RESEARCH REVIEW JOURNALS
Volume-04
Issue-04
April -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

# Some Cyclic Codes and their Weight Distributions

[1]Sunil Kumar, [2]Manju Pruthi & [*3]Rahul

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

**ARTICLE DETAILS**

**Article History**
*Published Online:* 15 April 2019

**Keywords**
Cyclic Code, Weight Distribution.

**[*]Corresponding Author**
*Email: rahulydv92[at]yahoo.com*

**ABSTRACT**

Let $\mathbb{F}_q$ be a field with $q$ elements such that $gcd(7p, q(q-1)) = 1$ and $q^2 \equiv 1(mod\ 7p^s)$, where $p > 7$ is prime. In this paper, we give all primitive idempotents in a ring $\mathbb{F}_q[x]/\langle x^{7p^s} - 1\rangle$. We give the weight distributions of all irreducible cyclic codes of length $7p^s$ over $\mathbb{F}_q$.

## 1. INTRODUCTION

Let $\mathbb{F}_q$ be field with $q$ elements. Let $\mathcal{C}$ be a $[n, k]$ linear code over $\mathbb{F}_q$, that is , it is $k$-dimensional subspace of $\mathbb{F}_q^n$. 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 a 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 the field $\mathbb{F}_q$ corresponds to the subset of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Then $\mathcal{C}$ is said to be a cyclic code iff the corresponding subset is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Note that each ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is the principal ideal. Suppose that $g(x)$ is monic divisor of $x^n - 1$ in the field $\mathbb{F}_q$. Then code $\mathcal{C}$ which corresponds to $\langle g(x)\rangle$ is cyclic code, $g(x)$ is called the 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 a irreducible factor over $\mathbb{F}_q$, we refer the cyclic code as irreducible. 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 primitive idempotents.

A lot of papers investigated the primitive idempotents of $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ which are described as follows:
For $n$ = 2, 4, $l^m$ and $2l^m$, where $l$ is odd prime and $q$ (prime power) is primitive root modulo $n$, Arora and Pruthi got the primitive idempotents in $R_n$ in [2, 15]. For $n = 2^m$, $m \geq 3$. Pruthi gave explicit expressions of m + 1 idempotents in the ring $R_n$; Sharma et al. obtained all the primitive idempotents and irreducible cyclic codes in $R_n$ in [14, 17]. For $n = l_1^m l_2$, where $l_1, l_2, q$ are distinct odd primes, $q$ is a 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 the $3m + 2$ primitive idempotents in the ring $R_n$ in [4]. For $n = l_1^m l_2^m$, where $l_1, l_2, q$ are distinct odd primes, $gcd(\phi(l_1^m), \phi(l_2^m)) = 2$, $ord_{l_1^{m_1}}(q) = \frac{\phi(l_1^{m_1})}{2}$ and $ord_{l_2^{m_2}}(q) = \frac{\phi(l_2^{m_2})}{2}$. Singh and Pruthi presented explicit expressions for all the $4m_1m_2 + 2m_1 + 2m_2 + 1$ primitive idempotents in the 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 explicit expressions for the $2m + 1$ primitive idempotents in $R_n$ in [1]. For $n = 2l^m$, $m \geq 1$, where $l$ is an odd prime and $ord_{2l^m}(q) = \frac{\phi(2l^m)}{2}$. Batra and Arora got explicit expressions for $4m + 2$ primitive idempotents in $R_n$ in [3]. For $n = l^m$, $m \geq 1$, where $l$ is an odd prime and $l/(q-1)$, Chen et ' al. recursively gave the primitive idempotents and the minimum Hamming distances of the codes generated by those primitive idempotents in $R_n$ in [6]. For $n = l_1^m l_2^m$, $m_1 \geq 1, m_2 \geq 1$ where $l_1, l_2$ are distinct primes and $l_1 l_2/(q-1)$; $n = 4l^m$ and $8l^m$, where $l$ is an odd prime and $l/(q-1)$, Li and Yue et al. obtained all primitive idempotents and the minimum Hamming distances of the codes generated by those primitive idempotents in $R_n$, respectively in [10, 11]. In [12] Fengwei Li and Qin Yue take $F_q$, a finite field with $q$ elements such that $l^v \| (q^t - 1)$ and $gcd(l, q(q-1)) = 1$, where $l, t$ are primes and $v$ is a positive integer. They gave all primitive idempotents in a ring $F_q[x]/\langle x^{l^m} - a\rangle$ for a $\in F_q^*$. Specially for $t = 2$, they gave the weight distributions of all irreducible constacyclic codes and their dual codes of length $l^m$ over $F_q$. In [7], S. Kumar, Pankaj and M. Pruthi take $F_l$, a finite field with $l$ elements and $n = 2^a p_1^{a_1} p_2^{a_2} \dots p_e^{a_e}$, where $a, a_1, a_2, \dots, a_e$ are positive integers and $p_1, p_2, \dots, p_e$ are distinct odd primes and $4p_1, p_2, \dots, p_e/l - 1$. They study the factorization of $x^{2^a p_1^{a_1} p_2^{a_2} \dots p_e^{a_e}} - 1$ over $F_l$ and all primitive idempotents in the 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 obtain the dimensions and the minimum hamming distances of all irreducible cyclic codes of length $2^a p_1^{a_1} p_2^{a_2} \dots p_e^{a_e}$ over $F_l$. In [16], S. Sehrawat and M. Pruthi considered the group algebra FG, where characteristic of the field F does not divide order of the group G. They gave explicit expressions for the idempotents in the group algebra of dihedral group of order $2n$, for every $n$. They also described [$2n$, $2n$-1, 2] MDS and [$2n$, $2n$-2, 2] group codes for every $n$ corresponding to the linear idempotents and in case of non-linear idempotents Dihedral group codes of length 16, 20,24 are constructed.
Let $A_i$ be number of code words with Hamming weight '$i$' in code $\mathcal{C}$ of length $n$. The weight enumerator of $\mathcal{C}$ is defined as

