TRACE DESCRIPTION AND HAMMING WEIGHTS OF IRREDUCIBLE CONSTACYCLIC CODES

ANURADHA SHARMA
Department of Mathematics, IIIT-Delhi
New Delhi, 110020, India

SAROJ RANI
Department of Mathematics, IIT Delhi
New Delhi, 110016, India

(Communicated by Sergio R. López-Permouth)

Abstract. Irreducible constacyclic codes constitute an important family of error-correcting codes and have applications in space communications. In this paper, we provide a trace description of irreducible constacyclic codes of length $n$ over the finite field $\mathbb{F}_q$ of order $q$, where $n$ is a positive integer and $q$ is a prime power coprime to $n$. As an application, we determine Hamming weight distributions of some irreducible constacyclic codes of length $n$ over $\mathbb{F}_q$. We also derive a weight-divisibility theorem for irreducible constacyclic codes, and obtain both lower and upper bounds on the non-zero Hamming weights in irreducible constacyclic codes. Besides illustrating our results with examples, we list some optimal irreducible constacyclic codes that attain the distance bounds given in Grassl’s Table [8].

1. Introduction

Irreducible constacyclic codes form an algebraically rich family of error-correcting codes, and can be easily encoded and decoded using linear shift registers. They are building blocks for all the constacyclic codes, which are generalizations of cyclic and negacyclic codes. Their error-performance relative to various communication channels is measured by their Hamming weight distributions. This motivated many authors to study Hamming weight distributions of irreducible constacyclic codes. However, Ding [5] pointed out that the problem of determination of Hamming weight distributions is notoriously difficult for irreducible cyclic codes, which form a special class of irreducible constacyclic codes. In fact, many authors have worked on this problem using various techniques and obtained weight distributions of irreducible cyclic codes in certain special cases ([1]-[3], [5, 6, 11, 13, 14, 16], [18]-[22], [24]). On the other hand, extending the results derived in Sharma et al. [19, 20], Grover and Bhandari [9] determined weight distributions of some irreducible constacyclic codes of length $p^n$ ($n \geq 1$) over $\mathbb{F}_q$, where $p$ is a prime and $q$ is a prime power coprime to $p$. In another line of related work, Dong and Yin [7] provided a trace description of irreducible constacyclic codes over finite fields. As an application, they determined the weight distribution of a negacyclic code having a primitive polynomial as its...
check-polynomial. Therefore weight distributions of irreducible constacyclic codes are known only in a few cases.

In this paper, we provide a trace description for irreducible constacyclic codes over finite fields, which is different from the one given in [7]. With the help of this trace description, we further relate the problem of determination of weight distributions of irreducible constacyclic codes over finite fields with the evaluation of certain Gaussian periods. As a consequence, we determine weight distributions of irreducible constacyclic codes in certain special cases. We also derive a weight-divisibility theorem and obtain bounds on the Hamming weights of non-zero codewords in irreducible constacyclic codes.

This paper is organized as follows: In Section 2, we state some preliminaries. In Section 3, we provide a trace description of simple-root irreducible constacyclic codes over finite fields (Theorem 3.1). We also observe that in order to determine weight distributions of all the irreducible $\xi$-constacyclic codes over $\mathbb{F}_q$, it is enough to determine the same for the non-degenerate irreducible $\xi$-constacyclic code $\mathcal{M}^{(m,i)}_1$ of length $m$ over $\mathbb{F}_q$ for $0 \leq i \leq q-2$ (Theorem 3.2), where $\mathbb{F}_q$ is the finite field of order $q$, $\xi$ is a primitive element of $\mathbb{F}_q$ and $m$ is a positive integer with $\gcd(q, m) = 1$. Furthermore, we relate the problem of determination of weight distribution of the irreducible constacyclic code $\mathcal{M}^{(m,i)}_1$ with the evaluation of Gaussian periods (Theorem 3.3) and determine weight distributions in certain special cases (Theorems 3.7-3.16). In Section 4, we derive a weight-divisibility theorem for irreducible constacyclic codes (Theorems 4.1) and obtain bounds on the non-zero Hamming weights in these codes (Theorem 4.3). In Section 5, we apply our results to determine the weight distribution of the code $\mathcal{M}^{(m,i)}_1$ over $\mathbb{F}_q$ for some special values of $q$, $m$ and $i$ (Table 1). We also list some optimal irreducible constacyclic codes, which attain the distance bounds given in Grassl’s Table [8] (Table 2).

2. Some preliminaries

Let $\mathbb{F}_q$ denote the finite field with $q$ elements. For a non-zero element $\lambda \in \mathbb{F}_q$, a $\lambda$-constacyclic code $\mathcal{C}$ of length $n$ over $\mathbb{F}_q$ is defined as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ satisfying the following property: $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies that $(\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. Furthermore, under the standard vector space isomorphism from $\mathbb{F}_q^n$ onto $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$ defined as $(c_0, c_1, \ldots, c_{n-1}) \mapsto \sum_{j=0}^{n-1} c_j x^j + \langle x^n - \lambda \rangle$, one can identify each $\lambda$-constacyclic code $\mathcal{C}$ of length $n$ over $\mathbb{F}_q$ as an ideal of the quotient ring $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$. As $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$ is also a principal ideal ring, there exists a unique monic polynomial $g(x) \in \mathcal{C}$ that generates the code $\mathcal{C}$ and is a factor of $x^n - \lambda$ in $\mathbb{F}_q[x]$. The zeros of $g(x)$ are called zeros of $\mathcal{C}$, while the zeros of $\frac{x^n - \lambda}{g(x)}$ are called non-zeros of $\mathcal{C}$. For each non-zero $\lambda \in \mathbb{F}_q$, minimal ideals of the quotient ring $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$ are called irreducible $\lambda$-constacyclic codes of length $n$ over $\mathbb{F}_q$. Now we shall state some preliminaries that we need to determine weight distributions of simple-root irreducible constacyclic codes over finite fields.

Let $q = p^r$, where $p$ is a prime and $r$ is a positive integer. Let $N$ be a positive integer coprime to $q$ and let $k$ be the multiplicative order of $q$ modulo $N$. Let $r = q^k$ and let us write $r - 1 = q^k - 1 = NL$ for some integer $L \geq 1$. Then for $0 \leq j \leq L - 1$, the $j$th cyclotomic class of order $L$ in $\mathbb{F}_r$ is defined as $\mathcal{C}_j^{(L,r)} = \{ \theta^{L+i} : 0 \leq i < \frac{(r-1)}{L} \}$, where $\theta$ is a primitive element of $\mathbb{F}_r$. Note that $\mathbb{F}_r^* = \mathbb{F}_r \setminus \{0\} = \bigcup_{j=0}^{L-1} \mathcal{C}_j^{(L,r)}$. 

**Advances in Mathematics of Communications**

Volume 12, No. 1 (2018), 123–141
With cyclotomic classes of order $L$, there are associated certain character sums, which are called Gaussian periods and are defined as

$$
\eta_j^{(L,r)} = \sum_{x \in C_j^{(L,r)}} \chi_1(x)
$$

for $0 \leq j \leq L - 1$, where $\chi_1$ is the canonical additive character of $\mathbb{F}_r$. Further, the period polynomial of order $L$, denoted by $\Psi_{L,r}(x)$, is defined as

$$
\Psi_{L,r}(x) = \prod_{j=0}^{L-1} (x - \eta_j^{(L,r)}).
$$

In the following lemma, we state some basic properties of Gaussian periods:

**Lemma 2.1** ([23]). The Gaussian periods $\eta_j^{(L,r)} (0 \leq j \leq L-1)$ satisfy the following properties:

(a) $\eta_j^{(L,r)} = \eta_{j+uL}$ for any integer $u$.

(b) $\sum_{j=0}^{L-1} \eta_j^{(L,r)} = -1$.

(c) For $0 \leq i \leq L - 1$, we have $\eta_j^{(L,r)} \eta_{i+j}^{(L,r)} = \sum_{h=0}^{L-1} \mathcal{A}^{(L,r)}_{i} \eta_{i+h}^{(L,r)} + f\nu_i$, where $\nu_i = \begin{cases} 1 & \text{if } i = 0; \\ 0 & \text{otherwise}, \end{cases}$

where for $0 \leq i, h \leq L - 1$, $\mathcal{A}^{(L,r)}_{i}$ is the $(i, h)$th cyclotomic number of order $L$ and is defined as the number of elements in the set $(\mathcal{C}^{(L,r)}_i + 1) \cap \mathcal{C}^{(L,r)}_h$.

The Gaussian periods are further related to Gaussian sums, which are as discussed below: Let $L$ be a positive divisor of $r-1$ and $\psi$ be a multiplicative character of $\mathbb{F}_r$ having order $L$. Then the Gaussian sum of order $L$ is defined as

$$
G(\psi) = \sum_{c \in \mathbb{F}_r^*} \psi(c) \chi_1(c),
$$

where $\chi_1$ is the canonical additive character of $\mathbb{F}_r$. For a non-trivial character $\psi$, we have

$$
|G(\psi)| = r^{1/2}.
$$

Further for $0 \leq j \leq L - 1$, the following relation is well-known:

$$
\eta_j^{(L,r)} = \frac{1}{L} \sum_{h=0}^{L-1} e^{-2\pi i jh/L} G(h).
$$

Henceforth we will follow the same notations as in Section 2.

