International Journal of Statistics and Applied Mathematics

ISSN: 2456-1452
Maths 2023; 8(4): 01-07

https://www.mathsjournal.com
Received: 03-02-2023
Accepted: 10-03-2023

Inderjit Singh
Department of Mathematics, Dayanand P.G. College, Hisar, Haryana, India

Seema Rani
Department of Mathematics, FGM Govt. College, Adampur Hisar, Haryana, India

Ranjeet Singh
Department of Mathematics, Govt. College, Siwani Bhiwani, Haryana, India

Corresponding Author:
Inderjit Singh
Department of Mathematics, Dayanand P.G. College, Hisar, Haryana, India

Weight distribution of irreducible cyclic codes of length $2p^m$

Inderjit Singh, Seema Rani and Ranjeet Singh

Abstract
Let F_q be the finite field with q elements, p, q be two odd primes with gcd(p, q) = 1. Let q be primitive root modulo $2p^m$, $m \geqslant 1$ be an integer. In this paper, we obtain weight distribution of all the irreducible cyclic codes of length $2p^m$ over F_q by using their generating polynomials.
Mathematics Subject Classification (2020) 11A03; 15A07; 11R09; 11T 06; 11T 22; 11T 71; 94B05; 94B15.

Keywords: Generating polynomials, primititve root, weight distribution

1. Introduction

Let F_q be the finite field with q elements, n be a positive integer with $\gcd(n, q) = 1$. By Wedderburn Artin Theorem every semi-simple ring can be written as direct sum of its minimal ideals. Each minimal ideal of R_n represents an irreducible cyclic code of length n under the 1-1 correspondence $c_0 + c_1x + \ldots + c_{n-1}x^{n-1} \longrightarrow (c_0, c_1, \ldots, c_{n-1})$.We also know that every cyclic code of length n with digits in finite field F_q forms a vector space having q^n elements. Thus we denote a cyclic code of length n over F_q by F^n. A minimal ideal in R_n is called an irreducible cyclic code of length n over F_q. If is an irreducible cyclic code of length n over F_q and v, then the weight of v is defined to be the number of non-zero entries in v. We denote it by $wt(v)$. If $A^{(n)}$ denotes the number of codewords of weight w in C, then $A^{(n)}$, $A^{(n)}$, . . . , $A^{(n)}$ is called weight distribution of C. The weight distribution of irreducible cyclic code is important due to its application in error detection and correction of codes. Thus the problem of determining the weight distribution of a code is of much interest. Many authors have worked on this problem for a long time. Ding [4] determined the weight distribution q-arry irreducible cyclic codes of length n provided $2 \leqslant \frac{q^t-1}{n} \leqslant$ where $t = O_n(q)$ (the multiplicative order of q modulo n) Sharma, Bakshi and Raka [2] determined the weight distribution of all ir-reducible cyclic codes of length 2^m over F_q. In [1], Sharma and Bakshi have obtained the weight distribution of some irreducible cyclic codes of length p^m where p is an odd prime co-prime to q and $m \geqslant 1$ is an integer.Further Kumar *et al.* [17, 18] have obtained weight distribution of some irreducible cyclic codesof length p^m, $2p^m$ and n by different technique.Apart from this Batra and Arora [8], have discussed the generating polynomial and minimum distanceof some cyclic codes of length $2p^n$.

In this paper, we determine the weight distribution of all irreducible cyclic codes of length $2p^m$ over F_q, where q is primitive root modulo p^m and p is anodd prime such that $gcd(2p, q) = 1$ and $m \geqslant 1$ is an integer.

2. Cyclotomic Cosets Modulo $2p^m$

Let $S = \{0, 1, 2, \ldots, 2p^m - 1\}$. For $a, b \in S$, say that $a \sim b$ if $a \cong bq^i (\text{mod } 2p^m)$ for some integer $i \geq 0$. This defines an equivalence relation on the set S. The equivalence classes due to this relation are called q −cyclotomic cosets modulo $2p^m$. The q – cyclotomic coset containing $s \in S$ is denoted by $C_s = \{s, sq, sq^2, \ldots, sq^{t_s-1}\}$, where t_s is the least positive integer such that $sq^{t_s} \equiv s \text{ (mod } 2p^m)$ and $|C_s|$ denotes the cardinality of C_s.

In this section, we describe the q −cyclotomic cosets modulo $2p^m$, where p and q are distinct odd primes and $o(q)_{2p^m} = \frac{\varphi(2p^m)}{d}$, d is a positive integer and φ is Euler's phi-function.

2.1. Theorem If p and q are odd primes such that $o(q)_{2p^m} = \varphi(2p^m)/d$, d is a positive integer, then $2(md+1)$ q- cyclotomic cosets (mod $2p^m$) are given by

(i) $C_0 = \{0\}$,

(ii) $C_{p^m} = \{p^m\}$.

