2.1 Introduction

Let F_l be a field of odd prime order l and $k \geq 1$ be an integer such that $\gcd(l, k) = 1$. It is well known that a cyclic code of a given length k over F_l is an ideal in the semisimple ring $R_k = \frac{F_l[x]}{<x^k - 1>}$. Since every ideal in R_k is the direct sum of its minimal ideals, to describe the complete set of ideals (codes over F_l) in R_k, it is sufficient to find its complete set of primitive idempotents. Let t denotes the order of l modulo k. Then $1 \leq t \leq \varphi(k)$. Arora and Pruthi [2, 87] computed a complete set of primitive idempotents of the minimal cyclic codes of length k, when $t = \varphi(k)$ and $k = 2, 4, p^n, 2p^n$, p is odd prime. While computing idempotent generators of minimal cyclic codes over finite field, Ferraz and Millies [45] gave a simple method of computing the results obtained by Arora and Pruthi. The minimal cyclic codes of length k, where $k = p^n$, $2^n, 2p^n$ $(n \geq 1)$, p odd prime and $t = \varphi(k)/2$ have been discussed by Batra *et al*. [6, 7, 8]. Bakshi and Raka [4] computed the minimal cyclic codes of length $p^n q$ $(n \geq 1)$, p and q distinct odd primes, where l is primitive root modulo p^n and q both with $\gcd\big(\varphi(2p^n), \varphi(q)\big) = 2$. Kumar *et.al* [65] computed primitive idempotents in R_k by using λ – mapping. In [66], they described the minimal cyclic codes of length $p^n q^m$, where p , q are distinct odd primes.

Sharma *et al*. [101] obtained the primitive idempotents in R_k, $k = p^n$, p odd prime and $t = \varphi(k)/e$ $(e \geq 1)$. Singh and Pruthi [102] obtained the primitive idempotents of the quadratic residue codes of length $p^n q^m$, where p , q are distinct odd primes. Sahni and Sehgal [95] described the primitive idempotents of minimal cyclic codes of length $p^n q$, where p, q are distinct odd primes, l is primitive root modulo p^n and q both, $\gcd(\varphi(p^n), \varphi(q)) = d$ and p does not divide $q - 1$. As discussed in Chapter 1, minimum distance is an important parameter for a minimal cyclic code. The authors mentioned above have also obtained the minimum distance for the minimal cyclic codes of various lengths. The papers [13], [14], [53], [55], [62], [63], [74] and [93] are also good references on minimum distances.

In this chapter, we consider the case when $k = 2p^n$, where p, l are distinct odd

primes and the multiplicative order of l modulo $2p^n$ is $\frac{\varphi(2p^n)}{d}, d$ is a positive integer. We obtain explicit expressions for all the $2(nd+1)$ primitive idempotents in R_k. The minimum distance, generating polynomial and dimension of the minimal cyclic codes generated by these primitive idempotents are also discussed. In Section 2.2, we obtain the cyclotomic cosets modulo $2p^n$ in Theorem 2.2.3 and some basic results for describing the primitive idempotents in R_k. In Section 2.3 (Theorem 2.3.2), the explicit expression of primitive idempotents are obtained. In Section 2.4 (Theorem 2.4.1 – 2.4.4), we discuss the dimension, generating polynomial and minimum distance of minimal cyclic codes of length $2p^n$. In Section 2.5, we describe the various parameters of minimal cyclic codes of length 22 and 26.

Throughout this chapter $o(l)_{2p^n}$ denotes the multiplicative order of l modulo $2p^n$.

2.2 Cyclotomic Cosets Modulo $2p^n$

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

In this section, we describe the $l-$ cyclotomic cosets modulo $2p^n$, where p and l are distinct odd primes and $o(l)_{2p^n} = \varphi(2p^n)/d, d$ is a positive a integer.

Lemma 2.2.1. Let p and l be distinct odd primes and $n \geq 1$ be an integer. If $o(l)_{2p^n} = \frac{\varphi(2p^n)}{d}, d$ is a positive a integer, then $o(l)_{2p^{n-j}} = \varphi(2p^{n-j})/d$, for all j; $0 \leq j \leq n-1$.

Proof. Let $o(l)_{2p^{n-j}} = \lambda_j$, $0 \leq j \leq n-1$.

Then

$$l^{\lambda_j} \equiv 1 (\text{mod } 2p^{n-j})$$

implies

$$l^{\lambda_j p^j} \equiv 1(mod\ 2p^n).$$

But $o(l)_{2p^n} = \frac{\varphi(2p^n)}{d}$

implies $\frac{\varphi(2p^n)}{d}$ divides $\lambda_j p^j$

or

$$\frac{\varphi(2p^{n-j})}{d} \text{ divides } \lambda_j. \tag{1.1}$$

Again $l^{\frac{\varphi(2p^n)}{d}} \equiv 1(\text{mod } 2p^n)$

$$\left(l^{\frac{\varphi(2p^{n-j})}{d}}\right)^{p^j} \equiv 1(\text{mod } 2p^n)$$

$$l^{\frac{\varphi(2p^{n-j})}{d}} \equiv 1\left(\text{mod } 2p^{n-j}\right).$$

But $o(l)_{2p^{n-j}} = \lambda_j$ implies λ_j divides $\frac{\varphi(2p^{n-j})}{d}$. (1.2)

From equation (1.1) and (1.2) we get

$$\lambda_j = \frac{\varphi(2p^{n-j})}{d}.$$

Lemma 2.2.2. For given p and l there always exists a fixed integer g satisfyin $\gcd(g, 2pl) = 1, o(g)_{2p} = \varphi(p), 1 < g < 2p$ such that $g, g^2, \dots, g^{d-1} \notin \left\{1, l, l^2, \dots, l^{\frac{\varphi(2p)}{d}-1}\right\}$ and for any $j,\ 1 \leq j < n$, and the set

$\{1, l, l^2, \dots, l^{\frac{\varphi(p^{n-j})}{d}-1}, g, gl, gl^2, \dots, gl^{\frac{\varphi(p^{n-j})}{d}-1}, g^{d-1},\ g^{d-1}l,$

$g^{d-1}l^2, \dots, g^{d-1}l^{\frac{\varphi(p^{n-j})}{d}-1}\}$ forms a reduced residue system modulo $2p^{n-j}$.

Proof. We know that reduced residue system (RRS) modulo $2p$ has $\varphi(2p)$ elements. Since gcd $(l, 2p) = 1$, then $\{1, l, l^2, \dots, l^{\frac{\varphi(2p)}{d}-1}\}$ is the subset of RRS modulo $2p$. As $\left\{1, l, l^2, \dots, l^{\frac{\varphi(2p)}{d}-1}\right\}$ contains only d elements of RRS modulo $2p$, therefore, there

always exists an element g such that $g \notin \{1, l, l^2, \dots, l^{\frac{\varphi(2p)}{d}-1}\}$ and is an element of RRS modulo $2p$.

Now, let if possible $g^k \equiv l^a \pmod{2p}$ for any $k, a;\ 1 \leq k \leq d-1$ and $0 \leq a \leq \frac{\varphi(p)}{d} - 1$.

Then, $(g^k)^{\frac{\varphi(p)}{d}} \equiv (l^a)^{\frac{\varphi(p)}{d}} \pmod{2p}$.

So, $\varphi(p)$ divides $\frac{\varphi(p)}{d}k$, which is a contradiction as $k < d$.

Therefore, $g, g^2, \dots, g^{d-1} \notin \left\{1, l, l^2, \dots, l^{\frac{\varphi(2p)}{d}-1}\right\}$. By our choice on l and g the elements of the set $\{1, l, l^2, \dots, l^{\frac{\varphi(p^{n-j})}{d}-1}, g, gl, gl^2, \dots, gl^{\frac{\varphi(p^{n-j})}{d}-1}, g^{d-1}, g^{d-1}l, g^{d-1}l^2, \dots, g^{d-1}l^{\frac{\varphi(p^{n-j})}{d}-1}\}$ are co prime to $2p$.

We want to prove that all these elements are incongruent mod $2p^{n-j}$.

Let $g^i l^k \equiv g^r l^t \pmod{2p^{n-j}}$ with $1 \leq r \leq i \leq d-1$ and $0 \leq k, t < \frac{\varphi(p^{n-j})}{d} - 1$.

Then $g^{i-r} \equiv l^{t-k} \pmod{2p^{n-j}}$ implies that $g^{i-r} \equiv l^{t-k} \pmod{2p}$ where $s \equiv t-k \pmod{\varphi(p)/d}$.

Therefore, $g^{i-r} \in \left\{1, l, l^2, \dots, l^{\frac{\varphi(2p)}{d}-1}\right\}$ for $0 \leq i - r < d$. Consequently, $i = r$.

Therefore, we get $l^k \equiv l^t \pmod{2p^{n-j}}$, where $0 \leq k, t < \varphi(p^{n-j})/d$.

But order of l mod $2p^{n-j}$ is $\varphi(p^{n-j})/d$, which gives us $k = t$.

Theorem 2.2.3. If p is an odd prime $o(l)_{2p^n} = \varphi(2p^n)/d$, d is a positive integer, then for the integer $n \geq 1$, there are $2(nd+1)$ $l-$cyclotomic cosets (mod $2p^n$) given by

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

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

For $0 \leq j \leq n-1, 0 \leq k \leq d-1$,

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

(iv) $C_{2g^k p^j} = \{2g^k p^j,\ 2g^k p^j l,\ 2g^k p^j l^2, \ldots, 2g^k p^j l^{\frac{\varphi(p^{n-j})}{d}-1}\}$,

where g is the fixed positive integer as defined in Lemma 2.2.2.

Proof. (i) $C_0 = \{0\}$ is trivial.

(ii) $C_{p^n} = \{p^n\}$ is also trivial.

(iii) By Lemma 2.2.2, $C_{g^k p^i}$ and $C_{g^h p^j}$ are pairwise disjoint whenever $k \neq h$ or $i \neq j$.

For fixed k and j, $0 \leq k \leq d-1, 0 \leq j \leq n-1$, as $o(l)_{2p^{n-j}} = \varphi(2p^{n-j})/d$, therfore

$g^k p^j l^{\frac{\varphi(2p^{n-j})}{d}} \equiv g^k p^j \pmod{2p^n}$.

