International Journal of Computer Sciences and Engineering
Vol.**11**, Issue **6**, pp.**45-47**, June **2023**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Paper

Weight Distribution of Minimal Cyclic Codes over a Finite Field

Inderjit Singh[1*], Seema Rani[2]

[1]Department of Mathematics, Dayanand College, Hisar, India
[2]Department of Mathematics, Govt. College, Adampur, India

**Corresponding Author:* vs.inderjit@gmail.com

Received: 28/Apr/2023; **Accepted**: 30/May/2023; **Published**: 30/Jun/2023. **DOI**: https://doi.org/10.26438/ijcse/v11i6.4547

***Abstract*:** Let F_q be the finite field with q elements, p, q be two odd primes with gcd(2p, q) = 1, multiplicative order of $\boldsymbol{q}$ modulo $2p^m$ is $p^d (0 \le d \le m-1)$, $m \geqslant 1$ be an integer. In this paper, we obtain weight distribution of all the minimal(irreducible) cyclic codesof length $2p^m$ over F_q by using their generating polynomials.

***Keywords*:** Primitive root, Weight distribution, Minimal Cyclic Codes

1. Introduction

Let F_q be the finite field with q elements, n be a positive integer with $\gcd(n, q) = 1$. A cyclic code $\mathcal{C}$ of length n over F_q is a linear subspace of F_q^n with the property that if $(a_0, a_1, \dots, a_{n-1}) \in \mathcal{C}$, then every cyclic shift $(a_{n-1}, a_0, \dots, a_{n-2})$ is in $\mathcal{C}$. Let $R_n = \frac{F_q[x]}{<x^n-1>}$.Then $F_q^n \cong R_n$ under the isomorphism$(a_0, a_1, \dots, a_{n-1}) \to a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. Therefore, we can regard a cyclic code $\mathcal{C}$ as an ideal in R_n .A minimal ideal in R_n is called an minimal cyclic code of length n over F_q. If $\mathcal{C}$ is a minimal cyclic code of length n over F_q and $v \in \mathcal{C}$, then the weight of v is defined to be the number of non-zero coordinates in v. We denote it by $wt(v)$. If A_w^n denotes the number of codewords of weight w in $\mathcal{C}$, then $A_0^{(n)}$, $A_1^{(n)}, \dots, A_n^{(n)}$ is called weight distribution of $\mathcal{C}$. Ding [4] determined the weight distribution of $q-$ ary minimal cyclic codes of length n provided $2 \le \frac{q^t-1}{n} \le 4$, $t = O_n(q) =$ multiplicative order of q modulo n. Sharma *et al.* [1-3] computed the weight distribution of all minimal cyclic codes of length 2^m and p^m over F_q. Kumar *et al.* [17-18] computed the weight distribution of some minimal cyclic codes of length p^m and $2p^m$ by using different technique.

In this paper, we determine the weight distribution of all minimal cyclic codes of length $2p^m$ over F_q, where $\gcd(2p, q) = 1$ and $m \ge 1$ is an integer under condition The multiplicative order of q modulo $2p^m$ is $p^d (0 \le d \le m-1)$.In Sections(1-3)introduction and elementary definitions and theorems are given. In Section 4. (Theorem 4.1) the weight distribution of $\mathbb{M}_1^{(2p^r)} (1 \le r \le m)$ is discussed. In Section 5, the weight distribution of minimal cyclic code of length 50 is obtained.

2. Cyclotomic Cosets Modulo $2p^m$

Let $S = \{0, 1, 2, \dots, 2p^m - 1\}$. For $a, b \in S$, say that $a \sim b$ if $a \cong bq^i (\text{mod } 2p^m)$ for some integer $i \ge 0$. 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 $C_s = \{s, sq, sq^2, \dots, sq^{t_s-1}\}$, where t_s is the least positive integer such that $sq^{t_s} \equiv s \pmod{2p^m}$ 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) $C_{p^m} = \{p^m\}$.