3. **Irreducible Constacyclic Codes and Their (Hamming) Weight Distributions**

Throughout this paper, let $n$ be a positive integer coprime to $q$. Let $\xi = \theta^{\frac{q-1}{n}}$ be a primitive element of $\mathbb{F}_q$. Let $0 \leq i \leq q - 2$ be a fixed integer and $\mathcal{R}_n = \mathbb{F}_q[x]/\langle x^n - \xi^i \rangle$ be the ring of residue classes of polynomials in $\mathbb{F}_q[x]$ modulo $x^n - \xi^i$. Then a $\xi^i$-constacyclic code of length $n$ over $\mathbb{F}_q$ is an ideal of the principal ideal ring $\mathcal{R}_n$ and an irreducible $\xi^i$-constacyclic code of length $n$ over $\mathbb{F}_q$ is a minimal ideal of the ring $\mathcal{R}_n$. In order to describe irreducible $\xi^i$-constacyclic codes of length $n$ over $\mathbb{F}_q$ more explicitly, we need to study $q$-cyclotomic cosets modulo $N = \frac{n(q-1)}{\gcd(i,q-1)}$. The $q$-cyclotomic coset modulo $N$ containing an integer $s$ is defined as the set $C_s^{(N)} = \{ s, sq, sq^2, \cdots, sq^{k_s-1}\}$, where $k_s$ is the least positive integer satisfying $sq^{k_s} \equiv s \pmod{N}$. If $S_N$ is a complete set of representatives of $q$-cyclotomic cosets
modulo $N$, then we have $x^N - 1 = \prod_{s \in S_N} M_s(x)$ with $M_s(x)$ as the minimal polynomial of $\eta^s$ over $\mathbb{F}_q$ for each $s \in S_N$, where $\eta$ is a primitive $N$th root of unity in some extension field of $\mathbb{F}_q$ satisfying $\eta^n = \xi^i$ (such an element $\eta$ exists in $\mathbb{F}_q$). From this, one can observe that $x^n - \xi^i = \prod_{s \in S_N} M_s(x)$, where the product runs over all $s \in S_N$ satisfying $s \equiv i \pmod{q-1}$. Then for each $s \in S_N$ satisfying $s \equiv i \pmod{q-1}$, the ideal generated by the polynomial $\frac{x^n - \xi^i}{M_s(x)}$, being a minimal ideal in $\mathcal{R}_n$, is an irreducible $\xi^i$-constacyclic code of length $n$ over $\mathbb{F}_q$ and is denoted by $\mathcal{M}_s(n,i)$. The elements of $\mathcal{M}_s(n,i)$ are called codewords. Throughout this paper, we shall denote elements of $\mathcal{R}_n$ by their representatives (in $\mathbb{F}_q[x]$) of degree less than $n$, and perform their addition and multiplication modulo $x^n - \xi^i$. We shall further identify elements of $\mathcal{R}_n$ with $n$-tuples over $\mathbb{F}_q$, i.e., the element $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \in \mathcal{R}_n$ is identified with the $n$-tuple $(a_0, a_1, a_2, \cdots, a_{n-1}) \in \mathbb{F}_q^n$ and vice versa. Under this identification, the Hamming weight of a codeword is defined as the number of its non-zero components. If $A_j$ ($0 \leq j \leq n$) denotes the number of codewords having Hamming weight $j$ in a code of length $n$ over $\mathbb{F}_q$, then the list $A_0, A_1, A_2, \cdots, A_n$ is called the (Hamming) weight distribution of the code. In order to determine weight distributions of irreducible constacyclic codes, we first provide a trace description of irreducible constacyclic codes in the following section.

3.1. Trace Representation of Irreducible Constacyclic Codes. In the following theorem, we first observe that all irreducible constacyclic codes over $\mathbb{F}_q$ are finite fields. Moreover, we provide a trace description of all the irreducible constacyclic codes of length $n$ over $\mathbb{F}_q$ by establishing a one-one correspondence between codewords of an irreducible constacyclic code and elements of a certain finite field.

**Theorem 3.1.** For each $s \in S_N$ with $s \equiv i \pmod{q-1}$, the irreducible $\xi^i$-constacyclic code $\mathcal{M}_s(n,i)$ is isomorphic to the finite field of order $q^{k_s}$, where $k_s$ is the least positive integer satisfying $sq^{k_s} \equiv s \pmod{N}$. Moreover, we have

$$\mathcal{M}_s(n,i) = \left\{ \frac{1}{n} \left( Tr_{q^{k_s}/q}(\gamma) + Tr_{q^{k_s}/q}(\gamma \beta) x + \cdots + Tr_{q^{k_s}/q}(\gamma \beta^{n-1}) x^{n-1} \right) : \gamma \in \mathbb{F}_{q^{k_s}} \right\},$$

or equivalently, $\mathcal{M}_s(n,i) = \left\{ \frac{1}{n} \left( Tr_{q^{k_s}/q}(\gamma), Tr_{q^{k_s}/q}(\gamma \beta), \cdots, Tr_{q^{k_s}/q}(\gamma \beta^{n-1}) \right) : \gamma \in \mathbb{F}_{q^{k_s}} \right\}$, where $Tr_{q^{k_s}/q}$ is the trace function from $\mathbb{F}_{q^{k_s}}$ onto $\mathbb{F}_q$ and $\beta^{-1}$ is a non-zero of the code $\mathcal{M}_s(n,i)$.

**Proof.** Working in a similar manner as in Theorem 9 of [15, Ch. 8], we see that $\mathcal{M}_s(n,i)$ is isomorphic to the finite field of order $q^{k_s}$. Next to construct an isomorphism from $\mathcal{M}_s(n,i)$ onto $\mathbb{F}_{q^{k_s}}$, we define a map $\vartheta : \mathcal{M}_s(n,i) \rightarrow \mathbb{F}_{q^{k_s}}$ as

$$\vartheta(a(x)) = a(\beta^{-1})$$

for all $a(x) \in \mathcal{M}_s(n,i)$, where $\beta^{-1}$ is a non-zero of the code $\mathcal{M}_s(n,i)$. It is clear that $\vartheta$ is a well-defined map and is a ring homomorphism. In order to show that $\vartheta$ is a bijection, we define another mapping $\varphi : \mathbb{F}_{q^{k_s}} \rightarrow \mathcal{M}_s(n,i)$ as

$$\varphi(\gamma) = \frac{1}{n} \sum_{j=0}^{n-1} Tr_{q^{k_s}/q}(\gamma \beta^j)x^j = c_s(x) \text{ (say)}$$

for each $\gamma \in \mathbb{F}_{q^{k_s}}$.

First of all, we will show that $\varphi$ is a well-defined map. For this, we need to show that $c_s(x) \in \mathcal{M}_s(n,i)$ for each $\gamma \in \mathbb{F}_{q^{k_s}}$. As $\{\eta^j : j \in C_s(N)\}$ are all the non-zeros
That is, we have \( c \over F \) it must have since \( s \) is satisfying it \( \equiv i (\text{mod } q - 1) \), we observe that in order to determine weight distributions of all the irreducible cyclic codes of length \( 3.2. \) Weight distributions of irreducible constacyclic codes. In particular, when \( \text{Remark 1.} \) Proof. Recall that the code \( M^{(m,i)} \) of length \( n \) over \( F_q \) has the generator polynomial \( x^n - \xi^i \) with \( M_s(x) = \prod_{j \in C^{(n,i)}} (x - \eta^j) \), where \( \eta \) is a primitive \( N \)th root of unity over \( F_q \) satisfying \( \eta^n = \xi^i \).
(a) To prove this, we first note that for each \( j \in C_s^{(N)} \), there exists an integer \( v \) satisfying \( j \equiv sq^v \pmod{N} \), which gives \( \eta^{jn/d} = \eta^{nq^v/d} = (\eta^{nq^v})^{s/d} = (\xi^v)^{s/d} = (\xi^{s/d}) \), as \( \gcd(s, n) = d \), \( \eta^n = \xi^i \) and \( \xi^{g^v} = \xi \). From this, it follows that \( \eta^j, j \in C_s^{(N)} \), are zeros of the polynomial \( (x^{n/d} - \xi^{is/d}) \), i.e., the polynomial \( M_s(x) \) divides \( (x^{n/d} - \xi^{is/d}) \) over \( \mathbb{F}_q \). As \( is \equiv i \pmod{q - 1} \), we have \( \xi^{is} = \xi^i \). Using this, we write
\[
x^n - \xi^i = \frac{(x^{n/d} - \xi^{s/d})}{M_s(x)} \left( \xi^{is(d-1)/d} + \xi^{is(d-2)/d}x^{n/d} + \cdots + x^{(d-1)n/d} \right).
\]
Further, it is easy to observe that the polynomial \( x^{n/d} - \xi^{is/d} \) generates the irreducible \( \xi^{is/d} \)-constacyclic code, namely \( M_s^{(n/d, is/d)} \), of length \( n/d \) over \( \mathbb{F}_q \). This induces a one-one correspondence between the codewords of the code \( M_s^{(n/d, is/d)} \) and the codewords of the code \( M_s^{(n, i)} \), which is given by
\[
c(x) \rightarrow c(x) \left( \xi^{is(d-1)/d} + \xi^{is(d-2)/d}x^{n/d} + \cdots + x^{(d-1)n/d} \right) \in M_s^{(n, i)}
\]
for every \( c(x) \in M_s^{(n/d, is/d)} \). From this, it follows immediately that the Hamming weight of any non-zero codeword in \( M_s^{(n, i)} \) is \( d \) times the Hamming weight of the corresponding non-zero codeword in \( M_s^{(n/d, is/d)} \), which implies that
\[
A_h = \begin{cases} 
B_{h/d} & \text{if } d \text{ divides } h; \\
0 & \text{otherwise}.
\end{cases}
\]