Hence, the cyclotomic coset modulo $2p^n$ containing $g^k p^j$ is $\{g^k p^j,\ g^k p^j l,\ g^k p^j l^2, \ldots, g^k p^j l^{\frac{\varphi(p^{n-j})}{d}-1}\}$.

(iv) By Lemma 2.2.2, $C_{2g^k p^i}$ and $C_{2g^h p^j}$ are pairwise disjoint whenever $k \neq h$ or $i \neq j$.

For fixed k and $j, 0 \leq k \leq d-1, 0 \leq j \leq n-1$, $2g^k p^j l^{\frac{\varphi(2p^{n-j})}{d}} \equiv 2g^k p^j \pmod{2p^n}$,

therefore, the cyclotomic coset modulo $2p^n$ containing $2g^k p^j$ is

$\{2g^k p^j,\ 2g^k p^j l,\ 2g^k p^j l^2, \ldots, 2g^k p^j l^{\frac{\varphi(p^{n-j})}{d}-1}\}$.

By the constructions of l-cyclotomic cosets in (i) – (iv), it follows that:

$$|C_0| = |C_{p^n}| = 1$$

and

$$|C_{g^k p^j}| = |C_{2g^k p^j}| = \varphi(p^{n-j})/d.$$

Then,

$$|C_0| + |C_{p^n}| + \sum_{k=0}^{d-1}\sum_{j=0}^{n-1}\left(\left|C_{g^k p^j}\right| + \left|C_{2g^k p^j}\right|\right)$$

$$= 1 + 1 + \sum_{k=0}^{d-1}\sum_{j=0}^{n-1}\left(\frac{\varphi\left(p^{n-j}\right)}{d} + \frac{\varphi\left(p^{n-j}\right)}{d}\right)$$

$$= 2 + 2\sum_{k=0}^{d-1}\sum_{j=0}^{n-1}\left(\frac{\varphi\left(p^{n-j}\right)}{d}\right)$$

$$= 2 + 2\sum_{j=0}^{n-1}\varphi(p^{n-j})$$

$= 2 + 2\,(p^n - 1) = 2p^n$.

Lemma 2.2.4. For any integer u, $g^u \in C_1$ if and only if $u \equiv 0 \pmod{d}$.

Proof. If $g^d \in C_{g^k}$ for some k, $0 < k < d$, then $g^d \equiv g^k l^t \pmod{2p^n}$ showing that $g^{d-k} \in C_1$ with $0 < d - k < d$, which contradicts Lemma 2.2.2.

Hence, $g^d \in C_1$.

Clearly $g^{ds} \in C_1$ for every positive integer s.

Thus, if $u \equiv 0 \pmod{d}$, $g^u \in C_1$.

Conversely, let $g^u \in C_1$.

Write $u = ds + r, 0 \leq r < d$.

Then $g^u \equiv l^a \pmod{2p^n}$, $0 \leq a < \varphi(p^n)/d$ gives that $g^r \in C_1$ and $0 \leq r < d$.

Then Lemma 2.2.2 implies that $r = 0$. Therefore, $u \equiv 0 \pmod{d}$.

Lemma 2.2.5. $-1 \in C_1$ if d is odd and $-1 \in C_1$ or $C_{g^{d/2}}$ if d is even.

Proof. Let $-1 \in C_{g^u}$, where $0 \leq u \leq d - 1$.

Therefore, $-1 \equiv g^u l^a \pmod{2p^n}$ for some $a, 0 \leq a < \varphi(p^n)/d$.

This implies that $g^{2u} l^{2a} \equiv 1 \pmod{2p^n}$ showing that $g^{2u} \in C_1$.

Therefore, by Lemma 2.2.4, $2u \equiv 0 \pmod{d}$ and $0 \leq u < d$.

Case (i) If d is odd and by above discussion, $u \equiv 0 \pmod{d}$.

But $0 \leq u < d$ implies that $u = 0$.

Hence $-1 \in C_1$.

Case (ii) If d is even and $2u \equiv 0 \pmod{d}$ implies $u \equiv 0 \pmod{d/2}$

Consequently, $u = 0$ or $u = /2$.

Observations 2.2.5(a).

(i) $-1 \in C_1$ or $-1 \in C_{g^{d/2}}$. If $-1 \in C_1$ then $-C_1 = C_1$ otherwise $-C_1 = C_{g^{d/2}}$.

(ii) If $-C_1 = C_1$ then $-C_{g^k p^j} = C_{g^k p^j}$ otherwise $-C_{g^k p^j} = C_{g^{k+d/2} p^j}$ for all $j, k;\ 0 \leq i \leq n-1$ and $0 \leq k \leq d-1$.

(iii) $2C_2 = C_{2g^k}$ for $0 \leq k \leq d-1$.

Lemma 2.2.6. For any odd prime p and positive integer n, if β is primitive p^nth root of unity in some extension field of F_{l^*} where l^* is an odd prime and $o(l^*)_{p^n} = \varphi(p^n)$, then

$$\sum_{s=0}^{\varphi(p^n)-1} \beta^{l^{*s}} = \begin{cases} -1 & if\ n = 1, \\ 0 & if\ n > 1. \end{cases}$$

Proof. Since $o(l^*)_{p^n} = \varphi(p^n)$, therefore the set $\{1, l^*, l^{*2}, \ldots, l^{*\varphi(p^n)-1}\}$ forms a reduced residue system mod p^n.

Hence,

$$\sum_{s=0}^{\varphi(p^n)-1} \beta^{l^{*s}} = \sum_{s=0}^{p^n-1} \beta^s - \sum_{\substack{s=1 \\ p/s}}^{p^n} \beta^s$$

$$= \sum_{s=1}^{p^n} \beta^s - \sum_{s=1}^{p^{n-1}} \beta^{ps}.$$

If $n > 1$, then $\beta \neq 1$ and $\beta^p \neq 1$, since β is p^nth root of unity.

Therefore, the above sums become zero being geometric series.

Then, $\sum_{s=0}^{\varphi(p^n)-1} \beta^{l^{*s}} = 0$.

If $n = 1$, then

$$\sum_{s=0}^{\varphi(p^n)-1} \beta^{l^{*s}} = \sum_{s=0}^{\varphi(p)-1} \beta^{l^{*s}}$$

$$= \frac{\beta^p - 1}{\beta - 1} - 1 = -1.$$

Hence the lemma follows.

Lemma 2.2.7. For any odd prime p and positive integer n, if β is primitive $2p^n$th root of unity in some extension field of F_{l^*} and $o(l^*)_{2p^n} = \varphi(2p^n))$, then

$$\sum_{s=0}^{\varphi(2p^n)-1} \beta^{l^{*s}} = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Proof. As $\{1, l^*, l^{*2}, \ldots, l^{*\varphi(2p^n)-1}\}$ is a reduced residue system mod $2p^n$, therefore

$$\sum_{s=0}^{\varphi(2p^n)-1} \beta^{l^{*s}} = \sum_{s=1}^{2p^n} \beta^s - \sum_{\substack{s=1 \\ p/s}}^{2p^n} \beta^s - \sum_{\substack{s=1 \\ 2/s}}^{2p^n} \beta^s + \sum_{\substack{s=1 \\ 2p/s}}^{2p^n} \beta^s$$

$$= \sum_{s=1}^{2p^n} \beta^s - \sum_{s=1}^{2p^{n-1}} \beta^{ps} - \sum_{s=1}^{p^n} \beta^{2s} + \sum_{s=1}^{p^{n-1}} \beta^{2ps}.$$

As $\beta \neq 1$, $\beta^p \neq 1$ and $\beta^2 \neq 1$, therefore the first three sums becomes zero being geometric series.

Then,

$$\sum_{s=0}^{\varphi(2p^n)-1} \beta^{l^{*s}} = \sum_{s=1}^{p^{n-1}} \beta^{2ps}.$$

If $n = 1$, then the summation on the right hand side becomes $\beta^{2p} = 1$.

If $n \geq 2$, we have $\beta^{2p} \neq 1$, therefore the right hand side becomes geometric series and its sum equals to 0.

Hence the lemma follows.

Notations 2.2.8.

Let α is primitive $2p^n$th root of unity in some extension field of F_l .

For $0 \leq i \leq n-1$ and $0 \leq k \leq d-1$, define

$$A_i^{(k)} = \sum_{s \in C_{g^k}} \alpha^{2p^i s}$$

and

$$B_i^{(k)} = \sum_{s \in C_{g^k}} \alpha^{p^i s}.$$

Since $C_{g^k l} = C_{g^k}$, therefore $(A_i^{(k)})^l = A_i^{(k)}$ and $(B_i^{(k)})^l = B_i^{(k)}$ so that each $A_i^{(k)}, B_i^{(k)} \in F_l$.

Lemma 2.2.9. For each $i, 0 \leq i \leq n-1$,

$$\sum_{k=0}^{d-1} A_i^{(k)} = \begin{cases} 0 & \text{if } i \leq n-2, \\ -p^{n-1} & \text{if } i = n-1. \end{cases}$$

Proof. For $0 \leq i \leq n-1$ and $0 \leq k \leq d-1$, $2g^k p^i l^s \equiv 2g^k p^i l^t (\text{mod } 2p^n)$ if and only if $l^s \equiv l^t (\text{mod } p^{n-i})$ if and only if $s \equiv t \ (\text{mod } \varphi(p^{n-i})/d)$. Therefore,

$$A_i^{(k)} = \sum_{s \in C_{g^k}} \alpha^{2p^i s} = \sum_{s=0}^{\frac{\varphi(p^n)}{d}-1} \alpha^{2g^k p^i l^s}$$

$$= \frac{\varphi(p^n)}{\varphi(p^{n-i})} \left(\sum_{s=0}^{\frac{\varphi(p^{n-i})}{d}-1} \alpha^{2g^k p^i l^s} \right)$$

$$= p^i \sum_{s=0}^{\frac{\varphi(p^{n-i})}{d}-1} \beta^{g^k l^s},$$

where $\beta = \alpha^{2p^i}$ is a primitive p^{n-i}th root of unity. Consequently,

$$\sum_{k=0}^{d-1} A_i^{(k)} = \sum_{k=0}^{d-1} \left(p^i \sum_{s=0}^{\frac{\varphi(p^{n-i})}{d}-1} \beta^{g^k l^s} \right).$$

As, by Lemma 2.2.2. for any $i,\ 1 \leq i < n$, the set

$$\{1, l, l^2, \ldots, l^{\frac{\varphi(p^{n-i})}{d}-1}, g, gl, gl^2, \ldots, gl^{\frac{\varphi(p^{n-i})}{d}-1}, g^{d-1}, g^{d-1}l, \ldots, g^{d-1}l^{\frac{\varphi(p^{n-i})}{d}-1}\}$$

forms a reduced residue system modulo p^{n-i}, therefore we have

$$\sum_{k=0}^{d-1} \left(p^i \sum_{s=0}^{\frac{\varphi(p^{n-i})}{d}-1} \beta^{g^k l^s} \right) = p^i \left(\sum_{s=1}^{p^{n-i}} \beta^s - \sum_{\substack{s=1 \\ p/s}}^{p^{n-i}} \beta^s \right)$$

$$= p^i \left(\sum_{s=1}^{p^{n-i}} \beta^s - \sum_{s=1}^{p^{n-i-1}} \beta^{ps} \right).$$

As $\beta \neq 1$, therefore the first sum become zero being geometric series.

