J. Algebra Comb. Discrete Appl.
8(3) • 167–195

Received: 21 September 2020
Accepted: 08 March 2021

Journal of Algebra Combinatorics Discrete Structures and Applications

Minimum distance and idempotent generators of minimal cyclic codes of length ${p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3}$

Research Article

Pankaj Kumar, Pinki Devi

Abstract: Let p_1, p_2, p_3, q be distinct primes and $m = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3}$. In this paper, it is shown that the explicit expressions of primitive idempotents in the semi-simple ring $R_m = F_q[x]/(x^m - 1)$ are the trace function of explicit expressions of primitive idempotents from $R_{{p_i}^{\alpha_i}}$. The minimal polynomials, generating polynomials and minimum distances of minimal cyclic codes of length m over F_q are also discussed. All the results obtained in [1], [3], [4], [5], [11] and [14] are simple corollaries to the results obtained in the paper.

2010 MSC: 94B05, 94B15

Keywords: Cyclotomic cosets, Primitive idempotents, Cyclic codes, Trace function

1. Introduction

Let p_1, p_2, p_3 and q be distinct primes and $m = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3}$.Then $R_m = F_q[x]/(x^m - 1)$ is a semi-simple ring. Every cyclic code C of length m over F_q is a direct sum of minimal cyclic codes in R_m. Therefore, we need to compute the minimal cyclic codes of length m over F_q. A minimal cyclic code always has a primitive idempotent generator [12, Theorem 1, Chapter 8], therefore, the study of minimal cyclic codes need the computation of explicit expressions of primitive idempotents in R_m. For $m = p^n$, Pruthi and Arora [13] obtained all the minimal cyclic codes of length m in $R_{p^n} = F_q[x]/(x^{p^n} - 1)$; q is a primitive root modulo p^n. In [7], Chen et al. studied the minimal cyclic codes of length l^m over F_q, where l is a prime divisor of $q - 1$ and m is a positive integer. Many authors have worked to compute the primitive central idempotents in semi-simple group algebra. In [2], Bakshi et al. have computed primitive central idempotents in semi-simple group algebra FG; F is finite fields and G is arbitrary meta-cyclic group. In another paper [9], they developed an algorithm to compute the primitive central idempotents in a semi-simple group algebra. Broche and Rio [6] developed a method to compute the primitive central idempotents and the wedderburn decomposition of a semi simple finite group algebra of

Pankaj Kumar, Pinki Devi (Corresponding Author); Department of Mathematics, Guru Jambheshwar University of Science and Technology, Hisar 125001, India (email: joshi78023@yahoo.com, pinkinarwal123@gmail.com).

https://doi.org/10.13069/jacodesmath.1000837 ISSN 2148-838X

an abelian-by-supersolvable group G. Ferraz and Milies [8] discussed a simple method of computing the idempotent generator of minimal abelain codes and discussed all the results as obtained in [1]. Sharma et al. [15] gave an algorithm to compute all the primitive idempotents over F_q in R_{p^n} by choosing fp^{n-1} as the order of q modulo p^n. Since $m = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3}$, therefore it is natural to ask that "Can one use the explicit expressions of primitive idempotents from $R_{p_i^{\alpha_i}}$ to compute the explicit expressions of primitive idempotents in R_m?" In this regard Bakshi et al. [4] used trace function to compute the explicit expressions of primitive idempotents in R_m; $m = m_1 m_2$ with $\gcd\big(O_{m_1}(q), O_{m_2}(q)\big) = 1$ or d, where $O_{m_i}(q)$ denotes the order of q modulo m_i. Kumar and Arora [10] defined a λ-mapping to compute the explicit expressions of primitive idempotents in R_m; $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ with the help of primitive idempotents from $R_{p_i^{\alpha_i}}$ in a single step under the following conditions:

(i) For each i, q is a primitive root modulo $p_i^{\alpha_i}$,

(ii) At most one prime factor of m is of the form $4k+1$ and the other prime factors of m are of the form $4k+3$,

(iii) $\gcd\big(\phi(p_i^{\alpha_i}), \phi(p_j^{\alpha_j})\big) = 2$, $1 \leq i \neq j \leq r$.

In this paper, we choose $m = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3}$, where p_i's are distinct primes and, for each $i, 1 \leq i \leq 3$, $O_{p_i^{\alpha_i}}(q) = \frac{\phi(p_i^{\alpha_i})}{r_i}$ and obtain the primitive idempotents and minimum distances of minimal cyclic codes in R_m over the finite field F_q. This paper is organized as follows:

In Section 2, we use λ- mapping to obtain the q-cyclotomic cosets and in Theorem 2.5, we count the number of distinct q-cyclotomic cosets modulo m. In Section 3, the primitive idempotents are obtained. In Theorem 3.5, we use λ-mapping and in Theorem 3.6 we use Trace function to compute the primitive idempotents in R_m with the help of primitive idempotents from $R_{p_i^{\alpha_i}}$. The minimal polynomials and the generating polynomials of some cyclic codes of length m are obtained in Section 4. In Section 5, we give a lower bound on minimum distances of cyclic codes of length m. We include examples in the last section. In Example 6.1, we choose $m = 715$ and count the total number of 3-cyclotomic cosets modulo 715. Then we obtain the explicit expression of $\theta_1^{715}(x)$ in R_{715} by λ product of polynomials and by Trace function (The explicit expressions of all primitive idempotents are shown in Appendix 1). In Example 6.2, the minimal cyclic codes of length 30 are discussed in $R_{30} = F_7[x]/(x^{30}-1)$. All the results obtained in [1], [3], [4], [5], [11] and [14] are simple corollaries to the results obtained in the paper.

2. Cyclotomic cosets modulo m

In this section we use λ-mapping [10, Definition(2.2)] to compute the q-cyclotomic cosets modulo m with the help of q^{v_i}-cyclotomic cosets modulo $p_i^{\alpha_i}$. Then we count the number of distinct q-cyclotomic cosets modulo m. Throughout this paper p_1, p_2, p_3 and q are distinct primes, $m = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3}$, for $1 \leq i \leq 3$, $O_{p_i^{\alpha_i}}(q) = \frac{\phi(p_i^{\alpha_i})}{r_i}$, $m_i = \frac{m}{p_i^{\alpha_i}}$, $A = \{0, 1, 2, ..., m-1\}$ and $A_i = \{0, 1, ..., p_i^{\alpha_i} - 1\}$, δ is a fixed primitive mth root of unity in some extension of F_{q^t} and $\delta_i = \delta^{m_i}$ is a fixed primitive ${p_i}^{\alpha_i}$th root of unity in the same extension of F_{q^t}. We denote the q-cyclotomic coset modulo m containing $s; 0 \leq s \leq m-1$ by $C_s^{m(q)} = \{s, sq, sq^2, ..., sq^{r-1}\}$, where r is the smallest positive integer such that $sq^r \equiv s (\bmod\ m)$ and, for a divisor i of r, $C_s^{m(q^i)} = \{s, sq^i, sq^{2i}, ..., sq^{i(\frac{r}{i}-1)}\}$ denote the q^i-cyclotomic coset modulo m containing s.

Definition 2.1. *[λ-mapping] The mapping λ from $A_1 \times A_2 \times A_3 \longrightarrow A$ defined by $\lambda(b_1, b_2, b_3) = b_1 m_1 + b_2 m_2 + b_3 m_3 (mod\ m)$, where $b_i \in A_i$ is called the λ-mapping. It is a one-one and onto mapping.*

Lemma 2.2. *Let v_1, v_2 and v_3 be positive integers. If $l = lcm(v_1, v_2, v_3)$, $l_1 = lcm(v_2, v_3)$, $l_2 = lcm(v_1, v_3)$ and $l_3 = lcm(v_1, v_2)$ then, for $1 \leq i \leq 3$*
(i) l_i divides l.
(ii) l divides $v_i l_i$ and, if $v_i l_i = u_i l$, where u_i is some positive integer, then $l_1 l_2 l_3 = l^2 lcm(u_1, u_2, u_3)$.

Theorem 2.3. *Let q be an odd prime with $gcd(q, m) = 1$. Further, let $O_m(q) = d$, $O_{m_i}(q) = d_i$, $v_i = \frac{O_{p_i^{\alpha_i}}(q) d_i}{d}$. Then*

$$C_1^{m(q)} = \bigcup_{j=0}^{t-1} \lambda\Big(C_{a_1 q^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 q^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big),$$

where $t = lcm(v_1, v_2, v_3)$.

Proof. By Definition 2.1, for $1 \in A$, there exists $(a_1, a_2, a_3) \in A_1 \times A_2 \times A_3$ such that

$$\lambda(a_1, a_2, a_3) = 1. \quad (1)$$

As $O_m(q) = d$, therefore, multiplying (1) by $q^k; 0 \leq k \leq d-1$, we get

$$\lambda(a_1, a_2, a_3) = 1$$

$$\lambda(a_1 q, a_2 q, a_3 q) = q$$

$$\lambda(a_1 q^2, a_2 q^2, a_3 q^2) = q^2$$

$$\vdots$$

$$\lambda(a_1 q^{d-1}, a_2 q^{d-1}, a_3 q^{d-1}) = q^{d-1}.$$

The left hand side of above equations has three columns namely

$$B_1 = \{a_1, a_1 q, a_1 q^2, \ldots, a_1 q^{d-1}\},$$

$$B_2 = \{a_2, a_2 q, a_2 q^2, \ldots, a_2 q^{d-1}\},$$

$$B_3 = \{a_3, a_3 q, a_3 q^2, \ldots, a_3 q^{d-1}\}.$$

As $O_{m_1}(q) = d_1$ and $v_1 = \frac{O_{p_1^{\alpha_1}}(q) d_1}{d}$, therefore, the subset $C_{a_1}^{p_1^{\alpha_1}(q^{v_1})}$ of B_1 will repeat with the set

$$\{(a_2, a_3), (a_2 q, a_3 q), (a_2 q^2, a_3 q^2), \ldots, (a_2 q^{d_1 - 1}, a_3 q^{d_1 - 1})\}.$$

Similarly, the subset $C_{a_2}^{p_2^{\alpha_2}(q^{v_2})}$ of B_2 will repeat with the set

$$\{(a_1, a_3), (a_1 q, a_3 q), (a_1 q^2, a_3 q^2), \ldots, (a_1 q^{d_2 - 1}, a_3 q^{d_2 - 1})\}$$

and $C_{a_3}^{p_3^{\alpha_3}(q^{v_3})}$ of B_3 will repeat with the set

$$\{(a_1, a_2), (a_1 q, a_2 q), (a_1 q^2, a_2 q^2), \ldots, (a_1 q^{d_3 - 1}, a_2 q^{d_3 - 1})\}.$$

Hence

$$C_{a_1}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3}^{p_3^{\alpha_3}(q^{v_3})} \subset \{(a_1, a_2, a_3), (a_1 q, a_2 q, a_3 q), \ldots, (a_1 q^{d-1}, a_2 q^{d-1}, a_3 q^{d-1})\}.$$

Similarly, we get

$$\begin{aligned}&C_{a_1q}^{p_1^{\alpha_1}(q^{v_1})}\times C_{a_2q}^{p_2^{\alpha_2}(q^{v_2})}\times C_{a_3q}^{p_3^{\alpha_3}(q^{v_3})}\\&\subset\{(a_1,a_2,a_3),(a_1q,a_2q,a_3q),\ldots,(a_1q^{d-1},a_2q^{d-1},a_3q^{d-1})\}.\end{aligned}$$

As the set

$$\{(a_1,a_2,a_3),(a_1q,a_2q,a_3q),\ldots,(a_1q^{d-1},a_2q^{d-1},a_3q^{d-1})\}$$

is finite, therefore, there exists a positive integer t; $t=\mathrm{lcm}(v_1,v_2,v_3)$ such that

$$\begin{aligned}&\bigcup_{j=0}^{t-1}\left(C_{a_1q^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{a_2q^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{a_3q^j}^{p_3^{\alpha_3}(q^{v_3})}\right)\\&\subset\{(a_1,a_2,a_3),(a_1q,a_2q,a_3q),...,(a_1q^{d-1},a_2q^{d-1},a_3q^{d-1})\}.\end{aligned}$$

Since $C_{a_iq^j}^{p_i^{\alpha_i}(q^{v_i})}$ contains $\frac{d}{d_i}$ elements, therefore,

$$\bigcup_{j=0}^{t-1}\left(C_{a_1q^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{a_2q^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{a_3q^j}^{p_3^{\alpha_3}(q^{v_3})}\right)$$

contains $\frac{td^3}{d_1d_2d_3}$ elements. (By Lemma 2.2) $\frac{td^3}{d_1d_2d_3}=d$, therefore,

$$\bigcup_{j=0}^{t-1}\left(C_{a_1q^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{a_2q^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{a_3q^j}^{p_3^{\alpha_3}(q^{v_3})}\right)$$

$$=\{(a_1,a_2,a_3),(a_1q,a_2q,a_3q),\ldots,(a_1q^{d-1},a_2q^{d-1},a_3q^{d-1})\}.$$

Equivalently,

$$\begin{aligned}&\bigcup_{j=0}^{t-1}\lambda\left(C_{a_1q^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{a_2q^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{a_3q^j}^{p_3^{\alpha_3}(q^{v_3})}\right)\\&=\lambda\{(a_1,a_2,a_3),(a_1q,a_2q,a_3q),\ldots,(a_1q^{d-1},a_2q^{d-1},a_3q^{d-1})\}=C_1^{m(q)}.\end{aligned}$$

□

Corollary 2.4. *Let $s\in A$. If $a_is\equiv b_ip_i^{\beta_i}(mod\ p_i^{\alpha_i})$ then*

$$C_s^{m(q)}=\bigcup_{j=0}^{t-1}\lambda\left(C_{b_1p_1^{\beta_1}q^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{b_2p_2^{\beta_2}q^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{b_3p_3^{\beta_3}q^j}^{p_3^{\alpha_3}(q^{v_3})}\right).$$