(iii)

For $0 \leq j \leq m{-}1$, $0 \leq k \leq d{-}1$,

(iii) $C_{g^k p^j} = \{g^k p^j, g^k p^j q, g^k p^j q^2, \ldots, g^k p^j q^{\frac{\varphi(2p^{m-j})}{d}-1}\}$,

(iv) $C_{2g^k p^j} = \{2g^k p^j, 2g^k p^j q, 2g^k p^j q^2, \ldots, 2g^k p^j q^{\frac{\varphi(2p^{m-j})}{d}-1}\}$, where g is primitive root modulo $2p^m$.

Proof. Trivial.

3. Weight Distribution of Minimal Cyclic Codes of Length $2p^m$

Definition 3.1. Let α be the primitive $2p^m$th root of unity in some extension of F_q . Then corresponding to the $q-$ cyclotomic coset C_s, $M_s^{(n)}(x) = \prod_{j \in C_s}(x - \alpha^j)$,

is called **minimal polynomial** of α^s over F_q .

Definition 3.2 Let $\mathbb{M}_s^{(2p^m)}$ be the minimal cyclic code of length $2p^m$ over F_q. It is well known that $\mathbb{M}_s^{(2p^m)}$ is the ideal in R_{2p^m} generated by $g(x) = \frac{x^{2p^m}-1}{M_s^{2p^m}(x)}$. Then $g(x)$ is called the generating polynomial of $\mathbb{M}_s^{(2p^m)}$.

Remark 3.3 If $C_{s_1}, C_{s_2}, \ldots, C_{s_k}$ are all the distinct $q-$ cyclotomic cosets modulo $2p^m$, then $\mathbb{M}_{s_1}^{(2p^m)}, \mathbb{M}_{s_2}^{(2p^m)}, \ldots, \mathbb{M}_{s_k}^{(2p^m)}$ are precisely all the distinct minimal cyclic codes of length $2p^m$ over F_q.

Theorem 3.4 Let F_q be the finite field with q elements, p, q be two odd primes with gcd$(p, q) = 1$ and $m \geq 1$ be an integer. Let the multiplicative order of q modulo $2p^m$ is $\varphi(2p^m)$. Then

(i) The codes $\mathbb{M}_0^{(2p^m)}, \mathbb{M}_{p^m}^{(2p^m)}, \mathbb{M}_{g^k p^j}^{(2p^m)}$ and $\mathbb{M}_{2g^k p^j}^{(2p^m)}$, $0 \leq j \leq m-1, 0 \leq k \leq d-1$, are precisely all the distinct minimal cyclic codes of length $2p^m$ over F_q, where φ denote the Euler's Phi function.

(ii) All the nonzero codewords in $\mathbb{M}_0^{(2p^m)}$ and $\mathbb{M}_{p^m}^{(2p^m)}$ have weight $2p^m$.

(iii) The codes $\mathbb{M}_{g^k p^j}^{(2p^m)}$ and $\mathbb{M}_{2g^k p^j}^{(2p^m)}$ are equivalent to $\mathbb{M}_{p^j}^{(2p^m)}$ and $\mathbb{M}_{2p^j}^{(2p^m)}$ respectively, therefore they have same weight distribution.

Proof. (i) By Theorem 2.1, C_0, C_{p^m}, $C_{g^k p^j}$ and $C_{2g^k p^j}$ are all distinct $q-$ cyclotomic cyclotomic cosets modulo $2p^m$. Therefore, by Remark 4.3.3 $\mathbb{M}_0^{(2p^m)}, \mathbb{M}_{p^m}^{(2p^m)}, \mathbb{M}_{g^k p^j}^{(2p^m)}$ and $\mathbb{M}_{2g^k p^j}^{(2p^m)}$, $0 \leq j \leq m-1, 0 \leq k \leq d-1$, are all the distinct minimal cyclic codes of length $2p^m$ over F_q.

(ii) By Definition 3.1, $x - 1$ is minimal polynomial of $\mathbb{M}_0^{(2p^m)}$, therefore by Definition 3.2,

$\frac{x^{2p^m}-1}{x-1} = 1 + x + x^2 + \cdots + x^{2p^m-1}$. is the generating polynomial of $\mathbb{M}_0^{(2p^m)}$.

Thus every non− zero codeword in $\mathbb{M}_0^{(2p^m)}$ has weight $2p^m$. Now, $\mathbb{M}_{p^m}^{(2p^m)}$ is the minimal cyclic code corresponding to $q-$ cyclotomic coset C_{p^m}. Then by Definition 3.1, the minimal polynomial of α^{p^m} is $x - \alpha^{p^m}$, where α is primitive $2p^m$th root of unity. Then, $\alpha^{p^m} = -1$.

By Definition 3.2, the generating polynomial of $\mathbb{M}_{p^m}^{(2p^m)}$ is

$$\frac{x^{2p^m}-1}{x+1} = -1 + x - x^2 + \cdots + x^{2p^m-1}.$$

Thus every non−zero codeword in $\mathbb{M}_{p^m}^{(2p^m)}$ has weight $2p^m$.

