The weight distribution of some irreducible cyclic codes

Anuradha Sharma\textsuperscript{a, *}, Gurmeet K. Bakshi\textsuperscript{b}

\textsuperscript{a} Department of Mathematics, Indian Institute of Technology Delhi, New Delhi 110016, India
\textsuperscript{b} Centre for Advanced Study in Mathematics, Panjab University, Chandigarh 160014, India

\begin{abstract}
Let $F_q$ be the finite field with $q$ elements, $p$ be an odd prime co-prime to $q$ and $m \geq 1$ be an integer. In this paper, we explicitly determine the weight distribution of all the irreducible cyclic codes of length $p^m$ over $F_q$ from their generating polynomials in three different cases, when (i) the multiplicative order of $q$ modulo $p^m$ is $\phi(p^m)$, (ii) the multiplicative order of $q$ modulo $p^m$ is a power of $p$, and (iii) the multiplicative order of $q$ modulo $p^m$ is twice a power of $p$.
\end{abstract}

\section{1. Introduction}

Let $F_q$ be the finite field with $q$ elements and let $n$ be a positive integer co-prime to $q$. A cyclic code $C$ of length $n$ over $F_q$ is a linear subspace of $F_q^n$ with the property that if $(a_0, a_1, a_2, \ldots, a_{n-1}) \in C$, then the cyclic shift $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is also in $C$. A cyclic code $C$ of length $n$ over $F_q$ is also called a $q$-ary cyclic code of length $n$. We can also regard $C$ as an ideal in the principal ideal ring $R_n := F_q[x]/(x^n - 1)$ under the vector space isomorphism from $F_q^n$ to $R_n$ given by $(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. It is known that any ideal $C$ in $R_n$ is generated by a unique monic polynomial $g(x)$, which is a divisor of $(x^n - 1)$, called the generating polynomial of $C$. A minimal ideal in $R_n$ is called an irreducible cyclic code of length $n$ over $F_q$.

If $C$ is a cyclic code of length $n$ over $F_q$ and $v \in C$, then the weight of $v$, $wt(v)$, is defined to be the number of non-zero coordinates in $v$. If $A_{w}^{(n)}$ denotes the number of codewords in $C$ of weight $w$, $w \geq 0$, then the list $A_{0}^{(n)}, A_{1}^{(n)}, \ldots, A_{n}^{(n)}$ is called the weight distribution of $C$. The weight distribution
of irreducible cyclic codes has been an interesting object of study for a long time and is known in some cases (see [1–7,9,10,12–14]). Ding [2] determined the weight distribution of \( q \)-ary irreducible cyclic codes of length \( n \) provided \( 2 \leq \frac{\phi(q) - 1}{n} \leq 4 \), where \( \phi(n) \) denotes the multiplicative order of \( q \) modulo \( n \). He also pointed out that the weight formulas become quite messy if \( \frac{\phi(q) - 1}{n} \geq 5 \) and therefore finding the weight distribution of \( q \)-ary irreducible cyclic codes is a notoriously difficult problem.

In the previous paper [12], the authors, along with Raka, have determined the weight distribution of all the irreducible cyclic codes of length \( 2^m \) over \( \mathbb{F}_q \). In this paper, we determine the weight distribution of all the irreducible cyclic codes of length \( p^m \) over \( \mathbb{F}_q \), where \( p \) is an odd prime co-prime to \( q \) and \( m \geq 1 \) is an integer, in three different cases, when (i) the multiplicative order of \( q \) modulo \( p^m \) is \( \phi(p^m) \); (ii) the multiplicative order of \( q \) modulo \( p^m \) is a power of \( p \); (iii) the multiplicative order of \( q \) modulo \( p^m \) is twice a power of \( p \). In Section 2, we list all the irreducible cyclic codes of length \( p^m \) over \( \mathbb{F}_q \) and show that in order to determine the weight distribution of any of these codes, it is sufficient to find the weight distribution of the \( q \)-ary irreducible cyclic code of length \( p^r \), \( 1 \leq r \leq m \), which corresponds to the \( q \)-cyclotomic coset containing 1 (Theorem 1). In Section 3, we find the weight distribution of the irreducible cyclic code of length \( p^r \), \( 1 \leq r \leq m \), which corresponds to the \( q \)-cyclotomic coset containing 1 in the three different cases listed above (Theorems 2–4). Finally, in Section 4, we also give some illustrative examples.

2. Irreducible cyclic codes and their weight distribution

Let \( \mathbb{F}_q \) be the finite field with \( q \) elements and let \( n \) be a positive integer co-prime to \( q \). Let \( \alpha \) denote a primitive \( n \)-th root of unity in some extension field of \( \mathbb{F}_q \). For any integer \( s \), \( 0 \leq s \leq n - 1 \), the \( q \)-cyclotomic coset of \( s \) modulo \( n \) is the set

\[
C_s := \{ s, sq, sq^2, \ldots, sq^{n_s} - 1 \},
\]

where \( n_s \) is the least positive integer such that \( sq^{n_s} \equiv s \pmod{n} \). Corresponding to the \( q \)-cyclotomic coset \( C_s \), define

\[
M_s^{(n)}(x) := \prod_{j \in C_s} (x - \alpha^j)
\]

and

\[
\mathcal{M}_s^{(n)} := \text{the ideal in } \mathbb{R}_n \text{ generated by } \frac{x^n - 1}{M_s^{(n)}(x)}.
\]

It is known that \( M_s^{(n)}(x) \) is the minimal polynomial of \( \alpha^s \) over \( \mathbb{F}_q \) and \( \mathcal{M}_s^{(n)} \) is an irreducible cyclic code of length \( n \) over \( \mathbb{F}_q \), called the \( q \)-ary irreducible cyclic code of length \( n \) corresponding to the \( q \)-cyclotomic coset \( C_s \). Furthermore, if \( C_{s_1}, C_{s_2}, \ldots, C_{s_k} \) are all the distinct \( q \)-cyclotomic cosets modulo \( n \), then \( \mathcal{M}_{s_1}^{(n)}, \mathcal{M}_{s_2}^{(n)}, \ldots, \mathcal{M}_{s_k}^{(n)} \) are precisely all the distinct irreducible cyclic codes of length \( n \) over \( \mathbb{F}_q \).

For details, see [8, Chapters 7 and 8]. We have the following:

**Theorem 1.** Let \( \mathbb{F}_q \) be the finite field with \( q \) elements, \( p \) be an odd prime co-prime to \( q \) and \( m \geq 1 \) be an integer. Let \( g \) be a primitive root modulo \( p^m \).

(i) The codes \( \mathcal{M}_0^{(p^m)}, \mathcal{M}_k^{(p^m)}, 0 \leq j \leq m - 1, 0 \leq k \leq \frac{\phi(p^m - j)}{\phi(p^m - j)} - 1 \), are precisely all the distinct irreducible cyclic codes of length \( p^m \) over \( \mathbb{F}_q \), where \( \phi \) denotes Euler’s Phi function.

(ii) All the non-zero codewords in \( \mathcal{M}_0^{(p^m)} \) have weight \( p^m \).
(iii) The code \( M_1^{(pr)} \) is equivalent to the code \( M_1^{(p^r)} \) and therefore they have the same weight distribution.

(iv) \( M_1^{(pr)} \) is the repetition code of the irreducible cyclic code \( M_1^{(p^m)} \) of length \( p^{m-j} \) corresponding to the \( q \)-cyclotomic coset containing \( 1 \), in the following three different cases:

3.1. The multiplicative order of \( q \) modulo \( pm \) is

Proof. By [11, Lemma 1], all the distinct \( q \)-cyclotomic cosets modulo \( pm \) are given by \( C_0, C_{g^k p^j}, \) \( 0 \leq j \leq m-1, 0 \leq k \leq \phi(p^{m-j})/\phi(p^{m-j})-1 \). Therefore, (i) follows. (ii) and (iii) are obvious. The proof of (iv) is similar to that of Lemma 2 of [12]. □

It thus follows from the above theorem that the weight distribution of all the \( q \)-ary irreducible cyclic codes of length \( pm \) can be determined from the weight distribution of \( q \)-ary irreducible cyclic code \( M_1^{(p^r)} \) of length \( p^r \) \((1 \leq r \leq m)\), which corresponds to the \( q \)-cyclotomic coset containing \( 1 \).