For $0 \le j \le m-1, 0 \le k \le d-1$,

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

(iv) $C_{2g^k p^j} =$

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

where g is primitive root modulo $2p^m$.

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 $C_{s_1}, C_{s_2}, \dots, C_{s_k}$ are all the distinct $q-$ cyclotomic cosets modulo $2p^m$, then $\mathbb{M}_{s_1}^{(2p^m)}, \mathbb{M}_{s_2}^{(2p^m)}, \dots, \mathbb{M}_{s_k}^{(2p^m)}$ 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.

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.

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 $p^d (0 \leq d \leq m-1)$.

Lemma 4.1. Let $o(q)_{2p} = t$ and $t = \frac{\varphi(2p)}{k}$, where k is any integer. If $q \equiv 1 \pmod{2p}$ and $2p^2$such that p does not divide $q-1$, then $o(q)_{2p^m} = tp^{m-1}$ for all $m \geq 1$.

Proof. As $q \equiv 1 \pmod{2p}$, $2p^2$and p does not divide $q-1$ gives $q^t = 1 + 2p\lambda$, where $2p$ does not divide λ. Then for any integer i, $q^{tp^i} = 1 + 2p^{i+1}\lambda_i$, where $2p$ does not divide λ_i. Let $o(q)_{2p^m} = h_m$, then for $i = m-1, q^{tp^{m-1}} = 1 + 2p^m\lambda_{m-1}$ implies $q^{tp^{m-1}} \equiv 1 \pmod{2p^m}$. Thus h_m divides tp^{m-1}. Also $q^{h_m} \equiv 1 \pmod{2p^m}$ yields that $q^{h_m} \equiv 1 \pmod{2p}$, which gives t divides h_m. Therefore, let $h_m = tp^d$for some d, $0 \leq d \leq m-1$. As $o(q)_{2p^m} = h_m$ implies $q^{h_m} \equiv 1 \pmod{2p^m}$ i.e. $q^{tp^d} \equiv 1 \pmod{2p^m}$. But $q^{tp^d} \equiv 1 + 2p^{d+1}\lambda_d$ which gives that $p^{d+1} \equiv 0 \pmod{p^m}$ implies $m \leq d+1$. Thus $d = m-1$. Hence, $h_m = tp^{m-1}$.

Lemma 4.2. Let multiplicative order of q modulo $2p^m$ is $p^d (0 \leq d \leq m-1)$. Then

$$o(q)_{2p^r} = \begin{cases} 1, & \text{if } r \leq m-d; \\ p^{r-(m-d)}, & \text{if } r > m-d. \end{cases}$$

Proof. Let $o(q)_{2p^{m-d}} = t$, then by Lemma 4.1, we get $o(q)_{2p^m} = tp^d$. But $o(q)_{2p^m} = p^d$. This gives, $t = 1$.
Now if $r \leq m-d$, then $o(q)_{2p^r} = 1$.
If $r > m-d$, then by using Lemma 4.1, we get $o(q)_{2p^r} = p^{r-(m-d)}$.

Lemma 4.3. If $r > m-d$ and$o(q)_{2p^r} = p^{r-(m-d)}$, then

$$\sum_{j=0}^{2p^{(m-d)}-1} \beta^{j+1} \left(e_{i+jp^{r-(m-d)}} + e_{i+jp^{r-(m-d)}+p^r} \right), 1 \leq i \leq p^{r-(m-d)},$$

constitute a basis of $\mathbb{M}_1^{(2p^r)}$ over F_q, where β is primitive $2p^{r-(m-d)}$th root of unity in F_q.

