International Journal of Engineering, Science and Mathematics
Vol. 8 Issue 5, May 2019,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com Double-Blind
Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

WEIGTH DISTRIBUTION OF CYCLIC CODES OF LENGTH mp^s

Sunil Kumar[1], Manju Pruthi[2], Rahul[3]
[1,2,3]*Department of Mathematics, Indira Gandhi University, Meerpur(Rewari)*-122502, *Haryana, India*

ABSTRACT. Let $\mathbb{F}_q$ be a field with q elements such that $gcd(mp, q(q-1)) = 1$ and $q^2 \equiv 1(mod\ mp^s)$, where m is prime and $p > m$ is prime. In this paper, we give all primitive idempotents in a ring $\mathbb{F}_q[x]/\langle x^{mp^s} - 1\rangle$. We give the weight distributions of all irreducible cyclic codes of length mp^s over $\mathbb{F}_q$.

KEYWORDS. Cyclic Codes, Primitive Idempotents, Weight Distributions.
MSC: 94B05, 94B15, 94A24, 11H71, 11T71, 11A07, 13A05.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a field with q elements. Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$, that is , it is a k-dimensional subspace of F_q^n. If for every codeword $(c_0, c_1, c_2, \dots\dots\dots, c_{n-1}) \in \mathcal{C}$, $(c_{n-1}, c_0, c_1, c_2, \dots\dots\dots, c_{n-2}) \in \mathcal{C}$ then we call $\mathcal{C}$ as a cyclic code. We identify the codeword $(c_0, c_1, c_2, \dots\dots\dots, c_{n-1})$ in $\mathcal{C}$ with the polynomial $c_0 + c_1x + c_2x^2 + \cdots c_{n-1}x^{n-1}$ in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. The code $\mathcal{C}$ of length n over field $\mathbb{F}_q$ corresponds to a subset of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Then $\mathcal{C}$ is said to be cyclic code iff the corresponding subset is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Observe that each ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is the principal ideal. Suppose that $g(x)$ is a monic divisor of $x^n - 1$ in the field $\mathbb{F}_q$. Then code $\mathcal{C}$ which corresponds to $\langle g(x)\rangle$ is a cyclic code, $g(x)$ is called a generator polynomial and $h(x) = (x^n - 1)/g(x)$ is referred to the parity-check polynomial of the code $\mathcal{C}$. If $h(x)$ has an irreducible factor over $\mathbb{F}_q$, we refer the cyclic code as irreducible. The Irreducible cyclic codes of length n over $\mathbb{F}_q$ can be viewed as the ideals of the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ generated by the primitive idempotents.

Many papers investigated the primitive idempotents of $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ which are mentioned as follows:
For n = 2, 4, l^m and $2l^m$, where l is an odd prime and q (prime power) is a primitive root modulo n, Arora and Pruthi got primitive idempotents in R_n in [2, 15]. For $n = 2^m$, $m \geq 3$, Pruthi gave all explicit expressions of the m + 1 idempotents in ring R_n; Sharma et al. has obtained all the primitive idempotents and the irreducible cyclic codes in R_n in [14, 17]. For $n = l_1^m l_2$, where l_1, l_2, q are the distinct odd prime numbers, q is the common primitive root modulo l_1^m and l_2, and $gcd\left(\frac{\phi(l_1^m)}{2}, \frac{\phi(l_2)}{2}\right) = 1$, Bakshi and Raka obtained all $3m + 2$ primitive idempotents in ring R_n in [4]. For $n = l_1^m l_2^m$, where l_1, l_2, q are the distinct odd prime numbers, $gcd(\phi(l_1^m), \phi(l_2^m)) = 2$, $ord_{l_1^{m_1}}(q) =$

$\frac{\phi(l_1^{m_1})}{2}$ and $ord_{l_2^{m_2}}(q) = \frac{\phi(l_2^{m_2})}{2}$. Singh and Pruthi presented all explicit expressions for all $4m_1m_2 + 2m_1 + 2m_2 + 1$ primitive idempotents in ring R_n in [18]. For $n = l^m$, $m \geq 1$, where l is an odd prime and $ord_{l^m}(q) = \frac{\phi(l^m)}{2}$. Arora et al. had given all explicit expressions for all the $2m + 1$ primitive idempotents in R_n in [1]. For $n = 2l^m$, $m \geq 1$, where l is an odd prime number and $ord_{2l^m}(q) = \frac{\phi(2l^m)}{2}$. Batra and Arora got all explicit expressions for $4m + 2$ primitive idempotents in the ring R_n in [3]. For $n = l^m$, $m \geq 1$, where l is an odd prime number and $l/(q-1)$, Chen et ' al. recursively gave all the primitive idempotents and the minimum Hamming distances of all the codes generated by those primitive idempotents in the ring R_n in [6]. For $n = l_1^m l_2^m$, $m_1 \geq 1, m_2 \geq 1$ where l_1, l_2 are the distinct prime numbers and $l_1 l_2/(q-1)$; $n = 4l^m$ and $8l^m$, where l is an odd prime number and $l/(q-1)$, Li and Yue et al. obtained all the primitive idempotents and the minimum Hamming distances of all the codes generated by those primitive idempotents in the ring R_n, respectively in [10, 11]. In [12] Fengwei Li and Qin Yue take F_q, finite field with q elements such that $l^v \| (q^t - 1)$, $gcd(l, q(q-1)) = 1$, where l, t are prime numbers and v is the positive integer. They gave all the primitive idempotents in the ring $F_q[x]/\langle x^{l^m} - a\rangle$ for a $\in F_q^*$. Specially for $t = 2$, they gave weight distributions of all irreducible constacyclic codes, and their dual codes of length l^m over the field F_q. In [7], Kumar, Pankaj and Pruthi take F_l, finite field with l elements and $n = 2^a p_1^{a_1} p_2^{a_2} \dots p_e^{a_e}$, where $a, a_1, a_2, \dots, a_e$ be positive integers and $p_1, p_2, \dots\dots\dots, p_e$ are distinct odd prime numbers and $4p_1, p_2, \dots\dots\dots, p_e/l - 1$. They have studied the factorization of $x^{2^a p_1^{a_1} p_2^{a_2} \dots p_e^{a_e}} - 1$ over the field F_l and all the primitive idempotents in ring $F_l[x]/\langle x^{2^a p_1^{a_1} p_2^{a_2} \dots p_e^{a_e}} - 1\rangle$. Moreover, they obtained the dimensions and minimum hamming distances of all the irreducible cyclic codes of length $2^a p_1^{a_1} p_2^{a_2} \dots p_e^{a_e}$ over the field F_l.