(b) To prove this, we see that if \( \gcd(s, n) = 1 \) and \( is \equiv i \pmod{q - 1} \), we have \( \gcd(s, N) = 1 \). This implies that \( |C_s^{(N)}| = |C_s^{(1)}| \), which further implies that the codes \( M_{s}^{(n, i)} \) and \( M_1^{(n, i)} \) are isomorphic (as fields). Now if \( s^{-1} \) is the multiplicative inverse of \( s \) modulo \( N \), then the map \( \mu_{s^{-1}} : R_n \rightarrow R_n \) defined as \( \mu_{s^{-1}}(c(x)) = c(x^{s^{-1}}) \) for every \( c(x) \in R_n \), is a ring automorphism. In order to show that \( \mu_{s^{-1}} \) is a weight-preserving isomorphism from \( M_1^{(n, i)} \) onto \( M_{s}^{(n, i)} \), we need to show that for every \( c(x) \in M_1^{(n, i)} \), the corresponding image \( \mu_{s^{-1}}(c(x)) \) lies in \( M_{s}^{(n, i)} \) and vice versa. For this, we see that \( c(x) \in M_1^{(n, i)} \) if and only if \( \eta^n \neq 0 \) for each \( j \in C_1^{(N)} \) if and only if \( c(\eta^{j s^{-1}}) \neq 0 \) for each \( j \in C_s^{(N)} \) if and only if \( \mu_{s^{-1}}(c(x)) \in M_{s}^{(n, i)} \), which proves (b).

To illustrate the above theorem, we see that all the distinct negacyclic codes of length 10 over \( \mathbb{F}_3 \) are given by \( M_1^{(10, 1)}, M_5^{(10, 1)} \) and \( M_{11}^{(10, 1)} \). As \( \gcd(5, 10) = 2 \), by Theorem 3.2(a), we note that the weight distribution \( A_0, A_1, \ldots, A_{10} \) of the code \( M_5^{(10, 1)} \) is given by \( A_0 = B_{h/5} \) if 5 divides \( h \) and \( A_h = 0 \) otherwise, where \( B_0, B_1, B_2 \) is the weight distribution of the code \( M_1^{(2, 1)} = \langle 1 \rangle = \mathbb{F}_3[x]/(x^2 + 1) \). It is easy to observe that \( B_0 = 1 \) and \( B_1 = B_2 = 4 \). From this, we obtain
\[
A_h = \begin{cases} 
1 & \text{if } h = 0; \\
4 & \text{if } h \neq 0 \text{ and } 5 \text{ divides } h; \\
0 & \text{otherwise}.
\end{cases}
\]
Further, as \( \gcd(11, 10) = 1 \), we note, by Theorem 3.2(b), that the codes \( M_1^{(10, 1)} \) and \( M_{11}^{(10, 1)} \) are permutation-equivalent, and hence have the same weight distribution.
In view of Theorem 3.2, we see that to determine weight distributions of all the irreducible constacyclic codes over \( F_q \), we need to determine the same for the irreducible constacyclic code \( M^{(m,i)}_1 \) for each integer \( m \geq 1 \).

3.3. Weight distribution of \( M^{(m,i)}_1 \). From now on, let \( m \) be a fixed positive integer coprime to \( q \) and \( r = q^k \), where \( k \) is the multiplicative order of \( q \) modulo \( \frac{m(q-1)}{\gcd(i,q-1)} \). Let \( L = \gcd \left( \frac{r-1}{q-1}, \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \right) \).

In this section, we shall relate the problem of determination of weight distribution of the irreducible constacyclic code \( M^{(m,i)}_1 \) with the evaluation of Gaussian periods of order \( L \). Towards this, we first evaluate all the non-zero Hamming weights in the code \( M^{(m,i)}_1 \) in terms of Gaussian periods of order \( L \) in the following theorem, whose proof comes after Lemmas 3.4 and 3.5.

**Theorem 3.3.** All the non-zero Hamming weights in the code \( M^{(m,i)}_1 \) are given by

\[
\frac{1}{m}(Tr_{r/q}(\gamma), Tr_{r/q}(\gamma \theta), \ldots, Tr_{r/q}(\gamma \theta^{m-1})) : \gamma \in F_q
\]

where \( Tr_{r/q} \) is the trace function from \( F_r \) onto \( F_q \).

Next, for each \( \gamma \in F_r \), let \( Z(r, \gamma) \) be the number of solutions \( y \in F_r \) of the trace equation \( Tr_{r/q}(\gamma y^T) = 0 \). In the following proposition, we relate the number \( Z(r, \gamma) \) with the Hamming weight of the corresponding codeword \( c_\gamma = \frac{1}{m}(Tr_{r/q}(\gamma), Tr_{r/q}(\gamma \theta), \ldots, Tr_{r/q}(\gamma \theta^{m-1})) \in M^{(m,i)}_1 \).

**Lemma 3.4.** For each \( \gamma \in F_r \), the Hamming weight of the codeword \( c_\gamma = \frac{1}{m}(Tr_{r/q}(\gamma), Tr_{r/q}(\gamma \theta), \ldots, Tr_{r/q}(\gamma \theta^{m-1})) \in M^{(m,i)}_1 \) is \( m \left( \frac{r - Z(r, \gamma)}{r-1} \right) \).

**Proof.** As \( \theta = \theta^{mT} \), we have \( c_\gamma = \frac{1}{m}(Tr_{r/q}(\gamma), Tr_{r/q}(\gamma \theta), \ldots, Tr_{r/q}(\gamma \theta^{m-1})) \). From this, it is clear that the Hamming weight of \( c_\gamma \) is equal to \( m - h \), where \( h \) equals the number of integers \( j \) (\( 0 \leq j \leq m-1 \)) satisfying \( Tr_{r/q}(\gamma \theta^{jT}) = 0 \). In other words, \( h \) equals the number of solutions of the equation \( Tr_{r/q}(\gamma y^T) = 0 \) in the set \( \{ \theta^j : 0 \leq j \leq m-1 \} \). Since \( y = 0 \) always satisfies \( Tr_{r/q}(\gamma y^T) = 0 \), the number of its non-zero solutions is \( Z(r, \gamma) - 1 \). Next we observe that for all integers \( j \) and \( u \), we have

\[
Tr_{r/q}(\gamma \theta^{(j+mu)_T}) = Tr_{r/q}(\gamma \theta^{jT}) \theta^{mu_T} = Tr_{r/q}(\gamma \theta^{jT}) \xi^u Tr_{r/q}(\gamma \theta^{mu_T}), \quad \text{as } \theta^{mu_T} = \xi^u \in F_q.
\]

From this, it follows that \( Tr_{r/q}(\gamma \theta^{j+mu}_T) = 0 \) if and only if \( Tr_{r/q}(\gamma \theta^{jT}) = 0 \). Thus if some \( \theta^j \) (\( 0 \leq j \leq m-1 \)) is a solution of the equation \( Tr_{r/q}(\gamma y^T) = 0 \), then \( \theta^j + m \theta^{j+2m}, \ldots, \theta^j + (m-1)m \) are also its solutions. As \( F_r^* = \{ \theta^j + mu : 0 \leq j \leq m-1, 0 \leq u \leq \frac{r-1}{r-1} \} \), we obtain \( h = m \left( \frac{Z(r, \gamma) - 1}{r-1} \right) \).

This proves the lemma.

From the above lemma and using the fact that \( Z(r, 0) = r \), we see that the Hamming weight of the codeword \( c_0 \) is \( m \left( \frac{r - Z(r, 0)}{r-1} \right) = 0 \). So from this point on,
we consider the codewords \( c_\gamma \), where \( \gamma \in \mathbb{F}_r^* \). The following lemma relates the number \( Z(r, \gamma) \) with Gaussian periods \( \eta_j^{(L,r)} \). Then the weight distribution \( \mathcal{A} \) of order \( L = \gcd \left( \frac{r-1}{q-1}, \frac{(r-1)gcd(q-1)}{m(q-1)} \right) \).