3. The weight distribution of \( M_1^{(p^r)}, 1 \leq r \leq m \)

Throughout this section, \( \mathbb{F}_q \) denotes the finite field with \( q \) elements, \( p \) an odd prime co-prime to \( q \) and \( m \geq 1 \), an integer. Let \( 1 \leq r \leq m \) be fixed throughout. In this section, we determine the weight distribution of \( q \)-ary irreducible cyclic code \( M_1^{(p^r)} \) of length \( p^r \) corresponding to the \( q \)-cyclotomic coset containing \( 1 \), in the following three different cases:

(i) the multiplicative order of \( q \) modulo \( pm \) is \( \phi(pm) \);
(ii) the multiplicative order of \( q \) modulo \( pm \) is a power of \( p \);
(iii) the multiplicative order of \( q \) modulo \( pm \) is twice a power of \( p \).

3.1. The multiplicative order of \( q \) modulo \( pm \) is \( \phi(pm) \)

We first fix some notations. Let \( \mathbb{Z} \) denote the set of integers. For any \( t, v \in \mathbb{Z}, t \geq 1 \) and \( v \geq 2 \), let

\[
P_t(v) := \left\{ (v_1, v_2, \ldots, v_t) \in \mathbb{Z}^t \mid 2 \leq v_j \leq p \text{ for all } j, \sum_{j=1}^t v_j = v \right\}.
\]

Given \((v_1, v_2, \ldots, v_t) \in P_t(v)\), set

\[
L(v_1, v_2, \ldots, v_t) := \left\{ (\ell_1, \ell_2, \ldots, \ell_t) \in \mathbb{Z}^t \mid \ell_j \geq v_j - 2 \text{ for all } j, \sum_{j=1}^t \ell_j \leq p - 2t \right\}.
\]

Given \((\ell_1, \ell_2, \ldots, \ell_t) \in L(v_1, v_2, \ldots, v_t)\), put \( A(v_1, v_2, \ldots, v_t; \ell_1, \ell_2, \ldots, \ell_t) \) to be equal to

\[
a(\ell_1, \ell_2, \ldots, \ell_t) \left( \begin{array}{c} \ell_1 \\ v_1 - 2 \end{array} \right) \left( \begin{array}{c} \ell_2 \\ v_2 - 2 \end{array} \right) \cdots \left( \begin{array}{c} \ell_t \\ v_t - 2 \end{array} \right) (q - 1)^t (q - 2)^{v-2t},
\]
where

\[
da_1 = \sum_{k_1=1}^{l_1} \sum_{k_2=1+\ell_1+2}^{l_2-k_1} \ldots \sum_{k_{t-1}=1}^{l_{t-1}} \sum_{k_t=1+\ell_{t-1}+2}^{l_t} 1. \quad (1)
\]

**Definition 1.** For any integer \( \nu \geq 0 \), define \( N(\nu) \) to be equal to

1, if \( \nu = 0 \);
0, if \( \nu = 1 \) or \( \nu \geq p + 1 \);
\( \sum_{\nu \geq 1} \sum_{(v_1,v_2,\ldots,v_t) \in P_t(\nu)} \sum_{(\ell_1,\ell_2,\ldots,\ell_t) \in L(v_1,v_2,\ldots,v_t)} A(v_1,v_2,\ldots,v_t;\ell_1,\ell_2,\ldots,\ell_t) \), otherwise.

We are now ready to state

**Theorem 2.** Let \( \mathbb{F}_q \) be the finite field with \( q \) elements, \( p \) be an odd prime co-prime to \( q \) and \( m \geq 1 \) be an integer. If the multiplicative order of \( q \) modulo \( p^m \) is \( \phi(p^m) \), then the weight distribution \( A_\nu^{(p^r)} \), \( \nu \geq 0 \), of the \( q \)-ary irreducible cyclic code \( \mathcal{M}_1^{(p^r)} \) is given by

\[
A_\nu^{(p^r)} = \sum N(w_1)N(w_2)\cdots N(w_{p^r-1}),
\]

where the summation runs over all tuples \( (w_1,w_2,\ldots,w_{p^r-1}) \) of non-negative integers \( w_i \)'s satisfying \( \sum_{i=1}^{p^r-1} w_i = \nu \).

We need some preparation to prove this theorem.

Let \( e_i, 1 \leq i \leq p^r \), be the canonical basis of \( \mathbb{F}_q^{p^r} \).

**Lemma 1.** If the multiplicative order of \( q \) modulo \( p^m \) is \( \phi(p^m) \), then the generating polynomial of \( \mathcal{M}_1^{(p^r)} \) is \( x^{p^r-1} - 1 \), and the vectors

\[
e_{i+p^r-1} - e_i, \quad 1 \leq i \leq (p-1)p^{r-1},
\]

constitute a basis of \( \mathcal{M}_1^{(p^r)} \) over \( \mathbb{F}_q \).

**Proof.** Let \( \alpha \) be a primitive \( p^r \)th root of unity in some extension of \( \mathbb{F}_q \). Then the generating polynomial \( g(x) \) of \( \mathcal{M}_1^{(p^r)} \) is \( x^{p^r-1} / M_\alpha(x) \) with \( M_\alpha(x) = \prod_{j \in C_1} (x - \alpha^j) \), where \( C_1 \) is the \( q \)-cyclotomic coset of \( 1 \) modulo \( p^r \). Observe that the multiplicative order of \( q \) modulo \( p^r \) is \( \phi(p^m) \) and \( 1 \leq r \leq m \) yields that the multiplicative order of \( q \) modulo \( p^r \) is \( \phi(p^r) = (p-1)p^{r-1} \). Therefore, the \( q \)-cyclotomic coset modulo \( p^r \) containing \( 1 \) is \( \{1,q,q^2,\ldots,q^{(p-1)p^{r-1}-1}\} \), which is a reduced residue system modulo \( p^r \). As a result, the roots of \( M_\alpha(x) \) are precisely all the primitive \( p^r \)th roots of unity. Also note that the roots of the polynomial

\[
x^{p^r-1} / x^{p^r-1} - 1 = 1 + x^{p^r-1} + x^{2^{p^r-1}} + \cdots + x^{(p-1)p^{r-1}}
\]

are also precisely all the primitive \( p^r \)th roots of unity, which gives \( M_\alpha(x) = x^{p^r-1} - 1 \) and hence \( g(x) = x^{p^r-1} - 1 \). Now, by [8, Chapter 7, Theorem 1], \( \mathcal{M}_1^{(p^r)} \) is the subspace of \( R_{p^r} \) spanned by \( g(x), xg(x), \ldots, x^{(p-1)p^{r-1}-1}g(x) \). But under the standard isomorphism from \( R_{p^r} \) to \( \mathbb{F}_q^{p^r} \), \( x^{p^r-1}g(x) \) corresponds to \( e_{i+p^r-1} - e_i \) for each \( i \), which proves the result. \( \square \)
For \( 1 \leq i \leq p^r - 1 \), let \( V_i \) be the vector subspace of \( \mathbb{F}_q^{p^r} \) spanned by
\[
e_{i+jp^r-1} - e_{i+(j-1)p^r-1}, \quad 1 \leq j \leq p - 1.
\]

**Definition 2.** We say that a vector \( v \in V_i \) is a nice vector if
\[
v = \sum_{j=k}^{k+\ell} \alpha_j (e_{i+jp^r-1} - e_{i+(j-1)p^r-1}),
\]
where \( 0 \neq \alpha_j \in \mathbb{F}_q, k \geq 1, \ell \geq 0, k + \ell \leq p - 1 \). The integer \( \ell \) is called the length of \( v \) denoted \( \ell(v) \); \( k \) is called the initial point of \( v \), denoted by \( I(v) \); and \( k + \ell \) is called the end point of \( v \), denoted by \( E(v) \).