Suppose A_i be the number of code words with the Hamming weight 'i' in code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ may be defined as

$$A(z) = 1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$$

The sequence $(1, A_1, A_2, \dots, A_n)$ is called weight distribution of the code $\mathcal{C}$. In coding theory, it is generally desirable to know weight distributions of the codes because they can be used to estimate error correcting capability and the error probability of the error detection and correction with respect to some algorithms.

In this paper, we shall always assume that $p > m$ is a prime number with $gcd(mp, q(q-1)) = 1$, $q^2 \equiv 1 (mod\ mp^s)$. We obtain all the primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{mp^s} - 1\rangle$. Next, we give all weight distributions of all the irreducible cyclic codes and their dual codes of length mp^s over the field $\mathbb{F}_q$.

Notation: ξ_e denotes the primitive e-th root of unity over the field $\mathbb{F}_{q^2}$.

This paper is organized as follows:

In Section 2, we recall some of the preliminary concepts and basic theorems.

In section 3, all the primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{mp^s} - 1\rangle$ are given.

In Section 4, the weight distributions are obtained of all the irreducible cyclic codes of length mp^s over the field $\mathbb{F}_q$.

2. PRELIMINARIES

Let $\mathcal{C}$ be the cyclic code. There is an unique codeword $c(x)$ which satisfies the relation $c^2(x) = c(x)$ and $\mathcal{C} = \langle c(x) \rangle$, then the codeword $c(x)$ is called the idempotent. The idempotent of an irreducible cyclic code is called primitive idempotent.

Lemma 2.1. Assume that $t \geq 2$. For any $a \in \mathbb{F}_q{}^*$ with $o(a) = l$, then the binomial $(x^t - \mathrm{a})$ is irreducible over the field $\mathbb{F}_q$ iff both the following two conditions are satisfied:

(i) Every prime divisor of t divides *k*, but does not divide $\frac{q-1}{l}$;

(ii) If $4/t$, then $4/(q-1)$.

Lemma 2.2 Let $\xi \in \mathbb{F}_q$ be the root of $x^t - 1$, where $\gcd(q,t) = 1$. Then

$$\sum_{j=0}^{\mathrm{t}-1} \xi^j = \begin{cases} 0 \text{ if } \xi \neq 1 \\ \mathrm{t} \text{ if } \xi = 1 \end{cases}$$

3. PRIMITIVE IDEMPOTENTS IN $\mathbb{F}_q[x]/\langle x^{mp^s} - 1 \rangle$

Let $\mathbb{F}_q$ be finite field having q elements. Fengwei Li and Qin Yue et al. gave all the primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{l^m} - 1 \rangle$, where $l^v \| (q^t - 1)$ and $gcd(l, q(q-1)) = 1$, where l, t are prime numbers and v is the positive integer. Let $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ be the finite fields having q and q^2 elements, respectively. Chen et al. [5] gave all the irreducible factorization of $(x^{l^s q^m} - \mathrm{a})$ over the field $\mathbb{F}_q$, where $a \in \mathbb{F}_q{}^*$, s be a non-negative integer, $l > 3$ is the prime number, $\gcd(l,q) = 1$ and $l/(q-1)$. In this section, we always assume that $p > m$ is a prime number having $\gcd(mp, q(q-1)) = 1$, $q^2 \equiv 1 (mod\ mp^s)$. We shall explicitly determine all the irreducible factors of $x^{mp^s} - 1$ in the polynomial ring $\mathbb{F}_q[x]$.

$$x^{mp^s} - 1 = \prod_{j=1}^{mp^s} (x - \xi_{mp^s}^j),$$

where ξ_{mp^s} is the mp^s-th root of unity in the field $\mathbb{F}_{q^2}$.

Definition 3.1 Let $T = \{ j : 1 \leq j < mp^s \}$, $T_{mp^s} = \{mp^s\}$,
$T_0 = \{p^s, 2p^s, 3p^s, 4p^s, 5p^s, \ldots\ldots\ldots, (m-1)p^s\}$, $T^* = T - T_0$, $T_r{}^* = \{ t = l^{s-r} v \in T : \gcd(v,p) = 1,\ 1 \leq t < mp^s \}$ for $1 \leq r \leq s$.

Define

$$\Psi_{\mathrm{r}}^*(\mathrm{x}) = \prod_{t \in T_r{}^*} \left(x - \xi_{mp^s}^t\right) , \qquad r = 1,2, \ldots\ldots\ldots, s$$

Note that $T_{mp^s} = \{mp^s\}$, $T_0 = \{p^s, 2p^s, 3p^s, 4p^s, 5p^s, \ldots\ldots\ldots, (m-1)p^s\}$ it is very clear that $T = T_0 \cup T_1{}^* \cup T_2{}^* \ldots\ldots \cup T_{s-1}{}^* \cup T_s{}^*$ and $|T_r{}^*| = m\phi(p^r)$ for $1 \leq r \leq s$.
where $\phi(1) = 1$, $\phi(p^r) = p^{r-1}(p-1)$, $r \geq 1$ (Euler phi −function)

$$x^{mp^s} - 1 = (\mathrm{x} - 1)\prod_{\mathrm{r}=0}^{s} \prod_{t \in S_r}(x - \xi_{mp^s}^{t}) = (\mathrm{x} - 1)\Psi_0^*(\mathrm{x})\Psi_1^*(\mathrm{x}) \ldots\ldots \Psi_s^*(\mathrm{x}). \quad (3.1)$$

