants 11601475, 61772015, the foundation of Science and Technology on Information Assurance Laboratory under Grant KJ-17-010, china, and the foundation of innovative Science and technology for youth in universities of Shandong Province China under Grant 2019KJ001.
with minimum Hamming distance \( d \). Let \( A_i \) be the number of codewords in \( C \) with Hamming weight \( i \). The weight enumerator of \( C \) is defined by

\[
1 + A_1 z + A_2 z^2 + \cdots + A_n z^n.
\]

The sequence \((1, A_1, A_2, \ldots, A_n)\) is called the weight distribution of \( C \). The study of the weight distribution of a linear code is important in both theory and application because the weight distribution of a code can be used to estimate the error correcting capability and the error probability of error detection and correction with respect to some algorithms.

Let \( N \) be a positive divisor of \( q - 1 \), \( \alpha \) a primitive element of \( \mathbb{F}_q \), \( C_0^{(N,q)} = \langle \alpha^N \rangle \) a cyclic subgroup of \( \mathbb{F}_q^* \), and \( C_i^{(N,q)} = \alpha^i \langle \alpha^N \rangle \), \( i = 0, \ldots, N - 1 \), the cosets. Let \( \psi \) be the canonical additive character of \( \mathbb{F}_q \). Gaussian periods of order \( N \) are defined by

\[
\eta_i^{(N,q)} = \sum_{x \in C_i^{(N,q)}} \psi(x), i = 0, 1, \ldots, N - 1,
\]

where \( \psi \) is the canonical additive character of \( \mathbb{F}_q \).

Gaussian periods are closely related to Gaussian sums. As applications, there are a lot of papers using Gaussian periods to give the weight distributions of linear codes and find strongly regular graphs, such as \([4-8, 13-15, 17-19, 24, 25, 27, 30, 31]\). The value of the Gaussian periods in general is very hard to compute, and it has been done only in certain special cases.

**Lemma 1.1.** \([20]\) When \( N = 2 \) and \( q = p^f \), the Gaussian periods are given by the following:

\[
\eta_0^{(2,q)} = \begin{cases} 
-1 + (-1)^{f-1} q^{\frac{1}{2}}, & \text{if } p \equiv 1 \pmod{4}, \\
-1 + (-1)^{f-1} (\sqrt{-1})^{f} q^{\frac{1}{2}}, & \text{if } p \equiv 3 \pmod{4},
\end{cases}
\]

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

The Gaussian periods in the semi-primitive case are well-known as follows.

**Lemma 1.2.** \([20]\) Assume that \( N > 2 \) and there exists a least positive integer \( e \) such that \( p^e \equiv -1 \pmod{N} \). Let \( q = p^{2er} \) for some positive integer \( r \).

1. If \( r, p, \) and \( \frac{p-1}{N} \) are all odd, then

\[
\eta_0^{(N,q)} = \frac{(N-1)\sqrt{q} - 1}{N}, \quad \eta_i^{(N,q)} = -\sqrt{q} - 1 \quad \text{for } i \neq N/2.
\]

2. In all other cases,

\[
\eta_0^{(N,q)} = \frac{(-1)^{r+1}(N-1)\sqrt{q} - 1}{N}, \quad \eta_i^{(N,q)} = \frac{(-1)^r \sqrt{q} - 1}{N} \quad \text{for } i \neq 0.
\]

For an odd prime \( l \) with \( l \equiv 3 \pmod{4} \) and \( l \neq 3 \), Myerson in \([20]\) gave the values of Gaussian periods of order \( l \) in the index 2 case. For more details to see \([1, 4, 14, 20]\).

In this paper, we determine the explicit values of \( \eta_i^{(l^m,q)}, i = 0, 1, \ldots, l^m - 1, \) and \( \eta_i^{(2^{l^m},q)}, i = 0, 1, \ldots, 2l^m - 1, \) in the index 2 case, which extend the results of Myerson in \([20]\). Moreover, we obtain the weight distributions of a class of linear codes over \( \mathbb{F}_q \). This paper is organized as follows. In Section 2, we give several results about Gaussian sums in index 2 case. In Section 3, let \( l \) be a prime with \( l \equiv 3 \pmod{4} \) and \( l \neq 3, N = l^m, f = \phi(N)/2 \) the multiplicative order of a prime \( p \) modulo \( N \), and \( q = p^f \). We obtain the explicit values of \( \eta_i^{(N,q)}, i = 0, 1, \ldots, N-1 \).
In Section 4, let \( l \) be a prime with \( l \equiv 3 \pmod{4} \) and \( l \neq 3 \), \( N = l^n \), \( f = \phi(N)/2 \) the multiplicative order of a prime \( p \) modulo \( N \), \( \gcd(p, 2N) = 1 \), and \( q = p^j \). We compute the explicit values of \( \eta_i^{(2N, q)} \), \( i = 0, 1, \ldots, 2N - 1 \). In Section 5, we give the weight distributions of a class of linear codes over \( \mathbb{F}_q \). In Section 6, we conclude this paper.

2. Some preliminaries

In this section, we present results on cyclotomic polynomials, Gaussian sums and Gaussian periods, which will be needed in the sequel. Throughout this paper, let \( p \) be a prime and \( q = p^f \) for a positive integer \( f \).

2.1. Cyclotomy and cyclotomic polynomials.

Let \( q - 1 = nN \) for two positive integers \( n > 1 \) and \( N > 1 \), and let \( \alpha \) be a fixed primitive element of \( \mathbb{F}_q \). Define \( C_i^{(N, q)} = \alpha^i(\alpha^N) \) for \( i = 0, 1, \ldots, N - 1 \), where \( \langle \alpha^N \rangle \) denotes the subgroup of the multiplicative group \( \mathbb{F}_q^* \) generated by \( \alpha^N \). The cosets \( C_i^{(N, q)} \) are called the cyclotomic classes of order \( N \) in \( \mathbb{F}_q \). The cyclotomic numbers of order \( N \) are defined by

\[
(i, j)_N = |(1 + C_i^{(N, q)}) \cap C_j^{(N, q)}|
\]

for all \( 0 \leq i \leq N - 1 \) and \( 0 \leq j \leq N - 1 \).

The following lemma is proved in [21].

**Lemma 2.1.** If \( q \equiv 1 \pmod{4} \), then

\[
(0, 0)_2 = \frac{q - 5}{4}, (0, 1)_2 = (1, 0)_2 = (1, 1)_2 = \frac{q - 1}{4}.
\]

If \( q \equiv 3 \pmod{4} \), then

\[
(0, 1)_2 = \frac{q + 1}{4}, (0, 0)_2 = (1, 0)_2 = (1, 1)_2 = \frac{q - 3}{4}.
\]

Let \( \alpha \) be a fixed primitive element of \( \mathbb{F}_q \) and \( \beta = \alpha^{\frac{q - 1}{2}} \). Then there are \( \phi(n) \) elements of order \( n \): \( \beta^i \), \( 0 \leq i \leq n - 1 \) and \( \gcd(i, n) = 1 \). Define the \( n \)-th cyclotomic polynomial over \( \mathbb{F}_q \):

\[
\Phi_n(x) = \prod_{\substack{0 \leq i \leq n - 1 \\\gcd(i, n) = 1}} (x - \beta^i).
\]

**Lemma 2.2.** [16, Exercise 2.57] If \( p \) is a prime and an integer \( m \) is divisible by \( p \), then \( \Phi_{mp}(x) = \Phi_m(x^p) \), where \( \Phi_n(x) \) is the \( n \)-th cyclotomic polynomial.

In particular, if \( n = t^t + 1 \), where \( l \) is a prime and \( t \geq 1 \) is an integer, then

\[
\Phi_{t^t+1}(x) = \Phi_l(x^t) = (x^t)^{t-1} + (x^t)^{t-2} + \ldots + 1.
\]

2.2. Gaussian periods and Gaussian sums.

Let \( \text{Tr}_{q/p} \) be the trace function from \( \mathbb{F}_q \) to \( \mathbb{F}_p \). An additive character of \( \mathbb{F}_q \) is a nonzero function \( \psi \) from \( \mathbb{F}_q \) to the set of complex numbers such that \( \psi(x + y) = \psi(x)\psi(y) \) for any pair \( (x, y) \in \mathbb{F}_q^2 \). For each \( b \in \mathbb{F}_q \), the function

\[
\psi_b(c) = \text{Tr}_{q/p}(bc) \quad \text{for all } b \in \mathbb{F}_q
\]
defines an additive character of \( F_q \), where \( \zeta_p = e^{\frac{2\pi i}{p}} \) denotes the \( p \)-th primitive root of unity. When \( b = 1 \), the character \( \psi_1 \) is called canonical additive character of \( F_q \). It is well known that

\[
\sum_{c \in F_q} \psi_b(c) = 0 \text{ for } b \neq 0.
\]

A multiplicative character of \( F_q \) is a nonzero function \( \chi \) from \( F_q \) to the set of complex numbers such that \( \chi(xy) = \chi(x) \chi(y) \) for all pairs \( (x, y) \in F_q^* \times F_q^* \). Let \( \alpha \) be a fixed primitive element of \( F_q \). For each \( j = 1, 2, \ldots, q - 1 \), the function \( \chi_j \) with \( \chi \)

\[
\chi_j(\alpha^k) = \zeta_q^{jk} \text{ for } k = 0, 1, \ldots, q - 2
\]

defines a multiplicative character with order \( \frac{q-1}{\gcd(q-1, j)} \) of \( F_q \), where \( \zeta_{q-1} \) denotes the \( (q - 1) \)-th primitive root of unity. Let \( \bar{\chi} \) be the conjugate character of \( \chi \) defined by \( \bar{\chi}(x) = \chi(x) \), where \( \bar{\chi} \) denotes the complex conjugate of \( \chi(x) \).

Let \( q \) be odd and \( j = (q - 1)/2 \) in (2), we then get a multiplicative character denoted by \( \eta \) such that \( \eta(c) = 1 \) if \( c \) is the square of an element and \( \eta(c) = -1 \) otherwise. This \( \eta \) is called the quadratic character of \( F_q \).

Let \( \chi \) be a multiplicative character of \( F_q \) and \( \psi \) an additive character of \( F_q \). Then the Gaussian sum \( G(\chi, \psi) \) is defined as

\[
G(\chi, \psi) = \sum_{x \in F_q^*} \chi(x)\psi(x).
\]

By \( G(\chi, \psi_b) = \bar{\chi}(b)G(\chi, \psi_1) \), we need consider \( G(\chi, \psi_1) \), briefly denoted by \( G(\chi) \), in the sequel. In general, the explicit determination of Gaussian sums is also a difficult problem. In some cases, Gaussian sums are explicitly determined in [4, 27]. For future use, we state the quadratic Gaussian sums here.