If $i \leq n-2$, we have $\beta^p \neq 1$.

So,

$$\sum_{s=1}^{p^{n-i-1}} \beta^{ps} = 0$$

Therefore,

$$\sum_{k=0}^{d-1} p^i \sum_{s=0}^{\frac{\varphi(p^{n-i})}{d}-1} \beta^{g^k l^s} = 0.$$

If $i = n-1$, then $\beta^p = 1$, therefore the sum of the last series becomes 1.

Thus, $\sum_{k=0}^{d-1} A_i^{(k)} = -p^{n-1}$ for $i = n-1$ and 0 for $i \leq n-2$.

Lemma 2.2.10. For each $i, 0 \leq i \leq n-1$,

$$\sum_{k=0}^{d-1} B_i^{(k)} = \begin{cases} 0 & \text{if } i \leq n-2, \\ p^{n-1} & \text{if } i = n-1. \end{cases}$$

Proof. For $0 \le i \le n-1$ and $0 \le k \le d-1$, $g^k p^i l^s \equiv g^k p^i l^t (\text{mod } 2p^n)$ if and only if $l^s \equiv l^t (\text{mod } 2p^{n-i})$ if and only if $s \equiv t (\text{mod } \varphi(p^{n-i})/d)$. Therefore,

$$B_i^{(k)} = \sum_{s \in C_{g^k}} \alpha^{p^i s} = \sum_{s=0}^{\frac{\varphi(p^n)}{d}-1} \alpha^{g^k p^i l^s}$$

$$= \frac{\varphi(p^n)}{\varphi(p^{n-i})} \sum_{s=0}^{\frac{\varphi(p^{n-i})}{d}-1} \alpha^{g^k p^i l^s}$$

$$= p^i \sum_{s=0}^{\frac{\varphi(p^{n-i})}{d}-1} \beta^{g^k l^s},$$

where $\beta = \alpha^{p^i}$ is a primitive $2p^{n-i}$th root of unity. Therefore,

$$\sum_{k=0}^{d-1} B_i^{(k)} = \sum_{k=0}^{d-1} \left(p^i \sum_{s=0}^{\frac{\varphi(p^{n-i})}{d}-1} \beta^{g^k l^s} \right).$$

As, for any $i, 1 \le i < n$, the set

$\{1, l, l^2, \dots, l^{\frac{\varphi(p^{n-i})}{d}-1}, g, gl, gl^2, \dots, gl^{\frac{\varphi(p^{n-i})}{d}-1}, g^{d-1}, g^{d-1}l, \dots, g^{d-1}l^{\frac{\varphi(p^{n-i})}{d}-1}\}$ form a reduced residue system modulo $2p^{n-i}$, therefore we have

$$\sum_{k=0}^{d-1} \left(p^i \sum_{s=0}^{\frac{\varphi(p^{n-i})}{d}-1} \beta^{l^s} \right) = p^i \left(\sum_{s=1}^{2p^{n-i}} \beta^s - \sum_{\substack{s=1 \\ p/s}}^{2p^{n-i}} \beta^s - \sum_{\substack{s=1 \\ 2/s}}^{2p^{n-i}} \beta^s + \sum_{\substack{s=1 \\ 2p/s}}^{2p^{n-i}} \beta^s \right)$$

$$= p^i \left(\sum_{s=1}^{2p^{n-i}} \beta^s - \sum_{s=1}^{2p^{n-i-1}} \beta^{ps} - \sum_{s=1}^{p^{n-i}} \beta^{2s} + \sum_{s=1}^{p^{n-i-1}} \beta^{2ps} \right).$$

As $\beta \ne 1$, $\beta^p \ne 1$ and $\beta^2 \ne 1$, therefore the first three sums become zero being geometric series.

If $\beta^{2p} \ne 1$ i.e. $i \ne (n-1)$, the sum of the last series also vanishes.

If $i = n-1$, the last series becomes $\beta^{2p} = 1$.

Thus, $\sum_{k=0}^{d-1} B_i^{(k)} = p^{n-1}$ for $i = n-1$ and 0 for $i \neq (n-1)$.

Lemma 2.2.11. For each $i, j;\ h, k;\ 0 \leq h, k \leq d-1$ and $0 \leq i, j \leq n$,

$$\sum_{s \in C_{g^h p^j}} \alpha^{2g^k p^i s} = \sum_{s \in C_{2g^h p^j}} \alpha^{2g^k p^i s} = \begin{cases} 1 & \text{if } j = n, \\ \dfrac{\varphi(p^{n-j})}{d} & \text{if } i + j \geq n, j \leq n-1, \\ \dfrac{1}{p^j} A_{i+j}^{(h+k)} & \text{if } i + j \leq n-1. \end{cases}$$

Proof. By Observation 2.2.5(a), $2C_2 = C_2$ or C_{2g}, so the two sums are equal.

Case (i) For $j = n$, $C_{g^h p^j} = C_{g^k p^n} = C_{p^n}$.

Therefore,

$$\sum_{s \in C_{g^h p^j}} \alpha^{2g^k p^i s} = \sum_{s \in C_{p^n}} \alpha^{2g^k p^i s}.$$

As α is $2p^n$th root of unity, so $\alpha^{2g^k p^{i+n} s} = 1$.

Therefore,

$$\sum_{s \in C_{p^n}} \alpha^{2g^k p^i s} = 1.$$

Case (ii) Let $i + j \geq n$ and $j \leq n-1$, then the above sum

$$\sum_{s \in C_{g^h p^j}} \alpha^{2g^k p^i s} = \sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \alpha^{2g^{(h+k)} p^{i+j} l^s} = \frac{\varphi(p^{n-j})}{d}.$$

Case (iii) If $i + j \leq n-1$, then

$$\sum_{s \in C_{g^h p^j}} \alpha^{2g^k p^i s} = \sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \alpha^{2g^{(h+k)} p^{i+j} l^s} = \sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \beta^{l^s},$$

where $\beta = \alpha^{2g^{(h+k)} p^{i+j}}$, then β is primitive p^{n-i-j} th root of unity.

Therefore, $\beta^{l^r} = \beta^{l^s}$ if and only if $l^r \equiv l^s \pmod{p^{n-i-j}}$ if and only if $r \equiv s \pmod{\frac{\varphi(p^{n-i-j})}{d}}$.

Then

$$\sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \beta^{l^s} = \frac{\varphi\left(2p^{n-j}\right)}{\varphi(p^{n-i-j})} \sum_{s=0}^{\frac{\varphi(p^{n-i-j})}{d}-1} \beta^{l^s}$$

$$= p^i \sum_{s=0}^{\frac{\varphi(p^{n-i-j})}{d}-1} \beta^{l^s}.$$

Also,

$$A_{i+j}^{(h+k)} = \sum_{s\in C_{g(h+k)}} \alpha^{2p^{i+j}s} = \sum_{s=0}^{\frac{\varphi(2p^n)}{d}-1} \beta^{l^s}$$

$$= \frac{\varphi(2p^n)}{d}.\frac{d}{\varphi(p^{n-i-j})} \sum_{s=0}^{\frac{\varphi(p^{n-i-j})}{d}-1} \beta^{l^s}$$

$$= p^{i+j} \sum_{s=0}^{\frac{\varphi(p^{n-i-j})}{d}-1} \beta^{l^s}.$$

This implies,

$$\sum_{s=0}^{\frac{\varphi(p^{n-i-j})}{d}-1} \beta^{l^s} = \frac{1}{p^{i+j}} A_{i+j}^{(h+k)}.$$

Thus, in view of above two values, we conclude that

$$\sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \beta^{l^s} = \frac{1}{p^j} A_{i+j}^{(h+k)}.$$

This proves the lemma.

Lemma 2.2.12. For each $i, j;\ h, k;\ 0 \le h, k \le d-1$ and $0 \le i, j \le n$,

$$\sum_{s\in C_{g^h p^j}} \alpha^{g^k p^i s} = \begin{cases} -1 & if\ i+j \ge n, j = n, \\ -\dfrac{\varphi\left(p^{n-j}\right)}{d} & if\ i+j \ge n, j \le n-1, \\ \dfrac{1}{p^j} B_{i+j}^{(h+k)} & if\ i+j \le n-1. \end{cases}$$

Proof. Case (i) For $j = n$, $C_{g^h p^j} = C_{g^k p^n} = C_{p^n}$.

Therefore,

$$\sum_{s \in C_{g^h p^j}} \alpha^{g^k p^i s} = \sum_{s \in C_{p^n}} \alpha^{g^k p^i s} = -1.$$

Case (ii) Let $i + j \geq n$ and $j \leq n-1$, then the above sum

$$\sum_{s \in C_{g^h p^j}} \alpha^{g^k p^i s} = \sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \alpha^{g^{(h+k)} p^{i+j} l^s} = -\frac{\varphi(p^{n-j})}{d}.$$

Case (iii) If $i + j \leq n-1$, then

$$\sum_{s \in C_{g^h p^j}} \alpha^{g^k p^i s} = \sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \alpha^{g^{(h+k)} p^{i+j} l^s} = \sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \beta^{l^s},$$

where $\beta = \alpha^{g^{(h+k)} p^{i+j}}$, then β is primitive $2p^{n-i-j}$ th root of unity.