Where $\Psi_0^*(\mathrm{x}) = \prod_{i \in T_0}(\mathrm{x} - \xi_{mp^s}^{i})$

For each $t = p^{s-r}v \in T_r^*$, $1 \leq r \leq s$, there is a $q-$coset $\Omega_{r,v} = \{t, tq\} \subset T_r^*$ and let $\Omega_{p^s,0} = \{t, tq\} \subset \{p^s, 2p^s, 3p^s, 4p^s, 5p^s, \ldots\ldots\ldots, (m-1)p^s\}$. Hence there is disjoint union

$$T_r^* = \bigcup_{k=1}^{\frac{m\Phi(p^r)}{2}} \Omega_{r,v}\,,\ |\Omega_{r,v}| = 2, where\ v \in T = \{y : \gcd(y,p) = 1\ and\ 1 \leq y < mp^s\ and\ y\ is\ odd\}$$

Thus each $q-$coset $\Omega_{r,v}$ corresponds to an irreducible polynomial over the field $\mathbb{F}_q$.

$$f_{r,v}(x) = \prod_{\mu=0}^{1}(x - \xi_{mp^s}^{p^{s-r}vq^{\mu}}) = \prod_{\mu=0}^{1}\left(x - \xi_{mp^r}^{vq^{\mu}}\right).$$

And T_{mp^s} corresponds to the irreducible polynomial $(x-1)$ over the field $\mathbb{F}_q$.

$\Omega_{p^s,0} = \{t, tq\} \subset \{p^s, 2p^s, 3p^s, 4p^s, 5p^s, \ldots\ldots\ldots, (m-1)p^s\}$ *corresponds to an irreducible polynomial,* $f_{p^s,0}(x) = \prod_{\mu=0}^{1}(x - \xi_m^{v_k q^{\mu}})$. So the number of irreducible factors of $x^{mp^s} - 1$ over the field $\mathbb{F}_q$ is:

$$1 + \frac{m-1}{2} + \frac{m(p^s-1)}{2} = 1 + \frac{(mp^s-1)}{2}.$$

Lemma 3.2 There are $1 + \frac{(mp^s-1)}{2}$ irreducible factors of the polynomial $x^{mp^s} - 1$ over the field $\mathbb{F}_q$ as follows: $x - 1$ for T_{mp^s} ; for elements of T_0, $f_{p^s,0}(x) = \prod_{\mu=0}^{1}(x - \xi_m^{v_k q^{\mu}})$, $k = 1, 2, 3, \ldots\ldots\ldots, \frac{m-1}{2}$ and for elements of T_r^*, $1 \leq r \leq s$

$$f_{r,v_k}(x) = \prod_{\mu=0}^{1}\left(x - \xi_{mp^r}^{v_k q^{\mu}}\right),\ k = 1,2, \ldots\ldots\ldots, \frac{m\phi(p^r)}{2} \quad (3.2)$$

Recall that the number of primitive idempotents in ring $\mathbb{F}_q[x]/\langle x^{mp^s} - 1\rangle$ are same as the number of irreducible factors of $x^{mp^s} - 1$ over $\mathbb{F}_q$.

Theorem 3.3 There are $1 + \frac{(mp^s-1)}{2}$ primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{mp^s} - 1\rangle$. These primitive idempotents are given as:

(i) The primitive idempotent

$$\theta_{s,mp^s}(x) = \frac{1}{mp^s}\sum_{i=0}^{mp^s-1}(x)^i$$

corresponds to the irreducible polynomial $x - 1$ over $\mathbb{F}_q$.

(ii) For elements of T_0, the primitive idempotents,

$$\theta_{p^s,0}(x) = \frac{1}{mp^s}\sum_{i=0}^{mp^s-1} Tr(\xi_m^{-v_k i})(x)^i\,, \text{where } k = 1, 2, 3, \ldots\ldots\ldots, \frac{m-1}{2}$$

corresponds to the irreducible polynomial $f_{p^s,0}(x) = \prod_{\mu=0}^{1}(x - \xi_m^{v_k q^{\mu}})$ over $\mathbb{F}_q$.

(iii) For $1 \leq r \leq s$, $p^{s-r}v_k \in T_r^*$

$$\theta_{s,v_k}(x) = \frac{1}{mp^s} \cdot \frac{x^{mp^s}-1}{x^{mp^r}-1} \sum_{i=0}^{mp^r-1} Tr(\xi_{mp^r}^{-v_k i})(x)^i \tag{3.3}$$

corresponds to the irreducible polynomial $f_{r,v_k}(x)$ over $\mathbb{F}_q$, $k = 1, 2, 3, \ldots\ldots\ldots, \frac{\mathrm{m}\Phi(p^r)}{2}$, respectively.

Proof: By Equation (3.1), we have $\mathbb{F}_{q^2}-$ algebra isomorphism:

$$\varphi : \mathbb{F}_{q^2}[x]/\langle x^{mp^s}-1\rangle \longrightarrow \prod_{j=0}^{mp^s-1} \mathbb{F}_{q^2}[x]/\langle (x-\xi_{mp^s}^j)\rangle, \tag{3.4}$$

$$\sum_{i=0}^{mp^s-1} a_i\, x^i \longmapsto \left(\sum_{i=0}^{mp^s-1} a_i\,, \sum_{i=0}^{mp^s-1} a_i \left(\xi_{mp^s}^1\right)^i, \ldots\ldots\ldots, \sum_{i=0}^{mp^s-1} a_i \left(\xi_{mp^s}^{mp^s-1}\right)^i \right)$$

Let M be the $mp^s \times mp^s$ character matrix as follows:

$$M = \begin{pmatrix} (\xi_{mp^s}^0)^0 & (\xi_{mp^s}^1)^0 & \cdots & (\xi_{mp^s}^{mp^s-1})^0 \\ (\xi_{mp^s}^0)^1 & (\xi_{mp^s}^1)^1 & \cdots & (\xi_{mp^s}^{mp^s-1})^1 \\ \vdots & \vdots & & \vdots \\ (\xi_{mp^s}^0)^{mp^s-1} & (\xi_{mp^s}^1)^{mp^s-1} & \cdots & (\xi_{mp^s}^{mp^s-1})^{mp^s-1} \end{pmatrix}$$