Theorem 3.5 (i) Let $1 \leq j \leq m$. The minimal cyclic code $\mathbb{M}_{p^{m-j}}^{(2p^m)}$ is the repetition code of the minimal cyclic code $\mathbb{M}_1^{(2p^j)}$ of length $2p^j$ corresponding to the $q-$ cyclotomic coset containing 1, repeated p^{m-j} times.

(ii) Let $w \geq 0$, then

$$A_w^{(2p^m)} = \begin{cases} 0, \text{if } p^j \text{ does not divide } w; \\ A_{w'}^{2p^{m-j}}, \text{if } w = 2p^j w', 0 \leq w' \leq 2p^{(m-j)}, \end{cases}$$

where $A_w^{2p^m}$ and $A_{w'}^{2p^{m-j}}$ denote the weight distribution of $\mathbb{M}_{p^j}^{(2p^m)}$ and $\mathbb{M}_1^{(2p^{m-j})}$ respectively.

Proof. Let α be the fixed $2p^m$th root of unity. By definition 3.2, the generating polynomial polynomial of $\mathbb{M}_{p^{m-j}}^{(2p^m)}$ is $\frac{x^{2p^m}-1}{M_{p^{m-j}}^{2p^m}(x)}$, where $M_{p^{m-j}}^{2p^m}(x) = \prod_{s \in C_{p^{m-j}}}(x-\alpha^s)$ and $C_{p^{m-j}}$ is cyclotomic coset modulo $2p^m$.

Now, $\frac{x^{2p^m}-1}{M_{p^{m-j}}^{2p^m}(x)} = \frac{(x^{2p^j}-1)}{\prod_{s \in C_{p^{m-j}}}(x-\alpha^s)}\left(1 + x^{2p^j} + x^{4p^j} + \cdots + x^{(p^{m-j}-1)2p^j}\right)$.

For any $s \in C_{p^{m-j}}$, α^s are roots of $x^{2p^j} - 1$.
Consequently, $\prod_{s \in C_{p^{m-j}}}(x-\alpha^s)$ is an irreducible factor of $x^{2p^j} - 1$.
It is clear that, $\prod_{s \in C_{p^{m-j}}}(x-\alpha^s) = \prod_{s=0}^{\varphi(p^j)-1}\left(x - \alpha^{p^{m-j}l^s}\right)$. Let $\alpha^{p^{m-j}} = \beta$, then $\prod_{s=0}^{\varphi(p^j)-1}\left(x - \alpha^{p^{m-j}l^s}\right) = \prod_{s=0}^{\varphi(p^j)-1}(x - \beta^{l^s})$, where β is the $2p^j$th root of unity Similarly, the generating polynomial of $\mathbb{M}_1^{(2p^j)}$ is $\frac{x^{2p^j}-1}{M_1^{2p^j}(x)}$, where $M_1^{2p^j}(x) = \prod_{s \in C_1}(x-\beta^s)$, where β is the $2p^j$th root of unity Also, $\prod_{s \in C_1}(x-\beta^s) = \prod_{s=0}^{\varphi(2p^j)-1}(x-\beta^{l^s})$, where C_1 is cyclotomic coset modulo $2p^j$. Consequently, $\prod_{s \in C_{2p^{m-j}}}(x-\alpha^s) = \prod_{s \in C_1}(x-\beta^s)$.
By the above discussion and Lemma 4.1, $\mathbb{M}_{2p^{m-j}}^{(2p^m)}$ is the repetition code of the minimal cyclic code $\mathbb{M}_1^{(2p^j)}$ of length $2p^j$ corresponding to the $q-$ cyclotomic coset containing 1, repeated p^{m-j} times.

4. Weight Distribution of $\mathbb{M}_1^{(2p^r)}(1 \leq r \leq m)$
Case (i) The multiplicative order of q modulo $2p^m$ is $\varphi(2p^m)$.
Lemma 4.1. If the multiplicative order of q modulo $2p^m$ is $\varphi(2p^m)$, then the generating polynomial of $\mathbb{M}_1^{(2p^r)}$ is $x^{p^{r-1}(p+1)} + x^{p^r} - x^{p^{r-1}} - 1$ and the vectors $e_{i+p^{r-1}(p+1)} + e_{i+p^r} - e_{i+p^{r-1}} - e_i, 1 \leq i \leq p^{r-1}(p-1)$ or $1 \leq i \leq \varphi(2p^r)$, constitute a basis of $\mathbb{M}_1^{(2p^r)}$ over F_q.
Proof. As multiplicative order of q modulo $2p^m$ is $\varphi(2p^m)$, therefore multiplicative order of q modulo $2p^r$ is $\varphi(2p^r)$, for $1 \leq r \leq m$.
Hence the $q-$ cyclotomic coset modulo $2p^r$ containing 1 is
$C_1 = \{1, q, q^2, \ldots, q^{\varphi(2p^r)-1}\}$.
This is a reduced residue system modulo $2p^r$. Let α be a primitive $2p^r$th root of unity.
By Definition 3.2, the generating polynomial $g(x)$ of $\mathbb{M}_1^{(2p^r)}$ is $\frac{x^{2p^r}-1}{M_1^{2p^r}(x)}$, where $M_1^{2p^r}(x) = \prod_{\alpha \in C_1}(x-\alpha^j)$.