Proof. By Theorem 2.3,

$$C_1^{m(q)}=\bigcup_{j=0}^{t-1}\lambda\left(C_{a_1q^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{a_2q^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{a_3q^j}^{p_3^{\alpha_3}(q^{v_3})}\right),$$

therefore, for $s\in A$, we have

$$C_s^{m(q)}=\bigcup_{j=0}^{t-1}\lambda\left(C_{a_1sq^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{a_2sq^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{a_3sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right).$$

If $a_i s \equiv b_i p_i^{\beta_i} (\text{mod } p_i^{\alpha_i})$ then clearly

$$C_s^{m(q)} = \bigcup_{j=0}^{t-1} \lambda\Big(C_{b_1 p_1^{\beta_1} q^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{b_2 p_2^{\beta_2} q^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{b_3 p_3^{\beta_3} q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big).$$

□

Theorem 2.5. *Let q be an odd prime with $gcd(q, m) = 1$. Further, let $O_{p_i^{\alpha_i}}(q) = \frac{\phi(p_i^{\alpha_i})}{r_i}$, $O_m(q) = d$, $O_{m_i}(q) = d_i$, $v_i = \frac{O_{p_i^{\alpha_i}}(q) d_i}{d}$ and $lcm(v_1, v_2, v_3) = t$. Then, the number of distinct q-cyclotomic cosets modulo m is*

$$\frac{\prod_{i=1}^{3} r_i \alpha_i v_i}{t} + \sum_{1 \le i < j \le 3} gcd\big(O_{p_i^{\alpha_i}}(q), O_{p_j^{\alpha_j}}(q)\big)\alpha_i \alpha_j r_i r_j + \sum_{i=1}^{3} \alpha_i r_i + 1.$$

Proof. Since $O_m(q) = d$, $O_{m_i}(q) = d_i$, $v_i = \frac{O_{p_i^{\alpha_i}}(q) d_i}{d}$, therefore, by Corollary 2.4,

$$C_s^{m(q)} = \bigcup_{j=0}^{t-1} \lambda\Big(C_{b_1 p_1^{\beta_1} q^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{b_2 p_2^{\beta_2} q^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{b_3 p_3^{\beta_3} q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big).$$

Consequently, the number of distinct q-cyclotomic cosets modulo m is equal to the number of distinct combinations of the form

$$\bigcup_{j=0}^{t-1} \lambda\Big(C_{b_1 p_1^{\beta_1} q^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{b_2 p_2^{\beta_2} q^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{b_3 p_3^{\beta_3} q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big).$$

We now count all such combinations by considering the following cases:

Case (1): $0 \le \beta_i \le \alpha_i - 1; 1 \le i \le 3$. In this case the number of distinct choices for $C_{b_i p_i^{\beta_i} q^j}^{p_i^{\alpha_i}(q^{v_i})}$ is $\alpha_i v_i r_i$. Therefore, the number of distinct combinations of the form

$$\bigcup_{j=0}^{t-1} \lambda\Big(C_{b_1 p_1^{\beta_1} q^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{b_2 p_2^{\beta_2} q^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{b_3 p_3^{\beta_3} q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big) \quad \text{is} \quad \frac{\prod_{i=1}^{r} r_i \alpha_i v_i}{t}.$$

These q-cyclotomic cosets are of the form $C_{s p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3}}^{m(q)}$; $\gcd(s, p_1 p_2 p_3) = 1$.

Case (2): $\beta_1 = \alpha_1, 0 \le \beta_2 \le \alpha_2 - 1, 0 \le \beta_3 \le \alpha_3 - 1$. By choosing $\beta_1 = \alpha_1$, we have fixed $C_{b_1 p_1^{\beta_1} q^j}^{p_1^{\alpha_1}(q^{v_1})} = \{0\}$. In other words we have a single choice of q^{v_1}-cyclotomic coset modulo $p_1^{\alpha_1}$. Consequently,

$$\bigcup_{j=0}^{t-1} \lambda\Big(C_{b_1 p_1^{\beta_1} q^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{b_2 p_2^{\beta_2} q^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{b_3 p_3^{\beta_3} q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big) = \bigcup_{j=0}^{t_{23}-1} \lambda\Big(C_{0}^{p_1^{\alpha_1}(q^{v_1})} \times C_{b_2 p_2^{\beta_2} q^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{b_3 p_3^{\beta_3} q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big),$$

where $t_{23} = v_2 = v_3 = \gcd\big(O_{p_2^{\alpha_2}}(q), O_{p_3^{\alpha_3}}(q)\big)$. Therefore, the number of q-cyclotomic cosets mod m of the form $C_{s p_1^{\alpha_1} p_2^{\beta_2} p_3^{\beta_3}}^{m(q)}$, where $\gcd(s, p_1 p_2 p_3) = 1$, is $\gcd\big(O_{p_2^{\alpha_2}}(q), O_{p_3^{\alpha_3}}(q)\big)\alpha_2 \alpha_3 r_2 r_3$.

Case (3): $0 \le \beta_1 \le \alpha_1 - 1, \beta_2 = \alpha_2, 0 \le \beta_3 \le \alpha_3 - 1$. In this case the number of distinct q cyclotomic cosets of the form $C_{s p_1^{\beta_1} p_2^{\alpha_2} p_3^{\beta_3}}^{m(q)}$ is $\gcd\big(O_{p_1^{\alpha_1}}(q), O_{p_3^{\alpha_3}}(q)\big)\alpha_1 \alpha_3 r_1 r_3$.

Case (4): $0 \le \beta_1 \le \alpha_1 - 1, 0 \le \beta_2 \le \alpha_2 - 1, \beta_3 = \alpha_3$. In this case the number of distinct q cyclotomic cosets of the form $C_{s p_1^{\beta_1} p_2^{\beta_2} p_3^{\alpha_3}}^{m(q)}$ is $\gcd\big(O_{p_1^{\alpha_1}}(q), O_{p_2^{\alpha_2}}(q)\big)\alpha_1 \alpha_2 r_1 r_2$.

Case (5): $\beta_1 = \alpha_1, \beta_2 = \alpha_2, 0 \leq \beta_3 \leq \alpha_3 - 1$. For this case

$$\bigcup_{j=0}^{t-1} \lambda\Big(C_{b_1 p_1^{\beta_1} q^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{b_2 p_2^{\beta_2} q^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{b_3 p_3^{\beta_3} q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big) = \lambda\Big(C_0^{p_1^{\alpha_1}(q^{v_1})} \times C_0^{p_2^{\alpha_2}(q^{v_2})} \times C_{b_3 p_3^{\beta_3} q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big).$$

Therefore, the number of cosets of the form $C^{m(q)}_{s p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\beta_3}}$ is $\alpha_3 r_3$.

Case (6): $\beta_1 = \alpha_1, 0 \leq \beta_2 \leq \alpha_2 - 1, \beta_3 = \alpha_3$. In this case $C^{m(q)}_{s p_1^{\alpha_1} p_2^{\beta_2} p_3^{\alpha_3}}$ is $\alpha_2 r_2$.

Case (7): $0 \leq \beta_1 \leq \alpha_1 - 1, \beta_2 = \alpha_2, \beta_3 = \alpha_3$. In this case $C^{m(q)}_{s p_1^{\beta_1} p_2^{\alpha_2} p_3^{\alpha_3}}$ is $\alpha_1 r_1$.

Case (8): $\beta_1 = \alpha_1, \beta_2 = \alpha_2, \beta_3 = \alpha_3$. For this case

$$\bigcup_{j=0}^{t-1} \lambda\Big(C_{b_1 p_1^{\beta_1} q^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{b_2 p_2^{\beta_2} q^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{b_3 p_3^{\beta_3} q^j}^{p_3^{\alpha_3}(q^{v_3})}\Big) = \lambda\Big(C_0^{p_1^{\alpha_1}(q^{v_1})} \times C_0^{p_2^{\alpha_2}(q^{v_2})} \times C_0^{p_3^{\alpha_3}(q^{v_3})}\Big).$$

Therefore, $C_0^{m(q)}$ is 1. As a result of above discussion, the number of distinct q-cyclotomic cosets modulo m is

$$\frac{\prod_{i=1}^{3} r_i \alpha_i v_i}{t} + \sum_{1 \leq i < j \leq 3} \gcd\big(O_{p_i^{\alpha_i}}(q), O_{p_j^{\alpha_j}}(q)\big)\alpha_i \alpha_j r_i r_j + \sum_{i=1}^{3} \alpha_i r_i + 1.$$

□

Corollary 2.6. *Let q be an odd prime with $gcd(q,m) = 1$. Further, let $O_{p_i^{\alpha_i}}(q) = \frac{\phi(p_i^{\alpha_i})}{r_i}$, $O_m(q) = d$, $O_{m_i}(q) = d_i$, $v_i = \frac{O_{p_i^{\alpha_i}}(q) d_i}{d}$ and $lcm(v_1, v_2, v_3) = t$. If $v_1 = v_2 = v_3$, then, the number of distinct q-cyclotomic cosets modulo m is*

$$\frac{\prod_{i=1}^{3}(r_i \alpha_i v_i + 1) + t - 1}{t}.$$

Proof. By Theorem 2.5,

$$\frac{\prod_{i=1}^{3} r_i \alpha_i v_i}{t} + \sum_{1 \leq i < j \leq 3} \gcd\big(O_{p_i^{\alpha_i}}(q), O_{p_j^{\alpha_j}}(q)\big)\alpha_i \alpha_j r_i r_j + \sum_{i=1}^{3} \alpha_i r_i + 1.$$

Therefore, for $\mathrm{lcm}(v_1, v_2, v_3) = t$ and $v_1 = v_2 = v_3$. As $\gcd(O_{p_i^{\alpha_i}}(q), O_{p_j^{\alpha_j}}(q)) \times \mathrm{lcm}\big(O_{p_i^{\alpha_i}}(q), O_{p_j^{\alpha_j}}(q)\big) = O_{p_i^{\alpha_i}}(q) \times O_{p_j^{\alpha_j}}(q)$. Use the above result in Theorem 2.5, we have

$$\frac{(\alpha_1 v_1 r_1)(\alpha_2 v_2 r_2)(\alpha_3 v_3 r_3)}{t} + \frac{(\alpha_1 v_1 r_1)(\alpha_2 v_2 r_2)}{t} + \frac{(\alpha_1 v_1 r_1)(\alpha_3 v_3 r_3)}{t} + \frac{(\alpha_2 v_2 r_2)(\alpha_3 v_3 r_3)}{t} + \frac{(\alpha_1 v_1 r_1)}{t} + \frac{(\alpha_2 v_2 r_2)}{t} + \frac{(\alpha_3 v_3 r_3)}{t} + 1$$

Further solve it. We get

$$\frac{\prod_{i=1}^{3}(r_i \alpha_i v_i + 1) + t - 1}{t}.$$

□

3. Primitive idempotents in R_m

For $1 \leq i \leq 3$, let $\theta_s^{p_i^{\alpha_i}(q^{v_i})}(x_i)$ and $\theta_s^{m(q)}(x)$ denote the primitive idempotents in $R_{p_i^{\alpha_i}} = F_{q^{v_i}}[x]/(x^{p_i^{\alpha_i}}-1)$ and $R_m = F_q[x]/(x^m-1)$ corresponding to $C_s^{p_i^{\alpha_i}(q^{v_i})}$ and $C_s^{m(q)}$ respectively. In this section, we give two different proofs to show that $\theta_s^{m(q)}(x)$ can be computed with the help of suitably chosen primitive idempotents $\theta_s^{p_i^{\alpha_i}(q^{v_i})}(x_i)$ from $R_{p_i^{\alpha_i}}$. The composition of $C_s^{m(q)}$ helps in choosing these $\theta_s^{p_i^{\alpha_i}(q^{v_i})}(x_i)$. By Theorem 2.5,

$$C_s^{m(q)} = \bigcup_{j=0}^{t-1} \lambda\Big(C_{a_1sq^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2sq^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3sq^j}^{p_3^{\alpha_3}(q^{v_3})}\Big),$$

therefore, in Theorem 3.5, we use λ product of polynomials [Definition 3.1] and show that

$$\theta_s^{m(q)}(x) = \sum_{j=0}^{t-1} \lambda\Big(\theta_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}(x_1)\theta_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}(x_2)\theta_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}(x_3)\Big).$$

In Theorem 3.6, we use trace function $Tr_{F_{q^t}|F_q}$ from $F_{q^t}[x]$ to $F_q[x]$ to show that

$$\theta_s^{m}(x) = Tr_{F_{q^t}|F_q}\Big(\theta_s^{p_1^{\alpha_1}(q^{v_1})}(x^{m_1})\theta_s^{p_2^{\alpha_2}(q^{v_2})}(x^{m_2})\theta_s^{p_3^{\alpha_3}(q^{v_3})}(x^{m_3})\Big),$$

where $\theta_s^{p_i^{\alpha_i}(q^{v_i})}(x^{m_i})$ is the polynomial obtained from $\theta_s^{p_i^{\alpha_i}(q^{v_i})}(x_i)$ by replacing x_i by x^{m_i}.

Definition 3.1. *[λ-product of $x_i^{b_i}$'s] Let x_1, x_2, x_3 be three variables. Define*

$$\lambda\big((\alpha_1x_1^{b_1}), (\alpha_2x_2^{b_2}), (\alpha_3x_3^{b_3})\big) = \alpha_1\alpha_2\alpha_3x^{\lambda(b_1,\ b_2,\ b_3)},$$

where $\alpha_i \in F_{q^t}$, $b_i \in A_i$ and call it the λ-product [10, Definition 3.1] of $x_i^{b_i}$'s.