Then we have

$$\varphi\left(\sum_{i=0}^{mp^s-1} a_i\, x^i\right) = (a_0, a_1, a_2, \ldots\ldots\ldots, a_{mp^s-1})M = (b_0, b_1, b_2, \ldots\ldots\ldots, b_{mp^s-1}). \tag{3.5}$$

By Lemma 2.2

$$M^{-1} = \frac{1}{mp^s} \begin{pmatrix} (\xi_{mp^s}^0)^{-0} & (\xi_{mp^s}^0)^{-1} & \cdots & (\xi_{mp^s}^0)^{-(mp^s-1)} \\ (\xi_{mp^s}^1)^{-0} & (\xi_{mp^s}^1)^{-1} & \cdots & (\xi_{mp^s}^1)^{-(mp^s-1)} \\ \vdots & \vdots & & \vdots \\ \left(\xi_{mp^s}^{(mp^s-1)}\right)^{-0} & \left(\xi_{mp^s}^{(mp^s-1)}\right)^{-1} & \cdots & \left(\xi_{mp^s}^{(mp^s-1)}\right)^{-(mp^s-1)} \end{pmatrix}$$

It is obvious that $(b_0, b_1, b_2, \ldots\ldots\ldots, b_{mp^s-1}) = (1,0, \ldots\ldots\ldots, 0) = e$ is the primitive idempotent of $\prod_{t=0}^{mp^s-1} \mathbb{F}_{q^2}[x]/\langle (x-\xi_{mp^s}^j)\rangle$. According to the inverse Fourier transform, we get the primitive idempotents $\theta_{s,mp^s}(x) = \sum_{i=0}^{mp^s-1} a_i\, x^i$ in the ring $\mathbb{F}_{q^2}[x]/\langle x^{mp^s}-1\rangle$, which just corresponds to the irreducible polynomial $x-1$ over the field $\mathbb{F}_q$.

Namely

$$\varphi\left(\theta_{s,mp^s}(x)\right) = (a_0, a_1, a_2, \ldots\ldots\ldots, a_{mp^s-1})T = e,$$

$$(a_0,\ a_1,\ a_2, \ldots\ldots\ldots, a_{mp^s-1}) = eT^{-1} = \frac{1}{mp^s}(1^{-0}, 1^{-1}, 1^{-2}, \ldots\ldots, 1^{-(mp^s-1)}),$$

$$\theta_{s,mp^s}(x) = \frac{1}{mp^s} \sum_{i=0}^{mp^s-1} (x)^i.$$

(ii) In equation 3.4, take $(b_0, b_1, b_2, \ldots\ldots\ldots, b_{mp^s-1})$, where $b_w = 1$ if $w \in \Omega_{p^s,0}$, otherwise $b_w = 0$. Hence,

$$(a_0, a_1, a_2, \dots, a_{mp^s-1}) = (b_0, b_1, b_2, \dots, b_{mp^s-1})M^{-1}$$
$$= \frac{1}{mp^s}\left(Tr(\xi_m^{-0.v_k}), Tr(\xi_m^{-1.v_k}), \dots\dots, Tr\left(\xi_m^{-v_k(mp^s-1)}\right)\right)$$

$\therefore$ $$\theta_{p^s,0}(x) = \frac{1}{mp^s}\sum_{t=0}^{mp^s-1} Tr(\xi_m^{-v_k t})(x)^t$$

corresponds to the polynomial $f_{p^s,0}(x) = \prod_{\mu=0}^{1}(x - \xi_m^{v_k q^\mu})$.

(*iii*)If $1 \le r \le s$, then we divide into two sub cases.

Sub case (i): If $r = s$ and each $t = v \in T_s^*$ with $gcd(v,p) = 1$. By Lemma 3.2, there is an irreducible polynomial $f_{s,v}(x) = \sum_{\mu=0}^{1}(x - \xi_{mp^r}^{vq^\mu})$ over the field $\mathbb{F}_q$. It is well-known that there is a natural $\mathbb{F}_{q^2}$ −algebra isomorphism-

$$\varphi_1 : \mathbb{F}_{q^2}[x]/\langle f_{s,v}(x)\rangle \longrightarrow \prod_{\mu=0}^{1}\mathbb{F}_{q^2}[x]/\langle x - \xi_{mp^s}^{vq^\mu}\rangle,$$

$$c(x) = \sum_{\mu=0}^{1} c_\mu\, x^\mu \longmapsto \left(\sum_{\mu=0}^{1} c_\mu\left(\xi_{mp^s}^{v}\right)^\mu, \sum_{\mu=0}^{1} c_\mu\left(\xi_{mp^s}^{vq}\right)^\mu\right).$$

Note that the identity of the ring $\mathbb{F}_{q^2}[x]/\langle f_{s,v}(x)\rangle$ is equal to identity of the ring $\mathbb{F}_q[x]/\langle f_{s,v}(x)\rangle$.

Let P be the 2×2 character matrix as follows:

$$\mathrm{P} = \begin{pmatrix} \left(\xi_{mp^s}^{v}\right)^0 & \left(\xi_{mp^s}^{vq}\right)^0 \\ \left(\xi_{mp^s}^{v}\right)^1 & \left(\xi_{mp^s}^{vq}\right)^1 \end{pmatrix}$$

$$\varphi_1(c(x)) = (c_0, c_1)P.$$

Take $c(x) = 1$, then we have $\varphi_1(1) = (1,0)P = (1,1)$.