Now, we assert that $M_1^{2p^r}(x) = \frac{x^{2p^r}-1}{(x^{p^{r-1}}+1)(x^{p^r}-1)}$.
If α is primitive $2p^r$th root of unity, then α^j is again primitive $2p^r$th root of unity for each $j \in C_1$.Since α is $2p^r$th root of unity, therefore $\alpha^{p^r} \neq 1$. So, α is a root of $(x^{p^r}+1)$.Thus,

$$x^{2p^r} - 1 = (x^{p^r}-1)(x^{p^{r-1}}+1)(1 - x^{p^{r-1}} + x^{2p^{r-1}} - \cdots + x^{(p-1)p^{r-1}}).$$

Consequently, $M_1^{2p^r}(x) = (1 - x^{p^{r-1}} + x^{2p^{r-1}} - \cdots + x^{(p-1)p^{r-1}})$.
Hence, $g(x) = (x^{p^r}-1)(x^{p^{r-1}}+1) = x^{p^{r-1}(p+1)} + x^{p^r} - x^{p^{r-1}} - 1$.
So $\mathbb{M}_1^{(2p^r)}$ is the subspace of R_{2p^r} spanned by $g(x), xg(x), \ldots, x^{(p-1)p^{r-1}-1}g(x)$.
But under the standard isomorphism $x^{i-1} \to e_i$ from R_{2p^r} to $F_q^{2p^r}$, $x^{i-1}g(x)$ corresponding to $e_{i+p^{r-1}(p+1)} + e_{i+p^r} - e_{i+p^{r-1}} - e_i$ for each i.

Remark 4.2
Let V_i be the vector subspaces of $F_q^{2p^r}$ spanned by

$e_{i+p^r+jp^{r-1}} + e_{i+p^r+(j-1)p^{r-1}} - e_{i+jp^{r-1}} - e_{i+(j-1)p^{r-1}}$ for $1 \leq i \leq p^{r-1}$ and $1 \leq j \leq p-1$. Then by the above lemma, $\mathbb{M}_1^{(2p^r)} \cong V_1 \oplus V_2 \oplus \ldots \oplus V_{p^{r-1}}$.

Definition 4.3 A vector $v \in V_i$ is called basic vector if $v = \sum_{j=k}^{k+l} \alpha_j \left(e_{i+p^r+jp^{r-1}} + e_{i+p^r+(j-1)p^{r-1}} - e_{i+jp^{r-1}} - e_{i+(j-1)p^{r-1}}\right)$, where $0 \neq \alpha_j \in F_q, k \geq 1, l \geq 0, k+l \leq p-1$. The integer l is called the length of v denoted by $l(v)$, k is called initial point of v, denoted by $I(v)$ and $k+l$ is called the end point of v denoted by $E(v)$.

Definition 4.4.4. Let $v_1, v_2, \dots, v_t \in V_i$. We say that $v_1, v_2, \dots, v_t$ is a chain in V_i if each v_j, $1 \leq j \leq t$, is a basic vector and $I(v_j) \geq E(v_{j-1}) + 2$ for $2 \leq j \leq t$. Note that each vector $v \in V_i$ can be written as the sum of $v_1, v_2, \dots, v_t$ and $wt\left(\sum_{j=1}^{t} v_j\right) = \sum_{j=1}^{t} wt(v_j)$.

Remark 4.5. Any $v \in V_i$ can be written as $v = \sum_{j=1}^{t} v_j$, where $v_1, v_2, \dots, v_t$ is a chain in V_i and $wt\left(\sum_{j=1}^{t} v_j\right) = \sum_{j=1}^{t} wt(v_j)$.
Notations 4.6. Let Z denote the set of integers. For any $t, \lambda \in Z, t \geq 1$ and $\lambda \geq 2$, let $B_t(\lambda) = \{(\lambda_1, \lambda_2, \dots, \lambda_t) \in Z^t : 2 \leq \lambda_j \leq p \text{ for all } j, \sum_{j=1}^{t} \lambda_j = \lambda\}$ and for any $(\lambda_1, \lambda_2, \dots, \lambda_t) \in B_t(\lambda)$, define $C_t(\lambda_1, \lambda_2, \dots, \lambda_t) = \left\{(l_1, l_2, \dots, l_t) \in Z^t : l_j \geq \lambda_j - 2 \text{ for all } j, \sum_{j=1}^{t} l_j \leq p - 2t\right\}$. Given any $(l_1, l_2, \dots, l_t) \in C_t(\lambda_1, \lambda_2, \dots, \lambda_t)$, let $A(\lambda_1, \lambda_2, \dots, \lambda_t; l_1, l_2, \dots, l_t) = a_{(l_1, l_2, \dots, l_t)} \binom{l_1}{\lambda_1 - 2} \binom{l_2}{\lambda_2 - 2} \cdots \binom{l_t}{\lambda_t - 2} (q-1)^t (q-2)^{\lambda - 2t} = \eta(\text{say})$,