$$A(z) = 1 + A_1z + A_2z^2 + \cdots + A_nz^n$$

The sequence $(1, A_1, A_2, \dots, A_n)$ is called the weight distribution of code $\mathcal{C}$. In coding theory it is often desirable to know the weight distributions

of codes because they can be used to estimate the error correcting capability and error probability of error detection and correction with respect to some algorithms.

In this paper, we will always assume that $p > 7$ is prime with $gcd\ (7p, q(q-1)) = 1$, $q^2 \equiv 1(mod\ 7p^s)$. We obtain all primitive idempotents in $\mathbb{F}_q[x]/\langle x^{7p^s} - 1\rangle$. Furthermore, we give the weight distribution of all irreducible cyclic codes and their dual codes of length $7p^s$over $\mathbb{F}_q$.

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

This paper is organized as follows:

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

In section 3, the primitive idempotents in $\mathbb{F}_q[x]/\langle x^{7p^s} - 1\rangle$ are given.

In Section 4, the weight distributions are obtained of all irreducible cyclic codes of length $7p^s$ over $\mathbb{F}_q$.

In section 5, we will give some examples to illustrate our main results.

## 2. PRELIMINARIES

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

**Lemma 2.1.** Assume that $n \geq 2$ For any $a \in \mathbb{F}_q{}^*$, $o(a) = k$ the binomial $x^n - a$ is irreducible over $\mathbb{F}_q$ if and only if both the following two conditions are satisfied:

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

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

**Lemma 2.2** *(See* [13, Lemma 6, chapter 7]) Let $\xi \in \mathbb{F}_q$ be a root of $x^n - 1$, where $\gcd(q, n) = 1$. Then

$$\sum_{i=0}^{n-1} \xi^i = \begin{cases} 0 & \text{if } \xi \neq 1 \\ n & \text{if } \xi = 1 \end{cases}$$

## 2. PRIMITIVE IDEMPOTENTS IN $\mathbb{F}_q[x]/\langle x^{7p^s} - 1\rangle$

Let $\mathbb{F}_q$ be the finite field with q elements. Fengwei Li and Qin Yue et al. gave all primitive idempotents in 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 and $v$ is positive integer. Let $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ be finite fields with $q$ and $q^2$ elements, respectively. Chen et al. [5] gave the irreducible factorization of $(x^{l^s q^m} - a)$ over $\mathbb{F}_q$, where $a \in \mathbb{F}_q{}^*$, $s$ is a non-negative integer, $l > 3$ is a prime, $\gcd(l, q) = 1$ and $l/(q-1)$. In this section, we assume $p > 7$ is a prime with $\gcd(7p, q(q-1)) = 1$, $q^2 \equiv 1(mod\ 7p^s)$. We shall explicitly determine the irreducible factors of $x^{7p^s} - 1$ in $\mathbb{F}_q[x]$.

$$x^{7p^s} - 1 = \prod_{j=1}^{7p^s} (x - \xi_{7p^s}^j),$$

where $\xi_{7p^s}$ is an $7p^s$-th root of unity in $\mathbb{F}_{q^2}$.

**Definition 3.1** Let $T = \{ j : 1 \leq j < 7p^s\}$, $T_{7p^s} = \{7p^s\}$, $T_0 = \{p^s, 2p^s, 3p^s, 4p^s, 5p^s, 6p^s\}$, $T^* = T - T_0$, $T_r{}^* = \{ t = l^{s-r} v \in T :$ $\gcd v, p=1,\ 1 \leq t < 7p^s$ for $1 \leq r \leq s$.

Define

$$\Psi_r^*(x) = \prod_{t \in T_r^*} \left(x - \xi_{7p^s}^t\right), \qquad r = 1,2, \ldots \ldots, s$$

Note that $T_{7p^s} = \{7p^s\}$, $T_0 = \{p^s, 2p^s, 3p^s, 4p^s, 5p^s, 6p^s\}$ it is clear that $T = T_0 \cup T_1{}^* \cup T_2{}^* \ldots \ldots \cup T_{s-1}{}^* \cup T_s{}^*$ and $|T_r{}^*| = 7\phi(p^r)$ for $1 \leq r \leq s$.

where $\phi(1) = 1$ , $\phi(p^r) = p^{r-1}(p-1)$, $r \geq 1$ (Euler $\phi$ −function)

$$x^{7p^s} - 1 = (x-1) \prod_{r=0}^{s} \prod_{t \in S_r} (x - \xi_{7p^s}^t) = (x-1)\Psi_0^*(x)\Psi_1^*(x) \ldots . \Psi_s^*(x). \tag{3.1}$$