In equation 3.4, take $(b_0, b_1, b_2, \dots\dots\dots, b_{mp^s-1})$, where $b_j = 1$ if $t \in \{v, vq\}$, otherwise $b_j = 0$. Hence

$$(a_0, a_1, a_2, \dots, a_{mp^s-1}) = (b_0, b_1, b_2, \dots, b_{mp^s-1})M^{-1}$$

$$= \frac{1}{mp^s}\left(Tr\left(\left(\xi_{mp^s}^{v}\right)^{-0}\right), Tr\left(\left(\xi_{mp^s}^{v}\right)^{-1}\right), \dots\dots, Tr\left(\left(\xi_{mp^s}^{v}\right)^{-(mp^s-1)}\right)\right)$$

(i)

Therefore there is a primitive idempotent

$$\theta_{s,v}(x) = \frac{1}{mp^s}\sum_{i=0}^{mp^s-1} Tr(\xi_{mp^s}^{-vi})(x)^i$$

in the ring $\mathbb{F}_q[x]/\langle x^{mp^s} - 1\rangle$ which corresponds to the irreducible polynomial $f_{s,v}(x)$ over the field $\mathbb{F}_q$.

Sub case (ii): If $1 \le r < s$ and for each $t = p^{s-r}v \in T_r^*$ $gcd(v,p) = 1$. By Lemma 3.2, there is an irreducible polynomial $f_{r,v} = \prod_{\mu=0}^{1}(x - \xi_{mp^r}^{vq^\mu})$ over $\mathbb{F}_q$. Replacing s by r in above discussion, we can get the primitive idempotent

$$\theta_{r,v}(x) = \frac{1}{mp^r} \sum_{i=0}^{mp^r-1} (Tr(\xi_{mp^r}^{-ui})(x)^i$$

In the ring $\mathbb{F}_q[x]/\langle x^{mp^r} - 1\rangle$ which corresponds to an irreducible polynomial $f_{r,v}(x)$. By (3.1), there is the natural $\mathbb{F}_q$ −algebraic isomorphism:

$$\varphi_2 : \frac{\mathbb{F}_q[x]}{\langle x^{mp^s} - 1\rangle} \to \frac{\mathbb{F}_q[x]}{\langle x^{mp^r} - 1\rangle} \times \prod_{i=r+1}^{s} \frac{\mathbb{F}_q[x]}{\langle \Psi_i(x)\rangle}$$

$$\theta_{s-r}(x) = \frac{1}{p^{s-r}} \cdot \frac{x^{mp^s}-1}{x^{mp^r}-1} \longmapsto (1,0,0,\dots\dots\dots,0)$$

Hence $\theta_{s,v_k}(x) = \theta_{s-r}(x)\theta_{r,v_k}(x)$ are the primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{mp^s} - 1\rangle$, which corresponds to the irreducible polynomials $f_{r,v}(x)$ over the field $\mathbb{F}_q$ for $k = 1,2,\dots\dots\dots,\frac{m\Phi(p^r)}{2}$.

■

4. THE WEIGHT DISTRIBUTIONS OF IRREDUCIBLE CYCLIC CODES OF LENGTH mp^s

In this section, we suppose that $q^2 \equiv 1(mod\ mp^s)$ and $gcd(mp, q(q-1)) = 1$, where $p > m$ be a prime number. In the following part, we give all the weight distributions of irreducible cyclic codes over the field $\mathbb{F}_q$ by primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{mp^s} - 1\rangle$.

Let $\mathcal{C}$ denotes the irreducible cyclic code of length mp^s generated by a primitive idempotent $\theta(x)$ whose parity-check polynomial is the irreducible divisor of $x^{mp^s} - 1$. Further, it is clear that $\mathcal{C} = \langle\theta(x)\rangle = \langle g(x)\rangle$, where $g(x) = \gcd(\theta(x), x^{mp^s} - 1)$ is called generator polynomial of the irreducible cyclic code $\mathcal{C}$.

Lemma 4.1. [8] Let $\mathcal{C}$ be the [*n, k'*] code over the field $\mathbb{F}_q$ with enumerator *A(z)* and let *B(z)* be weight enumerator of $\mathcal{C}^{\perp}$. Then

$$B(z) = q^{-k'}(1 + (q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right).$$

Lemma 4.2. *Suppose that* $1 \le r \le s$ *and* $gcd(p, v_k) = 1$. *Then all the two distinct columns of the following* $2 \times mp^r$ *matrix*

$$\begin{bmatrix} Tr(\xi_{mp^r}^{-v_k 0}) & Tr(\xi_{mp^r}^{-v_k 1}) \dots\dots & Tr(\xi_{mp^r}^{-v_k(mp^r-1)}) \\ Tr(\xi_{mp^r}^{-v_k(mp^r-1)}) & Tr(\xi_{mp^r}^{-v_k 0}) \dots\dots & Tr(\xi_{mp^r}^{-v_k(mp^r-2)}) \end{bmatrix}$$

are linear independent over the field $\mathbb{F}_q$.

Proof: Without loss of generality, we can suppose that $u = 1$. For $0 \le i < j \le mp^r - 1$, $Tr(\xi_{mp^r}^{-i}) = Tr(\xi_{mp^r}^{i}) = \xi_{mp^r}^{i} + \xi_{mp^r}^{-i}$ by $q = -1(mod\ mp^s)$ and the determinant

$$\begin{vmatrix} Tr(\xi_{mp^r}^{-i}) & Tr(\xi_{mp^r}^{-j}) \\ Tr(\xi_{mp^r}^{-(i-1)}) & Tr(\xi_{mp^r}^{-(j-1)}) \end{vmatrix} = Tr(\xi_{mp^r}^{j-i+1}) - Tr(\xi_{mp^r}^{j-i-1}) \neq 0$$

■

Theorem 4.3. *From theorem 3.3, the weight distributions of all irreducible cyclic codes of length* mp^s *as follows:-*

(i) $\mathcal{C}_0 = \langle \theta_{s,mp^s}(x) \rangle$ *is an* $[mp^s, 1, mp^s]$ *cyclic code with parity-check polynomial* $x - 1$.