Where

$$a_{(l_1, l_2, \dots, l_t)} = \sum_{k_1=1}^{p-\sum_{i=1}^{t} l_i - 2t+1} \sum_{k_2=k_1+l_1+2}^{p-\sum_{i=2}^{t} l_i - 2(t-1)+1} \cdots \sum_{k_{t-1}=k_{t-2}+l_{t-2}+2}^{p-\sum_{i=t-1}^{t} l_i - 3} \sum_{k_t=k_{t-1}+l_{t-1}+2}^{p-l_t-1} 1 .$$

Lemma 4.7
(i) If $0 \neq v \in V_i$, then $4 \leq wt(v) \leq 2p$.
(ii) If $v \in V_i$ is basic vector of length l, then $4 \leq wt(v) \leq 2l + 4$.

Proof. (i) Let $v \in V_i$. Then

$$v = \sum_{j=1}^{p-1} \alpha_j \left(e_{i+p^r+jp^{r-1}} + e_{i+p^r+(j-1)p^{r-1}} - e_{i+jp^{r-1}} - e_{i+(j-1)p^{r-1}}\right)$$

$$= \alpha_1 \left(e_{i+p^r+p^{r-1}} + e_{i+p^r} - e_{i+p^{r-1}} - e_i\right)$$

$$+\alpha_2 \left(e_{i+p^r+2p^{r-1}} + e_{i+p^r+p^{r-1}} - e_{i+2p^{r-1}} - e_{i+p^{r-1}}\right) + \cdots$$

$$+ \alpha_{p-2} \left(e_{i+p^r+(p-2)p^{r-1}} + e_{i+p^r+(p-3)p^{r-1}} - e_{i+(p-2)p^{r-1}} - e_{i+(p-3)p^{r-1}}\right)$$

$$+\alpha_{p-1} \left(e_{i+p^r+(p-1)p^{r-1}} + e_{i+p^r+(p-2)p^{r-1}} - e_{i+(p-1)p^{r-1}} - e_{i+(p-2)p^{r-1}}\right)$$

$$= \alpha_1 \left(e_{i+p^r} - e_i\right) + \left\{\alpha_1 \left(e_{i+p^r+p^{r-1}} - e_{i+p^{r-1}}\right) + \alpha_2 \left(e_{i+p^r+p^{r-1}} - e_{i+p^{r-1}}\right)\right\}$$

$$+ \cdots + \left\{\alpha_{p-2} \left(e_{i+p^r+(p-2)p^{r-1}} - e_{i+(p-2)p^{r-1}}\right) + \alpha_{p-1} \left(e_{i+p^r+(p-2)p^{r-1}} - e_{i+(p-2)p^{r-1}}\right)\right\} + \alpha_{p-1} \left(e_{i+p^r+(p-1)p^{r-1}} - e_{i+(p-1)p^{r-1}}\right)$$

$$= \alpha_1 \left(e_{i+p^r} - e_i\right) + \alpha_{p-1} \left(e_{i+p^r+(p-1)p^{r-1}} - e_{i+(p-1)p^{r-1}}\right)$$

$$+(\alpha_1 + \alpha_2) \left(e_{i+p^r+(p-2)p^{r-1}} - e_{i+(p-2)p^{r-1}}\right) + \cdots + (\alpha_{p-1} + \alpha_{p-2}) \left(e_{i+p^r+(p-2)p^{r-1}} - e_{i+(p-2)p^{r-1}}\right)$$

$$= \alpha_1 \left(e_{i+p^r} - e_i\right) + \alpha_{p-1} \left(e_{i+p^r+(p-1)p^{r-1}} - e_{i+(p-1)p^{r-1}}\right)$$

$$+ \sum_{j=1}^{p-2} (\alpha_j + \alpha_{j+1}) \left(e_{i+p^r+jp^{r-1}} - e_{i+jp^{r-1}}\right) \qquad (1)$$

$\alpha_j \in F_q$. If $v \neq 0$, then at least one $\alpha_j \neq 0$.

hus from (1), we have $wt(v) \geq 4$.

For maximum weight we assume $\alpha_j \neq 0$, for $j = 1, 2, \dots, p-2$.

Thus from (1), we have $wt(v) \leq 2p$.
(ii) Let $v \in V_i$ is basic vector of length l, then by Definition 4.3, $v = \sum_{j=k}^{k+l} \alpha_j \left(e_{i+p^r+jp^{r-1}} + e_{i+p^r+(j-1)p^{r-1}} - e_{i+jp^{r-1}} - e_{i+(j-1)p^{r-1}}\right)$,

Where
$0 \neq \alpha_j \in F_q, k \geq 1, l \geq 0, k+l \leq p-1$.

Then,
$v = \alpha_k\left(e_{i+p^r+(k-1)p^{r-1}} - e_{i+(k-1)p^{r-1}}\right) + \alpha_{k+l}\left(e_{i+p^r+(k+l)p^{r-1}} - e_{i+(k+l)p^{r-1}}\right)$

$+\sum_{j=k}^{k+l-1}(\alpha_j+\alpha_{j+1})\left(e_{i+p^r+jp^{r-1}} - e_{i+jp^{r-1}}\right)$ (2)

Since v is basic vector, so $\alpha_j \neq 0$ and the sum in (2) has l terms, therefore $4 \leq wt(v) \leq 2l+4$.