Where $\Psi_0^*(x) = \prod_{i \in T_0}(x - \xi_{7p^s}^i)$

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 $\Omega_{p^s,0} = \{p^s, 2p^s, 3p^s, 4p^s, 5p^s, 6p^s\}$. Hence there is a disjoint union

$$T_r{}^* = \bigcup_{k=1}^{\frac{7\Phi(p^r)}{2}} \Omega_{r,v}\ ,\ |\Omega_{r,v}| = 2, where\ v \in T = \{y : \gcd(y, p) = 1\ and\ 1 \leq y < 7p^s\ and\ y\ is\ odd\}$$

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

$$f_{r,v}(x) = \prod_{\mu=0}^{1}(x - \xi_{7p^s}^{p^{s-r}vq^{\mu}}) = \prod_{\mu=0}^{1}\left(x - \xi_{7p^r}^{vq^{\mu}}\right).$$

And $T_{7p^s}$ corresponds to irreducible polynomial $(x-1)$ over $\mathbb{F}_q$. $\Omega_{p^s,0} = \{p^s, 2p^s, 3p^s, 4p^s, 5p^s, 6p^s\}$ *corresponds to irreducible polynomial,* $f_{p^s,0}(x) = \prod_{\mu=0}^{1}(x - \xi_7^{v_k q^{\mu}})$. So the number of irreducible factors of $x^{7p^s} - 1$ over the field $\mathbb{F}_q$ is:

$$1 + 3 + \frac{7(p^s-1)}{2} = 1 + \frac{(7p^s - 1)}{2}$$

**Lemma 3.2** There are $1 + \frac{(7p^s-1)}{2}$ irreducible factors of the polynomial $x^{7p^s} - 1$ over the field $\mathbb{F}_q$ as follows: $x - 1$ for $T_{7p^s}$ ; for elements of $T_0$ , $f_{p^s,0}(x) = \prod_{\mu=0}^{1}(x - \xi_7^{v_k q^{\mu}})$ ,$k = 1,2,3$ and for elements of $T_r{}^*$, $1 \le r \le s$

$$f_{r,v_k}(x) = \prod_{\mu=0}^{1}\left(x - \xi_{7p^r}^{v_k q^{\mu}}\right),\ k = 1,2,\dots\dots, \frac{7\phi(p^r)}{2} \tag{3.2}$$

Recall that the number of primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{7p^s} - 1\rangle$ coincides with the number of irreducible factors of $x^{7p^s} - 1$ over $\mathbb{F}_q$.

**Theorem 3.3** There are $1 + \frac{(7p^s-1)}{2}$ primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{7p^s} - 1\rangle$ . These primitive idempotents are given as:

(i) The primitive idempotent

$$\theta_{s,7p^s}(x) = \frac{1}{7p^s}\sum_{i=0}^{7p^s-1}(x)^i$$

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

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

$$\theta_{p^s,0}(x) = \frac{1}{7p^s}\sum_{i=0}^{7p^s-1} Tr(\xi_7^{-v_k i})(x)^i \text{, where } k = 1,2,3$$

corresponds to the irreducible polynomial $f_{p^s,0}(x) = \prod_{\mu=0}^{1}(x - \xi_7^{v_k q^{\mu}})$ over $\mathbb{F}_q$.

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

$$\theta_{s,v_k}(x) = \frac{1}{7p^s}\cdot\frac{x^{7p^s}-1}{x^{7p^r}-1}\sum_{i=0}^{7p^r-1} Tr(\xi_{7p^r}^{-v_k i})(x)^i \tag{3.3}$$

corresponds to the irreducible polynomial $f_{r,v_k}(x)$ over $\mathbb{F}_q$ , $k = 1,2,\dots\dots\dots, \frac{7\Phi(p^r)}{2}$, respectively.

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

$$\varphi : \mathbb{F}_{q^2}[x]/\langle x^{7p^s} - 1\rangle \longrightarrow \prod_{j=0}^{7p^s-1}\mathbb{F}_{q^2}[x]/\langle (x - \xi_{7p^s}^{j})\rangle, \tag{3.4}$$

$$\sum_{i=0}^{7p^s-1} a_i\, x^i \longmapsto \left(\sum_{i=0}^{7p^s-1} a_i\,, \sum_{i=0}^{7p^s-1} a_i\left(\xi_{7p^s}^{1}\right)^i, \dots\dots\dots, \sum_{i=0}^{7p^s-1} a_i\left(\xi_{7p^s}^{7p^s-1}\right)^i\right)$$

Let $M$ be the $7p^s \times 7p^s$ character matrix as follows

$$M = \begin{pmatrix} (\xi_{7p^s}^{0})^0 & (\xi_{7p^s}^{1})^0 & \cdots & (\xi_{7p^s}^{7p^s-1})^0 \\ (\xi_{7p^s}^{0})^1 & (\xi_{7p^s}^{1})^1 & \cdots & (\xi_{7p^s}^{7p^s-1})^1 \\ \vdots & \vdots & & \vdots \\ (\xi_{7p^s}^{0})^{7p^s-1} & (\xi_{7p^s}^{1})^{7p^s-1} & \cdots & (\xi_{7p^s}^{7p^s-1})^{7p^s-1} \end{pmatrix}$$

Then we have

$$\varphi\left(\sum_{i=0}^{7p^s-1} a_i\, x^i\right) = (a_0, a_1, a_2, \dots\dots\dots, a_{7p^s-1})M = (b_0, b_1, b_2, \dots\dots\dots, b_{7p^s-1}). \tag{3.5}$$