Definition 3.2. *Let $f(x) = \sum a_ix^i \in F_{q^t}[x]$. Then, the trace function $Tr_{F_{q^t}|F_q} : F_{q^t}[x] \to F_q[x]$ is defined as*

$$Tr_{F_{q^t}|F_q}\big(f(x)\big) = \sum Tr_{F_{q^t}|F_q}(a_i)x^i.$$

Further, for $f(x), g(x), h(x) \in F_{q^t}[x]$, if

$$f(x)g(x)h(x) = \sum c_ix^i, \text{ then } Tr_{F_{q^t}|F_q}\big(f(x)g(x)h(x)\big) = \sum Tr_{F_{q^t}|F_q}(c_i)x^i.$$

Definition 3.3. *[3, Theorem 1] The $\theta_s^{m(q)}(x) = \sum_{i=0}^{m-1}\epsilon_ix^i$, where $\epsilon_i = \epsilon_i^{C_s^{m(q)}} = \frac{1}{m}\big(\sum_{s\in C_s^{m(q)}}\delta^{-is}\big)$ and δ is a fixed primitive mth root of unity in some extension of F_q, is a primitive idempotent in R_m corresponding to $C_s^{m(q)}$.*

Note 3.4. *In the following theorems, δ is a fixed primitive mth root of unity in some extension of F_{q^t} and therefore, $\delta_i = \delta^{m_i}$ is a primitive $p_i^{\alpha_i}$th root of unity in the same extension of F_{q^t}.*

Theorem 3.5. *If $\lambda(a_1, a_2, a_3) = 1$ and*

$$C_s^{m(q)} = \bigcup_{j=0}^{t-1} \lambda\Big(C_{a_1sq^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2sq^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3sq^j}^{p_3^{\alpha_3}(q^{v_3})}\Big),$$

then

$$\theta_s^{m(q)}(x) = \sum_{j=0}^{t-1} \lambda\Big(\theta_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}(x_1)\theta_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}(x_2)\theta_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}(x_3)\Big),$$

where v_i and t are same as defined in Theorem 2.3.

Proof. First we compute the coefficient of x^k in

$$\sum_{j=0}^{t-1}\lambda\Big(\theta_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}(x_1)\theta_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}(x_2)\theta_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}(x_3)\Big).$$

By Definition 3.3

$$\theta_{sq^j}^{p_i^{\alpha_i}(q^{v_i})}(x_i)=\sum_{s_i=0}^{p_i^{\alpha_i}-1}\epsilon_{s_i}x_i^{s_i}; 1\leq i\leq 3,$$

where

$$\epsilon_{s_i}=\epsilon_{s_i}^{C_{sq^j}^{p_i^{\alpha_i}(q^{v_i})}}=\frac{1}{p_i^{\alpha_i}}\sum_{sq^j\in C_{sq^j}^{p_i^{\alpha_i}(q^{v_i})}}\delta_i^{-s_i sq^j}.$$

Since $1=\lambda(a_1,a_2,a_3)$, therefore, $k=\lambda(a_1k,a_2k,a_3k)$. Then, by Definition 3.1 the coefficient of x^k in

$$\sum_{j=0}^{t-1}\lambda\Big(\theta_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}(x_1)\theta_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}(x_2)\theta_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}(x_3)\Big)\quad\text{is}$$

$$\sum_{j=0}^{t-1}\epsilon_{a_1k}^{C_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}}\epsilon_{a_2k}^{C_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}}\epsilon_{a_3k}^{C_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}}$$

$$=\sum_{j=0}^{t-1}\Big(\frac{1}{p_1^{\alpha_1}}\sum_{sq^j\in C_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}}\delta_1^{-a_1ksq^j}\Big)\Big(\frac{1}{p_2^{\alpha_2}}\sum_{sq^j\in C_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}}\delta_2^{-a_2ksq^j}\Big)$$
$$\Big(\frac{1}{p_3^{\alpha_3}}\sum_{sq^j\in C_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}}\delta_3^{-a_3ksq^j}\Big)$$

$\delta_i=\delta^{m_i}$, therefore, we get

$$\sum_{j=0}^{t-1}\epsilon_{a_1k}^{C_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}}\epsilon_{a_2k}^{C_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}}\epsilon_{a_3k}^{C_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}}=$$

$$\sum_{j=0}^{t-1}\frac{1}{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}\sum_{(sq^j,sq^j,sq^j)\in\left(C_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)}\delta^{-(m_1a_1ksq^j+m_2a_2ksq^j+m_3a_3ksq^j)}$$
$$=\sum_{j=0}^{t-1}\frac{1}{m}\sum_{(sq^j,sq^j,sq^j)\in\left(C_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)}\delta^{-k(m_1a_1+m_2a_2+m_3a_3)sq^j}$$

$$=\sum_{j=0}^{t-1}\frac{1}{m}\sum_{(sq^j,sq^j,sq^j)\in\left(C_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)}\delta^{-k\lambda(a_1,a_2,a_3)sq^j}$$
$$=\sum_{j=0}^{t-1}\frac{1}{m}\sum_{(sq^j,sq^j,sq^j)\in\left(C_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}\times C_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}\times C_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)}\delta^{-ksq^j}. \tag{2}$$

Now we obtain the coefficient of x^k in $\theta_s^{m(q)}(x)$. By Definition 3.3, the coefficient of x^k in $\theta_s^{m(q)}(x)$ is

$$\epsilon_k = \epsilon_k^{C_s^{m(q)}} = \frac{1}{m} \sum_{s \in C_s^{m(q)}} \delta^{-ks}$$

$$= \frac{1}{m} \sum_{s \in \bigcup_{j=0}^{t-1} \lambda\left(C_{a_1 sq^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 sq^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)} \delta^{-ks}$$

$$= \frac{1}{m} \sum_{j=0}^{t-1} \sum_{sq^j \in \lambda\left(C_{a_1 sq^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 sq^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)} \delta^{-ksq^j}.$$

Since $sq^j = \lambda(a_1 sq^j, a_2 sq^j, a_3 sq^j)$, therefore,

$$\epsilon_k = \frac{1}{m} \sum_{j=0}^{t-1} \sum_{\lambda(a_1 sq^j, a_2 sq^j, a_3 sq^j) \in \lambda\left(C_{a_1 sq^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 sq^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)} \delta^{-ksq^j}$$

$$= \frac{1}{m} \sum_{j=0}^{t-1} \sum_{(a_1 sq^j, a_2 sq^j, a_3 sq^j) \in \left(C_{a_1 sq^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 sq^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)} \delta^{-ksq^j}$$

$$= \frac{1}{m} \sum_{j=0}^{t-1} \sum_{(sq^j, sq^j, sq^j) \in \left(C_{sq^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{sq^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)} \delta^{-ksq^j}. \tag{3}$$

By (2) and (3) we get that the coefficient of x^k is same in $\theta_s^{m(q)}(x)$ and in

$$\sum_{j=0}^{t-1} \lambda\Big(\theta_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}(x_1)\theta_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}(x_2)\theta_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}(x_3)\Big).$$

Hence

$$\theta_s^{m(q)}(x) = \sum_{j=0}^{t-1} \lambda\Big(\theta_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}(x_1)\theta_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}(x_2)\theta_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}(x_3)\Big).$$

□

Theorem 3.6. *If $\lambda(a_1, a_2, a_3) = 1$ and*

$$C_s^{m(q)} = \bigcup_{j=0}^{t-1} \lambda\Big(C_{a_1 sq^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 sq^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 sq^j}^{p_3^{\alpha_3}(q^{v_3})}\Big),$$

then

$$\theta_s^{m(q)}(x) = Tr_{F_{q^t}|F_q}\Big(\theta_s^{p_1^{\alpha_1}(q^{v_1})}(x^{m_1})\theta_s^{p_2^{\alpha_2}(q^{v_2})}(x^{m_2})\theta_s^{p_3^{\alpha_3}(q^{v_3})}(x^{m_3})\Big),$$

where v_i and t are same as defined in Theorem 2.3.

Proof. Since $t = \mathrm{lcm}(v_1, v_2, v_3)$, the $F_{q^{v_i}} \subset F_{q^t}$ and therefore, we can multiply $\theta_s^{p_1^{\alpha_1}(q^{v_1})}(x^{m_1}) \in F_{q^{v_1}}[x], \theta_s^{p_2^{\alpha_2}(q^{v_2})}(x^{m_2}) \in F_{q^{v_2}}[x]$ and $\theta_s^{p_3^{\alpha_3}(q^{v_3})}(x^{m_3})$
$\in F_{q^{v_3}}[x]$.

$$\text{Let} \quad \theta_s^{p_1^{\alpha_1}(q^{v_1})}(x^{m_1})\theta_s^{p_2^{\alpha_2}(q^{v_2})}(x^{m_2})\theta_s^{p_3^{\alpha_3}(q^{v_3})}(x^{m_3}) = \sum c_k x^k.$$

We compute the coefficient of x^k in

$$\mathrm{Tr}_{F_{q^t}|F_q}\Big(\theta_s^{p_1^{\alpha_1}(q^{v_1})}(x^{m_1})\theta_s^{p_2^{\alpha_2}(q^{v_2})}(x^{m_2})\theta_s^{p_3^{\alpha_3}(q^{v_3})}(x^{m_3})\Big).$$

By Definition 3.3

$$\theta_s^{p_i^{\alpha_i}(q^{v_i})}(x^{m_i}) = \sum_{s_i=0}^{p_i^{\alpha_i}-1} \epsilon_{s_i} x^{m_i s_i}; 1 \le i \le 3,$$

where

$$\epsilon_{s_i} = \epsilon_{s_i}^{C_s^{p_i^{\alpha_i}(q^{v_i})}} = \frac{1}{p_i^{\alpha_i}} \sum_{s \in C_s^{p_i^{\alpha_i}(q^{v_i})}} \delta_i{}^{-s_i s}. \tag{4}$$

As $1 = \lambda(a_1, a_2, a_3)$, therefore, $k = \lambda(a_1k, a_2k, a_3k) = \big(m_1a_1k + m_2a_2k + m_3a_3k\big)(\mathrm{mod}\ m)$. Therefore,

$$c_k = \epsilon_{a_1k}^{C_s^{p_1^{\alpha_1}(q^{v_1})}} \epsilon_{a_2k}^{C_s^{p_2^{\alpha_2}(q^{v_2})}} \epsilon_{a_3k}^{C_s^{p_3^{\alpha_3}(q^{v_3})}}$$

$$= \Big(\frac{1}{p_1^{\alpha_1}} \sum_{s \in C_s^{p_1^{\alpha_1}(q^{v_1})}} \delta_1{}^{-a_1ks}\Big)\Big(\frac{1}{p_2^{\alpha_2}} \sum_{s \in C_s^{p_2^{\alpha_2}(q^{v_2})}} \delta_2{}^{-a_2ks}\Big)\Big(\frac{1}{p_3^{\alpha_3}} \sum_{s \in C_s^{p_3^{\alpha_3}(q^{v_3})}} \delta_3{}^{-a_3ks}\Big).$$

$\delta_i = \delta^{m_i}$, therefore,

$$c_k = \frac{1}{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}} \sum_{(s,s,s) \in \big(C_s^{p_1^{\alpha_1}(q^{v_1})} \times C_s^{p_2^{\alpha_2}(q^{v_2})} \times C_s^{p_3^{\alpha_3}(q^{v_3})}\big)} \delta^{-(m_1a_1ks + m_2a_2ks + m_3a_3ks)}$$

$$= \frac{1}{m} \sum_{(s,s,s) \in \big(C_s^{p_1^{\alpha_1}(q^{v_1})} \times C_s^{p_2^{\alpha_2}(q^{v_2})} \times C_s^{p_3^{\alpha_3}(q^{v_3})}\big)} \delta^{-(m_1a_1 + m_2a_2 + m_3a_3)ks}$$

$$= \frac{1}{m} \sum_{(s,s,s) \in \big(C_s^{p_1^{\alpha_1}(q^{v_1})} \times C_s^{p_2^{\alpha_2}(q^{v_2})} \times C_s^{p_3^{\alpha_3}(q^{v_3})}\big)} \delta^{-ks}.$$

Since

$$(s, s, s) \in \Big(C_s^{p_1^{\alpha_1}(q^{v_1})} \times C_s^{p_2^{\alpha_2}(q^{v_2})} \times C_s^{p_3^{\alpha_3}(q^{v_3})}\Big)$$

$$\iff (a_1s, a_2s, a_3s) \in \Big(C_{a_1s}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2s}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3s}^{p_3^{\alpha_3}(q^{v_3})}\Big)$$

$$\iff \lambda(a_1s, a_2s, a_3s) \in \lambda\Big(C_{a_1s}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2s}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3s}^{p_3^{\alpha_3}(q^{v_3})}\Big)$$

$$\iff s \in \lambda\Big(C_{a_1 s}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 s}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 s}^{p_3^{\alpha_3}(q^{v_3})}\Big)$$

therefore,

$$c_k = \frac{1}{m} \sum_{s \in \lambda\left(C_{a_1 s}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 s}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 s}^{p_3^{\alpha_3}(q^{v_3})}\right)} \delta^{-ks}.$$

Then,

$$\mathrm{Tr}_{F_{q^t}|F_q}\Big(\theta_s^{p_1^{\alpha_1}(q^{v_1})}(x^{m_1})\theta_s^{p_2^{\alpha_2}(q^{v_2})}(x^{m_2})\theta_s^{p_3^{\alpha_3}(q^{v_3})}(x^{m_3})\Big) = \sum \mathrm{Tr}_{F_{q^t}|F_q}(c_k)x^k$$

$$= \sum \mathrm{Tr}_{F_{q^t}|F_q}\Big(\frac{1}{m} \sum_{s \in \lambda\left(C_{a_1 s}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 s}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 s}^{p_3^{\alpha_3}(q^{v_3})}\right)} \delta^{-ks}\Big)x^k$$

$$= \sum \Big(\frac{1}{m} \sum_{s \in \bigcup_{j=0}^{t-1} \lambda\left(C_{a_1 sq^j}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 sq^j}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 sq^j}^{p_3^{\alpha_3}(q^{v_3})}\right)} \delta^{-ks}\Big)x^k$$

$$= \sum \Big(\frac{1}{m} \sum_{s \in C_s} \delta^{-ks}\Big)x^k = \sum \epsilon_k x^k = \theta_s^{m(q)}(x).$$