**Lemma 3.5.** If \( \gamma \in \mathcal{C}^{(L,r)} \) for some \( j \) satisfying \( 0 \leq j \leq L - 1 \), then we have

\[
Z(r, \gamma) = \frac{1}{q} \left[ q + r - 1 + L(q-1)\eta_j^{(L,r)} \right].
\]

As a consequence, if \( \gamma_1, \gamma_2 \in \mathcal{C}^{(L,r)} \) for some \( j \) \( 0 \leq j \leq L - 1 \), then \( Z(r, \gamma_1) = Z(r, \gamma_2) \).

**Proof.** For proof, see Lemma 5 of Ding and Yang [6]. □

**Remark 2.** From Lemmas 3.4 and 3.5, we see that if \( \gamma_1, \gamma_2 \in \mathcal{C}^{(L,r)} \), then the Hamming weights of the codewords \( c_{\gamma_1}, c_{\gamma_2} \in \mathcal{M}^{(m,i)}_1 \) are equal.

**Proof of Theorem 3.3.** It follows from Lemmas 3.4 and 3.5. □

**Corollary 1.** For \( 0 \leq j \leq L - 1 \), the Gaussian period \( \eta_j^{(L,r)} \) is an integer. In other words, the period polynomial \( \Psi_{L,r}(x) \) has integer roots.

**Proof.** From the definition, it is clear that the Gaussian periods \( \eta_j^{(L,r)} \) \( 0 \leq j \leq L - 1 \), are algebraic integers. On the other hand, as the Hamming weight is always an integer, in view of Theorem 3.3, we see that \( \eta_j^{(L,r)} \) is a rational number for \( 0 \leq j \leq L - 1 \). From this, the desired result follows immediately. □

Now we proceed to determine the Hamming weight distribution of the code \( \mathcal{M}^{(m,i)}_1 \) in certain special cases. For this, we need the following theorem, which generalizes Theorem 6 of Sharma et al. [21].

**Theorem 3.6.** Suppose that the integers \( \alpha_1, \alpha_2, \cdots, \alpha_t \) are all the distinct zeros of the period polynomial \( \Psi_{L,r}(x) \) with their algebraic multiplicities as \( \alpha_1, \alpha_2, \cdots, \alpha_t \), respectively. Then the weight distribution \( \mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_m \) of the irreducible \( \xi^t \)-constacyclic code \( \mathcal{M}^{(m,i)}_1 \) over \( \mathbb{F}_q \) is given by

\[
\mathcal{A}_j = \begin{cases} 
1 & \text{if } j = 0; \\
\frac{a_j(r-1)}{L} & \text{if } j = \frac{m(q-1)(r-1-L\alpha_i)}{q(r-1)} \text{ for } 1 \leq i \leq t; \\
0 & \text{otherwise.}
\end{cases}
\]

(Note that the number of distinct non-zero weights of \( \mathcal{M}^{(m,i)}_1 \) is equal to the number of distinct integer roots of the period polynomial \( \Psi_{L,r}(x) \).)

**Proof.** In view of Remark 2, using Theorem 3.3 and the fact that \( |\mathcal{C}^{(L,r)}| = \frac{r-1}{L} \) for \( 0 \leq j \leq L - 1 \), the result follows immediately. □

Next we recall that \( \mathcal{M}^{(m,i)}_1 \) is the finite field of order \( r = q^k = p^h \), where \( k \) is the multiplicative order of \( q \) modulo \( m(q-1)/gcd(i,q-1) \). From now on, for \( 0 \leq h \leq m \), let \( \mathcal{A}_h \) denote the number of codewords in \( \mathcal{M}^{(m,i)}_1 \) having Hamming weight \( h \).

In the following theorem, we determine the weight distribution of \( \mathcal{M}^{(m,i)}_1 \) in the semi-primitive case, i.e., when \( -1 \in (p) \) modulo \( L \).
Theorem 3.7. Suppose that \( L = \gcd \left( \frac{r-1}{q-1}, \frac{r-1}{m(q-1)} \right) > 2 \), and that \(-1 \in \langle p \rangle\) modulo \( L \). Let \( b \) be the least positive integer satisfying \( p^b \equiv -1 \pmod{L} \). Then \( k\ell \equiv 0 \pmod{2b} \) and we have the following:

(a) When \( k\ell/2b \), \( p \), \((p^b + 1)/L \) all are odd, the weight distribution of \( M_1^{(m,i)} \) is given by

\[
\mathbb{A}_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{(r-1)}{(r-1)(L-1)} & \text{if } h = \frac{m(q-1)(r-(L-1)\sqrt{r})}{q(r-1)}; \\
0 & \text{if } h = \frac{m(q-1)(r+\sqrt{r})}{q(r-1)}; \\
0 & \text{otherwise}.
\end{cases}
\]

(b) In all other cases, the weight distribution of \( M_1^{(m,i)} \) is given by

\[
\mathbb{A}_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{(r-1)}{(r-1)(L-1)} & \text{if } h = \frac{m(q-1)(r+(1)\sqrt{r})}{q(r-1)}; \\
0 & \text{if } h = \frac{m(q-1)(r-\sqrt{r})}{q(r-1)}; \\
0 & \text{otherwise}.
\end{cases}
\]

Proof. By Proposition 20 of Myerson [17], we see that when \( k\ell/2b \), \( p \), \((p^b + 1)/L \) all are odd, Gaussian periods of order \( L \) are given by \( \eta_{L/2}^{(L,r)} = \frac{(L-1)\sqrt{r}}{L} \), \( \eta_k^{(L,r)} = -\sqrt{r} \) for \( 0 \leq k \leq L-1 \) and \( k \neq L/2 \), while in the remaining cases, Gaussian periods are given by \( \eta_{0}^{(L,r)} = \frac{(L-1)\sqrt{r}+1}{L} \), \( \eta_{k}^{(L,r)} = \frac{(-1)^{\ell} \sqrt{r}+1}{L} \) for \( 1 \leq k \leq L-1 \). Now by applying Theorem 3.6, the result follows.

In the following theorem, we determine the weight distribution of the code \( M_1^{(m,i)} \) in the quadratic residue case (or index 2 case), i.e., when the multiplicative order of \( p \) modulo \( L \) is \( \phi(L)/2 \).

Theorem 3.8. Let \( L = p_1^\lambda \), where \( 3 \neq p_1 \equiv 3 \pmod{4} \) is a prime and \( \lambda \) is a positive integer. Suppose that the multiplicative order of \( p \) modulo \( L = \phi(L)/2 \), (i.e., \( \langle p \rangle \) is the group of all quadratic residues modulo \( L \)) and \( r = \frac{\phi(L)}{\phi(\lambda)} \) for some positive integer \( s \). Let \( \psi \) be a multiplicative character of \( \mathbb{F}_p^\ast \) having order \( L \). For \( 1 \leq j \leq L \), let \( \nu_j \) be the highest exponent of \( p \) that divides \( j \) and \( \kappa_j := j/p_1^{\nu_j} \) (note that \( \kappa_j \) lies in the unit group of \( \mathbb{Z}/p_1^{\lambda-\nu_j} \mathbb{Z} \)). Let \( a, b \) be the integers satisfying \( a^2 + p_1 b^2 = 4p^e \) and \( a \equiv -2p^e p_1^{\frac{1}{2} + 2\epsilon} \pmod{p_1} \), where \( \epsilon \) is the ideal class number of \( \mathbb{Q}(\sqrt{-p_1}) \). Then the weight distribution of the code \( M_1^{(m,i)} \) is given by

\[
\mathbb{A}_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{r-1}{L} & \text{if } h = \frac{m(q-1)\left(-\sum_{t=0}^{\nu_j} p_1 \left(A_{t}^{(s,\lambda)} B_{t+1}^{(s,\lambda)} - A_{t+1}^{(s,\lambda)} B_{t+1}^{(s,\lambda)} \right) - \left(\frac{\nu_j}{p_1}\right) p_1^{\ell+1} B_{\nu_j+1}^{(s,\lambda)} \right)}{q(r-1)}; \\
0 & \text{for some integer } j, 1 \leq j \leq L; \\
0 & \text{otherwise},
\end{cases}
\]

where \( A_0 = A_{\lambda+1} = B_{\lambda+1} = 0 \) and the integers \( p_t^{(s,\lambda)} = (-1)^{s-1} p_t^{s(\lambda-1) \frac{\ell-2x}{2}} \).
\[ A_t^{(s,\lambda)} = \text{Re} \left( \frac{a+b\sqrt{-p_1}}{2} \right)^{s\lambda-t}, \quad B_t^{(s,\lambda)} = \frac{1}{\sqrt{p_1}} \text{Im} \left( \frac{a+b\sqrt{-p_1}}{2} \right)^{s\lambda-t} \]

are uniquely determined by the integers \( a \) and \( b \) for each integer \( t \geq 1 \) [4, p. 379, Th. 11.7.9]. (Here \( \left( \frac{\kappa}{p_1} \right) \) denotes the well-known Legendre symbol.)