By Lemma 2.2

$$M^{-1} = \frac{1}{7p^s}\begin{pmatrix} (\xi_{7p^s}^{0})^{-0} & (\xi_{7p^s}^{0})^{-1} & \cdots & (\xi_{7p^s}^{0})^{-(7p^s-1)} \\ (\xi_{7p^s}^{1})^{-0} & (\xi_{7p^s}^{1})^{-1} & \cdots & (\xi_{7p^s}^{1})^{-(7p^s-1)} \\ \vdots & \vdots & & \vdots \\ \left(\xi_{7p^s}^{(7p^s-1)}\right)^{-0} & \left(\xi_{7p^s}^{(7p^s-1)}\right)^{-1} & \cdots & \left(\xi_{7p^s}^{(7p^s-1)}\right)^{-(7p^s-1)} \end{pmatrix}$$

It is obvious that $(b_0, b_1, b_2, \dots\dots\dots, b_{7p^s-1}) = (1,0,0, \dots\dots..0) = e$ is the primitive idempotent of $\prod_{t=0}^{7p^s-1} \mathbb{F}_{q^2}[x]/\langle(x - \xi_{7p^s}^j)\rangle$. According to the inverse Fourier transform, we get the primitive idempotents $\theta_{s,7p^s}(x) = \sum_{i=0}^{7p^s-1} a_i\, x^i$ in $\mathbb{F}_{q^2}[x]/\langle x^{7p^s} - 1\rangle$, which just corresponds to irreducible polynomial $x - 1$ over the field $\mathbb{F}_q$.

Namely

$$\varphi\left(\theta_{s,7p^s}(x)\right) = (a_0, a_1, a_2, \dots\dots\dots, a_{7p^s-1})T = e,$$
$$(a_0,\ a_1,\ a_2, \dots\dots\dots, a_{7p^s-1}) = eT^{-1} = \frac{1}{7p^s}(1^{-0}, 1^{-1}, 1^{-2}, \dots\dots, 1^{-(7p^s-1)}),$$

$$\theta_{s,7p^s}(x) = \frac{1}{7p^s}\sum_{i=0}^{7p^s-1}(x)^i.$$

$(ii)$ In equation 3.4, take $(b_0, b_1, b_2, \dots\dots\dots, b_{7p^s-1})$, where $b_w = 1$ if $w \in \Omega_{p^s,0}$, otherwise $b_w = 0$.

Hence,

$$(a_0, a_1,\ a_2, \dots, a_{7p^s-1}) = (b_0, b_1, b_2, \dots, b_{7p^s-1})M^{-1}$$

$$= \frac{1}{7p^s}\left(Tr(\xi_7^{-0.v_k}), Tr(\xi_7^{-1.v_k}), \dots\dots, Tr\left(\xi_7^{-v_k(7p^s-1)}\right)\right)$$

$\therefore$ $$\theta_{p^s,0}(x) = \frac{1}{7p^s}\sum_{t=0}^{7p^s-1} Tr(\xi_7^{-v_k t})(x)^t$$

corresponds to the polynomial $f_{p^s,0}(x) = \prod_{\mu=0}^{1}(x - \xi_7^{v_k q^\mu})$.

$(iii)$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 the irreducible polynomial $f_{s,v}(x) = \sum_{\mu=0}^{1}(x - \xi_{7p^r}^{vq^\mu})$ over $\mathbb{F}_q$. It is well-known that there is a natural $\mathbb{F}_{q^2}$-algebra isomorphism-

$$\varphi_1 : \mathbb{F}_{q^2}[x]/\langle f_{s,v}(x)\rangle \longrightarrow \prod_{\mu=0}^{1}\mathbb{F}_{q^2}[x]/\langle x - \xi_{7p^s}^{vq^\mu}\rangle,$$
$$c(x) = \sum_{\mu=0}^{1} c_\mu\, x^\mu \ \longmapsto \left(\sum_{\mu=0}^{1} c_\mu\left(\xi_{7p^s}^{v}\right)^\mu, \sum_{\mu=0}^{1} c_\mu\left(\xi_{7p^s}^{vq}\right)^\mu\right).$$

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

Let P be a $2 \times 2$ character matrix as follow:

$$\mathrm{P} = \begin{pmatrix} \left(\xi_{7p^s}^{v}\right)^0 & \left(\xi_{7p^s}^{vq}\right)^0 \\ \left(\xi_{7p^s}^{v}\right)^1 & \left(\xi_{7p^s}^{vq}\right)^1 \end{pmatrix}$$
$$\varphi_1(c(x)) = (c_0, c_1)P.$$

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

In equation 3.4, take $(b_0, b_1, b_2, \dots\dots\dots, b_{7p^s-1})$, where $b_j = 1$ if $t \in \{v, vq\}$, otherwise $b_j = 0$ . Hence

$$(a_0, a_1,\ a_2, \dots, a_{7p^s-1}) = (b_0, b_1, b_2, \dots, b_{7p^s-1})M^{-1}$$

$$= \frac{1}{7p^s}\left(Tr\left(\left(\xi_{7p^s}^{v}\right)^{-0}\right), Tr\left(\left(\xi_{7p^s}^{v}\right)^{-1}\right), \dots\dots, Tr\left(\left(\xi_{7p^s}^{v}\right)^{-(7p^s-1)}\right)\right)$$

(i)

Therefore there is primitive idempotent

$$\theta_{s,v}(x) = \frac{1}{7p^s}\sum_{i=0}^{7p^s-1}(Tr(\xi_{7p^s}^{-vi})(x)^i$$

in the ring $\mathbb{F}_q[x]/\langle x^{7p^s} - 1\rangle$ which corresponds to the irreducible polynomial $f_{s,v}(x)$ over $\mathbb{F}_q$.