It completes the proof. As a result of Theorem 3.5 and Theorem 3.6, we have following results. □

Corollary 3.7. *If $v_1 = v_2 = v_3 = 1$ and if $1 = \lambda(a_1, a_2, a_3)$ and*

$$C_s^{m(q)} = \lambda\Big(C_{a_1 s}^{p_1^{\alpha_1}(q^{v_1})} \times C_{a_2 s}^{p_2^{\alpha_2}(q^{v_2})} \times C_{a_3 s}^{p_3^{\alpha_3}(q^{v_3})}\Big),$$

then

$$\theta_s^{m(q)}(x) = \lambda\Big(\theta_s^{p_1^{\alpha_1}(q^{v_1})}(x_1)\theta_s^{p_2^{\alpha_2}(q^{v_2})}(x_2)\theta_s^{p_3^{\alpha_3}(q^{v_3})}(x_3)\Big).$$

Corollary 3.8. *If $v_1 = v_2 = v_3 = 1$ and if $1 = \lambda(a_1, a_2, a_3)$ and*

$$C_s^{m(q)} = \lambda\Big(C_{a_1 s}^{p_1^{\alpha_1}(q)} \times C_{a_2 s}^{p_2^{\alpha_2}(q)} \times C_{a_3 s}^{p_3^{\alpha_3}(q)}\Big), \text{ then}$$

$$\theta_s^{m(q)}(x) = Tr_{F_q|F_q}\Big(\theta_s^{p_1^{\alpha_1}(q)}(x^{m_1})\theta_s^{p_2^{\alpha_2}(q)}(x^{m_2})\theta_s^{p_3^{\alpha_3}(q)}(x^{m_3})\Big)$$

$$= \theta_s^{p_1^{\alpha_1}(q)}(x^{m_1})\theta_s^{p_2^{\alpha_2}(q)}(x^{m_2})\theta_s^{p_3^{\alpha_3}(q)}(x^{m_3}).$$

Note 3.9. *If $\theta_s^{m(q)}(x) = \sum_{j=0}^{t-1} \lambda(\theta_{sq^j}^{p_1^{\alpha_1}(q^{v_1})}(x_1)\theta_{sq^j}^{p_2^{\alpha_2}(q^{v_2})}(x_2)\theta_{sq^j}^{p_3^{\alpha_3}(q^{v_3})}(x_3))$, then practically $\theta_s^{m(q)}(x) = \sum_{j=0}^{t-1} \lambda\big(\theta_{s_1 q^j}^{p_1^{\alpha_1}(q^{v_1})}(x_1)\theta_{s_2 q^j}^{p_2^{\alpha_2}(q^{v_2})}(x_2)\theta_{s_3 q^j}^{p_3^{\alpha_3}(q^{v_3})}(x_3)\big)$, where $s \equiv s_i (mod\ p_i^{\alpha_i})$. We have shown it by calculating expressions of all the primitive idempotents in R_{715} over F_3 in Appendix 1.*

4. Minimal and generating polynomials of minimal cyclic codes of length m

Let M_s^m denote the minimal cyclic code of length m corresponding to $C_s^{m(q)}$. Further, let $\eta_s^m(x)$ and $g_s^m(x)$ denote the minimal polynomial and generating polynomial of M_s^m respectively. Then $\eta_s^m(x) = \prod_{s \in C_s^{m(q)}}(x - \delta^s)$ and $g_s^m(x) = \frac{(x^m - 1)}{\eta_s^m(x)}$, where δ is a primitive mth root of unity. In this section we obtain minimal polynomials and generating polynomials of minimal cyclic codes of length m.

Note 4.1. *Since* $m = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$ *and* $gcd(m,q) = 1$, *therefore, the polynomials* $x^{p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}} - 1$; $0 \leq \beta_i \leq \alpha_i$ *and* $1 \leq i \leq 3$ *are separable over* F_q.

Lemma 4.2. *The expression* $\frac{f(x)}{h(x)}$, *where*

$$f(x) = \big(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}} - 1\big)\big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}} - 1\big)$$

$$\big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}} - 1\big)\big(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}} - 1\big),$$

and

$$h(x) = \big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}} - 1\big)\big(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}} - 1\big)$$

$$\big(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}} - 1\big)\big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}} - 1\big),$$

is a polynomial over F_q.

Proof. To prove that $\frac{f(x)}{h(x)}$ is a polynomial over F_q, it is sufficient to show that every root of $h(x)$ is a root of $f(x)$ also. Let

$$s = ap_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3};\ \ 0 \leq a \leq p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3} - 1,$$

be an integer. We consider the following cases:

Case (1): gcd$(a, p_1p_2p_3) = p_1$(or p_2 or p_3). In this case the δ^s is a multiple root of $h(x)$ with multiplicity 1. Moreover, it is a root of $f(x)$ also having multiplicity 1. Hence in this case δ^s has same multiplicity.

Case (2): gcd$(a, p_1p_2p_3) = p_1p_2$(or p_1p_3 or p_2p_3). In this case the δ^s is a multiple root of $h(x)$ with multiplicity 2. Moreover, it is a root of $f(x)$ also having multiplicity 2. Hence in this case δ^s has same multiplicity.

Case (3): gcd$(a, p_1p_2p_3) = p_1p_2p_3$. In this case the δ^s is a multiple root of $h(x)$ and $f(x)$ with multiplicity 4.

By above discussion we conclude that $h(x)|f(x)$. Further, for every a with $\gcd(a, p_1p_2p_3) = 1$, the δ^s is a root of $f(x)$ only. Therefore, $\frac{f(x)}{h(x)}$ is a polynomial of degree $\phi(p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3})$ over F_q, where ϕ is Euler's phi function. □

Theorem 4.3. *Let* $gcd(s,m) = p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}$. *Then,* $\prod_s \eta_s^m(x) = \frac{f(x)}{h(x)}$, *where* $f(x)$ *and* $h(x)$ *are same as defined in Lemma 4.2.*

The following results are easy to prove.

Theorem 4.4. *Let* $gcd(s,m) = p_1^{\alpha_1}p_2^{\beta_2}p_3^{\beta_3}$. *Then,*

$$\prod_s \eta_s^m(x) = \frac{\big(x^{p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}} - 1\big)\big(x^{p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}} - 1\big)}{\big(x^{p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}} - 1\big)\big(x^{p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}} - 1\big)}.$$

Theorem 4.5. *If* $gcd(s,m) = p_1^{\beta_1}p_2^{\alpha_2}p_3^{\beta_3}$, *then,*

$$\prod_s \eta_s^m(x) = \frac{\big(x^{p_1^{\alpha_1-\beta_1}p_3^{\alpha_3-\beta_3}} - 1\big)\big(x^{p_1^{\alpha_1-\beta_1-1}p_3^{\alpha_3-\beta_3-1}} - 1\big)}{\big(x^{p_1^{\alpha_1-\beta_1}p_3^{\alpha_3-\beta_3-1}} - 1\big)\big(x^{p_1^{\alpha_1-\beta_1-1}p_3^{\alpha_3-\beta_3}} - 1\big)}.$$

Theorem 4.6. *If $gcd(s,m) = p_1^{\beta_1} p_2^{\beta_2} p_3^{\alpha_3}$, then,*

$$\prod_s \eta_s^m(x) = \frac{\left(x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2}} - 1\right)\left(x^{p_1^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2-1}} - 1\right)}{\left(x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2-1}} - 1\right)\left(x^{p_1^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2}} - 1\right)}.$$

Theorem 4.7. *If $gcd(s,m) = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\beta_3}$, then*

$$\prod_s \eta_s^m(x) = \frac{\left(x^{p_3^{\alpha_3-\beta_3}} - 1\right)}{\left(x^{p_3^{\alpha_3-\beta_3-1}} - 1\right)}.$$

Theorem 4.8. *If $gcd(s,m) = p_1^{\alpha_1} p_2^{\beta_2} p_3^{\alpha_3}$, then*

$$\prod_s \eta_s^m(x) = \frac{\left(x^{p_2^{\alpha_2-\beta_2}} - 1\right)}{\left(x^{p_2^{\alpha_2-\beta_2-1}} - 1\right)}.$$

Theorem 4.9. *If $gcd(s,m) = p_1^{\beta_1} p_2^{\alpha_2} p_3^{\alpha_3}$, then,*

$$\prod_s \eta_s^m(x) = \frac{\left(x^{p_1^{\alpha_1-\beta_1}} - 1\right)}{\left(x^{p_1^{\alpha_1-\beta_1-1}} - 1\right)}.$$

Theorem 4.10. *If $gcd(s,m) = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$, then, $\eta_s^m(x) = \left(x-1\right)$.*

Theorem 4.11. *Let $gcd(s,m) = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3}$. Then $\prod_s g_s^m(x) = \frac{p(x)}{q(x)}$, where*

$$p(x) = \left(x^{p_1^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}} - 1\right)\left(x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2-1} p_3^{\alpha_3-\beta_3}} - 1\right)$$

$$\left(x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3-1}} - 1\right)\left(x^{p_1^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2-1} p_3^{\alpha_3-\beta_3-1}} - 1\right)$$

$$\left(\sum_{i=0}^{p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3}-1} x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3} i}\right) \quad \textit{and}$$

$$q(x) = \left(x^{p_1^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2-1} p_3^{\alpha_3-\beta_3}} - 1\right)\left(x^{p_1^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3-1}} - 1\right)$$

$$\left(x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2-1} p_3^{\alpha_3-\beta_3-1}} - 1\right).$$

Proof. Since

$$\prod_s g_s^m(x) = \frac{(x^m - 1)}{\prod_s \eta_s^m(x)}$$
$$= \frac{\left(x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}} - 1\right)\left(\sum_{i=0}^{p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3}-1} x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3} i}\right)}{\prod_s \eta_s^m(x)},$$

the result follows from Theorem 4.3, we have $\prod_s \eta_s^m(x) = \frac{f(x)}{h(x)}$, where $f(x)$ and $h(x)$ are same as defined in Lemma 4.2 Thus, we obtain $\prod_s g_s^m(x) = \frac{p(x)}{q(x)}$, where

$$p(x) = \left(x^{p_1^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}} - 1\right)\left(x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2-1} p_3^{\alpha_3-\beta_3}} - 1\right)$$

$$\left(x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3-1}} - 1\right)\left(x^{p_1^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2-1} p_3^{\alpha_3-\beta_3-1}} - 1\right)$$

$$\Big(\sum_{i=0}^{p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}-1} x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}i}\Big) \qquad \text{and}$$

$$q(x) = \big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}} - 1\big)\big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}} - 1\big)$$
$$\big(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}} - 1\big).$$

□

Theorem 4.12. *Let $gcd(s,m) = p_1^{\alpha_1}p_2^{\beta_2}p_3^{\beta_3}$. Then*

$$\prod_s g_s^m(x) =$$
$$\frac{\big(x^{p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}} - 1\big)\big(x^{p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}} - 1\big)\Big(\sum_{i=0}^{p_1^{\alpha_1}p_2^{\beta_2}p_3^{\beta_3}-1} x^{p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}i}\Big)}{\big(x^{p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}} - 1\big)}.$$

Proof.

$$\prod_s g_s^m(x) = \frac{x^m - 1}{\prod_s \eta_s^m(x)}$$
$$= \frac{\big(x^{p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}} - 1\big)\Big(\sum_{i=0}^{p_1^{\alpha_1}p_2^{\beta_2}p_3^{\beta_3}-1} x^{p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}i}\Big)}{\prod_s \eta_s^m(x)}.$$

□

The result follows from Theorem 4.4.
By using the same argument which we have used in Theorem 4.12, we have following results:

Theorem 4.13. *Let $gcd(s,m) = p_1^{\beta_1}p_2^{\alpha_2}p_3^{\beta_3}$. Then*

$$\prod_s g_s^m(x) =$$
$$\frac{\big(x^{p_1^{\alpha_1-\beta_1}p_3^{\alpha_3-\beta_3-1}} - 1\big)\big(x^{p_1^{\alpha_1-\beta_1-1}p_3^{\alpha_3-\beta_3}} - 1\big)\Big(\sum_{i=0}^{p_1^{\beta_1}p_2^{\alpha_2}p_3^{\beta_3}-1} x^{p_1^{\alpha_1-\beta_1}p_3^{\alpha_3-\beta_3}i}\Big)}{\big(x^{p_1^{\alpha_1-\beta_1-1}p_3^{\alpha_3-\beta_3-1}} - 1\big)}.$$

Theorem 4.14. *Let $gcd(s,m) = p_1^{\beta_1}p_2^{\beta_2}p_3^{\alpha_3}$. Then*

$$\prod_s g_s^m(x) =$$
$$\frac{\big(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2-1}} - 1\big)\big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}} - 1\big)\Big(\sum_{i=0}^{p_1^{\beta_1}p_2^{\beta_2}p_3^{\alpha_3}-1} x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}i}\Big)}{\big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}} - 1\big)}.$$

Theorem 4.15. *Let $gcd(s,m) = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\beta_3}$. Then*

$$\prod_s g_s^m(x) = \big(x^{p_3^{\alpha_3-\beta_3-1}} - 1\big)\Big(\sum_{i=0}^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\beta_3}-1} x^{p_3^{\alpha_3-\beta_3}i}\Big).$$

Proof.

$$\prod_s g_s^m(x) = \frac{x^m-1}{\prod_s \eta_s^m(x)} = \frac{\left(x^{p_3^{\alpha_3-\beta_3}}-1\right)\left(\sum_{i=0}^{p_1^{\alpha_1}p_2^{\beta_2}p_3^{\beta_3}-1} x^{p_3^{\alpha_3-\beta_3}i}\right)}{\prod_s \eta_s^m(x)},$$

∎

The result follows from Theorem 4.7.