Therefore, $\beta^{l^r} = \beta^{l^s}$ if and only if $l^r \equiv l^s \pmod{p^{n-i-j}}$ if and only if $r \equiv s \pmod{\frac{\varphi(p^{n-i-j})}{d}}$.

Then

$$\sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \beta^{l^s} = \frac{\varphi(2p^{n-j})}{\varphi(p^{n-i-j})} \left(\sum_{s=0}^{\frac{\varphi(p^{n-i-j})}{d}-1} \beta^{l^s} \right)$$

$$= p^i \sum_{s=0}^{\frac{\varphi(p^{n-i-j})}{d}-1} \beta^{l^s}.$$

Also,

$$B_{i+j}^{(h+k)} = \sum_{s \in C_{g^{(h+k)}}} \alpha^{p^{i+j} s} = \sum_{s=0}^{\frac{\varphi(2p^n)}{d}-1} \beta^{l^s}$$

$$= \frac{\varphi(2p^n)}{d} \cdot \frac{d}{\varphi(p^{n-i-j})} \sum_{s=0}^{\frac{\varphi(p^{n-i-j})}{d}-1} \beta^{l^s}$$

$$= p^{i+j} \sum_{s=0}^{\frac{\varphi(p^{n-i-j})}{d}-1} \beta^{l^s}.$$

Thus,

$$\sum_{s=0}^{\frac{\varphi(2p^{n-j})}{d}-1} \beta^{l^s} = \frac{1}{p^j} B_{i+j}^{(h+k)}.$$

This proves the lemma.

2.3 Evaluation of Primitive Idempotents in $R_{2p^n} = \frac{F_l[x]}{<x^{2p^n}-1>}$

If α is a primitive m^{th} root of unity in some extension field F_l then the polynomial

$M^s(x) = \prod_{i \in C_s}(x - \alpha^i)$ is the minimal polynomial of α^s over F_l.

Let $\theta_s(x)$ be the primitive idempotent and $\sigma_s(x) = \sum_{i \in C_s} x^i$.

Then $\theta_s(\alpha^j) = \begin{cases} 1 & \text{if } j \in C_s, \\ 0 & \text{if } j \notin C_s. \end{cases}$

Theorem 2.3.1. $\theta_s(x) = \sum_{i=0}^{m-1} \epsilon_i x^i$, where $\epsilon_i = \frac{1}{m} \sum_{j \in C_s} \alpha^{-ij}$ for all $i \geq 0$.

Proof.

$$\sum_{i=0}^{m-1} \theta_s(\alpha^j)\alpha^{-ij} = \sum_{j=0}^{m-1} \sum_{k=0}^{m-1} \varepsilon_k \alpha^{jk} \alpha^{-ij}$$

$$\sum_{k=0}^{m-1} \epsilon_k \sum_{j=0}^{m-1} \alpha^{j(k-i)} = m\epsilon_i.$$

Therefore, by the above discussion, we have

$$\epsilon_i = \frac{1}{m} \sum_{i=0}^{m-1} \theta_s(\alpha^j)\alpha^{-ij} = \frac{1}{m} \sum_{j \in C_s} \alpha^{-ij}.$$

Theorem 2.3.2. The $2(nd+1)$ primitive idempotents in R_{2p^n} are given by

(i) $\theta_0(x) = \frac{1}{2p^n}(1 + x + x^2 + \cdots + x^{2p^n-1})$,

(ii)

$$\theta_{p^n}(x) = \frac{1}{2p^n}\{1 - \sigma_{p^n}(x)\} + \frac{1}{2p^n}\left\{\sum_{k=0}^{d-1}\sum_{i=0}^{n-1}\left(\sigma_{2g^k p^i}(x) - \sigma_{g^k p^i}(x)\right)\right\},$$

(iii) For $0 \le j \le n-1, 0 \le k \le d-1$,

$$\theta_{g^k p^j}(x) = \frac{p-1}{2p^{j+1}d}\left\{1 - \sigma_{p^n}(x) + \sum_{h=0}^{d-1}\sum_{i=n-j}^{n-1}\left(\sigma_{2g^h p^i}(x) - \sigma_{g^h p^i}(x)\right)\right\}$$

$$+ \frac{1}{2p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\left(B_{i+j}^{(\gamma+h)}\sigma_{g^h p^i}(x) + A_{i+j}^{(\gamma+h)}\sigma_{2g^h p^i}(x)\right),$$

and

(iv)

$$\theta_{2g^k p^j}(x) = \frac{p-1}{2p^{j+1}d}\left\{1 + \sigma_{p^n}(x) + \sum_{h=0}^{d-1}\sum_{i=n-j}^{n-1}\left(\sigma_{g^h p^i}(x) + \sigma_{2g^h p^i}(x)\right)\right\}$$

$$+ \frac{1}{2p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1} A_{i+j}^{(\gamma+h)}\left(\sigma_{g^h p^i}(x) + \sigma_{2g^h p^i}(x)\right).$$

Proof. (i) Evaluation of $\boldsymbol{\theta_0(x)}$

By Theorem 2.3.1, $\theta_0(x) = \sum_{r=0}^{2p^n-1}\epsilon_r x^r$, where $\epsilon_r = \frac{1}{2p^n}\sum_{s\in C_0}\alpha^{-rs} = \frac{1}{2p^n}$ for all r.

Therefore, $\theta_0(x) = \frac{1}{2p^n}\left(1 + x + x^2 + \cdots + x^{2p^n-1}\right)$.

(ii) Evaluation of $\boldsymbol{\theta_{p^n}(x)}$

By Theorem 2.3.1,

$$\theta_{p^n}(x) = \sum_{r=0}^{2p^n-1}\epsilon_r x^r,$$

where $\epsilon_r = \frac{1}{2p^n}\sum_{s\in C_{p^n}} \alpha^{-rs}$.

Since by Observations 2.2.5(a), $-C_{p^n} = C_{p^n}$, therefore, $\epsilon_r = \frac{1}{2p^n}\sum_{s\in C_{p^n}} \alpha^{rs}$.

In a cyclotomic coset the value of ε_r remains same, we just need to calculate ϵ_0, ϵ_{p^n}, $\epsilon_{g^k p^i}$ and $\epsilon_{2g^k p^i}$ for $0 \le i \le n-1, 0 \le k \le d-1$.

Now,

$$\epsilon_0 = \frac{1}{2p^n}\sum_{s\in C_{p^n}} \alpha^0 = \frac{1}{2p^n},$$

$$\epsilon_{p^n} = \frac{1}{2p^n}\sum_{s\in C_{p^n}} \alpha^{p^n s} = -\frac{1}{2p^n}.$$

For $0 \le i \le n-1, 0 \le k \le d-1$, by using Lemma 2.2.11 and Lemma 2.2.12, we have

$$\epsilon_{g^k p^i} = \frac{1}{2p^n}\sum_{s\in C_{p^n}} \alpha^{g^k p^i s} = -\frac{1}{2p^n},$$

$$\epsilon_{2g^k p^i} = \frac{1}{2p^n}\sum_{s\in C_{p^n}} \alpha^{2g^k p^i s} = \frac{1}{2p^n}.$$

Thus,

$$\theta_{p^n}(x) = \frac{1}{2p^n}\{1-\sigma_{p^n}(x)\} + \frac{1}{2p^n}\left\{\sum_{k=0}^{d-1}\sum_{i=0}^{n-1}\left(\sigma_{2g^k p^i}(x) - \sigma_{g^k p^i}(x)\right)\right\}.$$

(iii) Evaluation of $\theta_{g^k p^j}(x)$ for $0 \le j \le n-1$ and $0 \le k \le d-1$.

If

$$\theta_{g^k p^j}(x) = \sum_{r=0}^{2p^n-1} \epsilon_r^{(k,j)} x^r,$$

Then, by Theorem 2.3.1 and Observations 2.2.5(a), we have

$$\epsilon_r^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{g^k p^j}} \alpha^{-rs} = \frac{1}{2p^n}\sum_{s\in C_{g^{k+u} p^j}} \alpha^{rs},$$

$u = 0$ or $u = d/2$ according as $-1 \in C_1$ or $-1 \in C_{g^{d/2}}$.

Thus,

$$\epsilon_r^{(k,j)} = \frac{1}{2p^n} \sum_{s \in C_{g^\gamma p^j}} \alpha^{rs},$$

where $\gamma \equiv k + u \pmod{d}$.

In a cyclotomic coset the value of ϵ_r remains same, we just need to calculate ϵ_0, ϵ_{p^n}, $\epsilon_{g^k p^i}$ and $\epsilon_{2g^k p^i}$

for $0 \leq i \leq n-1, 0 \leq k \leq d-1$.

Now,

$$\epsilon_0^{(k,j)} = \frac{1}{2p^n} \sum_{s \in C_{g^\gamma p^j}} \alpha^0 = \frac{\varphi(2p^{n-j})}{2p^n d},$$

$$\epsilon_{p^n}^{(k,j)} = \frac{1}{2p^n} \sum_{s \in C_{g^\gamma p^j}} \alpha^{p^n s} = -\frac{\varphi(p^{n-j})}{2p^n d}.$$

For $0 \leq i \leq n-1$, by using Lemma 2.2.11 and Lemma 2.2.12, we have

$$\epsilon_{g^h p^i}^{(k,j)} = \frac{1}{2p^n} \sum_{s \in C_{g^\gamma p^j}} \alpha^{g^h p^i s} = \frac{1}{2p^n} \begin{cases} -\dfrac{\varphi(p^{n-j})}{d} & \text{if } i + j \geq n, j \leq n-1, \\ \dfrac{1}{p^j} B_{i+j}^{(\gamma+h)} & \text{if } i \leq n-j-1. \end{cases}$$

$$\epsilon_{2g^h p^i}^{(k,j)} = \frac{1}{2p^n} \sum_{s \in C_{g^\gamma p^j}} \alpha^{2g^h p^i s} = \frac{1}{2p^n} \begin{cases} \dfrac{\varphi(p^{n-j})}{d} & \text{if } i + j \geq n, j \leq n-1, \\ \dfrac{1}{p^j} A_{i+j}^{(\gamma+h)} & \text{if } i \leq n-j-1. \end{cases}$$

Therefore,

$$\theta_{g^k p^j}(x) = \frac{p-1}{2p^{j+1}d} \left\{ 1 - \sigma_{p^n}(x) + \sum_{h=0}^{d-1} \sum_{i=n-j}^{n-1} \left(\sigma_{2g^h p^i}(x) - \sigma_{g^h p^i}(x) \right) \right\}$$

$$+\frac{1}{2p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\left(B_{i+j}^{(\gamma+h)}\sigma_{g^h p^i}(x)+A_{i+j}^{(\gamma+h)}\sigma_{2g^h p^i}(x)\right).$$

(iv) Evaluation of $\theta_{2g^k p^j}(x)$ for $0 \le j \le n-1$ and $0 \le k \le d-1$.