**Lemma 2.3.** [16] Suppose that \( q = p^l \) and \( \eta \) is the quadratic multiplicative character of \( F_q \), where \( p \) is an odd prime. Then

\[
G(\eta) = \begin{cases} 
(-1)^{l-1} \sqrt{q}, & \text{if } p \equiv 1 \pmod{4}, \\
(-1)^{l-1} (\sqrt{-1})^l \sqrt{q}, & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

The following result is useful in the sequel.

**Lemma 2.4.** [16] Let \( \psi \) be a nontrivial additive character of \( F_q \) and \( \chi \) a multiplicative character of \( F_q \) of order \( s = \gcd(n, q - 1) \). Then

\[
\sum_{x \in F_q} \psi(ax^n + b) = \psi(b) \sum_{j=1}^{s-1} \chi^j(a)G(\chi^j, \psi)
\]

for any \( a, b \in F_q \) with \( a \neq 0 \).

Let \( \mathbb{Z}/N\mathbb{Z} = \{0, 1, \ldots, N - 1\} \) be the ring of integers modulo \( N \) and \((\mathbb{Z}/N\mathbb{Z})^* \) a multiplicative group consisting of all invertible elements in \( \mathbb{Z}/N\mathbb{Z} \). If \( \langle p \rangle \) is a cyclic subgroup with a generator \( p \) of the group \((\mathbb{Z}/N\mathbb{Z})^* \) such that \( [(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = 2 \) and \(-1 \notin \langle p \rangle \subset (\mathbb{Z}/N\mathbb{Z})^* \), which is called a “quadratic residues” or “index 2” case. These Gaussian sums are explicitly determined, see [26] and its references for details. We list some results in the index 2 case below.
Lemma 2.5. \[12, 26\] Let \( l \equiv 3 \pmod{4} \) be a prime, \( l \neq 3 \), \( m \) a positive integer, \( N = l^m \), \( f = \phi(N)/2 \) the multiplicative order of a prime \( p \) modulo \( N \), and \( q = p^f \). Suppose that \( \sqrt{l} \) is a multiplicative character of order \( N \) over \( \mathbb{F}_q \).

(i) For \( 1 \leq i \leq N - 1 \), let \( i = ul^t \), \( 0 \leq t \leq m - 1 \) and \( \gcd(u, l) = 1 \). Then

\[
G(\chi^i) = \begin{cases} 
G(\chi^u) & \text{if } u \in (p) \subset \mathbb{Z}_N^*, \\
G(\chi^{lt}) & \text{if } u \notin (p) \subset \mathbb{Z}_N^*.
\end{cases}
\]

(ii) For \( 0 \leq t \leq m - 1 \),

\[
G(\chi^{lt}) = p^{\frac{t-\lambda l}{2}} \left( a + b\sqrt{-l} \right)^{lt},
\]

where \( h \) is the ideal class number of \( \mathbb{Q}(\sqrt{-l}) \), \( a, b \) are integers given by

\[
\begin{cases} 
a^2 + lb^2 = 4p^h, \\
2a \equiv -2p^{t-1+2h} \pmod{l}.
\end{cases}
\]

Let \( \mathcal{O} = \mathbb{Z}[\sqrt{-l}] \) be the set of all algebraic integers in \( \mathbb{Q}(\sqrt{-l}) \). Then \( p\mathcal{O} = \mathcal{P}_1\mathcal{P}_2 \), where \( \mathcal{P}_1 = \langle \frac{a+bl}{2} \rangle \) and \( \mathcal{P}_2 = \langle \frac{a-bl}{2} \rangle \). In fact, the multiplicative character \( \chi \) is correspondent to \( \mathcal{P}_2 \) (see [12]).

In Lemma 2.6, suppose that \( p \) is an odd prime. Let \( \chi \) be a multiplicative character of order \( 2N \) over \( \mathbb{F}_q \). For \( 1 \leq i \leq 2N - 1 \), by the Darvenport-Hasse product formula [2, Chapter 11.3],

\[
G(\chi^{2i}) = \chi^{2i}(2) \frac{G(\chi^i)G(\chi^{i+lm})}{G(\chi^{lm})} = \frac{G(\chi^i)G(\chi^{2i+lm})}{(\sqrt{p^f})^l}.
\]

If \( i \neq N \), then \( \chi^{i+lm} \) is a non-trivial character. Hence we have the following result.

Lemma 2.6. \[26\] Let \( l \equiv 3 \pmod{4} \) be a prime, \( l \neq 3 \), \( m \) a positive integer, \( N = l^m \), \( f = \phi(N)/2 \) the multiplicative order of a prime \( p \) modulo \( N \), \( \gcd(p, 2N) = 1 \), and \( q = p^f \). Suppose that \( \sqrt{l} \) is a multiplicative character of order \( 2N \) over \( \mathbb{F}_q \). If \( i \) is odd, \( 1 \leq i \leq 2N - 1 \) and \( i \neq N \). Then

\[
G(\chi^i) = \begin{cases} 
\sqrt{p^f} & \text{if } l \equiv 7 \pmod{8} \text{ or } i = N, \\
(-1)^{-\frac{p^f}{2}}(G(\chi^{p^{f}\sqrt{p^f}}))^{1/2} & \text{if } l \equiv 3 \pmod{8} \text{ and } i \neq N.
\end{cases}
\]

In Lemma 2.6, if \( i \) is even, then \( G(\chi^i) \) is given by Lemma 2.5.

Gaussian periods are closely related to Gaussian sums. By Lemma 2.4, it is known that

\[
\eta_i^{(N,q)} = \sum_{j=0}^{N-1} \psi(\alpha^i \alpha^j N) = \frac{1}{N} \sum_{x \in \mathbb{F}_q} (\psi(\alpha^i x^N) - 1)
\]

\[
= \frac{1}{N} \left( -1 + \sum_{j=1}^{N-1} \chi^j(\alpha^j)G(\chi^j) \right) = \frac{1}{N} \sum_{j=0}^{N-1} \zeta_N^{-ij}G(\chi^j),
\]

where \( \zeta_N = e^{2\pi i/N} \) is the \( N \)-th root of unity in the complex field, \( \chi \) is a multiplicative character of order \( N \) over \( \mathbb{F}_q^* \), \( \chi(\alpha) = \zeta_N \), and \( G(\chi^0) = -1 \).

The values of the Gaussian periods in general are also very hard to compute. However, they can be computed in a few cases. In this paper, we shall compute all the Gaussian periods of orders \( l^m \) and \( 2l^m \) in the index 2 case, where \( l \) is a prime
with \( l \equiv 3 \pmod{4} \) and \( l \neq 3 \). Furthermore, using these results we obtain the weight distributions of a class of \( p \)-ary linear codes.

3. Explicit values of Gaussian periods of order \( N \)

Let \( N = l^m \), where \( m \) is a positive integer and \( l \) is a prime with \( l \equiv 3 \pmod{4} \) and \( l \neq 3 \). Let \( f = \phi(N)/2 \) be the multiplicative order of a prime \( p \) modulo \( N \), i.e., \( f \) is the smallest positive integer such that \( p^f \equiv 1 \pmod{N} \). Let \( g = p^f \). In this section, we shall give the values of the Gaussian periods \( \eta_i^{(N,q)} \), \( i = 0, 1, \ldots, N - 1 \).

Let \( S = \{0, 1, \ldots, N-1\} \) be a set. Define subsets

\[
U_k = \{ u : 0 \leq u \leq l^k - 1, \gcd(u, l) = 1 \}, \quad k = 1, \ldots, m.
\]

In fact, \( U_1 \subset U_2 \subset \ldots \subset U_m \subset S \).

It is well known that we have a disjoint union

\[
S = \bigcup_{k=1}^{m} l^{m-k}U_k \bigcup \{0\}.
\]

Denote

\[
(5) \quad S = S_0 \cup S_1 \cup \cdots \cup S_m,
\]

where \( S_0 = \{0\} \) and \( S_k = l^{m-k}U_k \). In fact \( |S_k| = \phi(l^k) = |U_k|, \quad k = 1, \ldots, m \).

Let \( \gamma \) be a primitive root of \((\mathbb{Z}/l^m\mathbb{Z})^*\), then \( \gamma \) is also a primitive root of each \((\mathbb{Z}/l^k\mathbb{Z})^*\) for \( 1 \leq k \leq m \). Let \( H_k^{(0)} = \langle \gamma^2 \rangle \) be the subgroup of \((\mathbb{Z}/l^k\mathbb{Z})^*\), then \((\mathbb{Z}/l^k\mathbb{Z})^* = H_k^{(0)} \cup H_k^{(1)}\), where \( H_k^{(1)} = \gamma H_k^{(0)} \). In fact, by [11],

\[
H_k^{(0)} = \{ x = a_0 + a_1l + \ldots + a_{k-1}l^{k-1} | a_0 \in H_1^{(0)}, a_1, \ldots, a_{k-1} \in \mathbb{Z}/l\mathbb{Z} \},
\]

\[
H_k^{(1)} = \{ x = a_0 + a_1l + \ldots + a_{k-1}l^{k-1} | a_0 \in H_1^{(1)}, a_1, \ldots, a_{k-1} \in \mathbb{Z}/l\mathbb{Z} \}.
\]

Then \( |H_k^{(0)}| = |H_k^{(1)}| = \frac{\phi(l^k)}{2} \). It is clear that

\[
(\mathbb{Z}/l^k\mathbb{Z})^* = \{ u \pmod{l^k} : u \in U_k \}, \quad k = 1, \ldots, m.
\]

For convenience, denote \( U_k = (\mathbb{Z}/l^k\mathbb{Z})^*, \quad k = 1, \ldots, m \).

In the following, we shall use (4) and Lemma 2.5 to compute the values of \( \eta_i^{(N,q)} \), \( i = 0, 1, \ldots, N - 1 \).

Now we compute the value of \( \eta_0^{(N,q)} \) in case \( i = 0 \).

**Theorem 3.1.** The notation is as above. The value of \( \eta_0^{(N,q)} \) is equal to

\[
\eta_0^{(N,q)} = \frac{1}{N} \left( -1 + \sum_{g=1}^{m} \phi(l^g) \frac{\sigma_{h-l^m-g}}{2} \left( \left( \frac{a+b\sqrt{-l}}{2} \right)^{l^m-g} + \left( \frac{a-b\sqrt{-l}}{2} \right)^{l^m-g} \right) \right),
\]

where \( h \) is the ideal class number of \( \mathbb{Q}(\sqrt{-l}) \), \( a, b \) are integers given by (3), and \( \phi(\cdot) \) denotes the Euler function.