***Sub case (ii):*** If $1 \le r < s$ and each $t = p^{s-r}v \in T_r^*$ $gcd(v,p) = 1$. By Lemma 3.2, there is the irreducible polynomial $f_{r,v} = \prod_{\mu=0}^{1}(x - \xi 7prvq\mu)$ over $\mathbb{F}q$. Replacing s by $r$ in above discussion, we can get the primitive idempotent

$$\theta_{r,v}(x) = \frac{1}{7p^r}\sum_{i=0}^{7p^r-1}(Tr(\xi_{7p^r}^{-ui})(x)^i$$

In the ring $\mathbb{F}_q[x]/\langle x^{7p^r} - 1\rangle$ which corresponds to the irreducible polynomial $f_{r,v}(x)$.

By (3.1), there is a natural $\mathbb{F}_q$ −algebraic isomorphism:

$$\varphi_2: \frac{\mathbb{F}_q[x]}{\langle x^{7p^s}-1\rangle} \to \frac{\mathbb{F}_q[x]}{\langle x^{7p^r}-1\rangle} \times \prod_{i=r+1}^{s} \frac{\mathbb{F}_q[x]}{\langle \Psi_i(x)\rangle}$$

$$\theta_{s-r}(x) = \frac{1}{p^{s-r}} \cdot \frac{x^{7p^s}-1}{x^{7p^r}-1} \mapsto (1,0,0,\dots\dots,0)$$

Hence $\theta_{s,v_k}(x) = \theta_{s-r}(x)\theta_{r,v_k}(x)$ are primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{7p^s}-1\rangle$, which corresponds to irreducible polynomials $f_{r,v}(x)$ over $\mathbb{F}_q$ for $k = 1,2,\dots\dots,\frac{7\Phi(p^r)}{2}$.

******

## 4. THE WEIGHT DISTRIBUTIONS OF IRREDUCIBLE CYCLIC CODES OF LENGTH $7p^s$

In this section, suppose that $q^2 \equiv 1(mod\ 7p^s)$ and $gcd(7p, q(q-1)) = 1$, where $p > 7$ be a prime. In the following part, we give the weight distributions of the irreducible cyclic codes over the field $\mathbb{F}_q$ by the primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^{7p^s}-1\rangle$.

Let $\mathcal{C}$ denotes an irreducible cyclic code of length $7p^s$ generated by the primitive idempotent $\theta(x)$ whose parity-check polynomial is an irreducible divisor of $x^{7p^s}-1$. It is clear that $\mathcal{C} = \langle\theta(x)\rangle = \langle g(x)\rangle$, where $g(x) = \gcd(\theta(x), x^{7p^s}-1)$ is called the generator polynomial of 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 two distinct columns of following* $2 \times 7p^r$ *matrix*

$$\begin{bmatrix} Tr(\xi_{7p^r}^{-v_k 0}) & Tr(\xi_{7p^r}^{-v_k 1}) \dots\dots & Tr(\xi_{7p^r}^{-v_k(7p^r-1)}) \\ Tr(\xi_{7p^r}^{-v_k(7p^r-1)}) & Tr(\xi_{7p^r}^{-v_k 0}) \dots\dots & Tr(\xi_{7p^r}^{-v_k(7p^r-2)}) \end{bmatrix}$$

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

***Proof:*** Without loss of generality, we suppose that $u = 1$. For $0 \le i < j \le 7p^r - 1$, $Tr(\xi_{7p^r}^{-i}) = Tr(\xi_{7p^r}^{i}) = \xi_{7p^r}^{i} + \xi_{7p^r}^{-i}$ by $q = -1(mod\ 7p^s)$ and the determinant

$$\begin{vmatrix} Tr(\xi_{7p^r}^{-i}) & Tr(\xi_{7p^r}^{-j}) \\ Tr(\xi_{7p^r}^{-(i-1)}) & Tr(\xi_{7p^r}^{-(j-1)}) \end{vmatrix} = Tr(\xi_{7p^r}^{j-i+1}) - Tr(\xi_{7p^r}^{j-i-1}) \neq 0$$

*****

**Theorem 4.3.** [17] *From the theorem 3.3, the weight distributions of all irreducible cyclic codes of length* $7p^s$ *as follows:-*