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

$\theta_{2g^k p^j}(x) = \sum_{r=0}^{2p^n-1} \epsilon_r^{(k,j)} x^r$,

Then, by Theorem 2.3.1 and observations, we have

$$\epsilon_r^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{2g^k p^j}} \alpha^{-rs} = \frac{1}{2p^n}\sum_{s\in C_{2g^{k+u} p^j}} \alpha^{rs},$$

$u = 0$ or $u = d/2$ according as $-1 \in C_1$ or $-1 \in C_{g^{d/2}}$.

Thus,

$$\epsilon_r^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{2g^\gamma p^j}} \alpha^{rs},$$

where $\gamma \equiv k+u \pmod d$.

In a cyclotomic coset the value of ϵ_r remains same, we just need to calculate ϵ_0, ϵ_{p^n}, $\epsilon_{g^k p^i}$ and $\epsilon_{2g^k p^i}$

for $0 \le i \le n-1, 0 \le k \le d-1$.

Now,

$$\epsilon_0^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{2g^\gamma p^j}} \alpha^0 = \frac{\varphi(p^{n-j})}{2p^n d},$$

$$\epsilon_{p^n}^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{2g^\gamma p^j}} \alpha^{p^n s} = \frac{\varphi(p^{n-j})}{2p^n d}.$$

For $0 \le i \le n-1$, by using Lemma 2.2.11 and Lemma 2.2.12, we have

$$\epsilon_{g^h p^i}^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{2g^\gamma p^j}} \alpha^{g^h p^i s} = \frac{1}{2p^n}\begin{cases}\dfrac{\varphi(p^{n-j})}{d} & \text{if } i+j \ge n, j \le n-1,\\ \dfrac{1}{p^j}A_{i+j}^{(\gamma+k)} & \text{if } i \le n-j-1.\end{cases}$$

$$\epsilon_{2g^h p^i}^{(k,j)} = \frac{1}{2p^n} \sum_{s \in C_{2g^\gamma p^j}} \alpha^{2g^h p^i s} = \frac{1}{2p^n} \begin{cases} \frac{\varphi(p^{n-j})}{d} & \text{if } i+j \geq n, j \leq n-1, \\ \frac{1}{p^j} A_{i+j}^{(h+k)} & \text{if } i \leq n-j-1. \end{cases}$$

Therefore, we have

$$\theta_{2g^k p^j}(x) = \frac{1}{2p^n d} \Bigg\{ \varphi(p^{n-j}) + \varphi(p^{n-j}) \sigma_{p^n}(x) + \sum_{h=0}^{d-1} \sum_{i=n-j}^{n-1} \varphi(p^{n-j}) \left(\sigma_{g^h p^i}(x) + \sigma_{2g^h p^i}(x) \right) \Bigg\}$$

$$+ \frac{1}{2p^n} \sum_{h=0}^{d-1} \sum_{i=0}^{n-j-1} \frac{1}{p^j} A_{i+j}^{(\gamma+h)} \left(\sigma_{g^h p^i}(x) + \sigma_{2g^h p^i}(x) \right).$$

Hence solving this, we have

$$\theta_{2g^k p^j}(x) = \frac{p-1}{2p^{j+1} d} \Bigg\{ 1 + \sigma_{p^n}(x) + \sum_{h=0}^{d-1} \sum_{i=n-j}^{n-1} \left(\sigma_{g^h p^i}(x) + \sigma_{2g^h p^i}(x) \right) \Bigg\}$$

$$+ \frac{1}{2p^{n+j}} \sum_{h=0}^{d-1} \sum_{i=0}^{n-j-1} A_{i+j}^{(\gamma+h)} \left(\sigma_{g^h p^i}(x) + \sigma_{2g^h p^i}(x) \right).$$

Lemma 2.3.3. For $0 \leq i \leq n-1, 0 \leq k \leq d-1$, then

(I) $A_i^k = 0$ if $0 \leq i < n-1$.

(II) If d is even, then

$$\sum A_{n-1}^{(k)} = \begin{cases} p^{n-1} \frac{(\kappa-1)}{2} & \text{if } k \text{ is even; } p = \kappa^2, \\ -p^{n-1} \frac{(\kappa+1)}{2} & \text{if } k \text{ is odd,} \end{cases}$$

and

$$\sum A_{n-1}^{(k)} = \begin{cases} -p^{n-1} \frac{(1+\tau)}{2} & \text{if } k \text{ is even; } -p = \tau^2, \\ p^{n-1} \frac{(\tau-1)}{2} & \text{if } k \text{ is odd,} \end{cases}$$

according as $d/2$ is even or odd.

(III) If d is odd, then

$$\sum A_{n-1}^{(k)} = \begin{cases} p^{n-1}\dfrac{(\kappa-1)}{2} & \text{if } k \text{ is even; } \kappa^2 = \dfrac{(d-1)p+1}{d}, \\ -p^{n-1}\dfrac{(\kappa+1)}{2} & \text{if } k \text{ is odd.} \end{cases}$$

Proof. We know that

$$\theta_s(\alpha^j) = \begin{cases} 1 & \text{if } j \in C_s, \\ 0 & \text{if } j \notin C_s. \end{cases}$$

Therefore, $\theta_{2g^k p^j}\left(\alpha^{2g^k p^j}\right) = 1$.

Using Lemma 2.2.11, we get the value of $\sigma_{p^n}\left(\alpha^{2g^k p^j}\right) = 1$,

$$\sigma_{g^h p^i}\left(\alpha^{2g^k p^j}\right) = \begin{cases} \dfrac{\varphi\left(p^{n-i}\right)}{d} & \text{if } i \geq n-j, \\ \dfrac{1}{p^i} A_{i+j}^{(h+k)} & \text{if } i \leq n-j-1, \end{cases}$$

$$\sigma_{2g^h p^i}\left(\alpha^{2g^k p^j}\right) = \begin{cases} \dfrac{\varphi\left(p^{n-i}\right)}{d} & \text{if } i \geq n-j, \\ \dfrac{1}{p^i} A_{i+j}^{(h+k)} & \text{if } i \leq n-j-1. \end{cases}$$

Put all these values in $\theta_{2g^k p^j}\left(\alpha^{2g^k p^j}\right) = 1$, we have

$$1 = \frac{(p-1)}{2dp^{j+1}}\left(2 + 2\sum_{h=0}^{d-1}\sum_{i=n-j}^{n-1}\frac{\varphi\left(p^{n-j}\right)}{d}\right) + \frac{1}{p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^i}A_{i+j}^{(k+h+u)}A_{i+j}^{(k+h)}$$

$$= \frac{(p-1)}{dp^{j+1}}\left(1 + (p^j - 1)\right) + \frac{1}{p^n}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}A_{i+j}^{(k+h+u)}A_{i+j}^{(k+h)}.$$

This implies

$$\frac{1}{p^n}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}A_{i+j}^{(k+h+u)}A_{i+j}^{(k+h)} = 1 - \frac{(p-1)}{pd}$$

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}A_{i+j}^{(k+h+u)}A_{i+j}^{(k+h)} = \frac{p^{n-1}((d-1)p+1)}{d}. \qquad (2.1)$$

Further, $\theta_{2g^k p^j}\left(\alpha^{2g^m p^j}\right) = 0$ for some $k \neq m, 0 \leq k, m \leq d-1$.

Therefore, by using Lemma 2.2.11, we get the value of $\sigma_{p^n}\left(\alpha^{2g^m p^j}\right) = 1$,

$$\sigma_{g^h p^i}\left(\alpha^{2g^m p^j}\right) = \begin{cases} \dfrac{\varphi\left(p^{n-i}\right)}{d} & \text{if } i \geq n-j, \\ \dfrac{1}{p^i} A_{i+j}^{(h+m)} & \text{if } i \leq n-j-1, \end{cases}$$

$$\sigma_{2g^h p^i}\left(\alpha^{2g^m p^j}\right) = \begin{cases} \dfrac{\varphi\left(p^{n-i}\right)}{d} & \text{if } i \geq n-j, \\ \dfrac{1}{p^i} A_{i+j}^{(h+m)} & \text{if } i \leq n-j-1. \end{cases}$$

Put all these values in $\theta_{2g^k p^j}\left(\alpha^{2g^m p^j}\right) = 0$, we get

$$0 = \frac{(p-1)}{dp^{j+1}}\left(p^j\right) + \frac{1}{p^n}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}} A_{i+j}^{(k+h+u)} A_{i+j}^{(m+h)}.$$

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}} A_{i+j}^{(k+h+u)} A_{i+j}^{(m+h)} = \frac{(1-p)p^{n-1}}{d}. \tag{2.2}$$

Also, $\theta_{2g^k p^j}\left(\alpha^{2g^m p^{j-s}}\right) = 0$ for some $j \neq s, 0 \leq s < j \leq n-1, 0 \leq k, m \leq d-1$.

Therefore, by Lemma 2.2.11, we get the values of $\sigma_{p^n}\left(\alpha^{2g^m p^{j-s}}\right)$, $\sigma_{g^h p^i}\left(\alpha^{2g^m p^{j-s}}\right)$ and $\sigma_{2g^h p^i}\left(\alpha^{2g^m p^{j-s}}\right)$.