Lemma 4.8 If l, k, λ are integers satisfying $0 \leq l \leq p-1$, $1 \leq k \leq p-l-1$ and $2 \leq \lambda \leq l+2$, then the number of basic vectors in V_i is $\binom{l}{\lambda-2}(q-1)(q-2)^{\lambda-2}$.

Proof. For any basic vector $v \in V_i$ such that length of v is l and weight 2λ, then by equation (2),

$$v = \alpha_k\left(e_{i+p^r+(k-1)p^{r-1}} - e_{i+(k-1)p^{r-1}}\right) + \alpha_{k+l}\left(e_{i+p^r+(k+l)p^{r-1}} - e_{i+(k+l)p^{r-1}}\right) + \sum_{j=k}^{k+l-1}(\alpha_j+\alpha_{j+1})\left(e_{i+p^r+jp^{r-1}} - e_{i+jp^{r-1}}\right),$$

where $\alpha_j \in F_q$ are non zero for $k \leq j \leq k+l$.
Now we observe that the weight of v is 2λ if and only if out of a total of l sums $(\alpha_j+\alpha_{j+1}), 0 \leq j \leq k+l-1$, exactly $\lambda-2$ are non zero. That is possible if and only if there exists $i_1, i_2, \ldots, i_{\lambda-2} \leq k+l-1$ such that $(\alpha_{i_1}+\alpha_{i_2}) \neq 0, (\alpha_{i_2}+\alpha_{i_3}) \neq 0, \ldots, (\alpha_{i_{\lambda-2}}+\alpha_{i_{k+l}}) \neq 0$ and $\alpha_j+\alpha_{j+1}=0$, otherwise. We observe that the total number of choices of such a nice element v is $\binom{l}{\lambda-2}(q-1)(q-2)^{\lambda-2}$.

Remark 4.9. In the above lemma the number of basic vectors is independent of the choice of the initial point.
Definition 4.10. For any integer $\lambda \geq 0$, define

$$N(\lambda) = \begin{cases} 1, \text{if } \lambda = 0, \\ 0, \text{if } 1 \leq \lambda \leq 3 \text{ or } \lambda \geq 2p+1, \\ \sum_{t\geq 1}\sum_{(\lambda_1,\lambda_2,\ldots,\lambda_t)\in B_t(\lambda)}\sum_{(l_1,l_2,\ldots,l_t)\in C_t(\lambda_1,\lambda_2,\ldots,\lambda_t)} \eta, \text{otherwise.}\end{cases}$$

Lemma 4.11. Let λ be an integer such that $2 \leq \lambda \leq p$. Then, for each $i, 1 \leq i \leq p^{r-1}$, the number of vectors in V_i having weight 2λ are exactly $N(\lambda)$.

Proof. Let $A_i(2\lambda)$ be the set of all codewords in V_i having weight 2λ. Let $W_i(\lambda_1,\lambda_2,\ldots,\lambda_t; l_1,l_2,\ldots,l_t)$ be the set of all $v \in V_i$ such that $v = \sum_{j=1}^{t} v_j$, $v_1, v_2, \ldots, v_t$ is a chain in V_i and $wt(v_j) = 2\lambda_j, l(v_j) = l_j$ for $1 \leq j \leq t$. Then,

$$wt(v) = wt\left(\sum_{j=1}^{t} v_j\right) = \sum_{j=1}^{t} wt(v_j) = \sum_{j=1}^{t} 2\lambda_j = 2\lambda.$$

We claim that $A_i(2\lambda)$ is the disjoint union of $W_i(\lambda_1,\lambda_2,\ldots,\lambda_t; l_1,l_2,\ldots,l_t)$.
i.e.

$$A_i(2\lambda) = \bigcup_{t\geq 1}\bigcup_{(\lambda_1,\lambda_2,\ldots,\lambda_t)\in B_t(\lambda)}\bigcup_{(l_1,l_2,\ldots,l_t)\in C_t(\lambda_1,\lambda_2,\ldots,\lambda_t)} W_i(\lambda_1,\lambda_2,\ldots,\lambda_t; l_1,l_2,\ldots,l_t). \quad (3)$$

Let v be an arbitrary vector of W_i. Then by the above discussion $wt(v) = 2\lambda$. Consequently, $v \in A_i(2\lambda)$. Thus the union on right hand side is the sub set of $A_i(2\lambda)$. Now, let v be an arbitrary element of $A_i(2\lambda)$, then $wt(v) = 2\lambda$. By using Remark 4.5, we get $v = \sum_{j=1}^{t} v_j$, $v_1, v_2, \ldots, v_t$ is a chain in V_i and $wt(v_j) = 2\lambda_j, l(v_j) = l_j$, for $1 \leq j \leq t$. Then by Lemma 4.4.7, $4 \leq \lambda_j \leq 2p, l_j \geq \lambda_j - 2$ for all j. Also

$$\sum_{j=1}^{t} l_j = \sum_{j=1}^{t}\left(E(v_j)\right) - I(v_j))$$

$$= \sum_{j=2}^{t}\left(E(v_{j-1})\right) - I(v_j)) + E(v_t) - I(v_1).$$

As, $E(v_t) \leq p-1, I(v_1) \geq 1$, i.e. $-I(v_1) \leq -1$ and $\left(I(v_j) - E(v_{j-1})\right) \geq 2$, i.e. $\left(E(v_{j-1}) - I(v_j)\right) \leq -2$.