Proof. By Lemma 4.2, $o(q)_{2p^r} = p^{r-(m-d)}$ if $r > m-d$. Then $q-$ cyclotomic coset modulo $2p^r$ containing 1 is $C_1 = \{1, q, q^2, \dots, q^{p^{r-(m-d)-1}}\}$.
By Definition 3.1,$M_1^{2p^r}(x) = \prod_{j \in C_1}(x - \alpha^j)$. We observe that $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{p^{r-(m-d)}}}$ are all the roots of the $x^{p^{r-(m-d)}} - \alpha^{p^{r-(m-d)}}$. We claim that $\alpha^{p^{r-(m-d)}} \in F_q$. Let $\alpha^{-p^{r-(m-d)}} = \beta$, then β is primitive $2p^{m-d}th$ root of unity which gives $\beta^{2p^{m-d}} = 1$ and $\beta^s \neq 1$ for $s < 2p^{m-d}$. But by Lemma 4.14, multiplicative order of q modulo $2p^{m-d}$is 1. So, $q \equiv 1 \pmod{2p^{m-d}}$.Thus $\beta^q = \beta \in F_q$.Therefore, minimal polynomial of α is $x^{p^{r-(m-d)}} - \alpha^{p^{r-(m-d)}}$over F_q. By Definition 3.2, generating polynomial of $\mathbb{M}_1^{(2p^r)}$ is

$$g(x) = \frac{x^{2p^r}-1}{x^{p^{r-(m-d)}} - \alpha^{p^{r-(m-d)}}} = \left(\beta + \beta^2 x^{p^{r-(m-d)}} + \beta^3 x^{2p^{r-(m-d)}} + \cdots + x^{(p^{(m-d)}-1)p^{r-(m-d)}} \right)(x^{p^r} + 1).$$

As $\mathbb{M}_1^{(2p^r)}$ is a vector subspace of R_{2p^r} and spanned by $g(x), xg(x), \dots, x^{p^{r-(m-d)}}g(x)$. Since $R_{2p^r} \cong F_q^{2p^r}$under the standard isomorphism, then $x^{i-1}g(x)$ corresponds to $\sum_{j=0}^{2p^{(m-d)}-1} \beta^{j+1} \left(e_{i+jp^{r-(m-d)}} + e_{i+jp^{r-(m-d)}+p^r} \right), 1 \leq i \leq p^{r-(m-d)}$, which completes the proof.

Theorem 4.4. Let multiplicative order of q modulo $2p^m$ is $p^d (0 \leq d \leq m-1)$.

(i) If $r \leq m-d$, then weight of each non-zero codeword in $\mathbb{M}_1^{(2p^r)}$ is $2p^r$.

(ii) $r > m-d$, the weight distribution $A_w^{(2p^r)}, w \geq 0$ of $\mathbb{M}_1^{(2p^r)}$is given by

$$A_w^{(2p^r)} = \begin{cases} 0, & \text{if } 2p^{(m-d)} \text{does not divide } w; \\ \binom{p^{r-(m-d)}}{w'}(q-1)^{w'}, & \text{if } w = 2p^{(m-d)}w', 0 \leq w' \leq p^{r-(m-d)}. \end{cases}$$

Proof. (i) If $r \leq m-d$, by Lemma 4.2, $o(q)_{2p^r} = 1$. Let α be a primitive root of unity in some extension of F_q.Then $\alpha^{2p^r} = 1$ and $q \equiv 1(\text{mod } 2p^r)$. This implies $q-1 = \lambda 2p^r$, where λ be any scalar. Therefore, $1 = \alpha^{2p^r\lambda} = \alpha^{q-1}$ i.e. $\alpha \in F_q$. The minimal polynomial of α over F_q is $x-\alpha$. Thus generating polynomial of $\mathbb{M}_1^{(2p^r)}$ is $\frac{x^{2p^r}-1}{x-\alpha} = \alpha^{2p^r-1} + \alpha^{2p^r-2}x + \alpha^{2p^r-3}x^2 + \cdots + \alpha x^{2p^r-2} + x^{2p^r-1}$.