**Proof.** By Theorem 4.1 of Yang and Xia [25], for each integer \( t (1 \leq t \leq \lambda) \), we have

\[ G(\psi^{s\lambda-t}) = P_t^{(s,\lambda)} \left( A_t^{(s,\lambda)} + \sqrt{p_1} B_t^{(s,\lambda)} \right) . \]

Using (3) and working in a similar way as in Theorem 11.7.9 of [4], we obtain

\[ \eta_j^{(L,r)} = \frac{1}{L} \left[ -1 + \sum_{i=0}^{\nu_j} \left( A_t^{(s,\lambda)} P_t^{(s,\lambda)} - A_{t+1}^{(s,\lambda)} P_{t+1}^{(s,\lambda)} \right) - \left( \frac{\kappa_j}{p_1} \right) P_{\nu_j+1}^{t+1} B_{\nu_j+1}^{(s,\lambda)} P_{\nu_j+1}^{(s,\lambda)} \right] \]

for \( 0 \leq j \leq L - 1 \). Now by applying Theorem 3.6, the desired result follows immediately.

We shall next consider some non-semiprimitive and non-quadratic cases, and determine the weight distribution of \( \mathcal{M}_1^{(m,i)} \) for some special values of \( L \).

First of all, from Theorem 3.3, we observe that \( \mathcal{M}_1^{(m,i)} \) is a code with only one non-zero weight if and only if \( L = \gcd \left( \frac{r-1}{q-1}, \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \right) = 1 \). In fact, we have the following:

**Theorem 3.9.** When \( L = \gcd \left( \frac{r-1}{q-1}, \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \right) = 1 \), the weight distribution of \( \mathcal{M}_1^{(m,i)} \) is given by

\[ k_h = \begin{cases} 
1 & \text{if } h = 0; \\
r - 1 & \text{if } h = \frac{m(q-1)}{r-1}; \\
0 & \text{otherwise}.
\end{cases} \]

**Proof.** By Lemma 2.1(b), we have \( \eta_0^{(1,r)} = -1 \). Now applying Theorem 3.6, the result follows.

In the following theorems, we determine the weight distribution of \( \mathcal{M}_1^{(m,i)} \) for \( L \in \{2, 3, 4, 5, 6, 8, 12\} \) in non-semiprimitive and non-quadratic cases.

**Theorem 3.10.** When \( L = \gcd \left( \frac{r-1}{q-1}, \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \right) = 2 \), the weight distribution of \( \mathcal{M}_1^{(m,i)} \) is given by

\[ k_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{r-1}{2} & \text{if } h = \frac{m(q-1)}{q(r-1)}; \\
\frac{r-1}{2} & \text{if } h = \frac{m(q-1)}{q(r-1)}; \\
0 & \text{otherwise}.
\end{cases} \]

**Proof.** As \( L = 2 \), we see that \( k \) is even and \( q \) is odd, which implies that \( p^{k\ell} \equiv 1 \pmod{4} \). Then by Lemma 11 of Ding and Yang [6], we see that the period polynomial \( \Psi_{2,s}(x) \) has two distinct zeros, namely \( \frac{-1+\sqrt{T}}{2} \) and \( \frac{-1-\sqrt{T}}{2} \). Now by applying Theorem 3.6, the result follows.

**Theorem 3.11.** When \( p \equiv 1 \pmod{3} \) and \( L = \gcd \left( \frac{r-1}{q-1}, \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \right) = 3 \), the
weight distribution of $M_1^{(m,i)}$ is given by

$$
\mathcal{A}_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{r-1}{3} & \text{if } h = \frac{m(q-1)(r-c\sqrt{r})}{q(r-1)}; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r+c\sqrt{r})}{q(r-1)}; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r-\sqrt{r}+4a_1\sqrt{r})}{q(r-1)}; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r+\sqrt{r}-4a_1\sqrt{r})}{q(r-1)}; \\
0 & \text{otherwise},
\end{cases}
$$

where $c, d$ are integers satisfying $4\sqrt{r} = c^2 + 27d^2$, $c \equiv 1 \pmod{3}$ and $\gcd(c, p) = 1$. (Such a pair $(c, d)$ of integers exist [4, Lemma 3.0.1]. In fact, these conditions determine the integer $c$ uniquely and the integer $d$ up to sign.)

**Proof.** Since $L = 3$, we have $\frac{r-1}{q-1} \equiv 0 \pmod{3}$. When $p \equiv 1 \pmod{3}$, we have $q \equiv 1 \pmod{3}$, which gives $\frac{r-1}{q-1} \equiv \frac{q^k-1}{q-1} \equiv 1 + q + q^2 + \cdots + q^{k-1} \equiv k \pmod{3}$. From this, we obtain $k \equiv 0 \pmod{3}$, which implies that $k\ell \equiv 0 \pmod{3}$. Then by Theorem 16(c) of Myerson [17], we see that the period polynomial $\Psi_{3,\ell}(x)$ has three distinct zeros, namely $-\frac{1}{3} + \sqrt{r}$, $-\frac{1}{3} - \frac{1}{2}(c+9d)\sqrt{r}$ and $-\frac{1}{3} - \frac{1}{2}(c-9d)\sqrt{r}$. Now by applying Theorem 3.6, the result follows. \(\square\)

**Theorem 3.12.** When $p \equiv 1 \pmod{4}$ and $L = \gcd\left(\frac{r-1}{q-1}, \frac{(r-1)\gcd(q-1)}{m(q-1)}\right) = 4$, the weight distribution of $M_1^{(m,i)}$ is given by

$$
\mathcal{A}_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r+c\sqrt{r}+2a_1\sqrt{r})}{q(r-1)}; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r-\sqrt{r}+2a_1\sqrt{r})}{q(r-1)}; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r+\sqrt{r}-4a_1\sqrt{r})}{q(r-1)}; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r-\sqrt{r}+4a_2\sqrt{r})}{q(r-1)}; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r+\sqrt{r}-4a_2\sqrt{r})}{q(r-1)}; \\
0 & \text{otherwise},
\end{cases}
$$

where $a_1, b_1$ are integers satisfying $\sqrt{r} = a_1^2 + 4b_1^2$, $a_1 \equiv 1 \pmod{4}$ and $\gcd(a_1, p) = 1$. (Such a pair $(a_1, b_1)$ of integers exist [4, Lemma 3.0.1]. In fact, these conditions determine the integer $a_1$ uniquely and the integer $b_1$ up to sign.)

**Proof.** When $p \equiv 1 \pmod{4}$, we have $q \equiv 1 \pmod{4}$, which gives $\frac{r-1}{q-1} \equiv k \pmod{4}$. On the other hand, $L = 4$ implies that $\frac{r-2}{q-1} \equiv 0 \pmod{4}$, which gives $k \equiv 0 \pmod{4}$. As $k\ell \equiv 0 \pmod{4}$, by Theorem 17(d) of Myerson [17], we see that the period polynomial $\Psi_{4,\ell}(x)$ has 4 distinct zeros, namely $\frac{-1}{4} - \frac{1}{2}(c-9d)\sqrt{r}$, $\frac{-1}{4} - \frac{1}{2}(c+9d)\sqrt{r}$, $\frac{-1}{4} + \frac{1}{2}(c-9d)\sqrt{r}$, $\frac{-1}{4} + \frac{1}{2}(c+9d)\sqrt{r}$. In view of this and applying Theorem 3.6, the desired result follows. \(\square\)

In order to determine the weight distribution of the code $M_1^{(m,i)}$ in the case when $L = 5$, let $t, w, v, u$ be the integers satisfying the following Dickson’s system:

$$
(8) \quad 16\sqrt{r} = t^2 + 125w^2 + 50v^2 + 50u^2, \quad tw = c^2 - 4vu - u^2 \quad \text{and} \quad t \equiv 1 \pmod{5}.
$$

It is known [12] that there exist exactly four integral solutions $(t, w, v, u)$ of the Dickson’s system such that $p$ does not divide $t^2 - 125w^2$. Let us define a map $\sigma : \mathbb{Z}^4 \to \mathbb{Z}^4$ as $\sigma(t, w, v, u) = (t, -w, -u, v)$ for all $(t, w, v, u) \in \mathbb{Z}^4$. Note that $\sigma$ is a non-singular $\mathbb{Z}$-module homomorphism of order 4. Note that if $(t_0, w_0, v_0, u_0)$ is a solution of (8) such that $p$ does not divide $t_0^2 - 125w_0^2$, then $\sigma^4(t_0, w_0, v_0, u_0) = (t, w, v, u)$. 