*(i)* $\mathcal{C}_0 = \langle\theta_{s,7p^s}(x)\rangle$ *is an* $[7p^s, 1, 7p^s]$ *cyclic code with the 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* $[7p^s, 2, 6p^s]$ *cyclic code with parity check polynomial* $f_{p^s,0}(x) = x^2 - Tr(\xi_7^{v_k})x + 1$ *and its Hamming weight enumerator polynomial is*

$$1 + 7(q^{k'}-1)z^{6p^s} + (q^{2k'} - 1 - 7(q^{k'}-1))z^{7p^s}$$

*(iii)* *If* $1 \le r \le s$ *and* $7p^{s-r}v_k \in T_r^*$, $k = 1,2,\dots\dots,\frac{7\phi(p^r)}{2}$, *then each* $\mathcal{C}_{s,v_k} = \langle\theta_{s,v_k}(x)\rangle$ *is a* $[7p^s, 2, 7p^s - p^{s-r})]$ *cyclic code with parity-check polynomial*
$f_{r,v_k}(x) = x^2 - Tr(\xi_{7p^r}^{v_k})x + 1$ *and its Hamming weight enumerator polynomial is*

$$1 + 7p^r(q^{k'}-1)z^{(7p^s - p^{s-r})} + (q^{2k'} - 1 - 7p^r(q^{k'}-1))z^{7p^s}$$

***Proof:*** We only need to prove the case *(iii)*. Suppose that $1 \le r \le s$ *and* $7p^{s-r}v_k \in T_r^*$. Then we have $\xi_{p^r}^{qv_k} = \xi_{p^r}^{-v_k}$ by $p^s|(q+1)$. Let $R_s = \mathbb{F}_q[x]/\langle x^{7p^s}-1\rangle$ then by construction of primitive idempotent $\theta_{s,v_k}(x)$ we have

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

Where

$f_{r,v_k}(x) = \left(x - \xi_{7p^r}^{v_k}\right)\left(x - \xi_{7p^r}^{-v_k}\right) = x^2 - Tr(\xi_{7p^r}^{v_k})x + 1$ is parity check polynomial of $\mathcal{C}_{s,7p^{s-r}v_k}$.

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

It is clear that

$$\frac{x^{7p^s}-1}{x^{7p^r}-1}(x)^{7p^r} \equiv \frac{x^{7p^s}-1}{x^{7p^r}-1} mod(x^{7p^s}-1).$$

Let $f(x) \in R_s = \mathbb{F}_q[x]/\langle x^{7p^s}-1\rangle$ then the number of non-zero coefficients of $f(x)$ of degree at most $7p^s - 1$ 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

$$r(x)\ \theta_{s,v_k}(x) \in R_r = \mathbb{F}_q[x]/\langle x^{7p^r}-1\rangle \text{ and } (x)^{7p^r} \equiv 1\ mod(x^{7p^r}-1)$$

Suppose that $p^r r(x)\ \theta_{r,v_k}(x) \equiv [b_0 + b_1 x + \ldots\ldots\ldots, b_{7p^r-1}(x)^{7p^r-1}] mod(x^{7p^r} - 1)$,
Then

$$(b_0, b_1, \ldots\ldots\ldots, b_{7p^r-1}) = \frac{1}{7}(a_0, a_1)\begin{pmatrix} Tr(\xi_{7p^r}^{-v_k 0}) & Tr(\xi_{7p^r}^{-v_k 1}) & \ldots\ldots\ldots & Tr(\xi_{7p^r}^{-v_k(7p^r-1)}) \\ Tr(\xi_{7p^r}^{-v_k(7p^r-1)}) & Tr(\xi_{7p^r}^{-v_k 0}) & \ldots\ldots\ldots & Tr(\xi_{7p^r}^{-v_k(7p^r-2)}) \end{pmatrix}$$

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

$$\wedge_1 = \left\{ (a_0, a_1) \in \wedge : -\frac{a_0}{a_1} \in \left\{ \frac{Tr(\xi_{7p^r}^{-v_k(7p^r-1)})}{Tr(\xi_{7p^r}^{-v_k.0})}, \ldots\ldots, \frac{Tr(\xi_{7p^r}^{-v_k.(7p^r-2)})}{Tr(\xi_{7l^h}^{-v_k(7p^r-1)})} \right\} \right\}$$

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

If $(a_0, a_1) \in \wedge_0$ then $(b_0, b_1, \ldots\ldots\ldots, b_{7p^r-1}) = 0$ and $W\left(r(x)\theta_{s,v_k}(x)\right) = 0$.

If $(a_0, a_1) \in \wedge_1$ then only one of $b_0, b_1, \ldots\ldots\ldots, b_{7p^r-1}$ is equal to 0 and $W\left(r(x)\theta_{s,v_k}(x)\right) = p^{s-r}(7p^r - 1)$.

If $(a_0, a_1) \in \wedge_2$ then all $b_0, b_1, \ldots\ldots\ldots, b_{7p^r-1}$ are not equal to 0 and $W\left(r(x)\theta_{s,v_k}(x)\right) = 7p^s$

On the other hand, $|\wedge_0| = 1$, $|\wedge_1| = 7p^r(q^{k'} - 1)$ by Lemma 4.2, and $|\wedge_2| = (q^{2k'} - 1 - 7p^r(q^{k'} - 1))$, which provides frequency of weights. Hence the Hamming weights enumerator polynomial of each $\mathcal{C}_{s,v_k}$ is $1 + 7p^r(q^{k'} - 1)z^{(7p^s - p^{s-r})} + (q^{2k'} - 1 - 7p^r(q^{k'} - 1))z^{7p^s}$

*****

By Lemma 4.1, we have following result:

**Corollary 4.4.** [17] *In Theorem 4.3, if* $1 \le r \le s$, $7p^{s-r}v_k \in T_r^*$, $k = 1, \ldots\ldots\ldots, \frac{\phi(p^r)}{2}$, *then the Hamming weight enumerator polynomial of* $\mathcal{C}_{s,v_k}^{\perp}$ *is*

$q^{-2}((1 + (q-1)z)^{7p^s} + 7p^r(q-1)(z-1)^{(7p^s - p^{s-r})}(1 + (q-1)z)^{7p^{s-r}} - (q^2 - 1 - 7p^r(q-1))(z-1)^{7p^s})$.