Theorem 4.16. *Let* $gcd(s,m) = p_1^{\alpha_1}p_2^{\beta_2}p_3^{\alpha_3}$. *Then*

$$\prod_s g_s^m(x) = \left(x^{p_2^{\alpha_2-\beta_2-1}}-1\right)\left(\sum_{i=0}^{p_1^{\alpha_1}p_2^{\beta_2}p_3^{\alpha_3}-1} x^{p_2^{\alpha_2-\beta_2}i}\right).$$

Theorem 4.17. *Let* $gcd(s,m) = p_1^{\beta_1}p_2^{\alpha_2}p_3^{\alpha_3}$. *Then*

$$\prod_s g_s^m(x) = \left(x^{p_1^{\alpha_1-\beta_1-1}}-1\right)\left(\sum_{i=0}^{p_1^{\beta_1}p_2^{\alpha_2}p_3^{\alpha_3}-1} x^{p_1^{\alpha_1-\beta_1}i}\right).$$

Theorem 4.18. *Let* $gcd(s,m) = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$. *Then*

$$\prod_s g_s^m(x) = \sum_{i=0}^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}-1} x^i.$$

5. Minimum distance of minimal cyclic codes of length m

In this section, we compute a lower bound on minimum distance of minimal cyclic codes of length $m = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3}$. First we prove some results.

Lemma 5.1. *Let* $f(x) = a_1x^{t_1} + a_2x^{t_2} + ... + a_kx^{t_k}$ *be a polynomial over* F_q *and* $\{1,2,3,...k\} = \{i_1,i_2,i_3,...i_k\}$. *Further, let* m *be a positive integer such that* $t_i \equiv r_i(mod\ m)$. *Then* x^m-1 *divides* $f(x)$ *if and only if* $r_{i_1} = r_{i_2} = ... = r_{i_{n_1}}$, $r_{i_{n_1+1}} = r_{i_{n_1+2}} = ... = r_{i_{n_2}}$, $r_{i_{n_2+1}} = r_{i_{n_2+2}} = ... = r_{i_{n_3}}$, ..., $r_{i_{n_t+1}} = r_{i_{n_t+2}} = ... = r_{i_k}$, $a_{i_1} + a_{i_2} + ... + a_{i_{n_1}} = 0$, $a_{i_{n_1+1}} + a_{i_{n_1+2}} + ... + a_{i_{n_2}} = 0$, $a_{i_{n_2+1}} + a_{i_{n_2+2}} + ... + a_{i_{n_3}} = 0$, ..., $a_{i_{n_t+1}} + a_{i_{n_t+2}} + ... + a_{i_k} = 0$.

Proof. Since $x^m \equiv 1(\text{mod } x^m-1)$ and $t_i \equiv r_i(\text{mod } m)$, therefore, $\sum_{j=1}^k a_jx^{t_j} \equiv \sum_{j=1}^k a_jx^{r_j}(\text{mod } x^m-1)$. Consequently, x^m-1 divides $f(x)$ if and only if $\sum_{j=1}^k a_jx^{r_j} = 0$. Therefore, x^m-1 divides $f(x)$ if and only if $r_{i_1} = r_{i_2} = ... = r_{i_{n_1}}$, $r_{i_{n_1+1}} = r_{i_{n_1+2}} = ... = r_{i_{n_2}}$, $r_{i_{n_2+1}} = r_{i_{n_2+2}} = ... = r_{i_{n_3}}$, ..., $r_{i_{n_t+1}} = r_{i_{n_t+2}} = ... = r_{i_k}$, $a_{i_1} + a_{i_2} + ... + a_{i_{n_1}} = 0$, $a_{i_{n_1+1}} + a_{i_{n_1+2}} + ... + a_{i_{n_2}} = 0$, $a_{i_{n_2+1}} + a_{i_{n_2+2}} + ... + a_{i_{n_3}} = 0$, ..., $a_{i_{n_t+1}} + a_{i_{n_t+2}} + ... + a_{i_k} = 0$. ∎

Lemma 5.2. *Let*

$$t_1 \equiv t_2 \equiv t_3 \equiv t_4(mod\ \ p_1^{\alpha_1}p_2^{\alpha_2}),$$

$$t_1 \equiv t_3 \text{ and } t_2 \equiv t_4(mod\ p_2^{\alpha_2}p_3^{\alpha_3}),$$

$$t_1 \equiv t_2 \text{ and } t_3 \equiv t_4(mod\ p_1^{\alpha_1}p_3^{\alpha_3}).$$

Then

$$t_1 \equiv t_2 \equiv t_3 \equiv t_4(mod\ p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}).$$

Lemma 5.3. *The expression*

$$\frac{\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}}-1\right)\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}}-1\right)}{\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}}-1\right)\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}}-1\right)},$$

where all the above polynomials are separable over F_q, is a polynomial over F_q.

Proof. We know that if the polynomials $x^{ab}-1$, x^a-1 and x^b-1 are separable over F_q, then $\frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)}$ is a polynomial over F_q. Therefore, if we choose $x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}}=y$, then

$$\frac{\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}}-1\right)\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}}-1\right)}{\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}}-1\right)\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}}-1\right)}=\frac{\left(y^{p_2p_3}-1\right)\left(y-1\right)}{\left(y^{p_3}-1\right)\left(y^{p_2}-1\right)}.$$

Since all the polynomials are separable over F_q, the result follows from above discussion. □

Theorem 5.4. *Let C be the code of length $p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}$ generated by*

$$g(x)=\frac{p(x)(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}}-1)}{q(x)},$$

where

$$p(x)=\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}}-1\right)\left(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}}-1\right)$$
$$\left(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}}-1\right)$$

and

$$q(x)=\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}}-1\right)\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}}-1\right)$$
$$\left(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}}-1\right).$$

Then, the minimum distance of C is 8.

Proof. As

$$p(x)=g(x)\frac{q(x)}{\left(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}}-1\right)},$$

therefore, $p(x)$ is a codeword in C. The weight of $p(x)$ is 8, therefore, C has a codeword of weight 8. We will now show that C does not has a nonzero codeword of weight less than 8. By Lemma 5.3, $x^{p_i^{\alpha_i-\beta_i}p_j^{\alpha_j-\beta_j}}-1; 1\leq i<j\leq 3$ divides $g(x)$, therefore, $x^{p_i^{\alpha_i-\beta_i}p_j^{\alpha_j-\beta_j}}-1$ divides $c(x)$ also. We now show that C has no codeword of weight 2, 3, 4, 5, 6 and 7.

Case (1): C has no codeword of weight 2.

Let $c(x)=a_1x^{t_1}+a_2x^{t_2}$ be a codeword in C. As $x^{p_i^{\alpha_i-\beta_i}p_j^{\alpha_j-\beta_j}}-1; 1\leq i<j\leq 3$ divides $c(x)$, therefore, by Lemma 5.1,

$$t_1\equiv t_2(\text{mod } p_i^{\alpha_i-\beta_i}p_j^{\alpha_j-\beta_j}) \text{ and } a_1+a_2=0.$$

By Lemma 5.2),

$$t_1\equiv t_2(\text{mod } p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}) \text{ and } a_1+a_2=0.$$

Then, by Lemma 5.1, $x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}}-1$ divides $c(x)$. Therefore, $c(x)$ is a zero codeword. Hence C has no codeword of weight 2.

Case (2): C has no codeword of weight 3.
Let $c(x)=a_1x^{t_1}+a_2x^{t_2}+a_3x^{t_3}$. The $x^{p_i^{\alpha_i-\beta_i}p_j^{\alpha_j-\beta_j}}-1; 1\le i<j\le 3$ divides $c(x)$. By Lemma 5.1, it is possible only when

$$t_1\equiv t_2\equiv t_3 (\mathrm{mod}\ p_i^{\alpha_i-\beta_i}p_j^{\alpha_j-\beta_j}) \text{ and } a_1+a_2+a_3=0.$$

Lemma 5.2,

$$t_1\equiv t_2\equiv t_3 (\mathrm{mod}\ p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}) \text{ and } \ a_1+a_2+a_3=0.$$

Then, by Lemma 5.1, $x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}}-1$ divides $c(x)$. Therefore, $c(x)$ is a zero codeword. Hence C has no codeword of weight 3.

Case (3): C has no codeword of weight 4.
Let $c(x)=a_1x^{t_1}+a_2x^{t_2}+a_3x^{t_3}+a_4x^{t_4}$. Then, proceeding on similar steps as discussed in Case (1) and in Case (2), we get that either

$$t_{i_1}\equiv t_{i_2} (\mathrm{mod}\ p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}), a_{i_1}+a_{i_2}=0 \text{ and}$$

$$t_{i_3}\equiv t_{i_4} (\mathrm{mod}\ p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}), a_{i_3}+a_{i_4}=0,$$

$$\text{or} \qquad t_{i_1}\equiv t_{i_2}\equiv t_{i_3}\equiv t_{i_4} (\mathrm{mod}\ p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}) \text{ and}$$

$$a_{i_1}+a_{i_2}+a_{i_3}+a_{i_4}=0, \text{ where } \{1,2,3,4\}=\{i_1,i_2,i_3,i_4\}.$$

Then, by Lemma 5.1, $x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}}-1$ divides $c(x)$. Therefore, $c(x)$ is a zero codeword. Hence C has no codeword of weight 4.

Case (4): C has no codeword of weight 5.
Let $c(x)=a_1x^{t_1}+a_2x^{t_2}+a_3x^{t_3}+a_4x^{t^4}+a_5x^{t^5}$. Then we get following congruence relations:

$$t_{i_1}\equiv t_{i_2} (\mathrm{mod}\ p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}), a_{i_1}+a_{i_2}=0 \text{ and}$$

$$t_{i_3}\equiv t_{i_4}\equiv t_{i_5} (\mathrm{mod}\ p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}), a_{i_3}+a_{i_4}+a_{i_5}=0,$$

or

$$t_{i_1}\equiv t_{i_2}\equiv t_{i_3}\equiv t_{i_4}\equiv t_{i_5} (\mathrm{mod}\ p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}) \text{ and}$$

$$a_{i_1}+a_{i_2}+a_{i_3}+a_{i_4}+a_{i_5}=0, \text{ where } \{1,2,3,4,5\}=\{i_1,i_2,i_3,i_4,i_5\}.$$

Again, by Lemma 5.1 $x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}}-1$ divides $c(x)$. Therefore, $c(x)$ is a zero codeword. Hence C has no codeword of weight 5.

Case (5): C has no codeword of weight 6.

Let $c(x)=a_1x^{t_1}+a_2x^{t_2}+a_3x^{t_3}+a_4x^{t_4}+a_5x^{t_5}+a_6x^{t_6}$. Then we obtain the following congruence relations:

$$t_{i_1}\equiv t_{i_2} (\mathrm{mod}\ p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}), a_{i_1}+a_{i_2}=0 \ \text{ and}$$

$$t_{i_3} \equiv t_{i_4} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_3} + a_{i_4} = 0 \quad \text{and}$$

$$t_{i_5} \equiv t_{i_6} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_5} + a_{i_6} = 0$$

$$\text{or} \quad t_{i_1} \equiv t_{i_2} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_1} + a_{i_2} = 0 \quad \text{and}$$

$$t_{i_3} \equiv t_{i_4} \equiv t_{i_5} \equiv t_{i_6} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_3} + a_{i_4} + a_{i_5} + a_{i_6} = 0,$$

$$\text{or} \quad t_{i_1} \equiv t_{i_2} \equiv t_{i_3} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}),\ a_{i_1} + a_{i_2} + a_{i_3} = 0 \text{ and}$$

$$t_{i_4} \equiv t_{i_5} \equiv t_{i_6} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_4} + a_{i_5} + a_{i_6} = 0,$$

$$\text{or} \quad t_{i_1} \equiv t_{i_2} \equiv t_{i_3} \equiv t_{i_4} \equiv t_{i_5} \equiv t_{i_6} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}) \quad \text{and}$$

$$a_{i_1} + a_{i_2} + a_{i_3} + a_{i_4} + a_{i_5} + a_{i_6} = 0,$$

where $\{1,2,3,4,5,6\} = \{i_1, i_2, i_3, i_4, i_5, i_6\}$. Again, by Lemma 5.1, $x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}} - 1$ divides $c(x)$. Therefore, $c(x)$ is a zero codeword. Hence C has no codeword of weight 6.

Case (6): C has no codeword of weight 7.

$$\text{Let} \quad c(x) = a_1 x^{t_1} + a_2 x^{t_2} + a_3 x^{t_3} + a_4 x^{t_4} + a_5 x^{t_5} + a_6 x^{t_6} + a_7 x^{t_7}.$$

Then we obtain the following congruence relations:

$$t_{i_1} \equiv t_{i_2} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_1} + a_{i_2} = 0$$

and

$$t_{i_3} \equiv t_{i_4} \equiv t_{i_5} \equiv t_{i_6} \equiv t_{i_7} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}),$$

$$a_{i_3} + a_{i_4} + a_{i_5} + a_{i_6} + a_{i_7} = 0,$$

or

$$t_{i_1} \equiv t_{i_2} \equiv t_{i_3} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_1} + a_{i_2} + a_{i_3} = 0 \text{ and}$$

$$t_{i_4} \equiv t_{i_5} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_4} + a_{i_5} = 0 \text{ and}$$

$$t_{i_6} \equiv t_{i_7} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_6} + a_{i_7} = 0$$

or

$$t_{i_1} \equiv t_{i_2} \equiv t_{i_3} \equiv t_{i_4} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_1} + a_{i_2} + a_{i_3} + a_{i_4} = 0$$

$$\text{and } t_{i_5} \equiv t_{i_6} \equiv t_{i_7} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}), a_{i_5} + a_{i_6} + a_{i_7} = 0$$

or

$$t_{i_1} \equiv t_{i_2} \equiv t_{i_3} \equiv t_{i_4} \equiv t_{i_5} \equiv t_{i_6} \equiv t_{i_7} (\text{mod } p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3})$$

$$\text{and } a_{i_1} + a_{i_2} + a_{i_3} + a_{i_4} + a_{i_5} + a_{i_6} + a_{i_7} = 0. \text{ by Lemma 5.1}$$

$$x^{p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} p_3^{\alpha_3-\beta_3}} - 1 \text{ divides } \ c(x).$$

Consequently, $c(x)$ is a zero codeword. Hence C has no codeword of weight 7. It completes the proof. □

Corollary 5.5. *Let C^* be the code of length $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$ generated by*

$$g^*(x) = \frac{p(x)\big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}}-1\big)\Big(\sum_{i=0}^{p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}-1} x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}i}\Big)}{q(x)},$$

where $p(x)$ and $q(x)$ are same as defined in Theorem 5.4, then the minimum distance of C^* is $8p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}$.