Consequently, every non-zero codeword of $\mathbb{M}_1^{(2p^r)}$ is a scalar multiple of $\alpha^{2p^r-1} + \alpha^{2p^r-2}x + \alpha^{2p^r-3}x^2 + \cdots + \alpha x^{2p^r-2} + x^{2p^r-1}$. This gives that the only possible nonzero weight in $\mathbb{M}_1^{(2p^r)}$ is $2p^r$.

(i) If $r > m-d$, by Lemma 4.3, then basis of $\mathbb{M}_1^{(2p^r)}$ is $\sum_{j=0}^{2p^{(m-d)}-1}\beta^{j+1}\left(e_{i+jp^{r-(m-d)}} + e_{i+jp^{r-(m-d)}+p^r}\right), 1 \leq i \leq p^{r-(m-d)}$.

Let $c \in \mathbb{M}_1^{(2p^r)}$,

then $c = \sum_{i=1}^{p^{r-(m-d)}}\sum_{j=0}^{2p^{(m-d)}-1}\alpha_i\beta^{j+1}\left(e_{i+jp^{r-(m-d)}} + e_{i+jp^{r-(m-d)}+p^r}\right)$, $\alpha_i \in F_q$. It is easy to see that $wt(c) = 2p^{m-d}w'$, where $w'$is the number of nonzero α_i's. But total number of α_i's is $p^{r-(m-d)}$, so we can choose w' non-zero α_i's in $\binom{p^{r-(m-d)}}{w'}$ ways.

Consequently,

$$A_w^{(2p^r)} = \begin{cases} 0, & \text{if } 2p^{(m-d)} \text{ does not divide } w; \\ \binom{p^{r-(m-d)}}{w'}(q-1)^{w'}, & \text{if } w = 2p^{(m-d)}w', 0 \leq w' \leq p^{r-(m-d)}. \end{cases}$$

5. Example.

Example 5.1. Let $p = 5$, $q = 11$ and $o(11)_{2.5^m} = 5^d$, for some integer d.

As, $o(11)_{2.5^m} = 5^{m-1}$.

Therefore, $d = m-1$.Let r be a positive integer.

By Theorem 4.4, if $r = 1$, then the weight of each non-zero codeword in $\mathbb{M}_1^{(10)}$ is 10.

If $r = 2$, the weight distribution of $\mathbb{M}_1^{(50)}$ is given below :

$$A_1^{(50)} = A_2^{(50)} = A_3^{(50)} = A_4^{(50)} = A_5^{(50)} = A_6^{(50)} = A_7^{(50)} = A_8^{(50)} = A_9^{(50)} = A_{11}^{(50)} = A_{12}^{(50)} = A_{13}^{(50)} = A_{14}^{(50)} = A_{15}^{(50)} = A_{16}^{(50)} = A_{17}^{(50)} = A_{18}^{(50)} = A_{19}^{(50)} =$$
$$A_{21}^{(50)} = A_{22}^{(50)} = A_{23}^{(50)} = A_{24}^{(50)} = A_{25}^{(50)} = A_{26}^{(50)} = A_{27}^{(50)} = A_{28}^{(50)} = A_{29}^{(50)} =$$
$$A_{31}^{(50)} = A_{32}^{(50)} = A_{33}^{(50)} = A_{34}^{(50)} = A_{35}^{(50)} = A_{36}^{(50)} = A_{37}^{(50)} = A_{38}^{(50)} = A_{39}^{(50)} =$$
$$A_{41}^{(50)} = A_{42}^{(50)} = A_{43}^{(50)} = A_{44}^{(50)} = A_{45}^{(50)} = A_{46}^{(50)} = A_{47}^{(50)} = A_{48}^{(50)} = A_{49}^{(50)} = 0,$$
$$A_0^{(50)} = 0, A_{10}^{(50)} = \binom{5}{1}(11-1) = 50, A_{20}^{(50)} = \binom{5}{2}(11-1)^2 = 1000,$$
$$A_{30}^{(50)} = \binom{5}{3}(11-1)^3 = 10000, A_{40}^{(50)} = \binom{5}{4}(11-1)^4 = 50000$$
$$, A_{50}^{(50)} = \binom{5}{5}(11-1)^5 = 100000.$$