## 5. EXAMPLES

Here, we give some examples in support of our results.

*We assume that* $p > 7$ *is a prime with* $gcd(7p, q(q-1)) = 1$, $q \equiv -1(mod\ 7p^s)$, *s is a positive integer.*

*Example* 5.1: *Let* $p = 11, q = 1693, s = 2$. *Then* $7p^s = 847$, then we have $T = \{1,2,3, \ldots, 846\}$,
$T_{847} = \{847\}$ and $T_0 = \{121,242,363,484,605,726\}$. Since $q \equiv -1(mod\ 847)$ then the q cosets are given by
$T_1^* = \{11,22,33,44,55,66,77,88,99,110,132, \ldots, 836\}$, $T_2^* = \{1,2,3,4,5,6,7,8,9,10,12,13, \ldots, 846\}$. $\Omega_{1,1} = \{11, 836\}$, $\Omega_{1,2} = \{22, 825\}$, $\Omega_{1,3} = \{33, 814\}$, $\Omega_{1,4} = \{44, 803\}$, $\Omega_{1,5} = \{55, 792\}$, $\Omega_{1,6} = \{66, 781\}$, $\Omega_{1,7} = \{77, 770\}$, $\Omega_{1,8} = \{88, 759\}$, $\Omega_{1,9} = \{99, 748\}$, $\Omega_{1,10} = \{110, 737\}$, $\Omega_{1,12} = \{132, 715\}$, $\Omega_{1,13} = \{143, 704\}$, $\Omega_{1,14} = \{154, 693\}$, $\Omega_{1,15} = \{165, 682\}$, $\Omega_{1,16} = \{176, 671\}$, $\Omega_{1,17} = \{187, 660\}$, $\Omega_{1,18} = \{198, 649\}$, $\Omega_{1,19} = \{209, 638\}$, $\Omega_{1,20} = \{220, 627\}$, $\Omega_{1,21} = \{231, 616\}$, $\Omega_{1,23} = \{253, 594\}$, $\Omega_{1,24} = \{264, 583\}$, $\Omega_{1,25} = \{275, 572\}$, $\Omega_{1,26} = \{286, 561\}$, $\Omega_{1,27} = \{297, 550\}$, $\Omega_{1,28} = \{308, 539\}$, $\Omega_{1,29} = \{319, 528\}$, $\Omega_{1,30} = \{330, 517\}$, $\Omega_{1,31} = \{341, 506\}$, $\Omega_{1,32} = \{352, 495\}$, $\Omega_{1,34} = \{374, 473\}$ and so on.
$\Omega_{2,1} = \{1, 846\}$, $\Omega_{2,2} = \{2, 845\}$, $\Omega_{2,3} = \{3, 844\}$, $\Omega_{2,4} = \{4, 843\}$, $\Omega_{2,5} = \{5, 842\}$, $\Omega_{2,6} = \{6, 841\}$, $\Omega_{2,7} = \{7, 840\}$, $\Omega_{2,8} = \{8, 839\}$, $\Omega_{2,9} = \{9, 838\}$, $\Omega_{2,10} = \{10, 837\}$, $\Omega_{2,12} = \{12, 835\}$, $\Omega_{2,13} = \{13, 834\}$, $\Omega_{2,13} = \{14, 833\}$, $\Omega_{2,15} = \{15, 832\}$, $\Omega_{2,16} = \{16, 831\}$, $\Omega_{2,17} = \{17, 830\}$, $\Omega_{2,18} = \{18, 829\}$, $\Omega_{2,19} = \{19, 828\}$, $\Omega_{2,20} = \{20, 827\}$, $\Omega_{2,21} = \{21, 826\}$, $\Omega_{2,23} = \{23, 824\}$, $\Omega_{2,24} = \{24, 823\}$, $\Omega_{2,25} = \{25, 822\}$, $\Omega_{2,26} = \{26, 821\}$, $\Omega_{2,27} = \{27, 820\}$, $\Omega_{2,28} = \{28, 819\}$, $\Omega_{2,29} = \{29, 818\}$, $\Omega_{2,30} = \{30, 817\}$, $\Omega_{2,31} = \{31, 816\}$, $\Omega_{2,32} = \{32, 815\}$, $\Omega_{2,34} = \{34, 813\}$, $\Omega_{2,35} = \{35, 812\}$, $\Omega_{2,36} = \{36, 811\}$, $\Omega_{2,37} = \{37, 810\}$, $\Omega_{2,38} = \{38, 809\}$, $\Omega_{2,39} = \{39, 808\}$, $\Omega_{2,40} = \{40, 807\}$, $\Omega_{2,41} = \{41, 806\}$, $\Omega_{2,42} = \{42, 805\}$, $\Omega_{2,43} = \{43, 804\}$, $\Omega_{2,45} = \{45, 802\}$, $\Omega_{2,46} = \{46, 801\}$, $\Omega_{2,47} = \{47, 800\}$, $\Omega_{2,48} = \{48, 799\}$, $\Omega_{2,49} = \{49, 798\}$, $\Omega_{2,50} = \{50, 797\}$, $\Omega_{2,51} = \{51, 796\}$, $\Omega_{2,52} = \{52, 795\}$, $\Omega_{2,53} = \{53, 794\}$, $\Omega_{2,54} = \{54, 793\}$, $\Omega_{2,56} = \{56, 791\}$, $\Omega_{2,57} = \{57, 790\}$, $\Omega_{2,58} = \{58, 789\}$, $\Omega_{2,59} = \{59, 788\}$, $\Omega_{2,60} = \{60, 787\}$, $\Omega_{2,61} = \{61, 786\}$, $\Omega_{2,62} = \{62, 785\}$, $\Omega_{2,63} = \{63, 784\}$, $\Omega_{2,64} = \{64, 783\}$, $\Omega_{2,65} = \{65, 782\}$, $\Omega_{2,67} = \{67, 780\}$, $\Omega_{2,68} = \{68, 779\}$, $\Omega_{2,69} = \{69, 778\}$, $\Omega_{2,70} = \{70, 777\}$, $\Omega_{2,71} = \{71, 776\}$, $\Omega_{2,72} = \{72, 775\}$, $\Omega_{2,73} = \{73, 774\}$, $\Omega_{2,74} = \{74, 773\}$ and so on.