Proof. Since C^* is a repetition code of C, repeated $p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}$ times, where C is same as defined in Theorem 5.4, the result follows by Theorem 5.4. □

Similarly, we have the following easy results.

Corollary 5.6. *Let C^* be the code of length $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$ generated by*

$$\frac{\big(x^{p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3-1}}-1\big)\big(x^{p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3}}-1\big)\Big(\sum_{i=0}^{p_1^{\alpha_1}p_2^{\beta_2}p_3^{\beta_3}-1} x^{p_2^{\alpha_2-\beta_2}p_3^{\alpha_3-\beta_3}i}\Big)}{\big(x^{p_2^{\alpha_2-\beta_2-1}p_3^{\alpha_3-\beta_3-1}}-1\big)}$$

or generated by

$$\frac{\big(x^{p_1^{\alpha_1-\beta_1}p_3^{\alpha_3-\beta_3-1}}-1\big)\big(x^{p_1^{\alpha_1-\beta_1-1}p_3^{\alpha_3-\beta_3}}-1\big)\Big(\sum_{i=0}^{p_1^{\beta_1}p_2^{\alpha_2}p_3^{\beta_3}-1} x^{p_1^{\alpha_1-\beta_1}p_3^{\alpha_3-\beta_3}i}\Big)}{\big(x^{p_1^{\alpha_1-\beta_1-1}p_3^{\alpha_3-\beta_3-1}}-1\big)},$$

or generated by

$$\frac{\big(x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2-1}}-1\big)\big(x^{p_1^{\alpha_1-\beta_1-1}p_1^{\alpha_1-\beta_1}}-1\big)\Big(\sum_{i=0}^{p_1^{\beta_1}p_2^{\beta_2}p_3^{\alpha_3}-1} x^{p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}i}\Big)}{\big(x^{p_1^{\alpha_1-\beta_1-1}p_2^{\alpha_2-\beta_2-1}}-1\big)}.$$

Then the minimum distance of C^* is

$$4p_1^{\alpha_1}p_2^{\beta_2}p_3^{\beta_3} \quad or \quad 4p_1^{\beta_1}p_2^{\alpha_2}p_3^{\beta_3} \quad or \quad 4p_1^{\beta_1}p_2^{\beta_2}p_3^{\alpha_3}.$$

Corollary 5.7. *Let C^* be the code of length $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$ generated by*

$$\big(x^{p_3^{\alpha_3-\beta_3-1}}-1\big)\Big(\sum_{i=0}^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\beta_3}-1} x^{p_3^{\alpha_3-\beta_3}i}\Big)$$

or generated by

$$\big(x^{p_2^{\alpha_2-\beta_2-1}}-1\big)\Big(\sum_{i=0}^{p_1^{\alpha_1}p_2^{\beta_2}p_3^{\alpha_3}-1} x^{p_2^{\alpha_2-\beta_2}i}\Big),$$

or generated by

$$\big(x^{p_1^{\alpha_1-\beta_1-1}}-1\big)\Big(\sum_{i=0}^{p_1^{\beta_1}p_2^{\alpha_2}p_3^{\alpha_3}-1} x^{p_1^{\alpha_1-\beta_1}i}\Big).$$

Then, the minimum distance of C^* is

$$2p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\beta_3} \quad or \quad 2p_1^{\alpha_1}p_2^{\beta_2}p_3^{\alpha_3}, \quad or \quad 2p_1^{\beta_1}p_2^{\alpha_2}p_3^{\alpha_3}.$$

By Theorem 4.11, Theorem 4.12, Theorem 4.13, Theorem 4.14, Theorem 4.15, Theorem 4.16, Theorem 4.17 and Theorem 4.18 the codes M_s^m are sub-codes of the codes C^* defined in Corollary 5.5, Corollary 5.6 and Corollary 5.7 therefore, we have the following results

$$\begin{array}{ll}
\textbf{Minimal cyclic code} :: & \textbf{Minimum distance } d \\
M_s^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}; \quad \gcd(s,m) = p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3} :: & d \geq 8p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3} \\
M_s^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}; \quad \gcd(s,m) = p_1^{\alpha_1}p_2^{\beta_2}p_3^{\beta_3} :: & d \geq 4p_1^{\alpha_1}p_2^{\beta_2}p_3^{\beta_3} \\
M_s^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}; \quad \gcd(s,m) = p_1^{\beta_1}p_2^{\alpha_2}p_3^{\beta_3} :: & d \geq 4p_1^{\beta_1}p_2^{\alpha_2}p_3^{\beta_3} \\
M_s^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}; \quad \gcd(s,m) = p_1^{\beta_1}p_2^{\beta_2}p_3^{\alpha_3} :: & d \geq 4p_1^{\beta_1}p_2^{\beta_2}p_3^{\alpha_3} \\
M_s^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}; \quad \gcd(s,m) = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\beta_3} :: & d \geq 2p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\beta_3} \\
M_s^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}; \quad \gcd(s,m) = p_1^{\alpha_1}p_2^{\beta_2}p_3^{\alpha_3} :: & d \geq 2p_1^{\alpha_1}p_2^{\beta_2}p_3^{\alpha_3} \\
M_s^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}; \quad \gcd(s,m) = p_1^{\beta_1}p_2^{\alpha_2}p_3^{\alpha_3} :: & d \geq 2p_1^{\beta_1}p_2^{\alpha_2}p_3^{\alpha_3} \\
M_s^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}; \quad \gcd(s,m) = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3} :: & d = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}
\end{array}$$

Remark 5.1

(i) One can observe that the results obtained in this paper are sufficient to discuss all the parameters of all the minimal cyclic codes of length $m = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$.

(ii) One can easily observe that the minimum distance of the cyclic codes of length $m = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ is at least 2^k.

6. Examples

Example 6.1. *In this example we choose $\alpha_1 = \alpha_2 = \alpha_3 = 1$, $q = 3, p_1 = 5, p_2 = 11$ and $p_3 = 13$. First we count the number of 3-cyclotomic cosets modulo 715.*

As $O_5(3) = 4$, $O_{11}(3) = 5$ and $O_{13}(3) = 3$, therefore, $r_1 = 1, r_2 = 2, r_3 = 4$, $d = 60$, $d_1 = 15$, $d_2 = 12$, $d_3 = 20$. Then $v_1 = v_2 = v_3 = 1$ and $t = 1$. Hence by Corollary 2.6, the number of 3-cyclotomic cosets modulo 715 is

$$\frac{(1.1.1+1)(2.1.1+1)(4.1.1+1)+(1-1)}{1} = 30.$$

Since $\lambda(2, 10, 9) = 1$, therefore, by Corollary 2.4, the distinct 3-cyclotomic cosets modulo 715 are as:

$$C_1^{715(3)} = \lambda(C_1^{5(3)} \times C_2^{11(3)} \times C_1^{13(3)}), C_{383}^{715(3)} = \lambda(C_1^{5(3)} \times C_2^{11(3)} \times C_2^{13(3)}),$$

$$C_{493}^{715(3)} = \lambda(C_1^{5(3)} \times C_2^{11(3)} \times C_4^{13(3)}), C_{713}^{715(3)} = \lambda(C_1^{5(3)} \times C_2^{11(3)} \times C_8^{13(3)}),$$

$$C_{263}^{715(3)} = \lambda(C_1^{5(3)} \times C_1^{11(3)} \times C_1^{13(3)}), C_{318}^{715(3)} = \lambda(C_1^{5(3)} \times C_1^{11(3)} \times C_2^{13(3)}),$$

$$C_{428}^{715(3)} = \lambda(C_1^{5(3)} \times C_1^{11(3)} \times C_4^{13(3)}), C_{648}^{715(3)} = \lambda(C_1^{5(3)} \times C_1^{11(3)} \times C_8^{13(3)}),$$

$$C_{120}^{715(3)} = \lambda(C_0^{5(3)} \times C_1^{11(3)} \times C_1^{13(3)}), C_{175}^{715(3)} = \lambda(C_0^{5(3)} \times C_1^{11(3)} \times C_2^{13(3)}),$$

$$C_{285}^{715(3)} = \lambda(C_0^{5(3)} \times C_1^{11(3)} \times C_4^{13(3)}), C_{505}^{715(3)} = \lambda(C_0^{5(3)} \times C_1^{11(3)} \times C_8^{13(3)}),$$

$$C_{185}^{715(3)} = \lambda(C_0^{5(3)} \times C_2^{11(3)} \times C_1^{13(3)}), C_{240}^{715(3)} = \lambda(C_0^{5(3)} \times C_2^{11(3)} \times C_2^{13(3)}),$$

$$C_{350}^{715(3)} = \lambda(C_0^{5(3)} \times C_2^{11(3)} \times C_4^{13(3)}), C_{570}^{715(3)} = \lambda(C_0^{5(3)} \times C_2^{11(3)} \times C_8^{13(3)}),$$

$$C_{198}^{715(3)} = \lambda(C_1^{5(3)} \times C_0^{11(3)} \times C_1^{13(3)}), C_{253}^{715(3)} = \lambda(C_1^{5(3)} \times C_0^{11(3)} \times C_2^{13(3)}),$$

$$C_{363}^{715(3)} = \lambda(C_1^{5(3)} \times C_0^{11(3)} \times C_4^{13(3)}), C_{583}^{715(3)} = \lambda(C_1^{5(3)} \times C_0^{11(3)} \times C_8^{13(3)}),$$

$$C_{208}^{715(3)} = \lambda(C_1^{5(3)} \times C_1^{11(3)} \times C_0^{13(3)}), C_{273}^{715(3)} = \lambda(C_1^{5(3)} \times C_2^{11(3)} \times C_0^{13(3)}),$$

$$C_{55}^{715(3)} = \lambda(C_0^{5(3)} \times C_0^{11(3)} \times C_1^{13(3)}), C_{110}^{715(3)} = \lambda(C_0^{5(3)} \times C_0^{11(3)} \times C_2^{13(3)}),$$

$$C_{220}^{715(3)} = \lambda(C_0^{5(3)} \times C_0^{11(3)} \times C_4^{13(3)}), C_{440}^{715(3)} = \lambda(C_0^{5(3)} \times C_0^{11(3)} \times C_8^{13(3)}),$$

$$C_{65}^{715(3)} = \lambda(C_0^{5(3)} \times C_1^{11(3)} \times C_0^{13(3)}), C_{130}^{715(3)} = \lambda(C_0^{5(3)} \times C_2^{11(3)} \times C_0^{13(3)}),$$

$$C_{143}^{715(3)} = \lambda(C_1^{5(3)} \times C_0^{11(3)} \times C_0^{13(3)}), C_{0}^{715(3)} = \lambda(C_0^{5(3)} \times C_0^{11(3)} \times C_0^{13(3)}),$$

where

$$\begin{aligned}
&C_0^{5(3)} = \{0\}, C_1^{5(3)} = \{1,2,3,4\}, C_0^{11(3)} = \{0\}, C_1^{11(3)} = \{1,3,4,5,9\},\\
&C_2^{11(3)} = \{2,6,7,8,10\}, C_0^{13(3)} = \{0\}, C_1^{13(3)} = \{1,3,9\},\\
&C_2^{13(3)} = \{2,6,5\}, C_4^{13(3)} = \{4,12,10\} \text{ and } C_8^{13(3)} = \{8,11,7\}.
\end{aligned}$$

We now compute the explicit expression of primitive idempotent $\theta_1^{715}(x)$ *in* $R_{715} = F_3[x]/(x^{715}-1)$.