Put all these values in $\theta_{2g^k p^j}\left(\alpha^{2g^m p^{j-s}}\right) = 0$, we get

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}} A_{i+j}^{(k+h+u)} A_{i+j-s}^{(m+h)} = 0. \tag{2.3}$$

Put $j = n-1$ in equations (2.1), (2.2) and (2.3), we get the following equations

$$\sum_{h=0}^{d-1} A_{n-1}^{(k+h+u)} A_{n-1}^{(k+h)} = \frac{p^{2n-2}((d-1)p+1)}{d}, \tag{2.4}$$

$$\sum_{h=0}^{d-1} A_{n-1}^{(k+h+u)} A_{n-1}^{(m+h)} = \frac{(1-p)p^{2n-2}}{d}, \tag{2.5}$$

$$\sum_{h=0}^{d-1} A_{n-1}^{(k+h+u)} A_{n-1-s}^{(m+h)} = 0, \qquad \forall\ 1 \le s \le n-1. \tag{2.6}$$

Again put $j = n-2$ in equation (2.1), we get

$$\sum_{h=0}^{d-1} \sum_{i=0}^{1} \frac{1}{p^{i+n-2}} A_{i+n-2}^{(k+h+u)} A_{i+j-2}^{(k+h)} = \frac{p^{n-1}((d-1)p+1)}{d}$$

This implies

$$\sum_{h=0}^{d-1} \left(\frac{1}{p^{n-2}} A_{n-2}^{(k+h+u)} A_{n-2}^{(k+h)} + \frac{1}{p^{n-1}} A_{n-1}^{(k+h+u)} A_{n-1}^{(k+h)} \right) = \frac{p^{n-1}((d-1)p+1)}{d}.$$

$$\sum_{h=0}^{d-1} \frac{1}{p^{n-2}} A_{n-2}^{(k+h+u)} A_{n-2}^{(k+h)} + \sum_{h=0}^{d-1} \frac{1}{p^{n-1}} A_{n-1}^{(k+h+u)} A_{n-1}^{(k+h)} = \frac{p^{n-1}((d-1)p+1)}{d}.$$

Using equation (2.4), we have

$$\sum_{h=0}^{d-1} \frac{1}{p^{n-2}} A_{n-2}^{(k+h+u)} A_{n-2}^{(k+h)} + \frac{p^{n-1}((d-1)p+1)}{d} = \frac{p^{n-1}((d-1)p+1)}{d}.$$

$$\sum_{h=0}^{d-1} \frac{1}{p^{n-2}} A_{n-2}^{(k+h+u)} A_{n-2}^{(k+h)} = 0.$$

Similarly, for $j = n-3$, we get

$$\sum_{h=0}^{d-1} \frac{1}{p^{n-3}} A_{n-3}^{(k+h+u)} A_{n-3}^{(k+h)} = 0$$

Continuing in this way, we conclude that,

$$\sum_{h=0}^{d-1} A_j^{(k+h+u)} A_j^{(k+h)} = 0, \qquad \forall\ 0 \le \mathrm{j} < n-1, \qquad 0 \le \mathrm{k} \le \mathrm{d}-1.$$

Like this, using equation (2.2) and (2.5), we have

$$\sum_{h=0}^{d-1} A_j^{(k+h+u)} A_j^{(m+h)} = 0,$$

for $0 \le j < n-1,\ 0 \le k, m \le d-1.$

Also from equation (2.3) and (2.6), we obtain

$$\sum_{h=0}^{d-1} A_j^{(k+h+u)} A_{j-s}^{(m+h)} = 0,$$

for $0 \le s \le j < n-1,\ 0 \le k, m \le d-1.$

(I) Let us suppose that there exists an integer $i_s,\ \ 0 \le i_s \le d-1$ such that $A_{n-s-1}^{(i_s)} \neq 0.$

For $m = 0;\ k + u = d, d+1, \ldots, d-1$, (2.6) gives us d equations as follows:

$$A_{n-1-s}^{(0)} A_{n-1}^{(0)} + A_{n-1-s}^{(1)} A_{n-1}^{(1)} + \cdots + A_{n-1-s}^{(d-1)} A_{n-1}^{(d-1)} = 0,$$

$$A_{n-1-s}^{(0)} A_{n-1}^{(1)} + A_{n-1-s}^{(1)} A_{n-1}^{(2)} + \cdots + A_{n-1-s}^{(d-1)} A_{n-1}^{(0)} = 0,$$

$$A_{n-1-s}^{(0)} A_{n-1}^{(d-1)} + A_{n-1-s}^{(1)} A_{n-1}^{(0)} + \cdots + A_{n-1-s}^{(d-1)} A_{n-1}^{(d-2)} = 0.$$

Multiplying these equations respectively by $A_{n-1}^{(i_s+u)}, A_{n-1}^{(i_s+u+1)}, \ldots, A_{n-1}^{(i_s+u-1)}$ and then adding vertically, we get

$$A_{n-1-s}^{(0)} (A_{n-1}^{(i_s+u)} A_{n-1}^{(0)} + A_{n-1}^{(i_s+u+1)} A_{n-1}^{(1)} + \cdots + A_{n-1}^{(i_s+u-1)} A_{n-1}^{(d-1)})$$

$$+ A_{n-1-s}^{(1)} (A_{n-1}^{(i_s+u)} A_{n-1}^{(1)} + A_{n-1}^{(i_s+u+1)} A_{n-1}^{(2)} + \cdots + A_{n-1}^{(i_s+u-1)} A_{n-1}^{(0)}) +$$

.

.

.

$$+ A_{n-1-s}^{(i_s)} (A_{n-1}^{(i_s+u)} A_{n-1}^{(i_s)} + A_{n-1}^{(i_s+u+1)} A_{n-1}^{(i_s+1)} + \cdots + A_{n-1}^{(i_s+u-1)} A_{n-1}^{(i_s-1)}) +$$

.

.

.

$$+A_{n-1-s}^{(d-1)}(A_{n-1}^{(i_s+u)}A_{n-1}^{(d-1)}+A_{n-1}^{(i_s+u+1)}A_{n-1}^{(0)}+\cdots+A_{n-1}^{(i_s+u-1)}A_{n-1}^{(d-2)}) \quad =0.$$

This gives

$$A_{n-1-s}^{(0)}\sum_{h=0}^{d-1}A_{n-1}^{(i_s+h+u)}A_{n-1}^{(h)}+A_{n-1-s}^{(1)}\sum_{h=0}^{d-1}A_{n-1}^{(i_s+h+u)}A_{n-1}^{(h+1)}+\cdots$$

$$+A_{n-1-s}^{(d-1)}\sum_{h=0}^{d-1}A_{n-1}^{(i_s+h+u)}A_{n-1}^{(h-1)}+A_{n-1-s}^{(i_s)}\sum_{h=0}^{d-1}A_{n-1}^{(i_s+h+u)}A_{n-1}^{(h+i_s)}=0.$$

Using (2.5) equation

$$A_{n-1-s}^{(0)}\frac{(1-p)p^{2n-2}}{d}+A_{n-1-s}^{(1)}\frac{(1-p)p^{2n-2}}{d}+\cdots+A_{n-1-s}^{(d-1)}\frac{(1-p)p^{2n-2}}{d}$$

$$+A_{n-1-s}^{(i_s)}\sum_{h=0}^{d-1}A_{n-1}^{(i_s+h+u)}A_{n-1}^{(h+i_s)}=0.$$

Now, using (2.4) equation, we get

$$\left(\frac{p^{2n-2}(1-p)}{d}\right)\left(\sum_{\substack{k=0\\k\neq i_s}}^{d-1}A_{n-s-1}^{(k)}\right)+\frac{p^{2n-2}(d-1)p+1}{d}A_{n-s-1}^{(i_s)}=0.$$

Adding and abstracting $A_{n-s-1}^{(i_s)}$ in left brackets of above equation gives us

$$\left(\frac{p^{2n-2}(1-p)}{d}\right)\left(\sum_{k=0}^{d-1}A_{n-s-1}^{(k)}\right)-\left(\frac{p^{2n-2}(1-p)}{d}\right)A_{n-s-1}^{(i_s)}$$

$$+\frac{p^{2n-2}(d-1)p+1}{d}A_{n-s-1}^{(i_s)}=0.$$

But by Lemma 2.2.9,

$$\sum_{k=0}^{d-1}A_j^{(k)}=0, \qquad \text{for } j<n-1.$$

Thus,

$$\left(\frac{p^{2n-2}(d-1)p+1}{d}-\frac{p^{2n-2}(1-p)}{d}\right)\left(A_{n-s-1}^{(i_s)}\right)=0.$$

This implies

$$(p^{2n-2}p)A_{n-s-1}^{(i_s)}=0,$$

gives us that $A_{n-s-1}^{(i_s)}=0$ in F_l.

As $1 \leq s \leq n-1$ is arbitrary, we obtained that $A_j^{(k)}=0$ for all $0 \leq j < n-1$ and $1 \leq k \leq d-1$.

(II) For $k=0$ and $m=1,2,\ldots,d-1$, (2.4) and (2.5) gives the following d equations:

$$A_{n-1}^{(u)}A_{n-1}^{(0)}+A_{n-1}^{(u+1)}A_{n-1}^{(1)}+\cdots+A_{n-1}^{(u-1)}A_{n-1}^{(d-1)}=\frac{p^{2n-2}((d-1)p+1)}{d},$$

$$A_{n-1}^{(u)}A_{n-1}^{(1)}+A_{n-1}^{(u+1)}A_{n-1}^{(2)}+\cdots+A_{n-1}^{(u-1)}A_{n-1}^{(0)}=\frac{(1-p)p^{2n-2}}{d},$$

$$A_{n-1}^{(u)}A_{n-1}^{(2)}+A_{n-1}^{(u+1)}A_{n-1}^{(3)}+\cdots+A_{n-1}^{(u-1)}A_{n-1}^{(1)}=\frac{(1-p)p^{2n-2}}{d},$$

$$\vdots$$

$$A_{n-1}^{(u)}A_{n-1}^{(d-1)}+A_{n-1}^{(u+1)}A_{n-1}^{(0)}+\cdots+A_{n-1}^{(u-1)}A_{n-1}^{(d-2)}=\frac{(1-p)p^{2n-2}}{d}.$$

Adding and subtracting alternate equations, we get

$$\left(A_{n-1}^{(0)}-A_{n-1}^{(1)}+A_{n-1}^{(2)}-\cdots-A_{n-1}^{(d-1)}\right)\left(A_{n-1}^{(u)}-A_{n-1}^{(u+1)}+A_{n-1}^{(u+2)}-\cdots-A_{n-1}^{(u-1)}\right)$$
$$=(p)p^{2n-2}, \tag{2.7}$$

whenever d is even.