(ii) *For the elements of* T_0, $\mathcal{C}_{p^s,0} = \langle \theta_{p^s,0}(x) \rangle$ *is a* $[mp^s, 2, (m-1)p^s]$ *cyclic code with parity check polynomial* $f_{p^s,0}(x) = x^2 - Tr(\xi_m^{v_k})x + 1$ *and its Hamming weight enumerator polynomial is given by*

$$1 + m(q^{k'} - 1)z^{(m-1)p^s} + (q^{2k'} - 1 - m(q^{k'} - 1))z^{mp^s}.$$

(iii) *If* $1 \le r \le s$ *and* $mp^{s-r}v_k \in T_r^*$, $k = 1, 2, \ldots\ldots, \frac{m\phi(p^r)}{2}$, *then each* $\mathcal{C}_{s,v_k} = \langle \theta_{s,v_k}(x) \rangle$ *is a* $[mp^s, 2, mp^s - p^{s-r}]$ *cyclic code with parity-check polynomial* $f_{r,v_k}(x) = x^2 - Tr(\xi_{mp^r}^{v_k})x + 1$ *and its Hamming weight enumerator polynomial is given by*

$$1 + mp^r(q^{k'} - 1)z^{(mp^s - p^{s-r})} + (q^{2k'} - 1 - mp^r(q^{k'} - 1))z^{mp^s}.$$

Proof: We only need to prove the case *(iii)*. Suppose that $1 \le r \le s$ *and* $mp^{s-r}v_k \in T_r^*$. Then, we have $\xi_{p^r}^{qv_k} = \xi_{p^r}^{-v_k}$ by $p^s | (q+1)$. Let $R_s = \mathbb{F}_q[x]/\langle x^{mp^s} - 1 \rangle$ then by the construction of the primitive idempotent $\theta_{s,v_k}(x)$ we get

$$\mathcal{C}_{s,v_k} = \langle \theta_{s,v_k}(x) \rangle = R_s\theta_{s,v_k}(x) \cong \mathbb{F}_q[x]/\langle f_{r,v_k}(x) \rangle,$$

Where

$f_{r,v_k}(x) = \left(x - \xi_{mp^r}^{v_k}\right)\left(x - \xi_{mp^r}^{-v_k}\right) = x^2 - Tr(\xi_{mp^r}^{v_k})x + 1$ is the parity check polynomial of $\mathcal{C}_{s,mp^{s-r}v_k}$.

Hence $\mathcal{C}_{s,v_k} = \{r(x)\theta_{s,v_k}(x) : r(x) = a_0 + a_1(x);\ a_0, a_1 \in \mathbb{F}_q\}$.

Further it is clear that

$$\frac{x^{mp^s} - 1}{x^{mp^r} - 1}(x)^{mp^r} \equiv \frac{x^{mp^s} - 1}{x^{mp^r} - 1} mod(x^{mp^s} - 1).$$

Let $f(x) \in R_s = \mathbb{F}_q[x]/\langle x^{mp^s} - 1 \rangle$ then the number of non-zero coefficients of $f(x)$ of degree atmost $mp^s - 1$ is called the Hamming weight, which is denoted by $W(f(x))$.

For $r(x)\,\theta_{s,v_k}(x) \in \mathcal{C}_{s,v_k}$ and $gcd(v_k, p^r) = 1$,

$$W\left(r(x)\theta_{s,v_k}(x)\right) = p^{s-r}W\left(r(x)\theta_{r,v_k}(x)\right),$$

Where

$r(x)\,\theta_{s,v_k}(x) \in R_r = \mathbb{F}_q[x]/\langle x^{mp^r} - 1 \rangle$ and $(x)^{mp^r} \equiv 1\ mod(x^{mp^r} - 1)$.

Assume that $p^r r(x)\,\theta_{r,v_k}(x) \equiv [b_0 + b_1x + \ldots\ldots\ldots, b_{mp^r-1}(x)^{mp^r-1}] mod\left(x^{mp^r} - 1\right)$,

Then, we have

$$(b_0, b_1, \ldots\ldots\ldots, b_{mp^r-1})$$

$$= \frac{1}{m}(a_0, a_1)\begin{pmatrix} Tr(\xi_{mp^r}^{-v_k 0}) & Tr(\xi_{mp^r}^{-v_k 1}) & \ldots\ldots\ldots & Tr(\xi_{mp^r}^{-v_k(mp^r-1)}) \\ Tr(\xi_{mp^r}^{-v_k(mp^r-1)}) & Tr(\xi_{mp^r}^{-v_k 0}) & \ldots\ldots\ldots & Tr(\xi_{mp^r}^{-v_k(mp^r-2)}) \end{pmatrix}$$

We shall divide $\wedge = \{(a_0, a_1) \in \mathbb{F}_q \times \mathbb{F}_q\}$ into three subsets:

$$\wedge_1 = \left\{ (a_0, a_1) \in \wedge : -\frac{a_0}{a_1} \in \left\{ \frac{Tr(\xi_{mp^r}^{-v_k(mp^r-1)})}{Tr(\xi_{mp^r}^{-v_k.0})}, \dots\dots\dots, \frac{Tr(\xi_{mp^r}^{-v_k.(mp^r-2)})}{Tr(\xi_{ml^h}^{-v_k(mp^r-1)})} \right\} \right\}$$

$$\wedge_0 = \{(0,0)\}, \quad \wedge_2 = \wedge \setminus (\wedge_0 \cup \wedge_1).$$

If $(a_0, a_1) \in \wedge_0$, then $(b_0, b_1, \dots\dots\dots, b_{mp^r-1}) = 0$ and $W\left(r(x)\theta_{s,v_k}(x)\right) = 0$.

If $(a_0, a_1) \in \wedge_1$, then only one of $b_0, b_1, \dots\dots\dots, b_{mp^r-1}$ is equal to 0 and $W\left(r(x)\theta_{s,v_k}(x)\right) = p^{s-r}(mp^r - 1)$.

If $(a_0, a_1) \in \wedge_2$, then all $b_0, b_1, \dots\dots\dots, b_{mp^r-1}$ are not equal to 0 and $W\left(r(x)\theta_{s,v_k}(x)\right) = mp^s$.

On the other hand, $|\wedge_0| = 1$, $|\wedge_1| = mp^r(q^{k'} - 1)$ by Lemma 4.2, and $|\wedge_2| = (q^{2k'} - 1 - mp^r(q^{k'} - 1))$, which provides the frequency of the weights. Hence the Hamming weight enumerator polynomial of each $\mathcal{C}_{s,v_k}$ is $1 + mp^r(q^{k'} - 1)z^{(mp^s - p^{s-r})} + (q^{2k'} - 1 - mp^r(q^{k'} - 1))z^{mp^s}$.