**Definition 3.** Let \( v_1, v_2, \ldots, v_t \in V_i \). We say that \( v_1, v_2, \ldots, v_t \) is a chain in \( V_i \) if each \( v_j, 1 \leq j \leq t \), is a nice vector and \( I(v_j) \geq E(v_{j-1}) + 2 \) for \( 2 \leq j \leq t \).

**Remark 1.**
(i) If \( v_1, v_2, \ldots, v_t \) is a chain in \( V_i \), then \( \text{wt}(\sum_{j=1}^{t} v_j) = \sum_{j=1}^{t} \text{wt}(v_j) \).
(ii) Any \( v \in V_i \) can be written as \( v = \sum_{j=1}^{p} v_j \), where \( v_1, v_2, \ldots, v_t \) is a chain in \( V_i \).

**Lemma 2.**
(i) If \( 0 \neq v \in V_i \), then \( 2 \leq \text{wt}(v) \leq p \).
(ii) If \( v \in V_i \) is a nice vector of length \( \ell \), then \( 2 \leq \text{wt}(v) \leq \ell + 2 \).
(iii) If \( \ell, k, v \) are integers satisfying \( 0 \leq \ell \leq p - 1, 1 \leq k \leq p - \ell - 1 \) and \( 2 \leq v \leq \ell + 2 \), then the number of nice vectors in \( V_i \) of length \( \ell \), weight \( v \) and initial point \( k \) is \( (\ell + 1)^2(q - 1)(q - 2)^{v-2} \). (Note that this number is independent of the choice of the initial point and \( i \).)

**Proof.** (i) Let \( v \in V_i \). Then
\[
v = \sum_{j=1}^{p-1} \alpha_j (e_{i+jp^r-1} - e_{i+(j-1)p^r-1})
\]
\[
= -\alpha_1 e_i + \alpha_{p-1} e_{i+(p-1)p^r-1} + \sum_{j=1}^{p-2} (\alpha_j - \alpha_{j+1}) e_{i+jp^r-1}. \tag{2}
\]

\( \alpha_j \in \mathbb{F}_q \). If \( v \neq 0 \), then at least one \( \alpha_j \neq 0 \), which gives \( \text{wt}(v) \geq 2 \). Also it is clear from (2) that \( \text{wt}(v) \leq p \). This proves (i).
(ii) is similar to (i).
(iii) If \( v \in V_i \) is a nice vector of length \( \ell \), weight \( v \) and \( I(v) = k \), then
\[
v = \sum_{j=k}^{k+\ell} \alpha_j (e_{i+(j-1)p^r-1})
\]
\[
= -\alpha_1 e_{i+(k-1)p^r-1} + \alpha_{k+\ell} e_{i+(k+\ell)p^r-1} + \sum_{j=k}^{k+\ell-1} (\alpha_j - \alpha_{j+1}) e_{i+jp^r-1}.
\]
where $0 \neq \alpha_j \in \mathbb{F}_q$, $k \leq j \leq k + \ell$. Now observe that the weight of $v$ is $v$ if and only if out of a total of $\ell$ differences $\alpha_j - \alpha_{j+1}$ ($k \leq j \leq k + \ell - 1$), exactly $(v - 2)$ are non-zero, which happens if and only if there exist $i_1, i_2, \ldots, i_{v-2}, k \leq i_1 < i_2 < \cdots < i_{v-2} \leq k + \ell - 1$ such that $\alpha_{i_1} = \alpha_{i_1+1} = \cdots = \alpha_{i_2}, \alpha_{i_2} \neq \alpha_{i_2+1}, \alpha_{i_2+1} = \alpha_{i_2+2} = \cdots = \alpha_{i_3}, \alpha_{i_3} \neq \alpha_{i_3+1}, \alpha_{i_3+1} = \alpha_{i_3+2} = \cdots = \alpha_{i_4}, \alpha_{i_4} \neq \alpha_{i_4+1}, \alpha_{i_4+1} = \alpha_{i_4+2} = \cdots = \alpha_{i_{v-2}+1}, \alpha_{i_{v-2}+1} = \alpha_{i_{v-2}+2} = \cdots = \alpha_{k+\ell}$. It can be seen that the total number of choices of such a nice vector $v$ is $(q-1)(q-2)^{v-2}$.

Lemma 3. Let $1 \leq i \leq p^{l-1}$. Given an integer $v$ satisfying $2 \leq v \leq p$, there are precisely $N(v)$ elements in $V_i$ having weight $v$.

Proof. Let $A(v)$ denote the set of all codewords in $V_i$ having weight $v$. For any $t \geq 1$, $(v_1, v_2, \ldots, v_t) \in P_t(v)$, and $(\ell_1, \ell_2, \ldots, \ell_t) \in L(v_1, v_2, \ldots, v_t)$, let

$$V_i(v_1, v_2, \ldots, v_t; \ell_1, \ell_2, \ldots, \ell_t) := \left\{ \sum_{j=1}^t v_j \mid v_1, v_2, \ldots, v_t \text{ is a chain in } V_i, \ wt(v_j) = v_j, \ \ell(v_j) = \ell_j, \ 1 \leq j \leq t \right\}.$$  

We assert that

$$A(v) = \bigcup_{t \geq 1} \bigcup_{(v_1, v_2, \ldots, v_t) \in P_t(v)} \bigcup_{(\ell_1, \ell_2, \ldots, \ell_t) \in L(v_1, v_2, \ldots, v_t)} V_i(v_1, v_2, \ldots, v_t; \ell_1, \ell_2, \ldots, \ell_t),$$

and moreover, this union is disjoint. It follows from Remark 1(i), that the right-hand side of (3) is contained in the left-hand side. Now, let $v \in A(v)$. By Remark 1, $v = \sum_{j=1}^t v_j$, where $v_1, v_2, \ldots, v_t$ is a chain in $V_i$ and $v = wt(v) = \sum_{j=1}^t wt(v_j)$. Let $v_j = wt(v_j)$ and $\ell_j = \ell(v_j)$. By Lemma 2, $2 \leq v_j \leq p$, $\ell_j \geq v_j - 2$ for all $j$. Also, $\sum_{j=1}^t \ell_j = \sum_{j=1}^t (E(v_j) - I(v_j)) = \sum_{j=2}^t (E(v_{j-1}) - I(v_{j-1})) + E(v_1) - I(v_1) \leq p - 2t$, as $I(v_1) \geq 1$, $E(v_t) \leq p - 1$ and $I(v_j) - E(v_{j-1}) \geq 2$. This gives $(\ell_1, \ell_2, \ldots, \ell_t) \in L(v_1, v_2, \ldots, v_t)$ and $v \in V_i(v_1, v_2, \ldots, v_t; \ell_1, \ell_2, \ldots, \ell_t)$, which proves the assertion (3). It is clear that the union in the right-hand side of (3) is disjoint.