**Proof.** By (4), we have

\[
\eta_i^{(N,q)} = \frac{1}{N} \sum_{j=0}^{N-1} G(\chi^j).
\]

By \( j = l^{m-g}v \in S \) and (5), we have

\[
\eta_0^{(N,q)} = \frac{1}{N} \left( -1 + \sum_{g=1}^{m} \sum_{v \in U_g} G(\chi^{l^m-g}v) \right).
\]
Note that for $g = 1, \ldots, m$, we know that $v \in U_g = H^{(0)}_g \cup H^{(1)}_g$ and $|H^{(0)}_g| = |H^{(1)}_g| = \frac{\phi(l^g)}{2}$. By Lemma 2.5,

$$
\sum_{g=1}^{m} \frac{m}{\phi(l^g)} G(\chi^{l^m-g}) = \sum_{g=1}^{m} \frac{\phi(l^g)}{2} G(\chi^{l^m-g}) + \sum_{g=1}^{m} \frac{\phi(l^g)}{2} G(\chi^{l^m-g})
$$

Thus

$$
\sum_{g=1}^{m} \frac{\phi(l^g)}{2} p^{l^m-g} \left( \frac{a + b\sqrt{-l}}{2} \right)^{l^m-g} + \left( \frac{a - b\sqrt{-l}}{2} \right)^{l^m-g}.
$$

Then

$$
\eta_0^{(N,q)} = \frac{1}{N} \left( -1 + \sum_{g=1}^{m} \frac{\phi(l^g)}{2} p^{l^m-g} \left( \frac{a + b\sqrt{-l}}{2} \right)^{l^m-g} + \left( \frac{a - b\sqrt{-l}}{2} \right)^{l^m-g} \right).
$$

This completes the proof.

In the following, we compute the Gaussian periods $\eta_i^{(N,q)}, i = 1, 2, \ldots, N - 1$. First, suppose that $i = l^{m-k}u \in S_k$ and $u \in H^{(0)}_k$. Let $j \in S$, i.e., $j = 0$ or $j = l^{m-g}v, 0 \leq v \leq l^g - 1, \gcd(v, l) = 1$. Then

$$
\eta_i^{(N,q)} = \frac{1}{N} \sum_{j=0}^{N-1} \zeta_N^{-ij} G(\chi^j)
$$

It is easy to see that

$$
(\zeta_N^{-2m-(k+g)})^{uv} = \begin{cases} 
1, & \text{if } k + g - m \leq 0, \\
\zeta_t^{-uv}, & \text{if } k + g - m = 1, \\
\zeta_t^{uv}, & \text{if } k + g - m = t \geq 2.
\end{cases}
$$

Set

$$
\eta_i^{(N,q)} = \frac{1}{N} (-1 + A + B + C),
$$

where

$$
A = \sum_{g=1}^{m-k} \sum_{v \in U_g} G(\chi^{l^m-gv}),
$$

$$
B = \sum_{v \in U_{m-k+1}} \zeta_t^{-uv} G(\chi^{l^k-v}),
$$

and

$$
C = \sum_{g=m-k+2}^{m} \sum_{v \in U_g} \zeta_t^{-uv} G(\chi^{l^m-gv}),
$$

where $t = k + g - m$. Note that $C = 0$ if $m - k + 2 > m$.

Now we compute the values of $A, B$ and $C$. 

Advances in Mathematics of Communications

Volume X, No. X (20XX), X–XX
Lemma 3.2. The notation is as above. Then
\[ A = \sum_{g=1}^{m-k} \phi(l)^2 \frac{1}{p} f^{l-hm^g} \left( \frac{a+b\sqrt{-l}}{2} \right)^{m^g} \left( \frac{a-b\sqrt{-l}}{2} \right)^{l-m^g}, \]
where \( h \) is the ideal class number of \( \mathbb{Q}(\sqrt{-l}) \), \( a,b \) are integers given by (3), and \( \phi(\cdot) \) denotes the Euler function.

Proof. 
\[ A = \sum_{g=1}^{m-k} \sum_{v \in U_g} G(\chi^{m^g v}), \]
where \( v \in H_{g}^{(0)} \cup H_{g}^{(1)} \). By Lemma 2.5, we obtain that
\[ A = \sum_{g=1}^{m-k} \frac{\phi(l)^2}{2} \left( G(\chi^{m^g}) + G(\chi^{l-m^g}) \right) \]
\[ = \sum_{g=1}^{m-k} \frac{\phi(l)^2}{2} f^{l-hm^g} \left( \frac{a+b\sqrt{-l}}{2} \right)^{m^g} \left( \frac{a-b\sqrt{-l}}{2} \right)^{l-m^g}. \]

Lemma 3.3. The notation is as above. Then
\[ B = l^{m-k} f^{l-hk^g} \left( \frac{-1-\sqrt{-l}}{2} (a+b\sqrt{-l})^k + \frac{-1+\sqrt{-l}}{2} (a-b\sqrt{-l})^k \right), \]
where \( h \) is the ideal class number of \( \mathbb{Q}(\sqrt{-l}) \) and \( a,b \) are integers given by (3).

Proof. By Lemma 2.5 and \( g = m-k + 1 \),
\[ B = \sum_{v \in U_g} \zeta_l uv G(\chi^{k-1 v}) = \sum_{v \in H_{g}^{(0)}} \zeta_l uv G(\chi^{k-1 v}) + \sum_{v \in H_{g}^{(1)}} \zeta_l uv G(\chi^{k-1 v}) \]
\[ = p f^{l-hk^g} \left( \frac{a+b\sqrt{-l}}{2} \right)^k \sum_{v \in H_{g}^{(0)}} \zeta_l uv + \left( \frac{a-b\sqrt{-l}}{2} \right)^k \sum_{v \in H_{g}^{(1)}} \zeta_l uv. \]

Fix \( u \in H_{k}^{(0)} \) and \( u = u_0 + u_1 l + \ldots + u_{k-1} l^{k-1} \), where \( u_0 \in H_{1}^{(0)} \) and \( u_1, \ldots, u_{k-1} \in \mathbb{Z}/l\mathbb{Z} \).

Suppose that \( v \in H_{g}^{(0)} \). By (6), let \( v = v_0 + v_1 l + \ldots + v_{g-1} l^{g-1} \), where \( v_0 \in H_{1}^{(0)} \) and \( v_1, \ldots, v_{g-1} \in \mathbb{Z}/l\mathbb{Z} \). Then \( \zeta_l uv = \zeta_l u_0 v_0 \) and \( -u_0 v_0 \in H_{1}^{(1)} \) by \( l \equiv 3 \pmod{4} \). Note that \( v_1, v_2, \ldots, v_{g-1} \in \mathbb{Z}/l\mathbb{Z} = \{0,1,\ldots,l-1\} \). Then the value of \( \sum_{v \in H_{g}^{(0)}} \zeta_l uv \) is exactly \( l^{g-1} = l^{m-k} \) times the value of \( \sum_{v \in H_{1}^{(0)}} \zeta_l u_0 v_0 \). Hence by Lemma 1.1,
\[ \sum_{v \in H_{g}^{(0)}} \zeta_l uv = l^{m-k} \sum_{v \in H_{1}^{(0)}} \zeta_l u_0 v_0 = l^{m-k} \frac{1-1-\sqrt{-l}}{2}. \]

Suppose that \( v \in H_{g}^{(1)} \). By (6), let \( v = v_0 + v_1 l + \ldots + v_{g-1} l^{g-1} \), where \( v_0 \in H_{1}^{(1)} \) and \( v_1, \ldots, v_{g-1} \in \mathbb{Z}/l\mathbb{Z} \). Then \( \zeta_l uv = \zeta_l u_0 v_0 \) and \( -u_0 v_0 \in H_{1}^{(0)} \) by \( l \equiv 3 \pmod{4} \).
Note that \(v_1, v_2, \ldots, v_{g-1} \in \mathbb{Z}/l\mathbb{Z} = \{0, 1, \ldots, l-1\}\). Then the value of \(\sum_{v \in H_k^{(1)}} \zeta_{l}^{-uv}\) is exactly \(l^{m-k}\) times the value of \(\sum_{v_0 \in H_k^{(1)}} \zeta_{l}^{-uvv_0}\). Hence by Lemma 1.1,\n
\[
(11) \quad \sum_{v \in H_k^{(1)}} \zeta_{l}^{-uv} = l^{m-k} \sum_{v_0 \in H_k^{(1)}} \zeta_{l}^{-uvv_0} = l^{m-k} \eta_0^{(2)} = l^{m-k} \frac{1 + \sqrt{l}}{2}.
\]

By \(g = m - k + 1\), the conclusion follows. \(\square\)

We are left to compute the value of \(C\).

**Lemma 3.4.** Suppose that \(t = g + k - m\) with \(t \geq 2\). Then \(C = 0\).

**Proof.** Suppose that \(u \in H_k^{(0)}\).

\[
C = \sum_{g = m-k+2}^{m} \sum_{v \in U_g} \zeta_{l}^{-uv} G(\chi^{l^{m-g}v})
\]

\[
= \sum_{g = m-k+2}^{m} \sum_{v \in H_k^{(0)}} \zeta_{l}^{-uv} G(\chi^{l^{m-g}v}) + \sum_{g = m-k+2}^{m} \sum_{v \in H_k^{(1)}} \zeta_{l}^{-uv} G(\chi^{l^{m-g}v})
\]

\[
= G(\chi^{l^{m-g}}) \sum_{g = m-k+2}^{m} \sum_{v \in H_k^{(0)}} \zeta_{l}^{-uv} + G(\chi^{l^{m-g}}) \sum_{g = m-k+2}^{m} \sum_{v \in H_k^{(1)}} \zeta_{l}^{-uv}.
\]

By the notation in (5), since \(i = l^{m-k}u \in l^{m-k}U_k = S_k\) and \(j = l^{m-g}v \in l^{m-g}U_g = S_g, iS_g = l^{m-1}U_i = S_i\) and \(|iS_g| = l^{m-k}|S_i|\).

Note that \(u \in H_k^{(0)}\). Then \(-1 \in H_k^{(1)}, -l^{m-k}u(l^{m-g}H_k^{(0)}) = l^{m-t}H_k^{(1)}, \) and \(-l^{m-k}u(l^{m-g}H_k^{(1)}) = l^{m-t}H_k^{(0)}\). Moreover \(-l^{m-k}u(l^{m-g}H_k^{(0)}) = l^{m-k}|l^{m-t}H_k^{(1)}|\) and \(-l^{m-k}u(l^{m-g}H_k^{(1)}) = l^{m-k}|l^{m-t}H_k^{(0)}|\).