First we use λ*- product of polynomials to compute* $\theta_1^{715}(x)$. *The*

$$C_1^{715(3)} = \lambda\Big(C_1^{5(3)} \times C_2^{11(3)} \times C_1^{13(3)}\Big)$$

therefore, by Theorem 3.5,

$$\theta_1^{715}(x) = \lambda\Big(\theta_1^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_1^{13(3)}(x_3)\Big).$$

As the expression of $\theta_1^{5(3)}(x_1)$ *in* $R_5 = F_3[x_1]/(x_1^5-1)$ *is*

$$\theta_1^{5(3)}(x_1) = 2\sigma_0(x_1) + \sigma_1(x_1),$$

where $\sigma_s(x_1) = \sum_{s \in C_s^{5(3)}} x_1^s$,

the expression of $\theta_1^{11(3)}(x_2)$ *in* $R_{11} = F_3[x_2]/(x_2^{11} - 1)$ *is*

$$\theta_1^{11(3)}(x_2) = \sigma_0(x_2) + \sigma_1(x_2),$$

where $\sigma_s(x_2) = \sum_{s \in C_s^{11(3)}} x_2^s$,

and, the expression of $\theta_1^{13(3)}(x_3)$ *in* $R_{13} = F_3[x_3]/(x_3^{13} - 1)$ *is*

$$\theta_1^{13(3)}(x_3) = 2\sigma_2(x_3) + 2\sigma_4(x_3) + \sigma_8(x_3),$$

where $\sigma_s(x_3) = \sum_{s \in C_s^{13(3)}} x_3^s$,

therefore, by Definition 3.1, the

$$\lambda\Big(\theta_1^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_1^{13(3)}(x_3)\Big)$$

$$\lambda\Big(\big(2\sigma_0(x_1) + \sigma_1(x_1)\big)\big(\sigma_0(x_2) + \sigma_1(x_2)\big)\big(2\sigma_2(x_3) + 2\sigma_4(x_3) + \sigma_8(x_3)\big)\Big)$$

$$= \sigma_{\lambda(0,0,2)}(x) + \sigma_{\lambda(0,0,4)}(x) + 2\sigma_{\lambda(0,0,8)}(x) + \sigma_{\lambda(0,1,2)}(x) + \sigma_{\lambda(0,1,4)}(x) + 2\sigma_{\lambda(0,1,8)}(x) + 2\sigma_{\lambda(1,0,2)}(x) + 2\sigma_{\lambda(1,0,4)}(x) + \sigma_{\lambda(1,0,8)}(x) + 2\sigma_{\lambda(1,1,2)}(x) + 2\sigma_{\lambda(1,1,4)}(x) + \sigma_{\lambda(1,1,8)}(x).$$

Hence

$$\theta_1^{715(3)}(x) = \sigma_{110}(x) + \sigma_{220}(x) + 2\sigma_{440}(x) + \sigma_{175}(x) + \sigma_{285}(x) + 2\sigma_{505}(x) + 2\sigma_{253}(x) + 2\sigma_{363}(x) + \sigma_{583}(x) + 2\sigma_{318}(x) + 2\sigma_{428}(x) + \sigma_{648}(x).$$

We now compute the $\theta_1^{715(3)}(x)$ *by Trace function of the product of explicit expressions of*

$$\Big(\theta_1^{5(3)}(x^{143})\theta_1^{11(3)}(x^{65})\theta_1^{13(3)}(x^{55})\Big).$$

As $\theta_1^{5(3)}(x) = 2 + x + x^2 + x^3 + x^4$, *therefore,*

$$\theta_1^{5(3)}(x^{143}) = 2 + x^{143} + x^{283} + x^{429} + x^{572}.$$

Similarly, $\theta_1^{11(3)}(x) = 1 + x + x^3 + x^4 + x^5 + x^9$, *therefore,*

$$\theta_1^{11(3)}(x^{65}) = 1 + x^{65} + x^{195} + x^{260} + x^{325} + x^{585}$$

and

$\theta_1^{13(3)}(x) = 2x^2 + 2x^6 + 2x^5 + 2x^4 + 2x^{10} + 2x^{12} + x^8 + x^{11} + x^7$
implies that

$$\theta_1^{13(3)}(x^{55}) = 2x^{110} + 2x^{330} + 2x^{275} + 2x^{220} + 2x^{550} + 2x^{660} + x^{440} + x^{605} + x^{385}.$$

On writing the the product

$$\Big(\theta_1^{5(3)}(x^{143})\theta_1^{11(3)}(x^{65})\theta_1^{13(3)}(x^{55})\Big)$$

in terms of $\sigma_s(x) = \sum_{s\in C_s^{715(3)}} x^s$ *in* R_{715}*, we get*

$$\begin{aligned}&\left(\theta_1^{5(3)}(x^{143})\theta_1^{11(3)}(x^{65})\theta_1^{13(3)}(x^{55})\right)\\&= \sigma_{110}(x) + \sigma_{220}(x) + 2\sigma_{440}(x) + \sigma_{175}(x) + \sigma_{285}(x) + 2\sigma_{505}(x)\\&+2\sigma_{253}(x) + 2\sigma_{363}(x) + \sigma_{583}(x) + 2\sigma_{318}(x) + 2\sigma_{428}(x) + \sigma_{648}(x).\end{aligned}$$

As $t = 1$*, therefore, by Theorem 3.6,*

$$\begin{aligned}&\theta_1^{715}(x) = Tr_{F_3|F_3}\left(\theta_1^{5(3)}(x^{143})\theta_1^{11(3)}(x^{65})\theta_1^{13(3)}(x^{55})\right)\\&= \sigma_{110}(x) + \sigma_{220}(x) + 2\sigma_{440}(x) + \sigma_{175}(x) + \sigma_{285}(x) + 2\sigma_{505}(x) +\\&2\sigma_{253}(x) + 2\sigma_{363}(x) + \sigma_{583}(x) + 2\sigma_{318}(x) + 2\sigma_{428}(x) + \sigma_{648}(x).\end{aligned}$$

Example 6.2. *In this example we obtain 7-cyclotomic cosets modulo 30, all the explicit expressions of primitive idempotents in* $R_{30} = F_7[x]/(x^{30} - 1)$*, minimal polynomials, generating polynomials and minimum distances of all the minimal cyclic codes of length 30 over* F_7*.*
Here 7 is primitive root modulo 2, quadratic residue modulo 3 and primitive root modulo 5. Therefore,

$$O_2(7) = 1, O_3(7) = 1 \quad \text{and} \quad O_5(7) = 4.$$

Thus

$$d = 4, d_1 = 4, d_2 = 4, d_3 = 1,$$

$$v_1 = 1, v_2 = 1, v_3 = 1,$$

$t = 1$ *and* $\lambda(1, 1, 1) = 1$*. Hence*

$$\lambda(C_1^{2(7)} \times C_1^{3(7)} \times C_1^{5(7)}) = C_1^{30(7)}, \lambda(C_1^{2(7)} \times C_2^{3(7)} \times C_1^{5(7)}) = C_{11}^{30(7)},$$

$$\lambda(C_0^{2(7)} \times C_0^{3(7)} \times C_1^{5(7)}) = C_6^{30(7)}, \lambda(C_0^{2(7)} \times C_1^{3(7)} \times C_0^{5(7)}) = C_{10}^{30(7)},$$

$$\lambda(C_0^{2(7)} \times C_1^{3(7)} \times C_1^{5(7)}) = C_4^{30(7)}, \lambda(C_0^{2(7)} \times C_2^{3(7)} \times C_0^{5(7)}) = C_{20}^{30(7)},$$

$$\lambda(C_0^{2(7)} \times C_2^{3(7)} \times C_1^{5(7)}) = C_2^{30(7)}, \lambda(C_1^{2(7)} \times C_0^{3(7)} \times C_0^{5(7)}) = C_{15}^{30(7)},$$

$$\lambda(C_1^{2(7)} \times C_0^{3(7)} \times C_1^{5(7)}) = C_3^{30(7)}, \lambda(C_1^{2(7)} \times C_1^{3(7)} \times C_0^{5(7)}) = C_{25}^{30(7)},$$

$$\lambda(C_1^{2(7)} \times C_2^{3(7)} \times C_0^{5(7)}) = C_5^{30(7)}, \lambda(C_0^{2(7)} \times C_0^{3(7)} \times C_0^{5(7)}) = C_0^{30(7)},$$

where $C_0^{2(7)} = \{0\}, C_1^{2(7)} = \{1\}$*,* $C_0^{3(7)} = \{0\}, C_1^{3(7)} = \{1\}, C_2^{3(7)} = \{2\}$*,* $C_0^{5(7)} = \{0\}$ *and* $C_1^{5(7)} = \{1, 2, 3, 4\}$.

1. *The twelve primitive idempotents are:*

$$\theta_0^{(30)}(x) = \frac{1}{30}[\sigma_0(x) + \sigma_6(x) + \sigma_{10}(x) + \sigma_4(x) + \sigma_{20}(x) + \sigma_2(x)$$

$$+\sigma_{15}(x) + \sigma_3(x) + \sigma_{25}(x) + \sigma_1(x) + \sigma_5(x) + \sigma_{11}(x)],$$

$$\theta_1^{(30)}(x) = \frac{1}{30}[4\sigma_0(x) - \sigma_6(x) + 2\sigma_{10}(x) - 4\sigma_4(x) + \sigma_{20}(x) - 2\sigma_2(x)$$
$$-4\sigma_{15}(x) + \sigma_3(x) - 2\sigma_{25}(x) + 4\sigma_1(x) - \sigma_5(x) + 2\sigma_{11}(x)],$$

$$\theta_{11}^{(30)}(x) = \frac{1}{30}[4\sigma_0(x) - \sigma_6(x) + \sigma_{10}(x) - 2\sigma_4(x) + 2\sigma_{20}(x) - 4\sigma_2(x)$$
$$-4\sigma_{15}(x) + \sigma_3(x) - \sigma_{25}(x) + 2\sigma_1(x) - 2\sigma_5(x) + 4\sigma_{11}(x)],$$

$$\theta_4^{(30)}(x) = \frac{1}{30}[4\sigma_0(x) - \sigma_6(x) + 2\sigma_{10}(x) - 4\sigma_4(x) + \sigma_{20}(x) - 2\sigma_2(x)$$
$$+4\sigma_{15}(x) - \sigma_3(x) + 2\sigma_{25}(x) - 4\sigma_1(x) + \sigma_5(x) - 2\sigma_{11}(x)],$$

$$\theta_2^{(30)}(x) = \frac{1}{30}[4\sigma_0(x) - \sigma_6(x) + \sigma_{10}(x) - 2\sigma_4(x) + 2\sigma_{20}(x) - 4\sigma_2(x)$$
$$+4\sigma_{15}(x) - \sigma_3(x) + \sigma_{25}(x) - 2\sigma_1(x) + 2\sigma_5(x) - 4\sigma_{11}(x)],$$

$$\theta_3^{(30)}(x) = \frac{1}{30}[4\sigma_0(x) - \sigma_6(x) + 4\sigma_{10}(x) - \sigma_4(x) + 4\sigma_{20}(x) - \sigma_2(x)$$
$$-4\sigma_{15}(x) + \sigma_3(x) - 4\sigma_{25}(x) + \sigma_1(x) - 4\sigma_5(x) + \sigma_{11}(x)],$$

$$\theta_{25}^{(30)}(x) = \frac{1}{30}[\sigma_0(x) + \sigma_6(x) + 4\sigma_{10}(x) + 4\sigma_4(x) + 2\sigma_{20}(x) + 2\sigma_2(x)$$
$$-\sigma_{15}(x) - \sigma_3(x) - 4\sigma_{25}(x) - 4\sigma_1(x) - 2\sigma_5(x) - 2\sigma_{11}(x)],$$

$$\theta_5^{(30)}(x) = \frac{1}{30}[\sigma_0(x) + \sigma_6(x) + 2\sigma_{10}(x) + 2\sigma_4(x) + 4\sigma_{20}(x) + 4\sigma_2(x)$$
$$-\sigma_{15}(x) - \sigma_3(x) - 2\sigma_{25}(x) - 2\sigma_1(x) - 4\sigma_5(x) - 4\sigma_{11}(x)],$$

$$\theta_6^{(30)}(x) = \frac{1}{30}[4\sigma_0(x) - \sigma_6(x) + 4\sigma_{10}(x) - \sigma_4(x) + 4\sigma_{20}(x) - \sigma_2(x)$$
$$+4\sigma_{15}(x) - \sigma_3(x) + 4\sigma_{25}(x) - \sigma_1(x) + 4\sigma_5(x) - \sigma_{11}(x)],$$

$$\theta_{10}^{(30)}(x) = \frac{1}{30}[\sigma_0(x) + \sigma_6(x) + 4\sigma_{10}(x) + 4\sigma_4(x) + 2\sigma_{20}(x) + 2\sigma_2(x)$$
$$+\sigma_{15}(x) + \sigma_3(x) + 4\sigma_{25}(x) + 4\sigma_1(x) + 2\sigma_5(x) + 2\sigma_{11}(x)],$$

$$\theta_{20}^{(30)}(x) = \frac{1}{30}[\sigma_0(x) + \sigma_6(x) + 2\sigma_{10}(x) + 2\sigma_4(x) + 4\sigma_{20}(x) + 4\sigma_2(x)$$
$$+\sigma_{15}(x) + \sigma_3(x) + 2\sigma_{25}(x) + 2\sigma_1(x) + 4\sigma_5(x) + 4\sigma_{11}(x)],$$

$$\theta_{15}^{(30)}(x) = \frac{1}{30}[\sigma_0(x) + \sigma_6(x) + \sigma_{10}(x) + \sigma_4(x) + \sigma_{20}(x) + \sigma_2(x)$$
$$-\sigma_{15}(x) - \sigma_3(x) - \sigma_{25}(x) - \sigma_1(x) - \sigma_5(x) - \sigma_{11}(x)].$$

2. *The minimal polynomials of M_s^{30} are:*

$$\eta_0^{30}(x) = (x-1), \eta_1^{30}(x) = (x^4 + 5x^3 + 4x^2 + 6x + 2),$$

$$\eta_{11}^{30}(x) = (x^4 + 3x^3 + 2x^2 + 6x + 4), \eta_2^{30}(x) = (x^4 + 2x^3 + 4x^2 + x + 2),$$

$$\eta_4^{30}(x) = (x^4 + 4x^3 + 2x^2 + x + 4), \eta_3^{30}(x) = (x^4 - x^3 + x^2 - x + 1),$$

$$\eta_6^{30}(x) = (x^4 + x^3 + x^2 + x + 1), \eta_{10}^{30}(x) = (x-2),$$

$$\eta_{20}^{30}(x) = (x-4), \eta_5^{30}(x) = (x-3), \eta_{25}^{30}(x) = (x-5), \eta_{15}^{30}(x) = (x+1).$$

3. *The generating polynomials of M_s^{30} are:*

$$g_0^{30}(x) = \sum_{i=0}^{29} x^i,$$

$$g_{15}^{30}(x) = \sum_{i=0}^{29} (-1)^i x^i,$$

$$g_5^{30}(x) = (x^{24} + x^{18} + 2x^{12} + 6x^6 + 1)(x^5 + 3x^4 + 2x^3 + 6x^2 + 4x + 5),$$

$$g_{25}^{30}(x) = (x^{24} + x^{18} + x^{12} + x^6 + 1)(x^5 + 5x^4 + 4x^3 + 6x^2 + 2x + 3),$$

$$g_{10}^{30}(x) = (x^{27} + x^{24} + 2x^{21} + x^{18} + x^{15} + x^{12} + 2x^9 + x^6 + x^3 + 1)(x^2 + 2x + 4),$$

$$g_{20}^{30}(x) = (x^{27} + x^{24} + 2x^{21} + x^{18} + x^{15} + x^{12} + 2x^9 + x^6 + x^3 + 1)(x^2 + 4x + 2),$$

$$g_1^{30}(x) = (x^{25} - 4x^{20} + 2x^{15} - x^{10} + 4x^5 - 2)(x+2),$$

$$g_{11}^{30}(x) = (x^{25} - 2x^{20} + 4x^{15} - x^{10} + 2x^5 - 4)(x+4),$$

$$g_2^{30}(x) = (x^{25} + 4x^{20} + 2x^{15} + x^{10} + 4x^5 + 2)(x-2),$$

$$g_4^{30}(x) = (x^{25} + 2x^{20} + 4x^{15} + x^{10} + 2x^5 + 4)(x-4),$$

$$g_3^{30}(x) = (x^{25} - x^{20} + x^{15} - x^{10} + x^5 - 1)(x+1),$$

$$g_6^{30}(x) = (x^{25} + x^{20} + x^{15} + x^{10} + x^5 + 1)(x-1).$$

4. *The dimension and the minimum distance of M_s^{30} are:*

Code	M_0^{30}	M_1^{30}	M_{11}^{30}	M_2^{30}	M_4^{30}	M_3^{30}
Dimension	1	4	4	4	4	4
Minimum Distance	30	12	12	12	12	12

Code	M_6^{30}	M_5^{30}	M_{25}^{30}	M_{10}^{30}	M_{20}^{30}	M_{15}^{30}
Dimension	4	1	1	1	1	1
Minimum Distance	12	30	30	30	30	30

References

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

[2] G. K. Bakshi, S. Gupta, I. B. S. Passi, The algebraic structure of finite Metabelian group algebras, Communications in Algebra 43(6) (2015) 2240–2257.