We next assert that $|V_i(v_1, v_2, \ldots, v_t; \ell_1, \ell_2, \ldots, \ell_t)|$ equals

$$a_{(\ell_1, \ell_2, \ldots, \ell_t)} \left( \alpha_{v_1 - 2} \right) \left( \alpha_{v_2 - 2} \right) \cdots \left( \alpha_{v_t - 2} \right) (q-1)^t (q-2)^{v-2t},$$

where $a_{(\ell_1, \ell_2, \ldots, \ell_t)}$ is as given in Eq. (1). In order to find $|V_i(v_1, v_2, \ldots, v_t; \ell_1, \ell_2, \ldots, \ell_t)|$, we need to find the number of chains $v_1, v_2, \ldots, v_t$ in $V_i$ such that $wt(v_j) = v_j$ and $\ell(v_j) = \ell_j$ for all $j$. Let $k_j = I(v_j)$. Then, $k_1 \geq 1$, $k_1 + \ell_1 \leq p - 1$ and $k_1 + \ell_1 + 2 \leq k_j + 2 \leq k_j$ for $2 \leq j \leq t$. This gives

$$1 \leq k_1 \leq p - \sum_{i=1}^t \ell_i - 2t + 1,$$

$$k_1 + \ell_1 + 2 \leq k_2 \leq p - \sum_{i=2}^t \ell_i - 2(t - 1) + 1,$$

$$\ldots$$

$$k_{t-2} + \ell_{t-2} + 2 \leq k_{t-1} \leq p - \sum_{i=t-1}^t \ell_i - 3,$$

$$k_{t-1} + \ell_{t-1} + 2 \leq k_t \leq p - \ell_t - 1.$$
Therefore the total number of choices for the initial points \(k_1, k_2, \ldots, k_t\) is

\[
p - \sum_{i=1}^{t-2} \ell_i - 2t + 1 + p - \sum_{i=2}^{t-1} \ell_i - (t-1) + 1 + \cdots + p - \sum_{i=1}^{t-1} \ell_i - 3 + p - \ell_t - 1 - 1,
\]

which is equal to \(a(\ell_1, \ell_2, \ldots, \ell_t)\). By Lemma 2(iii), the number of nice vectors \(v_j\) of length \(\ell_j\), weight \(w_j\) and having a fixed initial point \(k_j\), is given by \((\ell_j - 1)(q - 1)(q - 2)^{v_j - 2}\) for each \(j, 1 \leq j \leq t\). Consequently, the total number of vectors in \(V_i(v_1, v_2, \ldots, \ell_1, \ell_2, \ldots, \ell_t)\) is given by

\[
a(\ell_1, \ell_2, \ldots, \ell_t) \left( \frac{\ell_1}{v_1 - 2} \right) \left( \frac{\ell_2}{v_2 - 2} \right) \cdots \left( \frac{\ell_t}{v_t - 2} \right) (q - 1)^{t} (q - 2)^{v - 2t},
\]

which proves the assertion (4). The lemma now immediately follows from (3) and (4).

\(\Box\)

We are now ready to prove Theorem 2.

**Proof of Theorem 2.** Let \(w \geq 0\) and let \(A(w)\) denote the codewords in \(M_1^{(p^r)}\) having weight \(w\). For any tuple \((w_1, w_2, \ldots, w_{p^r-1})\) of non-negative integers \(w_i\)'s satisfying \(\sum_{i=1}^{p^r-1} w_i = w\), define

\[
S_{(w_1, w_2, \ldots, w_{p^r-1})} = \left\{ \sum_{i=1}^{p^r-1} c_i \mid c_i \in V_i, \ wt(c_i) = w_i, 1 \leq i \leq p^r-1 \right\}.
\]

It follows from Lemma 1 and the definition of \(V_i\)'s that \(A(w) = \bigcup S_{(w_1, w_2, \ldots, w_{p^r-1})}\), where the union runs over all tuples \((w_1, w_2, \ldots, w_{p^r-1})\) of integers \(w_i\)'s satisfying \(w_i \geq 0\) and \(\sum_{i=1}^{p^r-1} w_i = w\), and also it is clear that the union is disjoint. Therefore,

\[
A^{(p^r)}_w = \left| \bigcup S_{(w_1, w_2, \ldots, w_{p^r-1})} \right| = \sum |S_{(w_1, w_2, \ldots, w_{p^r-1})}|.
\]

But \(|S_{(w_1, w_2, \ldots, w_{p^r-1})}| = N_1(w_1)N_2(w_2)\cdots N_{p^r-1}(w_{p^r-1})\), where \(N_i(w_i)\) is the number of codewords in \(V_i\) having weight \(w_i\). However, by Lemma 3, \(N_i(w_i)\) equals \(N(w_i)\) for any \(i\), which completes the proof. \(\Box\)

3.2. The multiplicative order of \(q\) modulo \(p^m\) is a power of \(p\)

**Theorem 3.** Let \(\mathbb{F}_q\) be the finite field with \(q\) elements, \(p\) be an odd prime co-prime to \(q\) and \(m \geq 1\) be an integer. Suppose that the multiplicative order of \(q\) modulo \(p^m\) is \(p^d\) for some integer \(d\) (note that \(0 \leq d < m\)). Then, if

(i) \(r \leq m - d\), the only possible non-zero weight in \(M_1^{(p^r)}\) is \(p^r\), which is attained by all its \(q - 1\) non-zero codewords.

(ii) \(r > m - d\), the weight distribution \(A^{(p^r)}_w\), \(w \geq 0\), of \(M_1^{(p^r)}\) is given by

\[
A^{(p^r)}_w = \begin{cases} 
0 & \text{if } p^{m-d} \text{ does not divide } w; \\
(\frac{p^{r-(m-d)}}{w}) (q - 1)^w & \text{if } w = p^{m-d} w', \ 0 \leq w' \leq p^{r-(m-d)}. 
\end{cases}
\]

In order to prove Theorem 3, we first prove the following:
Lemma 4. Let $p$, $q$, $m$, $d$ be as defined in Theorem 3. Then $O_{pr}(q)$, the multiplicative order of $q$ modulo $p^r$, is given by

\[ O_{pr}(q) = \begin{cases} 
1 & \text{if } r \leq m - d; \\
p^r - (m - d) & \text{if } r > m - d.
\end{cases} \]

Proof. First we assert that

\[ O_{p^{m-d}}(q) = 1. \]  \hfill (5)

To prove this, let $O_{p^{m-d}}(q) = t$. Working, as in [11, Lemma 1], we get $O_{p^r}(q) = tp^d$. As it is given that $O_{p^r}(q) = p^d$, we get $t = 1$, which proves (5).

If $r \leq m - d$, then by (5), we have $O_{pr}(q) = 1$. For the case $r > m - d$, working again as in [11, Lemma 1], we obtain that $O_{pr}(q) = p^{r-(m-d)}$. This proves the lemma. \( \square \)

Lemma 5. Let $p$, $q$, $m$, $d$ be as in Theorem 3. If $r > m - d$, then there exists a primitive $p^{m-d}$th root of unity $\beta \in \mathbb{F}_q$, such that the vectors

\[ \sum_{j=0}^{p^{m-d} - 1} \beta^{j+1} e_{i+jp^{r-(m-d)}} \quad 1 \leq i \leq p^{r-(m-d)}, \]

constitute a basis of $\mathcal{M}_1^{(p^r)}$ over $\mathbb{F}_q$.