Fix \(g = m - k + t, t \geq 2\). Then

\[
\sum_{v \in H_k^{(0)}} \zeta_{l}^{-uv} = l^{m-k} \sum_{v \in H_k^{(1)}} \zeta_{l}^{-uv}, \quad \sum_{v \in H_k^{(1)}} \zeta_{l}^{-uv} = l^{m-k} \sum_{v \in H_k^{(0)}} \zeta_{l}^{-uv}.
\]

Note that \(U_t = H_k^{(0)} \cup H_k^{(1)}\) for \(2 \leq t \leq m\). Then

\[
\Phi_t(x) = \Phi_t^{(0)}(x) \cdot \Phi_t^{(1)}(x),
\]

where \(\Phi_t^{(0)}(x) = \prod_{i \in H_k^{(0)}} (x - \zeta_i)\) and \(\Phi_t^{(1)}(x) = \prod_{i \in H_k^{(1)}} (x - \zeta_i)\). On the other hand, by Lemma 2.2 \(\Phi_t^{(0)}(x) = \Phi_{t-1}^{(0)}(x^l)\) and \(\Phi_t^{(1)}(x) = \Phi_{t-1}^{(1)}(x^l)\). Then \(\sum_{w \in H_k^{(i)}} \zeta_{l}^{w} = 0, i = 0, 1\). Hence

\[
(12) \quad \sum_{v \in H_k^{(0)}} \zeta_{l}^{-uv} = 0, \quad \sum_{v \in H_k^{(1)}} \zeta_{l}^{-uv} = 0, C = 0.
\]

\(\square\)

Similarly, we can also get that \(C = 0\) if \(u \in H_k^{(1)}\).

**Theorem 3.5.** If \(i = l^{m-k}u, u \in H_k^{(0)}, k = 1, 2, \ldots, m, \) then

\[
\eta_i^{(N,q)} = \frac{1}{N}(A + B - 1),
\]

\(\square\)
where

\[ A = \sum_{g=1}^{m-k} \frac{\phi(b)}{2} p_{\frac{t-\sqrt{-l}}{2}} \left( \frac{a+b\sqrt{-l}}{2} \right)^{m-g} + \left( \frac{a-b\sqrt{-l}}{2} \right)^{t-m} \],

and

\[ B = l^{m-k} p_{\frac{t-\sqrt{-l}}{2}} \left( \frac{-1 - \sqrt{-l}}{2} \left( \frac{a+b\sqrt{-l}}{2} \right)^{t-1} + \frac{-1 + \sqrt{-l}}{2} \left( \frac{a-b\sqrt{-l}}{2} \right)^{t-1} \right). \]

In A and B, \( h \) is the ideal class number of \( \mathbb{Q}(\sqrt{-l}) \), \( a, b \) are integers given by (3), and \( \phi(\cdot) \) denotes the Euler function.

Second, suppose that \( i = l^{m-k}u, u \in H_{k}^{(1)} \). We shall focus on computing the value of \( \eta_{i}^{(N,q)} \).

**Theorem 3.6.** If \( i = l^{m-k}u, u \in H_{k}^{(1)} \), then the value of \( \eta_{i}^{(N,q)} \) is

\[ \eta_{i}^{(N,q)} = \frac{1}{N} (A + B' - 1), \]

where \( A \) is defined as Theorem 3.5 and

\[ B' = l^{m-k} p_{\frac{t-\sqrt{-l}}{2}} \left( \frac{-1 + \sqrt{-l}}{2} \left( \frac{a+b\sqrt{-l}}{2} \right)^{t-1} + \frac{-1 - \sqrt{-l}}{2} \left( \frac{a-b\sqrt{-l}}{2} \right)^{t-1} \right). \]

In A and \( B' \), \( h \) is the ideal class number of \( \mathbb{Q}(\sqrt{-l}) \), \( a, b \) are integers given by (3), and \( \phi(\cdot) \) denotes the Euler function.

**Proof.** If \( u \in H_{k}^{(1)} \), then as above,

\[ \eta_{i}^{(N,q)} = \frac{1}{N} (-1 + A + B' + C), \]

where

\[ A = \sum_{g=1}^{m-k} G(\chi^{m-g}v), \]

\[ B' = \sum_{v \in \mathcal{U}_{m-k+1}} \zeta_{l}^{-uv} G(\chi^{t-1}v), \]

and \( k + g - m = t \geq 2 \),

\[ C = \sum_{g=m-k+2}^{m} \sum_{v \in \mathcal{U}_{g}} \zeta_{l}^{-uv} G(\chi^{m-g}v). \]

Note that \( u \in H_{k}^{(1)} \). In (10) and (11),

\[ \sum_{v \in H_{k}^{(0)}} \zeta_{l}^{-uv} = l^{m-k} \sum_{v_{0} \in H_{k}^{(0)}} \zeta_{l}^{-u_{0}v_{0}} = l^{g-1} \eta_{0}^{(2,l)} = l^{m-k} \frac{1 + \sqrt{-l}}{2}, \]

and

\[ \sum_{v \in H_{k}^{(1)}} \zeta_{l}^{-uv} = l^{m-k} \sum_{v_{0} \in H_{k}^{(1)}} \zeta_{l}^{-u_{0}v_{0}} = l^{g-1} \eta_{1}^{(2,l)} = l^{m-k} \frac{1 - \sqrt{-l}}{2}. \]

Thus

\[ B' = l^{m-k} p_{\frac{t-\sqrt{-l}}{2}} \left( \frac{-1 + \sqrt{-l}}{2} \left( \frac{a+b\sqrt{-l}}{2} \right)^{t-1} + \frac{-1 - \sqrt{-l}}{2} \left( \frac{a-b\sqrt{-l}}{2} \right)^{t-1} \right). \]
By Lemmas 3.2, 3.3, and 3.4, Theorem 3.6 is proved.

Theorems 3.1, 3.5 and 3.6 gave all the values of Gaussian periods of order $N$ over $\mathbb{F}_q$, where $l \equiv 3 \pmod{4}$, $l \neq 3$, is a prime and $N = l^m$.

**Corollary 1.** The assumptions are as above. If $m = 1$, then

$$
\eta_0 = \frac{1}{l}(-1 + p^{l-h} l - 1 \cdot a),
$$

and

$$
\eta_i = \frac{1}{l}(-1 + p^{l-h} - a + bl),
$$

where $i \in H_1^{(0)}$, $i' \in H_1^{(1)}$, and $a, b$ are integers given by (3).

4. Explicit values of Gaussian periods of order $2N$

Let $N = l^m$, where $l$ be a prime with $l \equiv 3 \pmod{4}$ and $l \neq 3$. Let $f = \phi(N)/2$ be the multiplicative order of a prime $p$ modulo $N$, i.e., $f$ the smallest positive integer such that $p^f \equiv 1 \pmod{N}$. Let $q = p^f$ and $\gcd(p, 2N) = 1$. In the following, we shall use (4) and Lemma 2.6 to compute the values of $\eta_i^{(2N, q)}$, $i = 0, 1, \ldots, 2N - 1$.

4.1. $l \equiv 7 \pmod{8}$. In this subsection, we always assume that $l \equiv 7 \pmod{8}$.

**Theorem 4.1.** The notation is as above. Suppose that $l \equiv 7 \pmod{8}$. The values of $\eta_0^{(2N, q)}$ and $\eta_N^{(2N, q)}$ are equal to as follows:

$$
\eta_0^{(2N, q)} = \frac{1}{2} \eta_0^{(N, q)} + \frac{1}{2} (\sqrt{p^{f}})^f, \eta_N^{(2N, q)} = \frac{1}{2} \eta_0^{(N, q)} - \frac{1}{2} (\sqrt{p^{f}})^f,
$$

where $\eta_0^{(N, q)}$ is defined as Theorem 3.1.

**Proof.** By (4), we have

$$
\eta_0^{(2N, q)} = \frac{1}{2N} \sum_{j=0}^{2N-1} \chi^j = \frac{1}{2N} \left( \sum_{j \text{ even}} \chi^j + \sum_{j \text{ odd}} \chi^j \right),
$$

where $\chi$ is the multiplicative character of order $2N$ over $\mathbb{F}_q$. Note that

$$
\sum_{j \text{ even}} \chi^j = N \eta_0^{(N, q)}.
$$

By Lemma 2.6,

$$
\sum_{j \text{ odd}} \chi^j = N (\sqrt{p^{f}})^f.
$$

By (4), we have

$$
\eta_N^{(2N, q)} = \frac{1}{2N} \sum_{j=0}^{2N-1} \zeta_{2N}^{-j} \chi^j = \frac{1}{2N} \left( \sum_{j \text{ even}} \chi^j - \sum_{j \text{ odd}} \chi^j \right),
$$

This completes the proof.

**Theorem 4.2.** If $i = l^{m-k} u$, where $1 \leq u \leq 2l^k - 1$, $\gcd(l, u) = 1$, and $k = 1, 2, \ldots, m$. Then

$$
\eta_i^{(2N, q)} = \frac{1}{2} \eta_i^{(N, q)}.
$$
Proof. By (4),
\[
\eta_i^{(2N,q)} = \frac{1}{2N} \sum_{j=0}^{2N-1} \zeta_{2N}^{-ij} G(\chi^j) = \frac{1}{2N} \left( \sum_{j \text{ even}} \zeta_{2N}^{-ij} G(\chi^j) + \sum_{j \text{ odd}} \zeta_{2N}^{-ij} G(\chi^j) \right) \\
= \frac{1}{2} \eta_i^{(N,q)} + \frac{1}{2N} (\sqrt{p^*})^f \sum_{j \text{ odd}} \zeta_{2N}^{-ij}.
\]

There is a canonical epimorphism: \( Z/(2l^m Z) \cong Z/(2\mathbb{Z}) \times Z/(l^m Z) \to Z/(2l^k Z) \cong Z/(2\mathbb{Z}) \times Z/(l^k Z) \), \( \zeta_{2N}^{l-m} = \zeta_{2k} \), and \( x^{2l^k} - 1 = (x^l - 1)(x^{l^k} + 1) \). Suppose that \( u \) is odd. Then for \( 0 \leq j \leq 2N-1 \) and \( j \) odd, \( \zeta_{2N}^{-ij} \) runs over all roots of \( x^{l^k} + 1 \) with multiplicity \( l^{m-k} \). Suppose that \( u \) is even. Then it runs over all roots of \( x^l - 1 \) with multiplicity \( l^{m-k} \). Hence
\[
\sum_{j \text{ odd}} \zeta_{2N}^{-ij} = 0, \quad \eta_i^{(2N,q)} = \frac{1}{2} \eta_i^{(N,q)}.
\]

4.2. \( l \equiv 3 \pmod{8} \). In this subsection, we always assume that \( l \equiv 3 \pmod{8} \).