\[\text{Advances in Mathematics of Communications} \quad \text{Volume 12, No. 1 (2018), 123–141}\]
Theorem 3.13. When \( p \equiv 1 \pmod{5} \) and \( L = \gcd\left( \frac{r-1}{q-1}, \frac{(r-1)\gcd(i, q-1)}{m(q-1)} \right) = 5 \), the weight distribution of \( \mathcal{M}_{1}^{m,i} \) is given by

\[
\hat{A}_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{r-1}{5} & \text{if } h = \frac{m(q-1)(r + \frac{5}{r}(t_3^3 - 25L_0))}{q(r-1)}; \\
\frac{r-1}{5} & \text{if } h = \frac{m(q-1)(r - \frac{5}{r}(t_3^3 - 25M_0))}{q(r-1)}; \\
\frac{r-1}{5} & \text{if } h = \frac{m(q-1)(r + \frac{5}{r}(t_3^3 - 25M_1))}{q(r-1)}; \\
\frac{r-1}{5} & \text{if } h = \frac{m(q-1)(r - \frac{5}{r}(t_3^3 - 25M_2))}{q(r-1)}; \\
0 & \text{otherwise},
\end{cases}
\]

where \( L_0 = 2t_0(v_0^2 + u_0^2) + 5u_0(11v_0^2 - 4v_0u_0 - 11u_0^2) \) and \( M_i = 2t_i^2u_i + 7t_iu_i^2 + 20t_iu_i - 3t_iu_i^2 + 125u_i^3 + 200w_i^2v_i - 150w_i^2u_i + 5w_i^2v_i - 20w_i^2u_i - 105w_iu_i^2 - 40v_i^3 - 60v_i^2u_i + 120v_iu_i^2 - 20u_i^3 \) for \( 0 \leq i \leq 3 \).

Proof. Here also, working in a similar way as in Theorems 3.11 and 3.12, one can show that \( k \equiv 0 \pmod{5} \) in the case when \( p \equiv 1 \pmod{5} \). Here by Theorem 1 of Hoshi [12], we see that the period polynomial \( \Psi_{5,r}(x) \) has five distinct zeros, namely \(-1 - \frac{5}{r}(t_3^3 - 25L_0), -1 + \frac{5}{r}(t_3^3 - 25M_0), -1 + \frac{5}{r}(t_3^3 - 25M_1), -1 + \frac{5}{r}(t_3^3 - 25M_2) \) and \(-1 + \frac{5}{r}(t_3^3 - 25M_3) \). Now by applying Theorem 3.6, we obtain the desired result. \( \square \)

To determine the weight distribution of \( \mathcal{M}_{1}^{m,i} \) in the case when \( L = 6 \) and \( p \equiv 1 \pmod{3} \), in [10], we see that there exist unique integers \( r_3 \) and \( s_3 \) satisfying \( 4p = r_3^2 + 3s_3^2 \), \( r_3 \equiv 1 \pmod{3} \), \( s_3 \equiv 0 \pmod{3} \) and \( 3s_3 = r_3(2\exp(\frac{p-1}{3}) + 1) \pmod{p} \). Now for each integer \( n \geq 1 \), let us define

\[
V_{j,n} = \zeta_6^{-j} \lambda^n + \zeta_6^j \lambda^n
\]

for \( 1 \leq j \leq 6 \), where \( \lambda = (r_3 + \sqrt{3}s_3)/2 \), \( \bar{\lambda} = (r_3 - \sqrt{3}s_3)/2 \) and \( \zeta_6 = \exp(2\pi i/6) \). In the following theorem, we consider the case \( L = 6 \) and determine the weight distribution of \( \mathcal{M}_{1}^{m,i} \).

Theorem 3.14. When \( p \equiv 1 \pmod{6} \) and \( L = \gcd\left( \frac{r-1}{q-1}, \frac{(r-1)\gcd(i, q-1)}{m(q-1)} \right) = 6 \), the weight distribution of \( \mathcal{M}_{1}^{m,i} \) is given by

\[
\hat{A}_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{(r-1)}{6} & \text{if } h = \frac{m(q-1)(r + (-1)^{(p-1)j} \sqrt{r}(V_{j,kt/3} + V_{j,krt/3} + (-1)^j \sqrt{\frac{r}{r-1}} \sqrt{r}))}{q(r-1)}; \\
0 & \text{otherwise},
\end{cases}
\]

where \( V_{j,kt/3} \) and \( V_{j,krt/3} \) (\( 1 \leq j \leq 6 \)) are as defined by (9).

Proof. Here also, working as above, one can observe that \( k \equiv 0 \pmod{6} \) when \( p \equiv 1 \pmod{6} \). Here by Proposition 3.2 of Gurak [10], we see that the period
polynomial $\Psi_{6,r}(x)$ has six distinct zeros, namely $6^{-1}\{(−1)^{j}+\frac{(r−1)qj}{2}−\sqrt{r}\}V_{j,2kt/3}−\sqrt{r}V_{j,k/3}−(−1)^{j}\frac{(r−1)qj}{2}−\sqrt{r}−1\}$ for $1 \leq j \leq 6$. Now by applying Theorem 3.6, the result follows.

To determine the weight distribution of the code $\mathcal{M}_{1}^{(m,i)}$ in the case when $L=8$, we need the following:

- If $p \equiv 1 \pmod{4}$, then there exist [10] unique integers $a_4$ and $b_4$ satisfying $p = a_4^2 + b_4^2$, $a_4 ≡ (−1)^{z+1} \pmod{4}$ and $b_4 ≡ a_4\xi^{(p−1)/4} \pmod{p}$, where $z$ is the least positive integer satisfying $\xi^z = 2$. Next for non-negative integers $j$ and $n$, define

$$Q_n = \pi^n + \bar{\pi}^n, \quad P_n = -i(\pi^n - \bar{\pi}^n),$$

$$Q_{j,n} = \varsigma_4^{-j}\pi^n + \varsigma_4^j\bar{\pi}^n, \quad P_{j,n} = -i(\varsigma_4^{-j}\pi^n - \varsigma_4^j\bar{\pi}^n),$$

where $\pi = a_4 + i b_4$ and $\varsigma_4 = e^{2\pi i/4}$.

- If $p \equiv 1 \pmod{8}$, then there exist [10] unique integers $a_8$ and $b_8$ satisfying $p = a_8^2 + 2\bar{b}_8^2$, $a_8 ≡ -1 \pmod{8}$ and $b_8 ≡ a_8\xi^{(p−1)/8} + \xi^{3(p−1)/8} \pmod{p}$.

- If $p \equiv 3 \pmod{8}$, then there exist [10] unique integers $a_8$ and $b_8$ satisfying $p = a_8^2 + 2\bar{b}_8^2$, $a_8 ≡ (−1)^{(p−3)/8} \pmod{4}$ and $b_8 ≡ a_8(\theta(q−1)/8 − \theta(1−q)/8) \pmod{p}$.

For each integer $n \geq 1$, we further define

$$T_n = \sigma^n + \bar{\sigma}^n \quad \text{and} \quad S_n = (\sigma^n - \bar{\sigma}^n)/(\sqrt{r}),$$

where $\sigma = a_8 + i b_8\sqrt{2}$ and $\bar{\sigma} = a_8 - i b_8\sqrt{2}$. Then in the following theorem, we consider the case $L=8$ and determine the weight distribution of the code $\mathcal{M}_{1}^{(m,i)}$.

**Theorem 3.15.** Let $L = \gcd\left(\frac{r−1}{q−1},\frac{(r−1)gcd(1,q−1)}{m(q−1)}\right) = 8$.

(a) When $p \equiv 1 \pmod{8}$, the weight distribution of $\mathcal{M}_{1}^{(m,i)}$ is given by

$$A_h = \begin{cases} 1 & \text{if } h = 0; \\ \frac{(r−1)^{j}q}{8} & \text{if } h = \frac{m(q−1)(r+(−1)^{j+1}(\sqrt{r}+\sqrt{r})Q_{j,kt/2}+\sqrt{r})T_{j,kt/4}+\Psi_{j,kt/2}}{q(r−1)} \text{ for } 1 \leq j \leq 8; \\ 0 & \text{otherwise,} \end{cases}$$

where

$$T_{j,kt/4} = \begin{cases} Q_{j/2,kt/4} & \text{if } j \text{ is even;} \\ (-1)^{j/4}Q_{0,kt/4} + (-1)^{(j−2)/4}P_{0,kt/4} & \text{if } j \text{ is odd,} \end{cases}$$

$$\Psi_{j,kt/2} = \begin{cases} T_{kt/2} & \text{if } j \text{ is even;} \\ S_{kt/2} & \text{if } j \text{ is odd} \end{cases}$$

with $Q_{j/2,kt/4}, Q_{0,kt/4}, P_{0,kt/4}$ are as defined by (10) and $T_{kt/2}, S_{kt/2}$ are as defined by (11).
and applying Theorem 3.6, the result follows.