■

By Lemma 4.1, we have the following conclusion:

Corollary 4.4. *In Theorem 4.3, if* $1 \le r \le s$, $mp^{s-r}v_k \in T_r^*$, $k = 1,2,\dots\dots\dots, \frac{m.\phi(p^r)}{2}$, *then the Hamming weight enumerator polynomial of* $\mathcal{C}_{s,v_k}^{\perp}$ *is* $q^{-2}((1 + (q-1)z)^{mp^s} + mp^r(q-1)(z-1)^{(mp^s - p^{s-r})}(1 + (q-1)z)^{mp^{s-r}} - (q^2 - 1 - mp^r(q-1))(z-1)^{mp^s})$.

5. EXAMPLE

In this section, we give a example in support of our results.

We assume that $p > 5$ *is a prime number with* $gcd(5p, q(q-1)) = 1$, $q \equiv -1(mod\ 5p^s)$, *m is a positive integer.*

Example 5.1: *Let* $p = 7, q = 3919, s = 2$. *Then* $5p^s = 245$, then we have $T = \{1,2,3,\dots,244\}$, $T_{245} = \{245\}$ and $T_0 = \{49,98,147,196\}$.

$T_1{}^* = \{7,14,21,28,35,42,56,63,\dots,238\}$, $T_2{}^* = \{1,2,3,4,5,6,8,9,\dots,244\}$.

Since $q \equiv -1(mod\ 245)$ the distinct q cosets are given by

$\Omega_{1,1} = \{7, 238\}$, $\Omega_{1,3} = \{21, 224\}$, $\Omega_{1,5} = \{35, 210\}$, $\Omega_{1,9} = \{63, 182\}$, $\Omega_{1,11} = \{77, 168\}$, $\Omega_{1,13} = \{91, 154\}$, $\Omega_{1,15} = \{105, 140\}$, $\Omega_{1,17} = \{119, 126\}$, $\Omega_{1,19} = \{133, 112\}$, $\Omega_{1,23} = \{161, 84\}$, $\Omega_{1,25} = \{175, 70\}$, $\Omega_{1,27} = \{189, 56\}$, $\Omega_{1,29} = \{203, 42\}$, $\Omega_{1,31} = \{217, 28\}$, $\Omega_{1,33} = \{231, 14\}$.

$\Omega_{2,1} = \{1, 244\}$, $\Omega_{2,3} = \{3, 242\}$, $\Omega_{2,5} = \{5, 240\}$, $\Omega_{2,9} = \{9, 236\}$, $\Omega_{2,11} = \{11, 234\}$, $\Omega_{2,13} = \{13, 232\}$, $\Omega_{2,15} = \{15, 230\}$, $\Omega_{2,17} = \{17, 228\}$, $\Omega_{2,19} = \{19, 226\}$, $\Omega_{2,23} = \{23, 222\}$, $\Omega_{2,25} = \{25, 220\}$, $\Omega_{2,27} = \{27, 218\}$, $\Omega_{2,29} = \{29, 216\}$, $\Omega_{2,31} = \{31, 214\}$, $\Omega_{2,33} = \{33, 212\}$, $\Omega_{2,37} = \{37, 208\}$, $\Omega_{2,39} = \{39, 206\}$, $\Omega_{2,41} = \{41, 204\}$, $\Omega_{2,43} = \{43, 202\}$, $\Omega_{2,45} = \{45, 200\}$, $\Omega_{2,47} = \{47, 198\}$, $\Omega_{2,51} = \{51, 194\}$, $\Omega_{2,53} = \{53, 192\}$, $\Omega_{2,55} = \{55, 190\}$, $\Omega_{2,57} = \{57, 188\}$, $\Omega_{2,59} = \{59, 186\}$, $\Omega_{2,61} = \{61, 184\}$, $\Omega_{2,65} = \{65, 180\}$, $\Omega_{2,67} = \{67, 178\}$, $\Omega_{2,68} = \{68, 177\}$, $\Omega_{2,69} = \{69, 176\}$, $\Omega_{2,71} = \{71, 174\}$, $\Omega_{2,73} = \{73, 172\}$, $\Omega_{2,75} = \{75, 170\}$, $\Omega_{2,79} = \{79, 166\}$, $\Omega_{2,81} = \{81, 164\}$, $\Omega_{2,83} = \{83, 162\}$, $\Omega_{2,85} = \{85, 160\}$, $\Omega_{2,87} = \{87, 158\}$, $\Omega_{2,89} = \{89, 156\}$, $\Omega_{2,93} = \{93, 152\}$, $\Omega_{2,95} = \{95, 150\}$, $\Omega_{2,97} = \{97, 148\}$, $\Omega_{2,99} = \{99, 146\}$, $\Omega_{2,101} = \{101, 144\}$, $\Omega_{2,103} = \{103, 142\}$, $\Omega_{2,107} = \{107, 138\}$, $\Omega_{2,109} = \{109, 136\}$, $\Omega_{2,111} = \{111, 134\}$, $\Omega_{2,113} = \{113, 132\}$, $\Omega_{2,115} = \{115, 130\}$, $\Omega_{2,117} = \{117, 128\}$, $\Omega_{2,121} = \{121, 124\}$, $\Omega_{2,123} =$