**Theorem 4.3.** The notation is as above. Suppose that \( l \equiv 3 \pmod{8} \). The values of \( \eta_0^{(2N,q)} \) and \( \eta_N^{(2N,q)} \) are given as follows:
\[
\eta_0^{(2N,q)} = \frac{1}{2} \eta_0^{(N,q)} + \frac{(-1)^{\frac{l-1}{4}}}{2Np^{f/2}} (p^f + \sum_{g=1}^{m} \frac{\phi(1^g)}{2} p^{f-h_t m-s} ((\frac{a+b\sqrt{-l}}{2})^{2l^m-s})) \\
\quad \quad \quad + (\frac{a-b\sqrt{-l}}{2})^{2l^m-s}),
\]
\[
\eta_N^{(2N,q)} = \frac{1}{2} \eta_0^{(N,q)} - \frac{(-1)^{(p-1)/4}}{2Np^{f/2}} (p^f + \sum_{g=1}^{m} \frac{\phi(1^g)}{2} p^{f-h_t m-s} ((\frac{a+b\sqrt{-l}}{2})^{2l^m-s})) \\
\quad \quad \quad + (\frac{a-b\sqrt{-l}}{2})^{2l^m-s}),
\]

where \( \eta_0^{(N,q)} \) is defined as Theorem 3.1.

**Proof.** By (4), we have
\[
\eta_0^{(2N,q)} = \frac{1}{2N} \sum_{j=0}^{2N-1} G(\chi^j) = \frac{1}{2N} \left( \sum_{j \text{ even}} G(\chi^j) + \sum_{j \text{ odd}} G(\chi^j) \right),
\]
where \( \chi \) is the multiplicative character of order \( 2N \over \mathbb{F}_q \). Note that
\[
\sum_{j \text{ even}} G(\chi^j) = N \eta_0^{(N,q)}.
\]
By Lemma 2.6 and \( G(\chi^j) = \frac{(-1)^{(p-1)/4} (G(\chi^{2j}))^2}{p^{f/2}} \) for \( j \) odd and \( j \neq N \),
\[
\sum_{j \text{ odd}} G(\chi^j) = \frac{(-1)^{(p-1)/4}}{p^{f/2}} \sum_{j=1}^{N-1} (G(\chi^{2j}))^2 + (-1)^{\frac{p-1}{2}} p^f.
\]
By the proof of Theorem 3.1,
\[
\sum_{j=1}^{N-1} (G(\chi^{2j}))^2 = \sum_{g=1}^{m} \frac{\phi(1^g)}{2} p^{f-h_t m-s} ((\frac{a+b\sqrt{-l}}{2})^{2l^m-s}) + (\frac{a-b\sqrt{-l}}{2})^{2l^m-s}.
\]
Hence
\[ \eta_0^{(2N,q)} = \frac{1}{2} \eta_0^{(N,q)} \]
\[ + \frac{(-1)^{p-1}}{2Np^f/2} (p^f + \sum_{g=1}^{m} \phi(l^g) p^{f-hm^m-g} \left( \left(\frac{a+b\sqrt{-l}}{2}\right)^{2l^m-g} + \left(\frac{a-b\sqrt{-l}}{2}\right)^{2l^m-g} \right)). \]

By (4), we have
\[ \eta_N^{(2N,q)} = \frac{1}{2N} \sum_{j=0}^{2N-1} \zeta_{2N}^{-j} G(\chi^j) = \frac{1}{2N} \left( \sum_{j \text{ even}} G(\chi^j) - \sum_{j \text{ odd}} G(\chi^j) \right). \]

This completes the proof. \(\square\)

**Theorem 4.4.** If \(i = 2ul^m-k\) is even, where \(1 \leq u \leq l^k-1 \), \(\gcd(l,u) = 1\), and \(k = 1,2,\ldots,m\). Then
\[ \eta_i^{(2N,q)} = \frac{1}{2} \eta_i^{(N,q)} + \frac{(-1)^{(p-1)/4}}{2Np^f/2} (p^f + A_2 + B_2), \]

where
\[ A_2 = \sum_{g=1}^{m-k} \phi(l^g) p^{f-hl^m-g} \left( \left(\frac{a+b\sqrt{-l}}{2}\right)^{2l^m-g} + \left(\frac{a-b\sqrt{-l}}{2}\right)^{2l^m-g} \right), \]
and
\[ B_2 = l^{m-k} p^{f-hl^{i'-1}} \left( \left(\frac{1}{2}-\frac{\sqrt{-l}}{2}\right)^{2l^{i'-1}} + \frac{1}{2} \left(\frac{a-b\sqrt{-l}}{2}\right)^{2l^{i'-1}} \right). \]

**Proof.** By (4),
\[ \eta_i^{(2N,q)} = \frac{1}{2N} \sum_{j=0}^{2N-1} \zeta_{2N}^{-ij} G(\chi^j) = \frac{1}{2N} \left( \sum_{j \text{ even}} \zeta_{2N}^{-ij} G(\chi^j) + \sum_{j \text{ odd}} \zeta_{2N}^{-ij} G(\chi^j) \right) \]
\[ = \frac{1}{2} \eta_i^{(N,q)} + \frac{(-1)^{(p-1)/4}}{2Np^f/2} (p^f + \sum_{j \text{ odd}, j \neq N} \zeta_{2N}^{-ij} G(\chi^{2j})) \]
\[ = \frac{1}{2} \eta_i^{(N,q)} + \frac{(-1)^{(p-1)/4}}{2Np^f/2} (p^f + \sum_{j=1}^{N-1} \zeta_{2N}^{-ij} G(\chi^{2j}))^2, \]
where \(i' = i/2 = ul^m-k\). By the proofs of Lemmas 3.2, 3.3, and 3.4,
\[ \sum_{j=1}^{N-1} \zeta_{2N}^{-ij} (G(\chi^{2j}))^2 = A_2 + B_2, \]
where
\[ A_2 = \sum_{g=1}^{m-k} \sum_{v \in \mathbb{Z}/(p^f)^*} G(\chi^{2l^m-v})^2 \]
\[ = \sum_{g=1}^{m-k} \phi(l^g) p^{f-hl^m-g} \left( \left(\frac{a+b\sqrt{-l}}{2}\right)^{2l^m-g} + \left(\frac{a-b\sqrt{-l}}{2}\right)^{2l^m-g} \right), \]
and
\[ B_2 = \sum_{v \in \mathbb{Z}/(l^m-k+1)^*} \zeta_{2N}^{-iv} G(\chi^{k-1+v})^2. \]
\[ \eta_i^{(2N,q)} = \frac{1}{2} \eta_i^{(N,q)} + \frac{(-1)^{(p-1)/4}}{2np^{1/2}} (p^f - A_2 - B_2), \]

where \( A_2 \) and \( B_2 \) are defined as Theorem 4.4.

Proof. By (4),
\[ \eta_i^{(2N,q)} = \frac{1}{2} \eta_i^{(N,q)} + \frac{(-1)^{(p-1)/4}}{2np^{1/2}} (p^f + \sum_{j \text{ odd}, p \not| N} \zeta_{2N}^{-ij}(G(2^j))^2). \]

Let \( T = \{ i : 0 \leq i \leq 2lm - 1 \} = S \cup (N + S) \), where \( N + S = \{ N + s : s \in S \} \). For convenience, denote
\[ (14) \quad T = T_0 \cup T_1 \cup \cdots \cup T_m, \]
where \( T_0 = \{ 0, N \} \) and \( T_k = \{ a \in T : l^{m-k} \parallel a \} = S_k \cup (N + S_k), k = 1, \ldots, m \). Suppose that \( j = l^{m-q} \in T \) and \( j \) is odd. Then
\[ j \in \{ N \} \bigcup_{g=1}^{m} l^{m-q}U_g', \]
where each \( U_g' = \{ 1 \leq i \leq 2^g - 1, \gcd(i, 2l) = 1 \} \). In fact, \( (\mathbb{Z}/2^g\mathbb{Z})^* = \{ u \mod 2^g : u \in U_g' \} \). For convenience, denote \( U_g' = (\mathbb{Z}/2^g\mathbb{Z})^*, g = 1, \ldots, m \).

By the proofs of Lemmas 3.2, 3.3, and 3.4,
\[ \sum_{j \text{ odd}, j \not \equiv N} \zeta_{2N}^{-ij}(G(2^j))^2 = \sum_{g=1}^{m} \sum_{v \in U_g'} (\zeta_{2N}^{-2^{m-k}g})^{uv} G(\chi^{l^{m-q}v})^2. \]

It is easy to know that
\[ (\zeta_{2N}^{-2^{m-(k+g)})})^{uv} = \begin{cases} -1, & \text{if } k + g - m \leq 0, \\ \zeta_{2^t}^{-uv}, & \text{if } k + g - m = 1, \\ \zeta_{2^t}^{uv}, & \text{if } k + g - m = t \geq 2. \end{cases} \]

Then
\[ (15) \quad \sum_{j \text{ odd}, j \not \equiv N} \zeta_{2N}^{-ij}(G(2^j)) = -A_2 + B_2' + C_2. \]

In (16), \( A_2 \) is defined as Theorem 4.4,
\[ B_2' = \sum_{v \in U_g'} \zeta_{l}^{-uv} G(\chi^{l^{k-1}v})^2 = -\sum_{v \in U_g'} \zeta_{l}^{-uv} G(\chi^{l^{k-1}v})^2 = -B_2, \]
and \( C_2 = 0 \) by the proof of Lemma 3.4. This completes the proof. \( \square \)
5. Applications

In this section, we always assume that \( l \) and \( p \) are primes with \( l \equiv 3 \pmod{4} \) and \( l \neq 3 \). Let \( N = l^m \) and \( f = \phi(N)/2 \) the multiplicative order of a prime \( p \) modulo \( N \). We define \( D = \{ x \in \mathbb{F}_q^* : \text{Tr}_{q/p}(x^{\frac{q-1}{2}}) = 0 \} = \{ x_1, \ldots, x_n \} \) as a defining set and a \( p \)-ary linear code as follows:

\[
C_D = \{ C = (\text{Tr}_{q/p}(cx_1), \text{Tr}_{q/p}(cx_2), \ldots, \text{Tr}_{q/p}(cx_n)) : c \in \mathbb{F}_q \}.
\]

If the set \( D \) is well chosen, the code \( C_D \) may have good parameters. This construction is generic in the sense that many known codes could be produced by selecting the defining set (see \([9, 10, 22, 23, 28, 29]\) for example). In general, we choose that \( l^m < q - 1 \). If \( q - 1 = l^m \), let \( V = \{ v \in \mathbb{F}_q : \text{Tr}_{q/p}(vx) = 0 \text{ for all } x \in D \} \) be a subspace of \( \mathbb{F}_q \) over \( \mathbb{F}_p \). Define the linear code as follows:

\[
C_D = \{ C = (\text{Tr}_{q/p}(cx_1), \text{Tr}_{q/p}(cx_2), \ldots, \text{Tr}_{q/p}(cx_n)) : c \in \mathbb{F}_q/V \}.
\]

In coding theory, it is often desirable to know the weight distributions of the codes because they can be used to estimate the error correcting capability and the error probability of error detection and correction with respect to some algorithms. The codes with few nonzero weights are of special interest in association schemes, secret sharing schemes, and frequency hopping sequences.