References

[1] A.Sharma, G. K. Bakshi and M. Raka,"The weight distribu- tion of some irreducible cyclic codes of length p^n", *Finite Fields Appl.*,Vol **18**, Issue **1**,pp**.144-159, 2012.**

[2] A.Sharma, G. K. Bakshi and M. Raka,"The weight distribution of irre- ducible cyclic codes of length 2^n", *Finite Fields Appl.*,Vol.**13,** Issue **4,** pp**.1086-1095, 2007**.

[3] A.Sharma, G. K. Bakshi, V. C. Dumir and M. Raka," Cyclotomic numbers and primitive idempotents in the ring $\frac{GF(q)[x]}{(x^{p^n}-1)}$ ", *Finite Fields Appl.*,Vol.**10,** Issue **4,** pp.**653-673, 2004**.

[4] C.Ding,"The weight distribution of some irreducible cyclic codes,"*IEEE Trans.Inform.Theory* ,Vol.**55,** Issue **3,** pp.**955-960, 2009.**

[5] M. Pruthi and S. K. Arora(1997), " Minimal Codes of Prime-Power Length", *Finite Fields Appl.*, Vol.**3,** Issue **3,** pp.**99-113, 1997.**

[6] S.Batra and S.K.Arora,"Some cyclic codes of length $2p^n$",*Codes Designs and Crypto.*, Vol.**61,** Issue **01,** pp**.41-69, 2011.**

[7] S. K. Arora and M. Pruthi, "Minimal cyclic codes of length $2p^n$", *Finite Fields Appl.*, Vol.**5,** pp**.177-187, 1999.**

[8] R. Singh and M. Pruthi,"Primitive idempotents of quadratic residue codes of length p^nq^m,"*Int.J.Algebra*,Vol.**5,** pp**.285-294, 2011.**

[9] S. Batra and S.K. Arora,"Minimal quadratic residue cyclic codesof length p^n(p odd prime),"*Korean J. Comput and Appl. Math.*, Vol.**8,** Issue **3,** pp.**531-547, 2001.**

[10] S.Rani,I.J.Singh and S.K. Arora, "Minimal cyclic codes of length $2p^nq$(p odd prime),"*Bull.Calcutta.Math Society* ,Vol.**106,** Issue **4,** pp**.281-96, 2014.**

[11] S. Rani, P,Kumar and I.J.Singh, "Minimal cyclic codes of length $2p^n$,"*Int. J. Algebra*, Vol.**7,** Issue **1-4,** pp**.79-90, 2013.**

[12] S. Rani, P,Kumar and I.J.Singh, "Quadratic residues codes of prime power length over Z_4,"*J.Indian Math.Soc.New Series* , Vol.**78,** Issue **1-4,** pp**.155-161, 2011.**

[13] Seema Rani, I.J.Singh and S.K.Arora,"Primitive idempotents of irre- ducible cyclic codes of length p^nq^m",*Far East Journal of Mathematical Sciences*, Vol.**77,** Issue **1,** pp**.17-32, 2013.**

[14] P. Kumar, M. Sangwan and S. K. Arora," The weight distributions of some irreducible cyclic codes of lengthp^n and $2p^n$,*Adv. Math. Commun*,Vol.**9,** pp**.277-289, 2015.**

[15] Riddhi, K. Singh and P. Kumar," Weight distributions of some irre- ducible cyclic codes of length *n, Indian Jour. Pure Appli. Math.* Vol.**53,** pp**.1073-1082, 2022.**

[16] Inderjit Singh, Pankaj Kumar and Monika Sangwan," Primitive idempotents in a semi- simple ring",*Asian E.Journal of mathematics*,Vol.**16,** Issue **4, 2023.**