Proof. By Lemma 4, the $q$-cyclotomic coset modulo $p^r$ containing 1 is $\{1, q, q^2, \ldots, q^{p^{r-(m-d)}-1}\}$. Therefore $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{p^{r-(m-d)}-1}}$ are precisely all the roots of the minimal polynomial of $\alpha$ over $\mathbb{F}_q$. We also observe that $x^{p^{r-(m-d)}-1} - \alpha^{p^{r-(m-d)}} \in \mathbb{F}_q[x]$ and $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{p^{r-(m-d)}-1}}$ are precisely all its roots. Therefore, $x^{p^{r-(m-d)}} - \alpha^{p^{r-(m-d)}}$ is the minimal polynomial of $\alpha$ over $\mathbb{F}_q$ and hence the generating polynomial $g(x)$ of $\mathcal{M}_1^{(p^r)}$ is $\frac{x^{p^{r-(m-d)}-1}}{x^{p^{r-(m-d)}-1} - \alpha^{p^{r-(m-d)}}} = \beta + \beta^2 x^{p^{r-(m-d)}} + \beta^3 x^{2p^{r-(m-d)}} + \cdots + \beta^{p^{m-d} - 1} x^{(p^{m-d} - 2)p^{r-(m-d)}} + \cdots x^{(p^{m-d} - 1)p^{r-(m-d)}}$, where $\beta = \alpha^{-p^{r-(m-d)}}$. Now, as a vector subspace of $R_{p^r}$, $\mathcal{M}_1^{(p^r)}$ is spanned by $g(x), xg(x), \ldots, x^{p^{r-(m-d)}-1}g(x)$. Since, under the standard isomorphism from $R_{p^r}$ to $\mathbb{F}_q$, $x^{p^{r-(m-d)}-1}g(x)$ corresponds to $\sum_{j=0}^{p^{m-d} - 1} \beta^{j+1} e_{i+jp^{r-(m-d)}}$ for $1 \leq i \leq p^{r-(m-d)}$, the result follows. \( \square \)

Proof of Theorem 3. (i) Let $\alpha$ be a primitive $p^r$th root of unity in some extension of $\mathbb{F}_q$. If $r \leq m - d$, by Lemma 4, the multiplicative order of $q$ modulo $p^r$ is 1. Therefore $\alpha^{q-1} = 1$, i.e., $\alpha \in \mathbb{F}_q$ and the minimal polynomial of $\alpha$ over $\mathbb{F}_q$ is $x - \alpha$. Hence $\mathcal{M}_1^{(p^r)}$ is a 1-dimensional subspace of $\mathbb{F}_q^r$ generated by $\frac{x^{p^r-1}}{x-\alpha} = \alpha^{p^r-1} + \alpha^{p^r-2}x + \cdots + \alpha x^{p^r-2} + x^{p^r-1}$ and therefore every codeword of $\mathcal{M}_1^{(p^r)}$ is a scalar multiple of $\alpha^{p^r-1} + \alpha^{p^r-2}x + \cdots + \alpha x^{p^r-2} + x^{p^r-1}$. This implies that the only possible non-zero weight in $\mathcal{M}_1^{(p^r)}$ is $p^r$, which is attained by all its $(q - 1)$ non-zero codewords.

(ii) If $r > m - d$, by Lemma 5, any codeword $c \in \mathcal{M}_1^{(p^r)}$ can be written as $c = \sum_{j=0}^{p^{m-d} - 1} \alpha_i \beta^{j+1} e_{i+jp^{r-(m-d)}}, \alpha_i \in \mathbb{F}_q$. Clearly, $\text{wt}(c)$ is $p^{m-d}w'$, where $w'$ is the number of non-zero $\alpha_i$’s. Thus $A_w^{(p^r)} = 0$ if $p^{m-d}$ does not divide $w$. Moreover a codeword in $\mathcal{M}_1^{(p^r)}$ has weight $w = p^{m-d}w'$ if and only if it is a linear combination of any $w'$ basis vectors over $\mathbb{F}_q$ out of a total $p^{r-(m-d)}$ basis vectors of $\mathcal{M}_1^{(p^r)}$. This implies that there are $(p^{r-(m-d)})(q - 1)^{w'}$ codewords in $\mathcal{M}_1^{(p^r)}$ having weight $p^{m-d}w'$, which proves the theorem. \( \square \)
3.3. The multiplicative order of $q$ modulo $p^m$ is twice a power of $p$

We now determine the weight distribution of $M_{1}^{(p^r)}$, when $O_{p^m}(q) = 2^{pd}$ for some $d \geq 0$. As $O_{p^m}(q)$ is a divisor of $\phi(p^m)$, we have $d \leq m - 1$. Let $u = \min(r, m - d)$. For any integer $v \geq 0$, define

$$n(v) := \begin{cases} 
1 & \text{if } v = 0; \\
(q - 1)p^u & \text{if } v = p^u - 1; \\
(q - 1)(q - p^u + 1) & \text{if } v = p^u; \\
0 & \text{otherwise.}
\end{cases}$$

In this case, we have the following:

**Theorem 4.** The weight distribution $A_{w}^{(p^r)}$, $w \geq 0$, of $M_{1}^{(p^r)}$ is given by

$$A_{w}^{(p^r)} = \sum_{n(w_1)n(w_2)\cdots n(w_{p^r-u})} n(w_1)n(w_2) \cdots n(w_{p^r-u}),$$

where the summation runs over all tuples $(w_1, w_2, \ldots, w_{p^r-u})$ of non-negative integers $w_i$’s satisfying $w_1 + w_2 + \cdots + w_{p^r-u} = w$.

**Lemma 6.** Let $p, q, m, d$ be as above. Then

$$O_{p^r}(q) = \begin{cases} 
2 & \text{if } r \leq m - d; \\
2^{p^r-(m-d)} & \text{if } r > m - d.
\end{cases}$$

**Proof.** Proof is similar to that of Lemma 4. □

**Lemma 7.** Let $p, q, m, d, u$ be as above. There exist non-zero $b_0, b_1, \ldots, b_{p^u-2} \in \mathbb{F}_q$ such that the following vectors

$$\mathfrak{R}_i := \sum_{j=0}^{p^u-2} b_j e_{i+jp^r-u}, \quad 1 \leq i \leq 2p^r-u,$$

constitute a basis of $M_{1}^{(p^r)}$ over $\mathbb{F}_q$.

**Proof.** By Lemma 6, the $q$-cyclotomic coset modulo $p^r$ containing 1 is $\{1, q, q^2, \ldots, q^{2p^r-u-1}\}$. Therefore, if $\alpha$ is a primitive $p^r$th root of unity in some extension of $\mathbb{F}_q$, then $\alpha, \alpha^q, \ldots, \alpha^{q^{2p^r-u-1}}$ are precisely all the zeros of the minimal polynomial of $\alpha$ over $\mathbb{F}_q$. We observe that

(i) $x^{p^r-u} - \alpha^{p^r-u} \in \mathbb{F}_q[x]$ and $\alpha, \alpha^q, \ldots, \alpha^{q^{2p^r-u-2}}$ are precisely all its zeros; and
(ii) $x^{p^r-u} - \alpha^{p^r-u}q \in \mathbb{F}_q[x]$ and $\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{2p^r-u-1}}$ are precisely all its zeros.

As a consequence,

$$(x^{p^r-u} - \alpha^{p^r-u})(x^{p^r-u} - \alpha^{p^r-u}q) = x^{2p^r-u} - (\alpha^{p^r-u} + \alpha^{p^r-u}q)x^{p^r-u} + 1$$

is the minimal polynomial of $\alpha$ over $\mathbb{F}_q$. Thus the generating polynomial $g(x)$ of the minimal ideal $M_{1}^{(p^r)}$ is $x^{2p^r-u} - (\alpha^{p^r-u} + \alpha^{p^r-u}q)x^{p^r-u} + 1$. By division algorithm, we have
\[ g(x) = \frac{x^{2p^r} - 1}{x^{2p^r} - (\alpha^{p^r - q} + \alpha^{p^r - u})x^{p^r - u} + 1} \]
\[ = b_0 + b_1 x^{p^r - u} + b_2 x^{2p^r - u} + \cdots + b_{p^u - 2} x^{(p^u - 2)p^r - u}, \]

where
\[ b_0 = -1, \quad b_1 = -(\alpha^{p^r - u} + \alpha^{p^r - q}), \]
\[ b_i - (\alpha^{p^r - u} + \alpha^{p^r - q})b_{i-1} + b_{i-2} = 0 \quad \text{for} \quad 2 \leq i \leq p^u - 2, \]

and
\[ b_{p^u - 3} = \alpha^{p^r - u} + \alpha^{p^r - q}, \quad b_{p^u - 2} = 1. \]

On solving the above recurrence relation, we get that
\[ b_i = \frac{-(\alpha^{p^r - u})^{(i+1)} + (\alpha^{p^r - u})^{q(i+1)}}{\alpha^{p^r - u} - \alpha^{p^r - q}}. \tag{6} \]

We claim that all the \( b_i \)'s are non-zero. Note that \( b_i = 0 \) if and only if \((\alpha^{p^r - u})(q-1)(i+1) = 1\), which holds if and only if \((q-1)(i+1) \equiv 0 \pmod{p^u}\), as \(\alpha^{p^r - u}\) is a primitive \(p^u\)th root of unity. By Lemma 6, \(q - 1\) is not divisible by \(p\). Therefore, we get \((i+1) \equiv 0 \pmod{p^u}\). But this is not possible, because \(1 \leq i + 1 \leq p^u - 1 < p^u\). This proves the claim.