In the following, we will use Gaussian periods of index 2 case to investigate the weight distribution of the linear code \( C_D \) defined as (17). We always denote by \( \alpha \) a primitive element in \( \mathbb{F}_q^* \) and \( \beta = \alpha^{\frac{q-1}{2}} \) an \( m \)-th primitive root of unity in \( \mathbb{F}_q \), where \( q = p^l \) and \( f = \frac{\phi(l^m)}{2} \). Without loss of generality, we assume that \( p \nmid f \).

Now we shall compute the length and the weight distribution of the linear code \( C_D \).

**Theorem 5.1.** Let \( C_D \) be the code defined in (17).

Suppose \( -l \nmid 1 \pmod{p} \). Then the length \( n \) of \( C_D \) is \( q - 1 - \frac{q-1}{l} \).

Suppose \( -l \equiv 1 \pmod{p} \). Then the length \( n \) is \( q - 1 - \frac{(l+1)(q-1)}{2l} \).

**Proof.** Let \( K = \langle \alpha^{\frac{q-1}{2m}} \rangle \) be a cyclic subgroup of \( \mathbb{F}_q^* \), i.e. \( K \subset \mathbb{F}_q^* \). Define a group homomorphism:

\[
\sigma : \mathbb{F}_q^* \rightarrow K, x \mapsto x^{\frac{q-1}{2m}}.
\]

Then

\[
\frac{\mathbb{F}_q^*}{\ker(\sigma)} \cong K, |\ker(\sigma)| = \frac{q-1}{l^m},
\]

Hence

\[
n = q - 1 - \frac{q-1}{l^m} \Omega,
\]

where \( \Omega = |\{ i : 0 \leq i \leq l^m - 1, \text{Tr}(\beta^i) = 0 \}| \).

Suppose that \( i = l^m-k_u \in S_k, \gcd(u,l) = 1 \), where \( k = 0, 1, \ldots, m \).

If \( k = 0 \), i.e. \( i = 0 \), then \( \text{Tr}_{q/p}(\beta^i) = \text{Tr}_{q/p}(\beta^0) = 0 \neq 0 \) by \( p \nmid f \).

If \( k = 1 \), \( i = l^m-1 \in S_1 \). Then \( \text{ord}(\beta^i) = 1 \) by \( \text{ord}(\beta) = l^m \), so \( \beta^i \in \mathbb{F}_p \) and \( \Phi(\beta^i) = 0 \). Let \( H_{1}^{(0)} \) and \( H_{1}^{(1)} \) be the sets consisting of all square elements and non-square elements in \( (\mathbb{Z}/l\mathbb{Z})^* = \mathbb{F}_q^* \), respectively, i.e. \( \mathbb{F}_q^* = H_{1}^{(0)} \cup H_{1}^{(1)} \). Then there is an irreducible factorization over \( \mathbb{F}_p \):

\[
\Phi(x) = \Phi^{(0)}(x)\Phi^{(1)}(x), \Phi^{(0)}(x) = \prod_{i \in H_{1}^{(0)}} (x - \xi_i), \Phi^{(1)}(x) = \prod_{i \in H_{1}^{(1)}} (x - \xi_i),
\]

where \( \xi_i \) are \( l^m \)-th roots of unity in \( \mathbb{F}_p \).
where $\xi_l = \alpha^{(q-1)/l}$ is an $l$-th primitive root of unity in $\mathbb{F}_q$.

Let $\mathcal{O} = \mathbb{Z}[\sqrt{-l}]$ be the algebraic integer ring of $\mathbb{Q}(\sqrt{-l})$. Then there is a prime ideal factorization of the prime $p$ in $\mathcal{O}$:

$$p\mathcal{O} = \mathcal{P}_1\mathcal{P}_2,$$

where $\mathcal{P}_1$ is a prime ideal $\mathcal{P}_1 = (\frac{a+b\sqrt{-l}}{2}p)$ of $\mathbb{Q}(\sqrt{-l})$ over $p$ and $\mathcal{P}_2$ is a prime ideal $\mathcal{P}_2 = (\frac{a-b\sqrt{-l}}{2}p)$ of $\mathbb{Q}(\sqrt{-l})$ over $p$.

By [12], take $\mathcal{P}_1$. Let

$$\zeta_i \equiv \xi_l \pmod{\mathcal{P}_1} \text{ and } \mathcal{O}/\mathcal{P}_1 = \mathbb{F}_p^{1 \frac{q-1}{l}} = \mathbb{F}_p(\xi_l),$$

where $\frac{q-1}{l}$ is the order of $p$ modulo $l$.

Suppose that $-l \neq 1 \pmod{p}$. Then

$$\sum_{i \in H_1^{(0)}} \zeta_i = \sum_{i \in H_1^{(0)}} \xi_i \equiv \frac{-1 + \sqrt{-l}}{2} \neq 0 \pmod{\mathcal{P}_1},$$

and

$$\sum_{i \in H_1^{(1)}} \zeta_i = \sum_{i \in H_1^{(1)}} \xi_i \equiv \frac{-1 - \sqrt{-l}}{2} \neq 0 \pmod{\mathcal{P}_1}.$$

Hence $\text{Tr}_{p^{(l-1)/2}/p}(\beta^i) \neq 0, i \in S_1$.

Suppose that $-l \equiv 1 \pmod{p}$. Without loss of generality, let $\sqrt{-l} \equiv 1 \pmod{\mathcal{P}_1}$ and

$$\sum_{i \in H_1^{(0)}} \zeta_i = \sum_{i \in H_1^{(0)}} \xi_i \equiv 0 \pmod{\mathcal{P}_1}, \sum_{i \in H_1^{(1)}} \zeta_i \equiv \sum_{i \in H_1^{(1)}} \xi_i \neq 0 \pmod{\mathcal{P}_1}.$$

Hence

$$\text{Tr}_{p^{(l-1)/2}/p}(\beta^i) \begin{cases} \neq 0, & \text{if } i \in S_0 \cup S_1, \\ = 0, & \text{if } i \in \cup_{k=2}^m S_k. \end{cases}$$

If $2 \leq k \leq m, i = l^{m-k}u \in S_k$. Then ord($\beta^i$) = $l^k$, so $\beta^i$ is a root of irreducible polynomial $\Phi_{l^k}(x) = \Phi_{l^{k-1}}(x^2)$. Hence $\text{Tr}_{q/p}(\beta^i) = 0$ by (12).

Suppose that $-l \neq 1 \pmod{p}$. Then

$$\text{Tr}_{q/p}(\beta^i) \begin{cases} \neq 0, & \text{if } i \in S_0 \cup S_1, \\ = 0, & \text{if } i \in \cup_{k=2}^m S_k. \end{cases}$$

Suppose that $-l \equiv 1 \pmod{p}$. Then

$$\text{Tr}_{q/p}(\beta^i) \begin{cases} \neq 0, & \text{if } i \in S_0 \text{ and } i/l^{m-1} \in H_1^{(1)}, \\ = 0, & \text{if } i \in \cup_{k=2}^m S_k \text{ and } i/l^{m-1} \in H_1^{(0)}. \end{cases}$$

Hence $n = \frac{q-1}{l^m} \cdot (\sum_{k=2}^m \phi(l^k)) = q - 1 - \frac{q-1}{\frac{q-1}{l}}$.

Suppose that $-l \neq 1 \pmod{p}$. We will compute $W_H(C)$, which is the Hamming weights of the codeword $C$ of $C_D$ with respect to $c \in \mathbb{F}_q^*$. If $c = 0$, then the Hamming weight of $C$ is 0. If $c \neq 0$, then $W_H(C) = n - Z(c)$ and

$$Z(c) = |\{x \in \mathbb{F}_q^* : \text{Tr}_{q/p}(cx) = 0, \text{Tr}_{q/p}(x^q) = 0\}|$$
where $\psi$ is the canonical additive character of $F_q$.

Let $i = sl^m + j$, where $0 \leq s \leq \frac{q-1}{lm} - 1$ and $0 \leq j \leq lm - 1$. Then

$$Z(c) = \frac{1}{p^2} \sum_{y \in F_p} \sum_{y \in F_p} \sum_{z \in F_p} \psi(ycx) \sum_{z \in F_p} \psi(zx^{q-1})$$

$$= \frac{1}{p^2} \sum_{i=0}^{q-2} \sum_{y \in F_p} \psi(yc^i) \sum_{z \in F_p} \psi(zx^{q-1+i}),$$

where $\text{gcd}(u, l) = 1$, $k = 0, 1, \ldots, m$. Using argument to the above, $\text{Tr}_{q/p}^{\beta_j} \neq 0$ if $k = 0, 1$ and $\text{Tr}_{q/p}^{\beta_j} = 0$ if $2 \leq k \leq m$. Hence

$$\sum_{z \in F_p} \psi(z^{\beta_j}) = \sum_{z \in F_p} \zeta_p^{\text{Tr}_{q/p}^{\beta_j}} = \begin{cases} 0, & \text{if } j \in S_0 \cup S_1, \\ p, & \text{if } j \in \bigcup_{k=2}^m S_k. \end{cases}$$

Note that $S_0 = \{0\}$. Therefore

$$Z(c) = \frac{1}{p^2} \sum_{y \in F_p} \sum_{s=0}^{\frac{q-1}{lm} - 1} \sum_{k=2}^m \sum_{u \in U_k} \psi(yca^{stm + lm - k}u) \cdot p$$

$$= \frac{1}{p} \sum_{y \in F_p} \sum_{s=0}^{\frac{q-1}{lm} - 1} \sum_{j=0}^{lm - 1} \psi(yca^{stm + j}) - \frac{1}{p} \sum_{y \in F_p} \sum_{s=0}^{\frac{q-1}{lm} - 1} \psi(yca^{stm})$$

$$= \frac{1}{p} \sum_{y \in F_p} \sum_{s=0}^{\frac{q-1}{lm} - 1} \psi(yca^{stm} + \text{Tr}_{q/p}^{\beta_j}).$$