[3] G. K. Bakshi, M. Raka, Minimal cyclic codes of length p^nq, Finite Fields and Their Applications 9(4) (2003) 432–448.

[4] G. K. Bakshi, M. Raka, A. Sharma, Idempotent generators of irreducible cyclic codes, In Number Theory & Discrete Geometry 6 (2008) 13–18.

[5] S. Batra, S. K. Arora, Some cyclic codes of length $2p^n$, Designs Codes Cryptography 61 (2011) 41–69.

[6] O. Broche, A. Del Río, Wedderburn decomposition of finite group algebras, Finite Fields and Their Applications 13(1) (2007) 71–79.

[7] B. Chen, H. Liu, G. Zhang, A class of minimal cyclic codes over finite fields, Designs Codes Cryptography 74 (2013) 285–300.

[8] R. A. Ferraz, P. M. César, Idempotents in group algebras and minimal abelian codes, Finite Fields and Their Applications 13(2) (2007) 382–393.

[9] S. Gupta, Finite Metabelian group algebras, International Journal of Pure Mathematical Sciences 17 (2016) 30–38.

[10] P. Kumar, S. K. Arora, λ-Mapping and primitive idempotents in semisimple ring $\Re_m$, Communications in Algebra 41(10) (2013) 3679–3694.

[11] P. Kumar, S. K. Arora, S. Batra, Primitive idempotents and generator polynomials of some minimal cyclic codes of length p^nq^m, International Journal of Information and Coding Theory 4 (2014) 191–217.

[12] F. J. MacWilliam, N. J. A. Sloane, The theory of error-correcting codes, edition = 1st, Elsevier, Amsterdam (2013).

[13] M. Pruthi, S. K. Arora, Minimal codes of prime-power length, Finite Fields and Their Applications 3(2) (1977) 99–113.

[14] A. Sahni, P. T. Sehgal, Minimal cyclic codes of length p^nq, Finite Fields and Their Applications 18(5) (2012) 1017–1036.

[15] A. Sharma, G. K. Bakshi, V. C. Dumir, M. Raka, Cyclotomic numbers and primitive idempotents in the ring $GF(q)[x]/(x^{p^n} - 1)$, Finite Fields and Their Applications 10(4) (2004) 653–673.

Appendix 1

The explicit expressions of 30 primitive idempotents in R_{715} are as follows:

Since

$$C_1^{715(3)} = \left(C_1^{5(3)} \times C_2^{11(3)} \times C_1^{13(3)}\right),$$

by Theorem 3.5

$$\theta_1^{715(3)}(x) = \lambda\left(\theta_1^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_1^{13(3)}(x_3)\right).$$

Hence

$$\theta_1^{715(3)}(x) = \sigma_{110}(x) + \sigma_{220}(x) + 2\sigma_{440}(x) + \sigma_{175}(x) + \sigma_{285}(x) + 2\sigma_{505}(x)$$

$$+2\sigma_{253}(x) + 2\sigma_{363}(x) + \sigma_{583}(x) + 2\sigma_{318}(x) + 2\sigma_{428}(x) + \sigma_{648}(x);$$

If we denote $a\sigma_s(x)$ by a(s), then under the above notation,
$\theta_1^{715(3)}(x)$= (110)+ (220)+ 2(440)+(175)+(285)+ 2(505)+ 2(253)+ 2(363)+ (583)+ 2(318) +2(428) +(648).

Since

$$C_1^{715(3)} = \left(C_1^{5(3)} \times C_2^{11(3)} \times C_1^{13(3)}\right) \text{ and } C_{383}^{715(3)} = \left(C_1^{5(3)} \times C_2^{11(3)} \times C_2^{13(3)}\right),$$

by Theorem 3.6,

$$\theta_{383}^{715(3)}(x) = \lambda\left(\theta_1^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_2^{13(3)}(x_3)\right) =$$
$$(55) + (110) + 2(220) + (120) + (175) + 2(285) + 2(198) + 2(253)$$
$$+(363) + 2(263) + 2(318) + (428).$$

Similarly, $\theta_{493}^{715(3)}(x) = \lambda\left(\theta_1^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_4^{13(3)}(x_3)\right)$= (55) + 2(110) + (440) + (120) + 2(175) + (505) + 2(198) + (253) + 2(583) + 2(263) + (318) + 2(648),

$\theta_{713}^{715(3)}(x) = \lambda\left(\theta_1^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_8^{13(3)}(x_3)\right)$ = 2(55) + (220) + (440) + 2(120) + (285) + (505) + (198) + 2(363) + 2(583) + (263) + 2(428) + 2(648),

$\theta_{263}^{715(3)}(x) = \lambda\left(\theta_1^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_1^{13(3)}(x_3)\right)$ = (110) + (220) + 2(440) + (240) + (350) + 2(570) + 2(253) + 2(363) + (583) + 2(383) + 2(493) + (713),

$\theta_{318}^{715(3)}(x) = \lambda\left(\theta_1^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_2^{13(3)}(x_3)\right)$ = (55) + (110) + 2(220) + (185) + (240) + 2(350) + 2(198) + 2(253) + (363) + 2(1) + 2(383) + (493),

$\theta_{428}^{715(3)}(x) = \lambda\left(\theta_1^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_4^{13(3)}(x_3)\right)$ = (55) + 2(110) + (440) + (185) + 2(240) + (570) + 2(198) + (253) + 2(583) + 2(1) + (383) + 2(713),

$\theta_{648}^{715(3)}(x) = \lambda\left(\theta_1^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_8^{13(3)}(x_3)\right)$ = 2(55) + (220) + (440) + 2(185) + (350) + (570) + (198) + 2(363) + 2(583) + (1) + 2(493) + 2(713),

$\theta_{120}^{715(3)}(x) = \lambda\left(\theta_0^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_1^{13(3)}(x_3)\right)$ = (110) + (220) + 2(440) + (240) + (350) + 2(570) +

$(253) + (363) + 2(583) + (383) + (493) + 2(713)$,

$\theta_{175}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_2^{13(3)}(x_3)\Big) = (55) + (110) + 2(220) + (185) + (240) + 2(350) + (198) + (253) + 2(363) + (1) + (383) + 2(493)$,

$\theta_{285}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_4^{13(3)}(x_3)\Big) = (55) + 2(110) + (440) + (185) + 2(240) + (570) + (198) + 2(253) + (583) + (1) + 2(383) + (713)$,

$\theta_{505}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_8^{13(3)}(x_3)\Big) = 2(55) + (220) + (440) + 2(185) + (350) + (570) + 2(198) + (363) + (583) + 2(1) + (493) + (713)$,

$\theta_{185}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_1^{13(3)}(x_3)\Big) = (110) + (220) + 2(440) + (175) + (285) + 2(505) + (253) + (363) + 2(583) + (318) + (428) + 2(648)$,

$\theta_{240}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_2^{13(3)}(x_3)\Big) = (55) + (110) + 2(220) + (120) + (175) + 2(285) + (198) + (253) + 2(363) + (263) + (318) + 2(428)$,

$\theta_{350}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_4^{13(3)}(x_3)\Big) = (55) + 2(110) + (440) + (120) + 2(175) + (505) + (198) + 2(253) + (583) + (263) + 2(318) + (648)$,

$\theta_{570}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_8^{13(3)}(x_3)\Big) = 2(55) + (220) + (440) + 2(120) + (285) + (505) + 2(198) + (363) + (583) + 2(263) + (428) + (648)$,

$\theta_{198}^{715(3)}(x) = \lambda\Big(\theta_1^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_1^{13(3)}(x_3)\Big) = 2(110) + 2(220) + (440) + 2(175) + 2(285) + (505) + 2(240) + 2(350) + (570) + (253) + (363) + 2(583) + (318) + (428) + 2(648) + (383) + (493) + 2(713)$,

$\theta_{253}^{715(3)}(x) = \lambda\Big(\theta_1^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_2^{13(3)}(x_3)\Big) = 2(55) + 2(110) + (220) + 2(120) + 2(175) + (285) + 2(185) + 2(240) + (350) + (198) + (253) + 2(363) + (263) + (318) + 2(428) + (1) + (383) + 2(493)$,

$\theta_{363}^{715(3)}(x) = \lambda\Big(\theta_1^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_4^{13(3)}(x_3)\Big) = 2(55) + (110) + 2(440) + 2(120) + (175) + 2(505) + 2(185) + (240) + 2(570) + (198) + 2(253) + (583) + (263) + 2(318) + (648) + (1) + 2(383) + (713)$,

$\theta_{583}^{715(3)}(x) = \lambda\Big(\theta_1^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_8^{13(3)}(x_3)\Big) = (55) + 2(220) + 2(440) + (120) + 2(285) + 2(505) + (185) + 2(350) + 2(570) + 2(198) + (363) + (583) + 2(263) + (428) + (648) + 2(1) + (493) + (713)$,

$\theta_{208}^{715(3)}(x) = \lambda\Big(\theta_1^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_0^{13(3)}(x_3)\Big) = 2(0) + 2(55) + 2(110) + 2(220) + 2(440) + 2(130) + 2(185) + 2(240) + 2(350) + 2(570) + (143) + (198) + (253) + (363) + (583) + (273) + (1) + (383) + (493) + (713)$,

$\theta_{273}^{715(3)}(x) = \lambda\Big(\theta_1^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_0^{13(3)}(x_3)\Big) = 2(0) + 2(55) + 2(110) + 2(220) + 2(440) + 2(65) + 2(120) + 2(175) + 2(285) + 2(505) + (143) + (198) + (253) + (363) + (583) + (208) + (263) + (318) + (428) + (648)$,

$\theta_{55}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_1^{13(3)}(x_3)\Big) = 2(110) + 2(220) + (440) + 2(175) + 2(285) + (505) + 2(240) + 2(350) + (570) + 2(253) + 2(363) + (583) + 2(318) + 2(428) + (648) + 2(383) + 2(493) + (713)$,

$\theta_{110}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_2^{13(3)}(x_3)\Big) = 2(55) + 2(110) + (220) + 2(120) + 2(175) + (285) + 2(185) + 2(240) + (350) + 2(198) + 2(253) + (363) + 2(263) + 2(318) + (428) + 2(1) + 2(383) + (493)$,

$\theta_{220}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_4^{13(3)}(x_3)\Big) = 2(55) + (110) + 2(440) + 2(120) + (175) + 2(505) + 2(185) +$

$(240) + 2(570) + 2(198) + (253) + 2(583) + 2(263) + (318) + 2(648) + 2(1) + (383) + 2(713)$,

$\theta_{440}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_8^{13(3)}(x_3)\Big) = (55) + 2(220) + 2(440) + (120) + 2(285) + 2(505) + (185) + 2(350) + 2(570) + (198) + 2(363) + 2(583) + (263) + 2(428) + 2(648) + (1) + 2(493) + 2(713)$,

$\theta_{65}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_2^{11(3)}(x_2)\theta_0^{13(3)}(x_3)\Big) = 2((0) + (55) + (110) + (220) + (440) + (130) + (185) + (240) + (350) + (570) + (143) + (198) + (253) + (363) + (583) + (273) + (1) + (383) + (493) + (713))$,

$\theta_{130}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_1^{11(3)}(x_2)\theta_0^{13(3)}(x_3)\Big) = 2((0) + (55) + (110) + (220) + (440) + (65) + (120) + (175) + (285) + (505) + (143) + (198) + (253) + (363) + (583) + (208) + (263) + (318) + (428) + (648))$,

$\theta_{143}^{715(3)}(x) = \lambda\Big(\theta_1^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_0^{13(3)}(x_3)\Big) = (0) + (55) + (110) + (220) + (440) + (65) + (120) + (175) + (285) + (505) + (130) + (185) + (240) + (350) + (570) + 2((143) + (198) + (253) + (363) + (583) + (208) + (263) + (318) + (428) + (648) + (273) + (1) + (383) + (493) + (713))$,

$\theta_{0}^{715(3)}(x) = \lambda\Big(\theta_0^{5(3)}(x_1)\theta_0^{11(3)}(x_2)\theta_0^{13(3)}(x_3)\Big) = (0) + (55) + (110) + (220) + (440) + (65) + (120) + (175) + (285) + (505) + (130) + (185) + (240) + (350) + (570) + (143) + (198) + (253) + (363) + (583) + (208) + (263) + (318) + (428) + (648) + (273) + (1) + (383) + (493) + (713)$.