Proof. Here also, working as above, we see that in the case

\( p \equiv 3 \pmod{8} \) and \( k \ell \equiv 0 \pmod{4} \), the weight distribution of the code \( M_{1}^{(m,i)} \) is given by

\[
A_{h} = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r-2\sqrt{7} S_{k\ell/2}-\sqrt{7})}{q(r-1)}; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r-2\sqrt{7} S_{k\ell/2}^{2}-\sqrt{7})}{q(r-1)}; \\
\frac{r-1}{8} & \text{if } h = \frac{m(q-1)(r-\sqrt{7} T_{k\ell/2}+3\sqrt{7})}{q(r-1)}; \\
\frac{r-1}{8} & \text{if } h = \frac{m(q-1)(r+2\sqrt{7} T_{k\ell/2}+3\sqrt{7})}{q(r-1)}; \\
0 & \text{otherwise}, 
\end{cases}
\]

where \( S_{k\ell/2} \) and \( T_{k\ell/2} \) are as defined by (11).

(c) When \( p \equiv 5 \pmod{8} \) and \( k \ell \equiv 0 \pmod{8} \), the weight distribution of the code \( M_{1}^{(m,i)} \) is given by

\[
A_{h} = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r-\sqrt{7}+\sqrt{7} P_{k\ell/2})}{q(r-1)}; \\
\frac{r-1}{4} & \text{if } h = \frac{m(q-1)(r+\sqrt{7} Q_{k\ell/2}+2\sqrt{7} Q_{k\ell/2})}{q(r-1)}; \\
\frac{r-1}{8} & \text{if } h = \frac{m(q-1)(r+\sqrt{7} Q_{k\ell/2}-2\sqrt{7} Q_{k\ell/2})}{q(r-1)}; \\
\frac{r-1}{8} & \text{if } h = \frac{m(q-1)(r+\sqrt{7} P_{k\ell/2}-2\sqrt{7} P_{k\ell/2})}{q(r-1)}; \\
\frac{r-1}{8} & \text{if } h = \frac{m(q-1)(r-\sqrt{7} P_{k\ell/2})}{q(r-1)}; \\
\frac{r-1}{8} & \text{if } h = \frac{m(q-1)(r+\sqrt{7} Q_{k\ell/2})}{q(r-1)}; \\
0 & \text{otherwise}, 
\end{cases}
\]

where \( P_{k\ell/2}, Q_{k\ell/2}, P_{k\ell/4}, Q_{k\ell/4} \) are as defined by (10).

Proof. Here also, working as above, we see that in the case \( p \equiv 1 \pmod{8} \), we have \( k \equiv 0 \pmod{8} \), which gives \( k \ell \equiv 0 \pmod{8} \). Now by using Proposition 3.3 of Gurak [10] and applying Theorem 3.6, the result follows.

\[
\text{Theorem 3.16. Let } L = \gcd \left( \frac{r-1}{q-1} \cdot \frac{(r-1) \gcd(i,q-1)}{m(q-1)} \right) = 12.
\]

(a) When \( p \equiv 1 \pmod{12} \), the weight distribution of the code \( M_{1}^{(m,i)} \) is given by

\[
A_{h} = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{r-1}{8} & \text{if } h = \frac{m(q-1)(r+\sqrt{7} Q_{j,k\ell/2}/2 V_{j,k\ell/2}/3+\sqrt{7} V_{j,k\ell/2}/3+\sqrt{7} V_{j,2k\ell/3}+\sqrt{7} V_{j,2k\ell/3}+(-1)^{j} \sqrt{7})}{q(r-1)}; \\
0 & \text{otherwise}, 
\end{cases}
\]

where \( Q_{j,k\ell/2} \) is as defined by (10) and \( V_{j,k\ell/3}, V_{j,2k\ell/3}, V_{2j,k\ell/3} \) are as defined by (9).

(b) When \( p \equiv 5 \pmod{12} \) and \( k \ell \equiv 0 \pmod{4} \), the weight distribution of the code \( M_{1}^{(m,i)} \) is given by
Hamming weights of irreducible constacyclic codes

\[ A_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{r-1}{6} & \text{if } h = \frac{m(q-1)(r+(-1)^{k+4}/4-1)\sqrt{7}}{q(r-1)}; \\
\frac{r-1}{6} & \text{if } h = \frac{m(q-1)(r+\sqrt{7})Q_{kt/2}((-1)^{k+4}/4-1)\sqrt{7}}{q(r-1)}; \\
\frac{r-1}{6} & \text{if } h = \frac{m(q-1)(r+\sqrt{7})Q_{kt/2}((-1)^{k+4}/4+1)\sqrt{7}}{q(r-1)}; \\
\frac{r-1}{6} & \text{if } h = \frac{m(q-1)(r+\sqrt{7})P_{kt/2}((-1)^{k+4}+1)\sqrt{7}}{q(r-1)}; \\
\frac{r-1}{12} & \text{if } h = \frac{m(q-1)(r+\sqrt{7})P_{kt/2}(2(-1)^{k+4}-1)\sqrt{7}}{q(r-1)}; \\
\frac{r-1}{12} & \text{if } h = \frac{m(q-1)(r+\sqrt{7})P_{kt/2}(2(-1)^{k+4}-1+5\sqrt{7})}{q(r-1)}; \\
\frac{r-1}{12} & \text{if } h = \frac{m(q-1)(r+\sqrt{7})P_{kt/2}(2(-1)^{k+4}-1+5\sqrt{7})}{q(r-1)}; \\
0 & \text{otherwise}, 
\end{cases} \]

where \( P_{kt/2}, \ Q_{kt/2} \) are as defined by (10).

(c) When \( p \equiv 7 \) (mod 12) and \( k \ell \equiv 0 \) (mod 6), the weight distribution of the code \( M_{(m,i)} \) is given by

\[ A_h = \begin{cases} 
1 & \text{if } h = 0; \\
\frac{(r-1)}{12} & \text{if } h = \frac{m(q-1)(r+(-1)^{k+4}/2)\sqrt{7}}{q(r-1)} \text{ when } j \ (1 \leq j \leq 12) \text{ is odd}; \\
\frac{(r-1)}{12} & \text{if } h = \frac{m(q-1)(r+(-1)^{k+4}/2)\sqrt{7}}{q(r-1)} \text{ when } 2 \parallel j \ (1 \leq j \leq 12); \\
\frac{(r-1)}{12} & \text{if } h = \frac{m(q-1)(r+(-1)^{k+4}/2)\sqrt{7}}{q(r-1)} \text{ when } 4 \parallel j \ (1 \leq j \leq 12); \\
0 & \text{otherwise}, 
\end{cases} \]

where \( v = 2(-1)^{k+4}/2(p+5)/6 \) and \( V_{j,k/3}, \ V_{j,2k/3} \) are as defined by (9) for \( 1 \leq j \leq 12 \). (Here by \( 4 | j \), we mean 4 divides \( j \). By \( 2 \parallel j \), we mean 2 divides \( j \) but 4 does not divide \( j \).)

Proof. Here also, working in a similar manner as above, when \( p \equiv 1 \) (mod 12), one can prove that \( k \equiv 0 \) (mod 12), which gives \( k \ell \equiv 0 \) (mod 12). Now by using Gurak [10, Proposition 3.4] and applying Theorem 3.6, the desired result follows.

4. Hamming weights of irreducible constacyclic codes

In an attempt to prove a weight-divisibility theorem (see [6, p. 440, Th. 14]) for irreducible cyclic codes, Ding and Yang [6] made the following two observations: (i) \( LN_{(L,r)}^{(L,r)} + 1 \equiv 0 \) (mod \( q \)) for \( 0 \leq j \leq L - 1 \) and (ii) \( \gcd \left( q - 1, \frac{(r-1)/m}{\gcd(q-1,\frac{r-1}{m})} \right) = 1. \)

However, we noticed that (ii) does not hold in general. In fact, Example 2 of Ding and Yang [6] contradicts this, i.e., when \( q = 3 \) and \( m = 40 \), we have \( k = 4 \) so that \( r = q^k = 81 \) and \( L = 2 \), which gives \( \gcd \left( q - 1, \frac{(r-1)/m}{\gcd(q-1,\frac{r-1}{m})} \right) = 2. \) Besides rectifying this error in the proof of Theorem 14 of [6], we derive a weight-divisibility theorem (Theorem 4.1) for irreducible constacyclic codes in the following theorem, whose proof comes after Lemma 4.2.
Theorem 4.1. Let \( s \in S_N \) satisfying \( si \equiv i \pmod{q - 1} \) be fixed. Let \( L = \gcd \left( \frac{r - 1}{q - 1}, \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \right) \) and \( T = \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \). Then the Hamming weight of every codeword in the irreducible constacyclic code \( M_s^{(m,i)} \) is divisible by
\[
\frac{\gcd(s, m) \gcd(i, q - 1)}{\gcd(i, q - 1, \frac{T}{q})}.
\]
To prove this theorem, we need the following lemma:

Lemma 4.2. Let \( L = \gcd \left( \frac{r - 1}{q - 1}, \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \right) \) and \( T = \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \). Then for \( 0 \leq j \leq L - 1 \), the following hold:
\[
\begin{align*}
a) & \quad L\eta_j^{(L,r)} + 1 \equiv 0 \pmod{q} \text{ and } \gcd(i, q - 1)L\eta_j^{(L,r)} \equiv 0 \pmod{T}.
\end{align*}
\]
Proof. To prove (a), by Theorem 3.3, we see that all the non-zero Hamming weights in \( M_1^{(m,i)} \) are given by \( w_j = \frac{m(q-1)(r-1-L\eta_j^{(L,r)})}{q(r-1)} \), where \( 0 \leq j \leq L - 1 \). From this, we see that for \( 0 \leq j \leq L - 1 \), the Hamming weight \( w_j \) is an integer if and only if both \( q \) and \( r - 1 \) divide \( m(q-1)(r-1-L\eta_j^{(L,r)}) \). This holds if and only if \( q \) divides \( L\eta_j^{(L,r)} + 1 \) and \( T \) divides \( \gcd(i, q - 1)L\eta_j^{(L,r)} \), which proves (a). Part (b) follows directly from (2) and (3), and using the fact that \( G(\psi^0) = -1 \).