Let $S = \{i : 0 \leq i \leq lm - 1\}$, $W = \{i \in S : lm - 1| i\}$, $W_1 = \{i \in S : lm| i\}$, and $W_2 = \{i \in S : lm - 1 || i\}$. Then we have the partition: $W = W_1 \cup W_2$. Hence

$$\sum_{y \in F_p} \sum_{s=0}^{\frac{q-1}{lm} - 1} \psi(yca^{stm}) = \sum_{y \in F_p} \sum_{s=0}^{\frac{q-1}{lm} - 1} \psi(yca^{stm} + \text{Tr}_{q/p}^{\beta_j}).$$

Therefore

$$Z(c) = \frac{1}{p} \sum_{y \in F_p} \sum_{i=0}^{q-2} \psi(yca^i) - \frac{1}{p} \sum_{y \in F_p} \sum_{s=0}^{\frac{q-1}{lm} - 1} \psi(yca^{lm - 1} s)$$

$$= \frac{q - 1}{p} + \frac{1}{p} \sum_{i=0}^{q-2} \psi(ca^i) - \frac{1}{p} \sum_{s=0}^{\frac{q-1}{lm} - 1} \psi(ca^{lm - 1} s).$$
Let $c = \alpha^j, j = 0, 1, \ldots, q - 2$, then $j = l^{m-1}b + i$, where $0 \leq b \leq \frac{q-1}{m-1} - 1$ and $0 \leq i \leq l^{m-1} - 1$. Hence

$$\sum_{s=0}^{\frac{q-1}{m-1}-1} \psi(c\alpha^{l^{m-1}b+i}) = \eta_i^{(l^{m-1},q)}.$$  

Therefore

$$Z(c) = \frac{(q-p)l^{m-1} - (q-1)}{pl^{m-1}} - \frac{p-1}{p} \eta_i^{(l^{m-1},q)}, 0 \leq i \leq l^{m-1} - 1,$$

where $\eta_i^{(l^{m-1},q)}$ is the Gauss period of index 2 of order $l^{m-1}$ over $\mathbb{F}_q$.

Let $S = \{s, 0 \leq s \leq l^{m-1} - 1\}$ and $S_k = \{t = l^{m-1-k}u \in S, \gcd(u, l) = 1\}$, where $k = 0, 1, \ldots, m - 1$ and $U_k = H_k(0) \cup H_k(1), k = 0, 1, \ldots, m - 1$. Recall that $W_H(C) = n - Z(c)$, its weight distribution is given by Table 1.

**Theorem 5.2.** Let $p$ and $l$ be primes with $l \equiv 3 \pmod{4}, l \neq 3$, and $-l \equiv 1 \pmod{p}$. Let $N = l^m(m \geq 2), f = \phi(N)/2$ the multiplicative order of $p$ modulo $N$, and $q = p^f$. Then $C_D$ defined as (17) is a $[q - 1 - \frac{q-1}{l^{m-1}}, \frac{(l-1)(l-2)}{2}]$ and $2m - 1$ weight linear code over $\mathbb{F}_q$. Its weight distribution is given by Table 1.

| Table 1. Weight distribution of the code in Theorem 5.2. |
|---------------------------------|----------------|
| Weight | Frequency |
| \frac{m-1}{p} \left(q - \frac{q-1}{l^{m-1}} + \eta_0^{(l^{m-1},q)}\right) | \frac{q-1}{l^{m-1}} - \frac{\phi(k)}{2} |
| \frac{m-1}{p} \left(q - \frac{q-1}{l^{m-1}} + \eta_i^{(l^{m-1},q)}\right), i = l^{m-1-k}u, u \in H_k(0) | \frac{q-1}{l^{m-1}} - \frac{\phi(k)}{2} |
| \frac{m-1}{p} \left(q - \frac{q-1}{l^{m-1}} + \eta_{i'}^{(l^{m-1},q)}\right), i' = l^{m-1-k}u, u \in H_k(1) | \frac{q-1}{l^{m-1}} - \frac{\phi(k)}{2} |

Where $\eta_0^{(l^{m-1},q)}$ is given by Theorem 3.1 and $m$ is replaced by $m - 1$.

When $i = l^{m-1-k}u, u \in H_k(0)$ for $k = 1, 2, \ldots, m - 1, \eta_i^{(l^{m-1},q)}$ is given by Theorem 3.5 and $m$ is replaced by $m - 1$.

When $i' = l^{m-1-k}u, u \in H_k(1)$ for $k = 1, 2, \ldots, m - 1, \eta_{i'}^{(l^{m-1},q)}$ is given by Theorem 3.6 and $m$ is replaced by $m - 1$.

Suppose that $-l \equiv 1 \pmod{p}$. Then we have the following result.

**Theorem 5.3.** Let $p$ and $l$ be primes with $l \equiv 3 \pmod{4}, l \neq 3$, and $-l \equiv 1 \pmod{p}$. Let $N = l^m(m \geq 2), f = \phi(N)/2$ the multiplicative order of $p$ modulo $N$, and $q = p^f$. Then $C_D$ defined as (17) is a $[q - 1 - \frac{q-1}{l^{m-1}}, \frac{(l-1)(l-2)}{2l^{m-1}}]$ and $2m + 1$
weight linear code over $\mathbb{F}_q$. Its weight distribution is given by Table 2.

| Weight | Frequency |
|--------|-----------|
| $(p-1)(2^{m+1}(x+1)(g-1)) + \frac{p^2}{2} \eta_0^{(m,q)} + \frac{(l-1)(p-1)}{2p} \eta_1^{(l,m,q)}$ | $\frac{1}{q}$ |
| $(p-1)(2^{m+1}(x+1)(g-1)) + \frac{p^2}{2} \eta_0^{(m,q)} + \frac{(l-1)(p-1)}{2p} \eta_1^{(l,m,q)}$ | $\frac{1}{q}$ |
| $(p-1)(2^{m+1}(x+1)(g-1)) + \frac{p^2}{2} \eta_0^{(m,q)} + \frac{(l-1)(p-1)}{2p} \eta_1^{(l,m,q)}$ | $\frac{1}{q}$ |
| $(p-1)(2^{m+1}(x+1)(g-1)) + \frac{p^2}{2} \eta_0^{(m,q)} + \frac{(l-1)(p-1)}{2p} \eta_1^{(l,m,q)}$ | $\frac{1}{q}$ |

where $\eta_0^{(m,q)}$ is given by Theorem 3.1 and $\eta_1^{(l,m,q)}$, $\eta_1^{(l,m,q)}$ are given by Theorems 3.5 and 3.6.

**Proof.** If $c = 0$, then the Hamming weight of $C$ is 0. If $c \neq 0$, then $W_H(C) = n - Z(c)$ and

$$Z(c) = \frac{1}{p^2} \sum_{x \in \mathbb{F}_q^*} \sum_{y \in \mathbb{F}_p} \psi(y(x^{-1} + \alpha^m y)) \sum_{z \in \mathbb{F}_p} \psi(z(x^{-1} + \alpha^m y))$$

where $\psi$ is the canonical additive character of $\mathbb{F}_q$.

Let $i = sl^m + j$, where $0 \leq s \leq \frac{q^m-1}{2}$ and $0 \leq j \leq l^m - 1$. Then

$$Z(c) = \frac{1}{p^2} \sum_{y \in \mathbb{F}_p} \sum_{s=0}^{\frac{q^m-1}{2}} \sum_{j=0}^{l^m-1} \psi(y\alpha^{sl^m+j}) \sum_{z \in \mathbb{F}_p} \psi(z\alpha^j),$$

where $\sum_{z \in \mathbb{F}_p} \psi(z\beta^j) = \sum_{z \in \mathbb{F}_p} z^{Tr_{\mathbb{F}_p}((\beta^j))}$.

Suppose that $-l \equiv 1 \pmod{p}$. Then by (19)

$$\sum_{z \in \mathbb{F}_p} \psi(z\beta^j) = \begin{cases} 0, & \text{if } j \in S_0 \text{ and } j/l^m-1 \in H_1^{(1)}, \\ p, & \text{if } j \in \cup_{k=2}^m S_k \text{ and } j/l^m-1 \in H_1^{(0)}. \end{cases}$$

Hence for $c \neq 0$,

$$Z(c) = \frac{1}{p^2} \sum_{y \in \mathbb{F}_p} \sum_{s=0}^{\frac{q^m-1}{2}} \sum_{k=2}^{l^m} \psi(y\alpha^{sl^m+l^m-k}u) \cdot p$$

$$+ \frac{1}{p^2} \sum_{y \in \mathbb{F}_p} \sum_{s=0}^{\frac{q^m-1}{2}} \sum_{u \in H_1^{(0)}} \psi(y\alpha^{sl^m+l^m-1}u) \cdot p$$

$$= \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{s=0}^{\frac{q^m-1}{2}} \psi(y\alpha^s) \cdot \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{s=0}^{\frac{q^m-1}{2}} \psi(y\alpha^s)$$
\[- \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{s=0}^{q-1} \sum_{u \in H_1^{(1)}} \psi(y c \alpha^s + t^{m-1} u) \]
\[= \frac{q-1}{p} + \frac{p-1}{p} \sum_{s=0}^{q-2} \psi(c \alpha^s) - \frac{1}{p} \cdot \frac{q-1}{l^m} - \frac{p-1}{p} \sum_{s=0}^{q-1} \psi(c \alpha^{l^m s}) \]
\[- \frac{(l-1)(q-1)}{2pl^m} \sum_{s=0}^{q-1} \sum_{u \in H_1^{(1)}} \psi(c \alpha^{l^m s + t^{m-1} u}) \]
\[- \frac{q-p}{p} - \frac{(l+1)(q-1)}{2pl^m} - \frac{p-1}{p} \sum_{s=0}^{q-1} \psi(c \alpha^{l^m s}) \]
\[- \frac{p-1}{p} \sum_{s=0}^{q-1} \sum_{u \in H_1^{(1)}} \psi(c \alpha^{l^m s + t^{m-1} u}). \]

Suppose that \(c \in \mathbb{F}_q^*\). Then \(c = \alpha^j (\alpha^m)^i, j = 0, \ldots, l^m - 1\).
If \(j \in S_0 = \{0\}\), then
\[Z(c) = \frac{q-p}{p} - \frac{(l+1)(q-1)}{2pl^m} - \frac{p-1}{p} \eta_0^{(l^m, q)} - \frac{(l-1)(p-1)}{2p} \eta_i^{(l^m, q)}, \]
where \(i' / l^{m-1} \in H_1^{(1)}\).
If \(j \in \bigcup_{k=2}^n S_k\), then by (6)
\[\frac{q-1}{l^m} \sum_{s=0}^{q-1} \sum_{u \in H_1^{(1)}} \psi(c \alpha^{l^m s + t^{m-1} u}) = \frac{l-1}{2} \eta_j^{(l^m, q)}, \]
Hence
\[Z(c) = \frac{q-p}{p} - \frac{(l+1)(q-1)}{2pl^m} - \frac{(p-1)(l+1)}{2p} \eta_j^{(l^m, q)}, \]
where \(\eta_j^{(l^m, q)}\) is defined as Theorems 3.5 and 3.6.