Now, \(M(\rho)\) is spanned by \(g(x), xg(x), \ldots, x^{2p^r - u} g(x)\) and under the standard isomorphism from \(R_{p^r} \) to \(\mathbb{F}_q\), \(x^j \mapsto g(x)\) corresponds to \(\mathfrak{M}_j\) for \(1 \leq j \leq 2p^r - u\), the result follows. \(\square\)

For \(1 \leq i \leq p^r - u\), let
\[ U_i := \text{the subspace of } \mathbb{F}_q^{2p^r} \text{ generated by } \mathfrak{M}_i \text{ and } \mathfrak{M}_{i+p^r - u}. \]

**Lemma 8.** For any \(v \geq 0\), the number of codewords in \(U_i\) of weight \(v\) is \(n(v)\).

**Proof.** It is enough to show that the only possible non-zero weights in \(U_i\) are \(p^v - 1\) and \(p^v\), and that there are precisely \((q - 1)p^u\) and \((q - 1)(q - p^u + 1)\) codewords in \(U_i\) having weight \(p^v - 1\) and \(p^v\) respectively. Let \(c \in U_i\) be a non-zero codeword. Then there exist \(\alpha_1, \alpha_2 \in \mathbb{F}_q\), not both zero, such that
\[ c = \alpha_1 \mathfrak{M}_i + \alpha_2 \mathfrak{M}_{i+p^r - u} \]
\[ = \alpha_1 b_0 e_i + \alpha_2 b_{p^u - 2} e_{i+(p^u - 1)p^r - u} + \sum_{j=1}^{p^u - 2} (\alpha_1 b_j + \alpha_2 b_{j-1}) e_{i+jp^r - u}. \]

**Case I.** One of the \(\alpha_1\) or \(\alpha_2\) is zero.

If \(\alpha_1 = 0\), then \(wt(c) = wt(\mathfrak{M}_{i+p^r - u}) = p^v - 1\). Similarly, if \(\alpha_2 = 0\), then \(wt(c) = wt(\mathfrak{M}_i) = p^v - 1\). Note that there are a total of \(2(q - 1)\) such codewords in \(U_i\).
Case II. Both $\alpha_1$ and $\alpha_2$ are non-zero.

We assert that among the possible non-zero entries $\alpha_1b_0$, $\alpha_1b_j + \alpha_2b_{j-1}$ ($1 \leq j \leq p^u - 2$), $\alpha_2b_{p^u-2}$ of $c$, at most one of the entries can be zero.

Clearly, $\alpha_1b_0$ and $\alpha_2b_{p^u-2}$ can’t be zero. If $\alpha_1b_j + \alpha_2b_{j-1} = 0$ and $\alpha_1b_k + \alpha_2b_{k-1} = 0$ for some $j, k$, $1 \leq j < k < p^u - 2$, then $\alpha_1(b_j - b_{j-1}) + \alpha_2(b_{k-1} - b_{j-1}) = 0$. But, using (6), we have $b_jb_{k-1} - b_kb_{j-1} = b_{k-j-1}$, which gives $\alpha_1b_{k-j-1} = 0$. This gives a contradiction, since both $\alpha_1$ and $b_{k-j-1}$ are non-zero. This proves our assertion.

As a consequence of the assertion, the weight of $c$ is either $p^u$ or $p^u - 1$. However $\text{wt}(c) = p^u - 1$ if and only if $\alpha_2 = -\alpha_1b_jb_{j-1}^{-1}$ for some $j, 1 \leq j \leq p^u - 2$. Since $-\alpha_1b_1b_0^{-1}$, $-\alpha_1b_2b_1^{-1}$, ..., $-\alpha_1b_{p^u-2}b_{p^u-3}$ are all distinct, we get that, for each choice of $\alpha_1$, there are $p^u - 2$ choices of $\alpha_2$. Hence there are $(q - 1)(p^u - 2)$ codewords $c$ having weight $p^u - 1$ with $\alpha_1$ and $\alpha_2$ both non-zero. The remaining $(q - 1)^2 - (q - 1)(p^u - 2)$ codewords have weight $p^u$.

Combining the two cases, the result follows. \hfill $\Box$

**Proof of Theorem 4.** Let $w \geq 0$. For any tuple $(w_1, w_2, \ldots, w_{p^u-1})$ of non-negative integers $w_i$’s satisfying $\sum_{i=1}^{p^u-1} w_i = w$, define

$$S(w_1, w_2, \ldots, w_{p^u-1}) = \left\{ \sum_{i=1}^{p^u-1} c_i \mid c_i \in U_1, \text{ wt}(c_i) = w_i, 1 \leq i \leq p^u-1 \right\}.$$  

It follows from Lemma 7 and the definition of $U_i$’s that $\bigcup_{i=1}^{p^u-1} S(w_1, w_2, \ldots, w_{p^u-1})$ is precisely the set of all the elements in $M_i(p^u)$ having weight $w$, where the union runs over all tuples $(w_1, w_2, \ldots, w_{p^u-1})$ of non-negative integers $w_i$’s satisfying $\sum_{i=1}^{p^u-1} w_i = w$. It is easily seen that the union is disjoint. Therefore,

$$A_{w}^{(p^u)} = \left| \bigcup_{i=1}^{p^u-1} S(w_1, w_2, \ldots, w_{p^u-1}) \right| = \sum_{i=1}^{p^u-1} |S(w_1, w_2, \ldots, w_{p^u-1})|.$$  

But $|S(w_1, w_2, \ldots, w_{p^u-1})| = N_1(w_1)N_2(w_2)\cdots N_{p^u-1}(w_{p^u-1})$, where $N_i(w_i)$ is the number of codewords in $U_i$ having weight $w_i$. However, by Lemma 8, $N_i(w_i)$ equals $n(w_i)$ for all $i$, which completes the proof. \hfill $\Box$

**4. Some examples**

In this section, we determine the weight distribution of the ternary irreducible cyclic codes $M_1^{(25)}$ and $M_1^{(49)}$, 7-ary irreducible cyclic code $M_1^{(2)}$ ($r \geq 1$), binary irreducible cyclic code $M_1^{(9)}$ and the quaternary code $M_1^{(25)}$.