$\{123, 122\}, \Omega_{2,125} = \{125, 120\}, \Omega_{2,127} = \{127, 118\}, \Omega_{2,129} = \{129, 116\}, \Omega_{2,131} = \{131, 114\}, \Omega_{2,135} = \{135, 110\}, \Omega_{2,137} = \{137, 108\}, \Omega_{2,139} = \{139, 106\}, \Omega_{2,141} = \{141, 104\}, \Omega_{2,143} = \{143, 102\}, \Omega_{2,145} = \{145, 100\}, \Omega_{2,149} = \{149, 96\}, \Omega_{2,151} = \{151, 94\}, \Omega_{2,153} = \{153, 92\}, \Omega_{2,155} = \{155, 90\}, \Omega_{2,157} = \{157, 88\}, \Omega_{2,159} = \{159, 86\}, \Omega_{2,163} = \{163, 82\}, \Omega_{2,165} = \{165, 80\}, \Omega_{2,167} = \{167, 78\}, \Omega_{2,169} = \{169, 76\}, \Omega_{2,171} = \{171, 74\}, \Omega_{2,173} = \{173, 72\}, \Omega_{2,177} = \{177, 68\}, \Omega_{2,179} = \{179, 66\}, \Omega_{2,181} = \{181, 64\}, \Omega_{2,183} = \{183, 62\}, \Omega_{2,185} = \{185, 60\}, \Omega_{2,187} = \{187, 58\}, \Omega_{2,191} = \{191, 54\}, \Omega_{2,193} = \{193, 52\}, \Omega_{2,195} = \{195, 50\}, \Omega_{2,197} = \{197, 48\}, \Omega_{2,199} = \{199, 46\}, \Omega_{2,201} = \{201, 44\}, \Omega_{2,205} = \{205, 40\}, \Omega_{2,207} = \{207, 38\}, \Omega_{2,209} = \{209, 36\}, \Omega_{2,211} = \{211, 34\}, \Omega_{2,213} = \{213, 32\}, \Omega_{2,215} = \{215, 30\}, \Omega_{2,219} = \{219, 26\}, \Omega_{2,221} = \{221, 24\}, \Omega_{2,223} = \{223, 22\}, \Omega_{2,225} = \{225, 20\}, \Omega_{2,227} = \{227, 18\}, \Omega_{2,229} = \{229, 16\}, \Omega_{2,233} = \{233, 12\}, \Omega_{2,235} = \{235, 10\}, \Omega_{2,237} = \{237, 8\}, \Omega_{2,239} = \{239, 6\}, \Omega_{2,241} = \{241, 4\}, \Omega_{2,243} = \{243, 2\}$, The three classes of irreducible cyclic codes of length 245 in $\mathbb{F}_q[x]/\langle x^{5l^m} - 1\rangle$ are the following:

(1) There is *one* [245,1,245] irreducible cyclic code with parity check polynomial $x - 1$.

(2) There are *two* [245,2,196] irreducible cyclic codes with parity check polynomial $x^2 - Tr(\xi_5)x + 1$ and its hamming weight enumerator polynomial is $1 + 5(3919^{k'} - 1)z^{196} + (3919^{2k'} - 1 - 5(3919^{k'} - 1))z^{245}$.

(3) There are $fifteen$ [245,2,238] irreducible cyclic codes with parity check polynomial $x^2 - Tr(\xi_{35})x + 1$ and its hamming weight enumerator polynomial is $1 + 35(3919^{k'} - 1)z^{238} + (3919^{2k'} - 1 - 35(3919^{k'} - 1))z^{245}$.

(4) There are *one hundred five* [245,2,244] irreducible cyclic codes with parity check polynomial $x^2 - Tr(\xi_{245})x + 1$ and its hamming weight enumerator polynomial is $1 + 245(3919^{k'} - 1)z^{244} + (3919^{2k'} - 1 - 245(3919^{k'} - 1))z^{245}$.

REFERENCES

[1] Arora, S. K., Batra, S., Cohen, S. D., and Pruthi, M., The primitive idempotents of a cyclic group algebra, Southeast Asian Bull. Math. 26, (2002) pp. 197-208.

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

[3] Batra, S., and Arora, S. K., Some cyclic codes of length $2p^n$, Des. Codes Cryptogr. 61, (2011) pp.41-69.

[4] Bakshi, G. K., and Raka, M., Minimal cyclic codes of length p^nq, Finite Fields Appl. 9, (2003) pp.432-448.

[5] Chen, B., Fan, Y., Lin, L., and Liu, H., Constacyclic codes over finite fields, Finite Fields Appl. 18, (2012) pp.1217-1231.

[6] Chen, B., Liu, H., and Zhang, G., A class of minimal cyclic codes over finite fields, Des. Codes Cryptogr. 74, (2015) pp.285-300.

[7] Kumar, S., Pankaj., Pruthi, M., The Minimum Hamming Distances of the irreducible cyclic codes of length $2^a p_1^{a_1} p_2^{a_2} \dots p_e^{a_e}$, Int. Journal of Mathematics and Statistics Invention vol.4, (2016) pp.44-70.

[8] Lidl, R., and Niederreiter, H., Finite Fields, Cambridge University Press, Cambridge (2008).

[9] Lint, J.H.van., Introduction to Coding Theory, Springer-Verlag, Berlin (2003).

[10] Li, F., Yue, Q., and Li, C., The minimum Hamming distances of irreducible cyclic codes, Finite Field Appl. 29, (2014) pp.225-242.

[11] Li, F., Yue, Q., and Li, C., The irreducible cyclic codes of length $4p^n$ and $8p^n$, Finite Field Appl. 34, (2015) pp.208-234.
[12] Li, F., Yue, Q., The primitive idempotents and weight distributions of irreducible constacyclic codes, Des. Codes Cryptogr. 3 DOI: 10.1007/s10623-017-0356 - 2(2017).
[13] MacWilliams, F.J., and Sloane, N.J.A., The Theory of Error Correcting Codes, North Holland, Amsterdam (1977).
[14] Pruthi, M., Cyclic codes of length 2^m, Proc. Indian Acad. Sci. Math. Sci. 111, (2001) pp.371-379.
[15] Pruthi, M., and Arora, S. K., Minimal cyclic codes of prime power length, Finite Fields Appl. 3, (1997) pp.99-113.
[16] Sharma, A., Bakshi, G. K., Dumir, V. C., and Raka, M., Irreducible cyclic codes of length 2^n, Ars Combin. 86, (2008) pp.133-146.
[17] Singh, R., and Pruthi, M., Primitive idempotents of irreducible quadratic residue cyclic codes of length $p^n q^m$, Int. J. Algebra 5, (2011) pp.285-294.
[18] Wan, Z., Lectures on Finite Fields and Galois Rings, World Scientific Publishing, Singapore (2003).