If \(j \in S_1\) and \(j = l^{m-1} v, v \in H_1^{(0)}\). Then there are \((1,0)_2 = \frac{l-3}{4}\) elements \(u \in H_1^{(1)}\) such that \(v + u \in H_1^{(0)}\); there are \((1,1)_2 = \frac{l-3}{4}\) elements \(u \in H_1^{(1)}\) such that \(v + u \in H_1^{(1)}\), and there is a unique \(u \in H_1^{(1)}\) such that \(v + u = 0\). Hence
\[Z(c) = \frac{q-p}{p} - \frac{(l+1)(q-1)}{2pl^m} - \frac{p-1}{p} \eta_0^{(l^m, q)} - \frac{(l-1)(p-1)}{4p} \eta_i^{(l^m, q)} - \frac{(l-3)(p-1)}{4p} \eta_i^{(l^m, q)}, \]
where \(i' / l^{m-1} \in H_1^{(0)}\) and \(i' / l^{m-1} \in H_1^{(1)}\).

If \(j \in S_1\) and \(j = l^{m-1} v, v \in H_1^{(1)}\). Then there are \((0,1)_2 = \frac{l+1}{4}\) elements \(u \in H_1^{(1)}\) such that \(v + u \in H_1^{(0)}\); there are \((1,0)_2 = \frac{l-3}{4}\) elements \(u \in H_1^{(0)}\) such that \(v + u \in H_1^{(1)}\). Hence
\[Z(c) = \frac{q-p}{p} - \frac{(l+1)(q-1)}{2pl^m} - \frac{(l+1)(p-1)}{4p} \eta_i^{(l^m, q)} - \frac{(l+1)(p-1)}{4p} \eta_i^{(l^m, q)} - \frac{(l+1)(p-1)}{4p} \eta_i^{(l^m, q)}, \]
where $i/l^m - 1 \in H^0_1$ and $i'/l^{m-1} \in H^1_1$.

Note that $W_H(C) = n - Z(c)$, we obtain the Table 2.

In the following, we list some examples.

**Example 1.** Let $p = 2$ and $l = 7$. The class number $h$ of $\mathbb{Q}(-7)$ is equal to 1 [3, P.514]. In Theorem 5.3, take $m = 1$, Magma figures out that $C_D$ defined as in (17) is a [3, 3] one-weight linear code over $\mathbb{F}_2$ with weight distribution $1 + 3z^2$. This experimental result coincides with the weight distribution in Table 2.

**Example 2.** Let $p = 3$ and $l = 11$. The class number $h$ of $\mathbb{Q}(-11)$ is equal to 1 [3, P.514]. In Theorem 5.3, take $m = 1$, Magma figures out that $C_D$ defined as in (17) is a [110, 5] two-weight linear code over $\mathbb{F}_3$ with weight distribution $1 + 22z^{90} + 220z^{72}$. This experimental result coincides with the weight distribution in Table 2.

**Example 3.** Let $p = 2$ and $l = 23$. The class number $h$ of $\mathbb{Q}(-23)$ is equal to 3 [3, P.514]. In Theorem 5.3, take $m = 1$, Magma figures out that $C_D$ defined as in (17) is a [979, 11] three-weight linear code over $\mathbb{F}_2$ with weight distribution $1 + 979z^{480} + 979z^{496} + 89z^{528}$. This experimental result coincides with the weight distribution in Table 2.

**Remark.** In fact, there are a lot of prime pairs $(p, l)$ suitable for Theorems 5.2 and 5.3.

Suppose that $p = 2, 3, 5$, or 7 and $l$ is prime with $l \equiv 3 \pmod{4}$ and $3 < l \leq 50$.

If $(p, l) \in \{(5, 11), (7, 31), (7, 47)\}$, then it is suitable for Theorem 5.2.

If $(p, l) \in \{(2, 7), (2, 23), (2, 47), (3, 23), (3, 47), (5, 19)\}$, then it is suitable for Theorem 5.3.

If $m = 1$, then $(p, l) = (3, 11)$ is suitable for Theorem 5.3.

6. Concluding Remarks

In this paper, we always assumed that $l$ is a prime with $l \equiv 3 \pmod{4}$ and $l \neq 3$, $N = l^m$ for a positive integer, $f = \phi(N)/2$ is the multiplicative order of a prime $p$ modulo $N$, and $q = p^I$, where $\phi(\cdot)$ is the Euler-function. Let $\alpha$ be a primitive element of the finite field $\mathbb{F}_q$ and $C_i^{(N, q)} = \alpha^i(\alpha^N)$ cosets, $i = 0, \ldots, N - 1$. We used Gaussian sums to obtain the explicit values of $\eta_i^{(N, q)} = \sum_{x \in C_i^{(N, q)}} \psi(x)$, $i = 0, 1, \ldots, N - 1$, where $N = l^m$ and $\psi$ is the canonical additive character of $\mathbb{F}_q$. Moreover, we also computed the explicit values of $\eta_i^{(2N, q)}$, $i = 0, 1, \ldots, 2N - 1$, if $p$ is an odd prime. Furthermore, assumed that the defining set $D$ of a linear code is $D = \{x \in \mathbb{F}_q^* : \mbox{Tr}_{q/p}(x^{2^{2N}}) = 0\}$, we obtained the weight distributions of the $p$-ary linear codes:

$$C_D = \{C = (\mbox{Tr}_{q/p}(cx_1), \mbox{Tr}_{q/p}(cx_2), \ldots, \mbox{Tr}_{q/p}(cx_n)) : c \in \mathbb{F}_q\},$$

where $\mbox{Tr}_{q/p}$ denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$.

Acknowledgments

The authors are very grateful to the reviewers and the Editor for their valuable suggestions that improved the quality of this paper.
REFERENCES

[1] L. Baumert and J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, DSN Prog. Rep., 16 (1973), 128–131.
[2] B. Berndt, R. Evans and K. Williams, Gauss and Jacobi Sums, New York, John Wiley & Sons Company, 1997.
[3] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.
[4] C. S. Ding and J. Yang, Hamming weights in irreducible cyclic codes, Discrete Math., 313 (2013), 434–446.
[5] C. S. Ding, Y. Liu, C. L. Ma and L. W. Zeng, The weight distributions of the duals of cyclic codes with two zeros, IEEE Trans. Inform. Theory, 57 (2011), 8000–8006.
[6] C. S. Ding, C. L. Li, N. Li and Z. C. Zhou, Three-weight cyclic codes and their weight distributions, Discrete Math., 339 (2016), 415–427.
[7] T. Feng and Q. Xiang, Strongly regular graphs from unions of cyclotomic classes, Journal of Combinatorial Theory Series B, 102 (2012), 982–995.
[8] Z. L. Heng and Q. Yue, A class of binary linear codes with at most three weights, IEEE Commun. Lett., 19 (2015), 1488–1491.
[9] Z. L. Heng and Q. Yue, Two classes of two-weight linear codes, Finite Fields Appl., 38 (2016), 72–92.
[10] Z. L. Heng and Q. Yue, Evaluation of the Hamming weights of a class of linear codes based on Gauss sums, Des. Codes Cryptogr., 83 (2017), 307–326.
[11] L. Q. Hu, Q. Yue and M. H. Wang, The linear complexity of Whitman’s generalize cyclotomic sequences of period $p^{m+1}q^{n+1}$, IEEE Trans. Inform. Theory, 58 (2012), 5534–5543.
[12] P. Langevin, Calcs de certaines sommes de Gauss, J. Number theory, 63 (1997), 59–64.
[13] C. J. Li and Q. Yue, The Walsh transform of a class of monomial functions and cyclic codes, Cryptogr. Commun., 7 (2015), 217–228.
[14] C. J. Li, Q. Yue and F. W. Li, Weight distributions of cyclic codes with respect to pairwise coprime order elements, Finite Fields Appl., 28 (2014), 94–114.
[15] F. W. Li, Q. Yue and F. M. Liu, The weight distribution of a class of cyclic codes containing a subclass with optimal parameters, Finite Fields Appl., 45 (2017), 183–202.
[16] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.
[17] Y. W. Liu and Z. H. Liu, On some classes of codes with a few weights, Adv. Math. Commun., 12 (2018), 415–428.
[18] J. Q. Luo and K. Q. Feng, On the weight distribution of two classes of cyclic codes, IEEE Trans. Inf. Theory, 54 (2008), 5332–5344.
[19] G. McGuire, On three weights in cyclic codes with two zeros, Finite Fields Appl., 10 (2004), 97–104.
[20] G. Myeerson, Period polynomials and Gauss sums for finite fields, Acta Arith., 39 (1981), 251–264.
[21] T. Storer, Cyclotomy and Difference Sets, Lectures in Advanced Mathematics, No. 2 Markham Publishing Co., Chicago, Ill. 1967.
[22] Q. Y. Wang, K. L. Ding, D. D. Lin and R. Xue, A kind of three-weight linear codes, Cryptogr. Commun., 9 (2017), 315–322.
[23] Q. Y. Wang, K. L. Ding and R. Xue, Binary linear codes with two weights, IEEE Commun. Lett., 19 (2015), 1097–1100.
[24] X. Q. Wang, D. B. Zheng, L. Hu and X. Y. Zeng, The weight distributions of two classes of binary cyclic codes, Finite Fields Appl., 34 (2015), 192–207.
[25] M. S. Xiong, The weight distributions of a class of cyclic codes, Finite Fields Appl., 18 (2012), 933–945.
[26] J. Yang and L. L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, Sci. China Math., 53 (2010), 2525–2542.
[27] J. Yang, M. S. Xiong, C. S. Ding and J. Q. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, IEEE Trans. Inform. Theory, 59 (2013), 5985–5993.
[28] S. D. Yang, X. L. Kong and C. M. Tang, A construction of linear codes and their complete weight enumerators, Finite Fields Appl., 48 (2017), 196–226.
[29] S. D. Yang and Z.-A. Yao, Complete weight enumerators of a class of linear codes, Discrete Math., 340 (2017), 729–739.
[30] Z. C. Zhou and C. S. Ding, *A class of three-weight cyclic codes*, *Finite Fields Appl.*, **25** (2014), 79–93.

[31] Z. C. Zhou, A. X. Zhang and C. S. Ding, *The weight enumerator of three families of cyclic codes*, *IEEE Trans. Inf. Theory*, **59** (2013), 6002–6009.

Received September 2018; 1st revision March 2019; final revision November 2019.

*E-mail address:* lfwzzu@126.com

*E-mail address:* yueqin@nuaa.edu.cn

*E-mail address:* sxmuzz@126.com