Adding and subtracting alternate equations, we get

$$\left(A_{n-1}^{(0)} - A_{n-1}^{(1)} + A_{n-1}^{(2)} - \cdots + A_{n-1}^{(d-1)}\right)\left(A_{n-1}^{(u)} - A_{n-1}^{(u+1)} + A_{n-1}^{(u+2)} - \cdots + A_{n-1}^{(u-1)}\right)$$
$$= \left(\frac{p^{2n-2}((d-1)p+1)}{d}\right), \qquad (2.8)$$

when d is odd.

If d is even, then by Lemma 2.2.5, $u = 0$ or $u = d/2$.

If u = 0, then equation (2.7) becomes

$$(A_{n-1}^{(0)} - A_{n-1}^{(1)} + A_{n-1}^{(2)} - \cdots - A_{n-1}^{(d-1)})^2 = pp^{2n-2}.$$

If $u = d/2$, then two different cases arises.

(i) If $u = d/2$ is even, then equation (2.7) becomes

$$\left(A_{n-1}^{(0)} - A_{n-1}^{(1)} + \cdots - A_{n-1}^{(d-1)}\right)\left(A_{n-1}^{(even)} - A_{n-1}^{(odd)} + \cdots - A_{n-1}^{(odd)}\right) = (p)p^{2n-2}$$

Or

$(A_{n-1}^{(0)} - A_{n-1}^{(1)} + A_{n-1}^{(2)} - \ldots - A_{n-1}^{(d-1)})^2 = pp^{2n-2}$, so that p is a quadratic residue modulo l.

Let $p = \kappa^2$.

Then

$$(A_{n-1}^{(0)} - A_{n-1}^{(1)} + A_{n-1}^{(2)} - \cdots - A_{n-1}^{(d-1)})^2 = \kappa^2 p^{2n-2}$$

or

$$A_{n-1}^{(0)} - A_{n-1}^{(1)} + A_{n-1}^{(2)} - \cdots - A_{n-1}^{(d-1)} = \kappa\, p^{n-1},$$

From Lemma 2.2.9,

$$A_{n-1}^{(0)} + A_{n-1}^{(1)} + A_{n-1}^{(2)} + \cdots + A_{n-1}^{(d-1)} = -p^{n-1}.$$

Adding above equations, we have

$$A_{n-1}^{(0)} + A_{n-1}^{(2)} + A_{n-1}^{(4)} + \cdots + A_{n-1}^{(d-2)} = \frac{(\kappa-1)p^{n-1}}{2}.$$

And subtracting above equations, we have

$$A_{n-1}^{(1)} + A_{n-1}^{(3)} + A_{n-1}^{(5)} + \cdots + A_{n-1}^{(d-1)} = -\frac{(\kappa+1)p^{n-1}}{2}.$$

(ii) If $u = d/2$ is odd, then equation (2.7) reduces to

$(A_{n-1}^{(0)} - A_{n-1}^{(1)} + A_{n-1}^{(2)} - \cdots - A_{n-1}^{(d-1)})^2 = -pp^{2n-2}$, so that p is a quadratic residue modulo l.

Let – $p = \tau^2$.Then using Lemma 2.2.9, we have

$$A_{n-1}^{(0)} + A_{n-1}^{(2)} + A_{n-1}^{(4)} + \cdots + A_{n-1}^{(d-2)} = \frac{(\tau-1)p^{n-1}}{2},$$

$$A_{n-1}^{(1)} + A_{n-1}^{(3)} + A_{n-1}^{(5)} + \cdots + A_{n-1}^{(d-1)} = -\frac{(\tau+1)p^{n-1}}{2}.$$

(III) If d is odd, then by Lemma 2.2.5, $u = 0$.

By equation (2.8), we get

$$(A_{n-1}^{(0)} - A_{n-1}^{(1)} + A_{n-1}^{(2)} - \cdots + A_{n-1}^{(d-1)})^2 = p^{2n-2}\,\frac{(p(d-1)+1)}{d},$$

so that $((d-1)p+1)/d$ is a quadratic residue modulo l.

Let $\kappa^2 = \frac{(d-1)p+1}{d}$.

Then

$$(A_{n-1}^{(0)} - A_{n-1}^{(1)} + A_{n-1}^{(2)} - \cdots + A_{n-1}^{(d-1)})^2 = \kappa^2 p^{2n-2}$$

or

$$A_{n-1}^{(0)} - A_{n-1}^{(1)} + A_{n-1}^{(2)} - \cdots + A_{n-1}^{(d-1)} = \kappa\, p^{n-1},$$

From Lemma 2.2.9,

$$A_{n-1}^{(0)} + A_{n-1}^{(1)} + A_{n-1}^{(2)} + \cdots + A_{n-1}^{(d-1)} = -p^{n-1}.$$

Adding above equations, we have

$$A_{n-1}^{(0)} + A_{n-1}^{(2)} + A_{n-1}^{(4)} + \cdots + A_{n-1}^{(d-1)} = \frac{(\kappa-1)p^{n-1}}{2}$$

and subtracting above equations, we have

$$A_{n-1}^{(1)} + A_{n-1}^{(3)} + A_{n-1}^{(5)} + \cdots + A_{n-1}^{(d-2)} = -\frac{(\kappa+1)p^{n-1}}{2}.$$

Lemma 2.3.4. For $0 \leq i \leq n-1,\ 0 \leq k \leq d-1$, then

(I) $B_i^k = 0$ if $0 \leq i < n-1$.

(II) If d is even, then

$$\sum B_{n-1}^{(k)} = \begin{cases} p^{n-1}\dfrac{(\kappa+1)}{2} & \text{if } k \text{ is even; } p = \kappa^2, \\ p^{n-1}\dfrac{(1-\kappa)}{2} & \text{if } k \text{ is odd,} \end{cases}$$

and

$$\sum B_{n-1}^{(k)} = \begin{cases} p^{n-1}\dfrac{(1-\tau)}{2} & \text{if } k \text{ is even; } -p = \tau^2, \\ p^{n-1}\dfrac{(\tau+1)}{2} & \text{if } k \text{ is odd,} \end{cases}$$

according as $d/2$ is even or odd.

(III) If d is odd, then

$$\sum B_{n-1}^{(k)} = \begin{cases} p^{n-1}\dfrac{(\kappa+1)}{2} & \text{if } k \text{ is even; } \kappa^2 = \dfrac{(d-1)p+1}{d}, \\ p^{n-1}\dfrac{(1-\kappa)}{2} & \text{if } k \text{ is odd.} \end{cases}$$

Proof. We know that

$$\theta_s(\alpha^j) = \begin{cases} 1 & \text{if } j \in C_s, \\ 0 & \text{if } j \notin C_s. \end{cases}$$

Therefore, $\theta_{g^k p^j}\left(\alpha^{g^k p^j}\right) = 1$.

Using Lemma 2.2.12, we get the value of $\sigma_{p^n}\left(\alpha^{g^k p^j}\right) = -1$,

$$\sigma_{g^h p^i}\left(\alpha^{g^k p^j}\right) = \begin{cases} -\dfrac{\varphi(p^{n-i})}{d} & \text{if } i \geq n-j, j \leq n-1, \\ \dfrac{1}{p^i} B_{i+j}^{(h+k)} & \text{if } i \leq n-j-1. \end{cases}$$

Using Lemma 2.2.11, we get the value of

$$\sigma_{2g^h p^i}\left(\alpha^{g^k p^j}\right)=\begin{cases}\dfrac{\varphi\left(p^{n-i}\right)}{d} & \text{if } i \geq n-j, j \leq n-1,\\ \dfrac{1}{p^i}A_{i+j}^{(h+k)} & \text{if } i \leq n-j-1.\end{cases}$$

Put all these values in $\theta_{g^k p^j}\left(\alpha^{g^k p^j}\right)=1$, we have

$$1=\frac{(p-1)}{2dp^{j+1}}\left(2+2\sum_{h=0}^{d-1}\sum_{i=n-j}^{n-1}\varphi(p^{n-j})\right)+\frac{1}{2p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^i}(A_{i+j}^{(k+h+u)}A_{i+j}^{(k+h)}+B_{i+j}^{(k+h+u)}B_{i+j}^{(k+h)})$$

$$=\frac{(p-1)}{dp^{j+1}}\left(1+(p^j-1)\right)+\frac{1}{2p^n}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}(A_{i+j}^{(k+h+u)}A_{i+j}^{(k+h)}+B_{i+j}^{(k+h+u)}B_{i+j}^{(k+h)}).$$

This implies

$$\frac{1}{2p^n}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}(A_{i+j}^{(k+h+u)}A_{i+j}^{(k+h)}+B_{i+j}^{(k+h+u)}B_{i+j}^{(k+h)})=1-\frac{(p-1)}{pd}.$$

This gives

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}(A_{i+j}^{(k+h+u)}A_{i+j}^{(k+h)}+B_{i+j}^{(k+h+u)}B_{i+j}^{(k+h)})=\frac{2p^{n-1}((d-1)p+1)}{d}.$$

Using (2.1), we get

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}B_{i+j}^{(k+h+u)}B_{i+j}^{(k+h)}=\frac{p^{n-1}\left((d-1)p+1\right)}{d}.$$

Further, $\theta_{g^k p^j}\left(\alpha^{g^m p^j}\right)=0$ for some $k \neq m, 0 \leq k, m \leq d-1$.