The four classes of irreducible cyclic codes of length 847 in $\mathbb{F}_q[x]/\langle x^{7p^s} - 1\rangle$ are the following:

*(1)* There is *one* [847,1,847] irreducible cyclic code with parity check polynomial $x - 1$.

*(2)* There are *six* [847,2,726] irreducible cyclic codes with parity check polynomial $x^2 - Tr(\xi_7)x + 1$ and its hamming weight enumerator polynomial is $1 + 20063736z^{726} + 8215363266000z^{847}$.

*(3)* There are *seven* [847,2,836] irreducible cyclic codes with parity check polynomial $x^2 - Tr(\xi_{77})x + 1$ and its hamming weight enumerator polynomial is $1 + 220701096z^{836} + 8215162629000z^{847}$.

*(4)* There are *seven* [847,2,846] irreducible cyclic codes with parity check polynomial $x^2 - Tr(\xi_{847})x + 1$ and its hamming weight enumerator polynomial is $1 + 2427712056z^{846} + 8212955618000z^{847}$.

Next two examples can also be completed using same method.

*Example 5.2: Take* $p = 11, q = 5081, s = 2$.

*Example 5.3: Take* $p = 11, q = 10163, s = 2$.

**References**


1. S. K. Arora, S. Batra, S. D. Cohen, and M. Pruthi, The primitive idempotents of a cyclic group algebra, Southeast Asian Bull. Math. 26, 197-208 (2002).
2. S. K. Arora and M. Pruthi, Minimal cyclic codes of length $2p^n$, Finite Fields Appl. 5, 177-187 (1999).
3. S. Batra and S. K. Arora, Some cyclic codes of length $2p^n$, Des. Codes Cryptogr. 61, 41-69 (2011).
4. G. K. Bakshi and M. Raka, Minimal cyclic codes of length $p^n$q, Finite Fields Appl. 9, 432-448 (2003).
5. B. Chen, Y. Fan, L. Lin, and H. Liu, Constacyclic codes over finite fields, Finite Fields Appl. 18, 1217-1231 (2012).
6. B. Chen, H. Liu, and G.Zhang, A class of minimal cyclic codes over finite fields, Des. Codes Cryptogr. 74, 285-300 (2015).
7. S. Kumar, Pankaj, M. Pruthi, 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, 44-70 (2016).
8. R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge (2008).
9. J.H.van Lint, Introduction to Coding Theory, Springer-Verlag, Berlin (2003).
10. F. Li, Q. Yue, and C. Li, The minimum Hamming distances of irreducible cyclic codes, Finite Field Appl. 29, 225-242 (2014).
11. F. Li, Q. Yue, and C. Li, The irreducible cyclic codes of length $4p^n$ and $8p^n$, Finite Field Appl.34, 208-234 (2015).
12. F. Li, Q.Yue, The primitive idempotents and weight distributions of irreducible constacyclic codes, Des. Codes Cryptogr. 3 DOI: 10.1007/s10623-017-0356 -2(2017).
13. F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes, North Holland, Amsterdam (1977).
14. M. Pruthi, Cyclic codes of length $2^m$, Proc. Indian Acad. Sci. Math. Sci. 111, 371-379 (2001).
15. M. Pruthi and S. K. Arora, Minimal cyclic codes of prime power length, Finite Fields Appl. 3, 99-113 (1997).
16. S. Sehrawat and M. Pruthi, Codes over dihedral groups, Journal of information and optimization sciences vol. 39, 889-901(2018).
17. A. Sharma, G. K. Bakshi, V. C. Dumir, and M. Raka, Irreducible cyclic codes of length $2^n$,Ars Combin. 86, 133-146 (2008).
18. R. Singh and M. Pruthi, Primitive idempotents of irreducible quadratic residue cyclic codes of length $p^n q^m$, Int. J. Algebra 5, 285-294 (2011).
19. Z. Wan, Lectures on Finite Fields and Galois Rings, World Scientific Publishing, Singapore (2003).


 