Therefore,

$$\sum_{j=1}^{t} l_j \leq \sum_{j=2}^{t} -2 + p - 1 - 1 = p - 2t.$$

This implies that $(l_1, l_2, , \dots, l_t) \in C_t(\lambda_1, \lambda_2, \dots, \lambda_t)$ and $\in W_i(\lambda_1, \lambda_2, \dots, \lambda_t; l_1, l_2, \dots, l_t)$. It is clear that the union of right hand side of (3) is disjoint. Now to evaluate $|W_i(\lambda_1, \lambda_2, \dots, \lambda_t; l_1, l_2, \dots, l_t)|$ we find out the number of chains $v_1, v_2, \dots, v_t$ in V_i such that $wt(v_j) = 2\lambda_j, l(v_j) = l_j$ for all j. As $k_j = I(v_j)$. Then $k_1 \geq 1, k_t + l_t \leq p - 1$ and $k_{j-1} + l_{j-1} + 2 \leq k_j$ for $2 \leq j \leq t$.

For $j = 2, k_1 + l_1 + 2 \leq k_2,$ (4)
For $j = 3, k_2 + l_2 + 2 \leq k_3,$
implies $k_2 \leq k_3 - l_2 - 2.$

Using k_2 in (4), we get

$k_1 + l_1 + 2 \leq k_3 - l_2 - 2,$

implies $k_1 \leq k_3 - (l_1 + l_2) - 2.2$ (5)

For $j = 4, k_3 + l_3 + 2 \leq k_4,$
implies $k_3 \leq k_4 - l_3 - 2.$

Using k_3 in (5), we ge

$k_1 \leq k_4 - (l_1 + l_2 + l_3) - 2.3$ (6)

Continuing in this way for $j = t$, we get

$k_1 \leq k_t - (l_1 + l_2 + l_3 + \cdots + l_{t-1}) - 2(t - 1).$ (7)

But $k_t \leq p - 1 - l_t$ and $k_1 \geq 1$. Using (4) to (7) inequalities, we get $k_1 \leq p - 1 - (l_1 + l_2 + l_3 + \cdots + l_{t-1} + l_t) - 2(t - 1)$.

Implies

$1 \leq k_1 \leq p - (l_1 + l_2 + l_3 + \cdots + l_{t-1} + l_t) - 2t + 1.$

By the above discussion the number of choices for k_1 is

$$\sum_{k_1=1}^{p-\sum_{j=1}^{t} l_j - 2t+1} 1.$$

Similarly, the number of choices for initial point k_2 of v_2 is

$$\sum_{k_2=k_1+l_1+2}^{p-\sum_{j=2}^{t} l_j - 2(t-1)+1} 1.$$

Therefore, total number of choices for initial points of $v_1, v_2, \dots, v_t$ is

$$= \sum_{k_1=1}^{p-\sum_{i=1}^{t} l_i - 2t+1} \ \sum_{k_2=k_1+l_1+2}^{p-\sum_{i=2}^{t} l_i - 2(t-1)+1} \cdots \sum_{k_{t-1}=k_{t-2}+l_{t-2}+2}^{p-\sum_{i=t-1}^{t} l_i - 3} \ \sum_{k_t=k_{t-1}+l_{t-1}+2}^{p-l_t-1} 1\,.$$

By using Lemma 4.8, the number of basic vectors v_j of length l_j weight λ_j and having a fixed initial point k_j is given by

$\binom{l_j}{\lambda_j - 2}(q-1)(q-2)^{\lambda_j - 2}$ for each $j, 1 \leq j \leq t$.

By using Notation 4.4.6, we get

$|W_i(\lambda_1, \lambda_2, \dots, \lambda_t; l_1, l_2, \dots, l_t)| = \eta.$ (8)

Using (3) and (8),

$|A_i(2\lambda)| = N(2\lambda)$ for $2 \le \lambda \le p$.

Theorem 4.12. Let F_q be the finite field with q elements; p, q be two odd primes with gcd(p, q)= 1 and $m \ge 1$ be an integer. If the multiplicative order of q modulo $2p^m$, then the weight distribution $A_{2w}^{(2p^r)}$, $w \ge 0$, of the minimal cyclic code $\mathbb{M}_1^{(2p^r)}$is given by

$A_{2w}^{(2p^r)} = \sum_{(w_1, w_2, \dots, w_{p^{r-1}})} \prod_{i=1}^{p^{r-1}} N(w_i)$, where $\sum_{i=1}^{p^{r-1}} w_i = w$.