Proof of Theorem 4.1. By Theorem 3.2, we observe that the Hamming weight of every non-zero codeword in \( M_s^{(m,i)} \) is \( \gcd(s, m) \) times the Hamming weight of some non-zero codeword in \( M_1^{(m,i)} \). So in order to prove this theorem, we need to prove that the Hamming weight of every non-zero codeword in \( M_1^{(m,i)} \) is divisible by \( \frac{\gcd(i, q - 1)}{\gcd(i, q - 1, \frac{T}{q})} \). For this, by Theorem 3.3, we see that all the non-zero Hamming weights in \( M_1^{(m,i)} \) are given by \( w_j = \frac{m(q-1)(r-1-L\eta_j^{(L,r)})}{q(r-1)} \) for \( 0 \leq j \leq L - 1 \). As \( \frac{m(q-1)}{r-1} = \frac{\gcd(i,q-1)}{q} \), each \( w_j \) can be rewritten as
\[
w_j = \frac{\gcd(i, q - 1)}{\gcd(i, q - 1, \frac{T}{q})} \left\{ \frac{\gcd(i, q - 1, \frac{T}{q}) (r - 1 - L\eta_j^{(L,r)})}{Tq} \right\}.
\]
Now applying Lemma 4.2(a), we see that \( \left\{ \frac{\gcd(i, q - 1, \frac{T}{q}) (r - 1 - L\eta_j^{(L,r)})}{Tq} \right\} \) is an integer for each \( j \), from which the desired result follows.

In the following theorem, we obtain both (optimal) lower and upper bounds on the non-zero Hamming weights in \( M_s^{(m,i)} \).

Theorem 4.3. Let \( s \in S_N \) satisfying \( si \equiv i \pmod{q - 1} \) be fixed. Let \( L = \gcd \left( \frac{r - 1}{q - 1}, \frac{(r-1)\gcd(i,q-1)}{m(q-1)} \right) \). If \( w \) is the Hamming weight of a non-zero codeword in the irreducible constacyclic code \( M_s^{(m,i)} \), then we have
\[
w \geq \gcd(s, m) \left\lfloor \frac{m(q-1)(r - [(L - 1)\sqrt{T}])}{q(r - 1)} \right\rfloor
\]
and
\[
w \leq \gcd(s, m) \left\lceil \frac{m(q-1)(r + [(L - 1)\sqrt{T}])}{q(r - 1)} \right\rceil.
\]
of the irreducible \( \xi \)

\[ x. \]

\[ (\text{Here for each real number } x, \lfloor x \rfloor \text{ denotes the floor of } x \text{ and } \lceil x \rceil \text{ denotes the ceiling of } x.)\]

**Proof.** By Theorems 3.2 and 3.3, we see that all the non-zero Hamming weights in \( M_{i}(m,i) \) are given by \( \gcd(s, m) \left( m(q-1)(r-1-L_0^{(r+i)}) / q(r-1) \right) \), where \( 0 \leq j \leq L - 1 \). Now using Lemma 4.2(b), we obtain the desired result. \( \square \)

5. Some Examples

In this section, by applying Theorems 3.7-3.16, we determine weight distribution of the irreducible \( \xi \)-constacyclic code \( M_{i}(m,i) \) over \( \mathbb{F}_q \) for several values of \( q, m \) and...
Table 2. Some examples of optimal irreducible constacyclic codes $\mathcal{M}_1^{(m,i)}$ over $\mathbb{F}_q$

$\begin{array}{cccccc}
q & m & k & i & L & d \\
3 & 20 & 4 & 1 & 2 & 12 \\
4 & 21 & 3 & 2 & 1 & 16 \\
4 & 7 & 3 & 0 & 3 & 4 \\
5 & 78 & 4 & 3 & 2 & 60 \\
5 & 6 & 2 & 3 & 1 & 5 \\
7 & 4 & 2 & 5 & 2 & 3 \\
7 & 57 & 3 & 5 & 1 & 49 \\
7 & 8 & 2 & 5 & 1 & 7 \\
7 & 19 & 3 & 3 & 4 & 15 \\
9 & 5 & 2 & 5 & 2 & 4 \\
\end{array}$

We also list some optimal irreducible constacyclic codes that attain the distance bounds given in Grassl’s table [8] (see Table 2).

References

[1] Y. Aubry and P. Langevin, On the weights of binary irreducible cyclic codes, Proc. Workshop Coding Cryptogr., Norway, 2005, 161–169.
[2] L. D. Baumert and R. J. McEliece, Weights of irreducible cyclic codes, Inform. Control, 20 (1972), 158–175.
[3] L. D. Baumert and J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, JPL Tech. Rep. 32-1526, 16 (1973), 128–131.
[4] B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi Sums, John Wiley & Sons Inc., New York, 1998.
[5] C. Ding, The weight distribution of some irreducible cyclic codes, IEEE Trans. Inf. Theory, 55 (2009), 955–960.
[6] C. Ding and J. Yang, Hamming weights in irreducible cyclic codes, Discrete Math., 313 (2013), 434–446.
[7] X. Dong and S. Yin, The trace representation of $\lambda$-constacyclic codes over the finite field $\mathbb{F}_q$, J. Liaoning Normal Univ.(Nat. Sci. ed.), 33 (2010), 129–131.
[8] M. Grassl, Code Tables: Bounds on the Parameters of Various Types of Codes, available at www.codetables.de
[9] P. Grover and A. K. Bhandari, A note on the weight distribution of minimal constacyclic codes, Bull. Malaysian Math. Sci. Soc., 39 (2016), 689–697.
[10] S. J. Gurak, Period polynomials for $\mathbb{F}_q$ of fixed small degree, CRM Proc. Lect. Notes, 36 (2004), 127–145.
[11] T. Helleseth, T. Klave and J. Mykkeltveit, The weight distribution of irreducible cyclic codes with block length $n_1((q^e-1)/N)$, Discrete Math., 18 (1977), 179–211.
[12] A. Hoshi, Explicit lifts of quantic Jacobi sums and period polynomials for $\mathbb{F}_q$, Proc. Japan Acad., 82 (2006), 87–92.
[13] P. Langevin, A new class of two weight codes, in Proc. 3rd Int. Conf. Finite Fields Appl., Cambridge Univ. Press, 1996, 181–187.
[14] F. MacWilliams and J. Seery, The weight distributions of some minimal cyclic codes, IEEE Trans. Inf. Theory, 27 (1981), 796–806.
[15] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland Publ. Co., Amsterdam, 1977.
[16] M. J. Moisio and K. O. Väänänen, Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes, IEEE Trans. Inf. Theory, 45 (1999), 1244–1249.
[17] G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith., 39 (1981), 251–264.
Hamming weights of irreducible constacyclic codes

[18] B. Schmidt and C. White, All two-weight irreducible cyclic codes?, *Finite Fields Appl.*, 8 (2002), 1–17.

[19] A. Sharma and G. K. Bakshi, The weight distribution of some irreducible cyclic codes, *Finite Fields Appl.*, 18 (2012), 144–159.

[20] A. Sharma, G. K. Bakshi and M. Raka, The weight distributions of irreducible cyclic codes of length $2^m$, *Finite Fields Appl.*, 13 (2007), 1086–1095.

[21] A. Sharma and A. K. Sharma, A note on weight distributions of irreducible cyclic codes, *Discrete Math. Algor. Appl.*, 6 (2014), 17 pages.

[22] Y. Song and Z. Li, The weight enumerator of some irreducible cyclic codes, preprint, arXiv:1202.2907v1

[23] T. Storer, *Cyclotomy and Difference Sets*, Markham Publ. Company, Chicago, 1967.

[24] C. Tang, Y. Qi, M. Xu, B. Wang and Y. Yang, A note on weight distributions of irreducible cyclic codes, in *Proc. Int. Conf. Inform. Commun. Tech. (ICT)*, 2014.

[25] J. Yang and L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Math.*, 53 (2010), 2525–2542.

Received for publication October 2016.

E-mail address: anuradha@iiitd.ac.in

E-mail address: iitsaroj@gmail.com