**4.1. Example 1**

Let $p = 5$, $r = 2$ and $q = 3$. As the multiplicative order of 3 modulo 25 is $\phi(25)$, we apply Theorem 2 to compute the weight distribution $A_1^{(25)}, A_1^{(2)}, \ldots, A_1^{(25)}$ of the ternary code $M_1^{(25)}$. For this purpose, we first compute the numbers $N(v)$, $v \geq 0$. By Definition 1, $N(0) = 1$ and $N(v) = 0$ if $v = 1$ or $v \geq 6$. We now compute $N(2), N(3), N(4)$ and $N(5)$. In this case, by (1), we have

$$a(\ell_1) = 4 - \ell_1 \quad \text{and} \quad a(\ell_1, \ell_2) = \frac{(2 - \ell_1 - \ell_2)(3 - \ell_1 - \ell_2)}{2}.$$
Therefore,

\[
N(2) = \sum_{\ell_1=0}^{3} A(2; \ell_1) = \sum_{\ell_1=0}^{3} a(\ell_1) \left( \begin{array}{c} \ell_1 \\ 0 \end{array} \right) (q - 1) = 20,
\]

\[
N(3) = \sum_{\ell_1=1}^{3} A(3; \ell_1) = \sum_{\ell_1=1}^{3} a(\ell_1) \left( \begin{array}{c} \ell_1 \\ 1 \end{array} \right) (q - 1) = 20,
\]

\[
N(4) = \sum_{\ell_1=2}^{3} A(4; \ell_1) + \sum_{\ell_1 \geq 0, \ell_2 \geq 0} A(2, 2; \ell_1, \ell_2)
= \sum_{\ell_1=1}^{3} a(\ell_1) \left( \begin{array}{c} \ell_1 \\ 2 \end{array} \right) (q - 1) + \sum_{\ell_1 \geq 0, \ell_2 \geq 0} a(\ell_1, \ell_2) \left( \begin{array}{c} \ell_1 \\ 0 \end{array} \right) \left( \begin{array}{c} \ell_2 \\ 0 \end{array} \right) (q - 1)^2 = 30,
\]

\[
N(5) = \sum_{\ell_1} A(5; \ell_1) + \sum_{\ell_1 \geq 0, \ell_2 \geq 1} A(2, 3; \ell_1, \ell_2) + \sum_{\ell_1 \geq 1, \ell_2 \geq 0} A(3, 2; \ell_1, \ell_2)
= a_3(q - 1) + a_{0,1}(q - 1)^2 + a_{1,0}(q - 1)^2 = 10.
\]

Now Theorem 1 gives the weight distribution of the ternary irreducible cyclic code \( M^{(25)}_1 \):

\[
A_0^{(25)} = N(0) = 1,
\]

\[
A_1^{(25)} = 0,
\]

\[
A_2^{(25)} = \frac{5!}{4!} N(2) = 100,
\]

\[
A_3^{(25)} = \frac{5!}{4!} N(3) = 100,
\]

\[
A_4^{(25)} = \frac{5!}{4!} N(4) + \frac{5!}{2!3!} N(2)^2 = 4150,
\]

\[
A_5^{(25)} = \frac{5!}{4!} N(5) + \frac{5!}{3!} N(2)N(3) = 8050,
\]

\[
A_6^{(25)} = \frac{5!}{3!} N(2)N(4) + \frac{5!}{2!3!} N(3)^2 + \frac{5!}{2!3!} N(2)^3 = 96000,
\]

\[
A_7^{(25)} = \frac{5!}{3!} N(2)N(5) + \frac{5!}{3!} N(3)N(4) + \frac{5!}{2!2!} N(2)^2N(3) = 256000,
\]

\[
A_8^{(25)} = \frac{5!}{3!} N(3)N(5) + \frac{5!}{2!3!} N(4)^2 + \frac{5!}{2!2!} N(2)N(4) + \frac{5!}{2!2!} N(2)N(3)^2 + \frac{5!}{3!} N(2)^4
= 1413000,
\]

\[
A_9^{(25)} = \frac{5!}{3!} N(4)N(5) + \frac{5!}{2!2!} N(2)^2N(5) + \frac{5!}{2!} N(2)N(3)N(4) + \frac{5!}{2!3!} N(3)^3
+ \frac{5!}{3!} N(2)^3N(3) = 4126000,
\]
\[ A_{10}^{(25)} = \frac{5!}{2!3!} N(5)^2 + \frac{5!}{2!} N(2) N(3) N(5) + \frac{5!}{2!2!} N(2) N(4)^2 + \frac{5!}{2!2!} N(3)^2 N(4) \\
+ \frac{5!}{3!} N(2) N(4) + \frac{5!}{2!2!} N(2) N(3)^2 + \frac{5!}{5!} N(2)^5 = 13941000, \]

\[ A_{11}^{(25)} = \frac{5!}{2!} N(2) N(4) N(5) + \frac{5!}{2!2!} N(3) N(5)^2 + \frac{5!}{3!} N(2) N(5) + \frac{5!}{2!2!} \frac{N(3) N(4)^2}{N(2)} \\
+ \frac{5!}{2!2!} N(2)^2 N(3) N(4) + \frac{5!}{3!} N(2) + \frac{5!}{4!} N(2)^4 N(3) = 36220000, \]

\[ A_{12}^{(25)} = \frac{5!}{2!2!} N(2) N(5)^2 + \frac{5!}{2!} N(3) N(4) N(5) + \frac{5!}{2!2!} N(2) N(3) N(5) + \frac{5!}{2!2!} N(4)^3 \\
+ \frac{5!}{2!2!} N(2) N(4) + \frac{5!}{2!} N(2) N(3) N(4) + \frac{5!}{4!} N(2)^4 N(4) + \frac{5!}{4!} N(3)^4 \\
+ \frac{5!}{2!3!} N(2) N(3) N(4) = 87490000, \]

\[ A_{13}^{(25)} = \frac{5!}{3!2!} N(3) N(5)^2 + \frac{5!}{2!2!} N(2) N(4)^2 + \frac{5!}{2!2!} N(2) N(3) N(4) N(5) + \frac{5!}{3!} N(3) N(5)^2 \\
+ \frac{5!}{3!} N(2) N(3) N(5) + \frac{5!}{3!} N(2) N(4)^3 + \frac{5!}{2!2!} N(3) N(4)^2 + \frac{5!}{2!3!} N(2)^3 N(4) \\
+ \frac{5!}{2!2!} N(2) N(3)^2 N(4) + \frac{5!}{4!} N(2) N(3) N(4)^4 = 302890000, \]

\[ A_{14}^{(25)} = \frac{5!}{2!3!} N(5)^3 + \frac{5!}{2!} N(2) N(3) N(5)^2 + \frac{5!}{2!} N(2) N(4)^2 N(5) + \frac{5!}{2!} N(3) N(4)^2 N(5) \\
+ \frac{5!}{3!} N(2) N(4) N(5) + \frac{5!}{2!2!} N(2)^2 N(3) N(4) + \frac{5!}{3!} N(3) N(4)^3 \\
+ \frac{5!}{2!2!} N(2) N(3) N(4)^2 + \frac{5!}{3!} N(2) + \frac{5!}{3!} N(3) N(3)^3 N(4) + N(3)^5 = 442410000, \]

\[ A_{15}^{(25)} = \frac{5!}{2!} N(2) N(4) N(5)^2 + \frac{5!}{2!2!} N(3) N(5)^2 + \frac{5!}{2!2!} N(2) N(3) N(4)^2 N(5) \\
+ \frac{5!}{2!2!} N(2) N(3) N(4) N(5) + \frac{5!}{3!} N(2) N(3) N(5) + \frac{5!}{4!} N(4) + \frac{5!}{2!3!} N(2)^2 N(4)^3 \\
+ \frac{5!}{2!2!} N(2) N(3)^2 N(4)^2 + \frac{5!}{4!} N(3)^4 N(4) = 551650000, \]

\[ A_{16}^{(25)} = \frac{5!}{3!} N(2) N(3) N(4) N(5)^2 + \frac{5!}{2!} N(3) N(5)^2 + \frac{5!}{2!2!} N(2) N(3) N(4)^2 N(5) \\
+ \frac{5!}{2!} N(2) N(3) N(4) N(5) + \frac{5!}{3!} N(2) N(3)^2 N(5) + \frac{5!}{4!} N(4) + \frac{5!}{2!3!} N(2)^2 N(4)^3 \\
+ \frac{5!}{2!2!} N(2) N(3)^2 N(4)^2 + \frac{5!}{4!} N(3)^4 N(4) = 581400000, \]
which is a power of 3, we apply Theorem 3 to compute the weight distribution of 7-ary irreducible
in order to compute the weight distribution of the binary irreducible cyclic code