Proof. Let $A(2w)$ be the set of codewords in $\mathbb{M}_1^{(2p^r)}$ of weight $2w, w \ge 0$. By Remark 4.2, $\mathbb{M}_1^{(2p^r)} \cong V_1 \oplus V_2 \oplus \dots \oplus V_{p^{r-1}}$, where V_i is the vector subspace of $F_q^{2p^r}$ spanned by $e_{i+p^r+jp^{r-1}} + e_{i+p^r+(j-1)p^{r-1}} - e_{i+jp^{r-1}} - e_{i+(j-1)p^{r-1}}$ for $1 \le i \le p^{r-1}$ and $1 \le j \le p-1$. Let x be any element of $\mathbb{M}_1^{(2p^r)}$ of weight $2w$. Then, by the above discussion x corresponds $v \in V_1 \oplus V_2 \oplus \dots \oplus V_{p^{r-1}}$such that $v = \sum_{i=1}^{p^{r-1}} v_i$ and $wt(v_i) = 2w_i$, satisfying $w = \sum_{i=1}^{p^{r-1}} w_i$. To determine the number of elements x in $\mathbb{M}_1^{(2p^r)}$having weight $2w$, we have to determine the number of v_i in V_i such that $wt(v_i) = 2w_i$. By Lemma 4.11, the number of v_i having weight $2w_i$ in V_i is $N(2w_i)$ for each $i, 1 \le i \le p^{r-1}$.

If we fix w_i, satisfying $w = \sum_{i=1}^{p^{r-1}} w_i$ for each $i, 1 \le i \le p^{r-1}$. Then by the above discussion, the number of codewords of weight $2w_i$ is $\prod_{i=1}^{p^{r-1}} N(2w_i)$. Consequently, $A_{2w}^{(2p^r)} = \sum_{(w_1, w_2, \dots, w_{p^{r-1}})} \prod_{i=1}^{p^{r-1}} N(2w_i)$, $w = \sum_{i=1}^{p^{r-1}} w_i$.

This completes the proof of the Theorem.

References

1. Sharma A, Bakshi GK, Raka M. The weight distribution of some irreducible cyclic codes of length p^n, Finite Fields Appl.2011.,doi:10.1016
2. Sharma A, Bakshi GK, Raka M. The weight distribution of irre-ducible cyclic codes of length 2^n, Finite Fields Appl. 2007;13(4):1086 1095.
3. Sharma A, Bakshi GK, Dumir VC, Raka M, Cyclotomicnumbers and primitive Idempotents in the ring $\frac{GF(q)[x]}{}$, Finite Fields Appl. 2004;10(4):653-673.
4. Ding C. The weight distribution of some irreducible cyclic codes, IEEE Trans. Inform. Theory. 2009;55(3):955-960.
5. MacWilliams FJ, Sloane NJA. The Theory of Error Cor-recting Codes, North Holland, Amsterdam. 1977.
6. Vermani LR. Elements of algebraic coding theory, Chapman and Hall,Landon.
7. Pruthi M, Arora SK. Minimal Codes of Prime-PowerLength, Finite Fields Appl. 1997;3:99-113.
8. Batra S, Arora SK. Some cyclic codes of length $2p^n$,Codes Designsand Crypto. 2011;61(01):41-69.
9. S. K. Arora and M. Pruthi, Minimal cyclic codes of length $2p^n$, *Finite Fields Appl.*, 5(1999)177 − 187.
10. Pless V. Introduction to the Theory of Error Correcting Codes Wiley, New York, 1998.
11. Singh R, Pruthi M. Primitive idempotents of quadratic residue codes of length p^nq^m, Int. J Algebra. 2011;5:285-294.
12. Batra S, Arora SK. Minimal quadratic residue cyclic codes of length p^n(p odd prime), Korean J. Comput and Appl. Math. 2001;8(3):531-547.
13. Rani S, Singh IJ, Arora SK. Minimal cyclic codes of length $2p^nq$(p odd prime), Bull. Calcutta. Math Society. 2014;106(4):281-296.
14. Rani S, Kumar P, Singh IJ. Minimal cyclic codes of length $2p^n$,"Int. J. Algebra. 2013;7(1- 4):79-90.
15. Rani S, Kumar P, Singh IJ. Quadratic residues codes of prime power length over Z_4, J Indian Math. Soc. New Series. 2011;78(1-4):155-161.
16. Seema Rani IJ Singh, Arora SK. Primitive idempotents of irre- ducible cyclic codes of length p^nq^m",Far East Journal of Mathematical Sciences. 2013;77(1):17-32.
17. Kumar P, Sangwan M, Arora SK. The weight distributions of some irreducible cyclic codes of length p^n and $2p^n$, Adv. Math. Commun. 2015;9:277–289.
18. Riddhi K Singh, Kumar P. Weight distributions of some irre- ducible cyclic codes of length n, Indian Jour. Pure Appli. Math. 2022;53:1073-1082.