4.4. Example 4

Let \( p = 3 \), \( r = 2 \) and \( q = 7 \). As the multiplicative order of 7 modulo \( 3^m \) is \( 3^{m-1} \),
which is a power of 3, we apply Theorem 3 to compute the weight distribution of 7-ary irreducible
cyclic code \( \mathcal{M}_1(7) \). Note that \( d = m - 1 \) in this case. By Theorem 3, we see that the only possible
non-zero weight in \( \mathcal{M}_1(7) \) is 3, which is attained by all its 6 non-zero codewords. If \( r \geq 2 \), the weight
distribution of \( \mathcal{M}_1(7) \) is given by

\[
A^{(25)}_{18} = \frac{5!}{3!} N(3)N(5)^3 + \frac{5!}{2!} N(4)^2 N(5)^2 + \frac{5!}{2!} N(2)^2 N(4)N(5)^3 + \frac{5!}{2!} N(2)^2 N(3)^2 N(5)^2
\]

\[
+ \frac{5!}{2!} N(2)N(3)N(4)^2 N(5) + \frac{5!}{3!} N(3)^3 N(4)N(5) + \frac{5!}{4!} N(2)N(4)^4
\]

\[
+ \frac{5!}{2!} N(3)^2 N(4)^3 = 516 000 000,
\]

\[
A^{(25)}_{19} = \frac{5!}{3!} N(4)(5)^3 + \frac{5!}{2!} N(2)^2 N(5)^3 + \frac{5!}{2!} N(2)N(3)N(4)N(5)^2 + \frac{5!}{2!} N(3)^3 N(5)^2
\]

\[
+ \frac{5!}{3!} N(2)N(4)^3 N(5) + \frac{5!}{2!} N(3)^2 N(4)^2 N(5) + \frac{5!}{4!} N(3)N(4)^4 = 381 600 000,
\]

\[
A^{(25)}_{20} = \frac{5!}{4!} N(5)^4 + \frac{5!}{3!} N(2)N(3)N(5)^3 + \frac{5!}{2!} N(2)N(4)^2 N(5)^2 + \frac{5!}{2!} N(3)^2 N(4)N(5)^2
\]

\[
+ \frac{5!}{3!} N(3)N(4)^3 N(5) + N(4)^5 = 230 350 000,
\]

\[
A^{(25)}_{21} = \frac{5!}{3!} N(2)N(4)(5)^3 + \frac{5!}{2!} N(3)^2 N(5)^3 + \frac{5!}{2!} N(2)N(4)^2 N(5)^2 + \frac{5!}{2!} N(3)^2 N(4)N(5)^2
\]

\[
= 110 500 000,
\]

\[
A^{(25)}_{22} = \frac{5!}{4!} N(2)N(5)^4 + \frac{5!}{3!} N(3)N(4)N(5)^3 + \frac{5!}{2!} N(4)^3 N(5)^2 = 40 000 000,
\]

\[
A^{(25)}_{23} = \frac{5!}{4!} N(3)N(5)^4 + \frac{5!}{2!} N(4)^2 N(5)^3 = 10 000 000,
\]

\[
A^{(25)}_{24} = \frac{5!}{4!} N(4)(5)^4 = 1 500 000,
\]

\[
A^{(25)}_{25} = N(5)^5 = 100 000.
\]

4.2. Example 2

Let \( p = 3 \), \( r = 2 \) be a positive integer and \( q = 7 \). As the multiplicative order of 7 modulo \( 3^m \) is \( 3^{m-1} \),
which is a power of 3, we apply Theorem 3 to compute the weight distribution of 7-ary irreducible
cyclic code \( \mathcal{M}_1(7) \). Note that \( d = m - 1 \) in this case. By Theorem 3, we see that the only possible
non-zero weight in \( \mathcal{M}_1(7) \) is 3, which is attained by all its 6 non-zero codewords. If \( r \geq 2 \), the weight
distribution of \( \mathcal{M}_1(7) \) is given by

\[
A^{(25)}_1 = \begin{cases} 
0 & \text{if } 3 \text{ does not divide } i, \\
\left(\frac{3^{r-1}}{j}\right)(q-1)^j & \text{if } i = 3j, \ 0 \leq j \leq 3^{r-1}.
\end{cases}
\]

4.3. Example 3

Let \( p = 7 \), \( r = 2 \) and \( q = 3 \). The multiplicative order of 3 modulo 49 is \( \phi(49) \). Working as in
Example 1, we obtain the weight distribution of the ternary code \( \mathcal{M}_1(49) \), which is given by Table 1.

4.4. Example 4

Let \( p = 3 \), \( r = 2 \) and \( q = 2 \). Here the multiplicative order of 2 modulo \( 3^m \) is \( 2 \cdot 3^{m-1} \). Therefore
in order to compute the weight distribution of the binary irreducible cyclic code \( \mathcal{M}_1(3) \), we apply
Theorem 4. Note that \( u = 1 \) in this case. By Theorem 4, the weight distribution \( A_i^{(9)} \), \( 0 \leq w \leq 9 \), of the binary code \( M_1^{(9)} \) is given by

\[
A_i^{(9)} = \sum \binom{w_1}{n} \binom{w_2}{n} \binom{w_3}{n},
\]

where the summation runs over all tuples \( (w_1, w_2, w_3) \) of integers \( w_i \)'s satisfying \( w_1 + w_2 + w_3 = w \), \( w_i \geq 0 \) for each \( i \), and

\[
n(w_i) = \begin{cases} 
1 & \text{if } w_i = 0, \\
3 & \text{if } w_i = 2, \\
0 & \text{otherwise}.
\end{cases}
\]

After a little calculation, we see that \( A_0^{(9)} = 1 \), \( A_2^{(9)} = \frac{3}{2} \binom{2}{2} \) \( = 9 \), \( A_4^{(9)} = \frac{3}{2} \binom{2}{2}^2 = 27 \), \( A_6^{(9)} = \binom{2}{2}^3 = 27 \) and \( A_1^{(9)} = A_3^{(9)} = A_5^{(9)} = A_7^{(9)} = A_8^{(9)} = A_9^{(9)} = 0 \). (Note that as the multiplicative order of 2 modulo \( 3^m \) is \( \phi(3^m) \), we can also compute the weight distribution of \( M_1^{(9)} \) using Theorem 2.)

4.5. Example 5

Let \( p = 5 \), \( r = 2 \) and \( q = 4 \). The multiplicative order of 4 modulo \( 5^m \) is \( 2 \cdot 5^{m-1} \). To compute the weight distribution of the quaternary irreducible cyclic code \( M_1^{(25)} \), we apply Theorem 4. Note that \( u = 1 \) in this case. By Theorem 4, the weight distribution \( A_w^{(25)} \), \( 0 \leq w \leq 25 \), of the quaternary code \( M_1^{(25)} \) is given by

\[
A_w^{(25)} = \sum n(w_1)n(w_2)n(w_3)n(w_4)n(w_5),
\]
where the summation runs over all tuples \((w_1, w_2, w_3, w_4, w_5)\) of integers \(w_i\)'s satisfying \(w_1 + w_2 + w_3 + w_4 + w_5 = w\), \(w_i \geq 0\) for each \(i\), and

\[
n(w_i) = \begin{cases} 
1 & \text{if } w_i = 0, \\
15 & \text{if } w_i = 4, \\
0 & \text{otherwise}.
\end{cases}
\]

This gives \(A_{25}^{(0)} = 1\), \(A_{25}^{(4)} = \frac{5!}{4!} n(4) = 75\), \(A_{25}^{(8)} = \frac{5!}{2!3!} n(4)^2 = 2250\), \(A_{25}^{(12)} = \frac{5!}{2!3!} n(4)^3 = 33750\), \(A_{25}^{(16)} = \frac{5!}{4!} n(4)^4 = 253125\), \(A_{25}^{(20)} = n(4)^5 = 759375\), and the remaining \(A_{w_5}^{(25)}\)'s are equal to zero.

**Acknowledgments**

The authors are grateful to the anonymous referees for their comments and suggestions which helped to write the paper in the present form.

**References**