Therefore, by using Lemma 2.2.12, we get the value of $\sigma_{p^n}\left(\alpha^{g^m p^j}\right)=-1$,

$$\sigma_{g^h p^i}\left(\alpha^{g^m p^j}\right)=\begin{cases}-\dfrac{\varphi\left(p^{n-i}\right)}{d} & \text{if } i \geq n-j, j \leq n-1,\\ \dfrac{1}{p^i}B_{i+j}^{(h+m)} & \text{if } i \leq n-j-1.\end{cases}$$

Using Lemma 2.2.11, we get the value of

$$\sigma_{2g^h p^i}\left(\alpha^{g^m p^j}\right) = \begin{cases} \dfrac{\varphi\left(p^{n-i}\right)}{d} & \text{if } i \geq n-j\,, \\ \dfrac{1}{p^i} A_{i+j}^{(h+m)} & \text{if } i \leq n-j-1. \end{cases}$$

Put all these values in $\theta_{g^k p^j}\left(\alpha^{g^m p^j}\right) = 0$, we get

$$0 = \frac{(p-1)}{dp^{j+1}}\left(p^j\right) + \frac{1}{2p^n}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}\left(A_{i+j}^{(k+h+u)}A_{i+j}^{(m+h)} + B_{i+j}^{(k+h+u)}B_{i+j}^{(m+h)}\right).$$

This gives

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}\left(A_{i+j}^{(k+h+u)}A_{i+j}^{(m+h)} + B_{i+j}^{(k+h+u)}B_{i+j}^{(m+h)}\right) = \frac{2(1-p)p^{n-1}}{d}.$$

Using (2.2), we get

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}\left(B_{i+j}^{(k+h+u)}B_{i+j}^{(m+h)}\right) = \frac{(1-p)p^{n-1}}{d}.$$

Also, $\theta_{g^k p^j}\left(\alpha^{g^m p^{j-s}}\right) = 0$ for some $j \neq s, 0 \leq s < j \leq n-1, 0 \leq k, m \leq d-1$. Therefore, by using Lemma 2.2.11 and Lemma 2.2.12, we get the value of $\sigma_{p^n}\left(\alpha^{g^m p^{j-s}}\right)$, $\sigma_{g^h p^i}\left(\alpha^{g^m p^{j-s}}\right)$ and $\sigma_{2g^h p^i}\left(\alpha^{g^m p^{j-s}}\right)$.

Put all these values in $\theta_{g^k p^j}\left(\alpha^{g^m p^{j-s}}\right) = 0$, we get

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}\left(A_{i+j}^{(k+h+u)}A_{i+j-s}^{(m+h)} + B_{i+j}^{(k+h+u)}B_{i+j-s}^{(m+h)}\right) = 0.$$

Using (2.3), we get

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}\left(B_{i+j}^{(k+h+u)}B_{i+j-s}^{(m+h)}\right) = 0, \text{for } 1 \leq s \leq j.$$

Put $j = n-1$ in above equations, we get the following:

$$\sum_{h=0}^{d-1} B_{n-1}^{(k+h+u)} B_{n-1}^{(k+h)} = \frac{p^{2n-2}((d-1)p+1)}{d}, \tag{2.9}$$

$$\sum_{h=0}^{d-1} B_{n-1}^{(k+h+u)} B_{n-1}^{(m+h)} = \frac{(1-p)p^{2n-2}}{d}, \tag{2.10}$$

$$\sum_{h=0}^{d-1} B_{n-1}^{(k+h+u)} B_{n-1-s}^{(m+h)} = 0 \text{ for all } 1 \leq s \leq n-1. \tag{2.11}$$

In view of above discussion, we conclude that,

$$\sum_{h=0}^{d-1} B_{j}^{(k+h+u)} B_{j}^{(k+h)} = 0,$$

$$\sum_{h=0}^{d-1} B_{j}^{(k+h+u)} B_{j}^{(m+h)} = 0,$$

$$\sum_{h=0}^{d-1} B_{j}^{(k+h+u)} B_{j-s}^{(m+h)} = 0,$$

for $0 \leq s \leq j < n-1,\ 0 \leq k,\ m \leq d-1$.

(I) As discussed in Lemma 2.3.3, we can prove $B_j^{(k)} = 0$, for all $0 \leq j < n-1$ and $0 \leq k \leq d-1$.

(II) For $k = 0$ and $m = 1, 2, \ldots, d-1$, (2.9) and (2.10) gives the following d equations:

$$B_{n-1}^{(u)} B_{n-1}^{(0)} + B_{n-1}^{(u+1)} B_{n-1}^{(1)} + \cdots + B_{n-1}^{(u-1)} B_{n-1}^{(d-1)} = \frac{p^{2n-2}((d-1)p+1)}{d},$$

$$B_{n-1}^{(u)} B_{n-1}^{(1)} + B_{n-1}^{(u+1)} B_{n-1}^{(2)} + \cdots + B_{n-1}^{(u-1)} B_{n-1}^{(0)} = \frac{(1-p)p^{2n-2}}{d},$$

$$B_{n-1}^{(u)} B_{n-1}^{(2)} + B_{n-1}^{(u+1)} B_{n-1}^{(3)} + \cdots + B_{n-1}^{(u-1)} B_{n-1}^{(1)} = \frac{(1-p)p^{2n-2}}{d},$$

.

.

.

$$B_{n-1}^{(u)}B_{n-1}^{(d-1)} + B_{n-1}^{(u+1)}B_{n-1}^{(0)} + \cdots + B_{n-1}^{(u-1)}B_{n-1}^{(d-2)} = \frac{(1-p)p^{2n-2}}{d}.$$

Adding and subtracting alternate equations, we get

$$\left(B_{n-1}^{(0)} - B_{n-1}^{(1)} + B_{n-1}^{(2)} - \cdots - B_{n-1}^{(d-1)}\right)\left(B_{n-1}^{(u)} - B_{n-1}^{(u+1)} + B_{n-1}^{(u+2)} - \cdots - B_{n-1}^{(u-1)}\right) = (p)p^{2n-2}, \quad (2.12)$$

when d is even.

Adding and subtracting alternate equations, we get

$$\left(B_{n-1}^{(0)} - B_{n-1}^{(1)} + B_{n-1}^{(2)} - \cdots + B_{n-1}^{(d-1)}\right)\left(B_{n-1}^{(u)} - B_{n-1}^{(u+1)} + B_{n-1}^{(u+2)} - \cdots + B_{n-1}^{(u-1)}\right) = p^{2n-2}\frac{(p(d-1)+1)}{2}, \quad (2.13)$$

when d is odd.

If d is even, then by Lemma 2.2.5, $u = 0$ or $u = d/2$.

If $u = 0$, then equation (2.12) becomes

$$(B_{n-1}^{(0)} - B_{n-1}^{(1)} + B_{n-1}^{(2)} - \cdots - B_{n-1}^{(d-1)})^2 = pp^{2n-2}.$$

If $u = d/2$, then two different cases arises.

(i) If $u = d/2$ is even, then equation (2.12) becomes

$$(B_{n-1}^{(0)} - B_{n-1}^{(1)} + B_{n-1}^{(2)} - \cdots - B_{n-1}^{(d-1)})^2 = pp^{2n-2}.$$

Let p = κ^2.

Then using Lemma 2.2.10, we have

$$+B_{n-1}^{(0)} + B_{n-1}^{(2)} + B_{n-1}^{(4)} + \cdots + B_{n-1}^{(d-2)} = \frac{(\kappa+1)p^{n-1}}{2},$$

$$B_{n-1}^{(1)} + B_{n-1}^{(3)} + B_{n-1}^{(5)} + \cdots + B_{n-1}^{(d-1)} = \frac{(1-\kappa)p^{n-1}}{2}.$$

(ii) If $u = d/2$ is odd, then equation (2.12) reduces to

$$(B_{n-1}^{(0)} - B_{n-1}^{(1)} + B_{n-1}^{(2)} - \cdots - B_{n-1}^{(d-1)})^2 = -pp^{2n-2}.$$

Let – p = τ^2. Then using Lemma 2.2.10, we have

$$B_{n-1}^{(0)} + B_{n-1}^{(2)} + B_{n-1}^{(4)} + \cdots + B_{n-1}^{(d-2)} = \frac{(1-\tau)p^{n-1}}{2},$$

$$B_{n-1}^{(1)} + B_{n-1}^{(3)} + B_{n-1}^{(5)} + \cdots + B_{n-1}^{(d-1)} = \frac{(1+\tau)p^{n-1}}{2}.$$

(iii) If d is odd, then by Lemma 2.2.5, $u = 0$.

By equation (2.13), we get

$$(B_{n-1}^{(0)} - B_{n-1}^{(1)} + B_{n-1}^{(2)} - \cdots + B_{n-1}^{(d-1)})^2 = p^{2n-2}\frac{(p(d-1)+1)}{d},$$

so that $\frac{(p(d-1)+1)}{d}$ ia quadratic residue modulo l.

Let $\kappa^2 = \frac{(p(d-1)+1)}{d}$. Then using Lemma 2.2.10, we have

$$B_{n-1}^{(0)} + B_{n-1}^{(2)} + B_{n-1}^{(4)} + \cdots + B_{n-1}^{(d-1)} = \frac{(\kappa+1)p^{n-1}}{2},$$

$$B_{n-1}^{(1)} + B_{n-1}^{(3)} + B_{n-1}^{(5)} + \cdots + B_{n-1}^{(d-2)} = \frac{(1-\kappa)p^{n-1}}{2}.$$

2.4 Dimension, Generating Polynomial and Minimum Distance of Minimal Cyclic Codes of Length $2p^n$

The dimension of minimal cyclic code $\mathcal{C}_s$ is the number of non-zeros of the generating idempotent θ_s; which is the cardinality of the cyclotomic coset C_s that is $\dim(\mathcal{C}_s) = |C_s|$. We denote the minimum distance of $\mathcal{C}_s$ by $d(\mathcal{C}_s)$.

Lemma 2.4.1. If C is the cyclic code of length m generated by $g(x)$ and is of minimum distance d, then the code $\boldsymbol{\mathcal{C}}$ is of length mk generated by $g(x)(1 + x^m + x^{2m} + \cdots + x^{(k-1)m})$ is a repetition code of C repeated k times and minimum distance is kd.

Proof. Trivial.

Theorem 2.4.2. $\mathcal{C}_0$ and $\mathcal{C}_{p^n}$ are equivalent codes, each of length $2p^n$, dimension 1 and minimum distance $2p^n$.

Proof. Clearly, the minimal polynomial of $\alpha^0 = 1$ is $x - 1$, therefore the generating

polynomial of $\mathcal{C}_0$ is $\frac{x^{2p^n}-1}{x-1} = 1 + x + x^2 + \cdots + x^{2p^n-1}$ and the minimal polynomial of α^{p^n} is $x + 1$. Therefore, the generating polynomial of $\mathcal{C}_{p^n}$ is

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

These obviously imply that $\mathcal{C}_0$ and $\mathcal{C}_{p^n}$ are equivalent codes, each of length $2p^n$, dimension 1 and minimum distance $2p^n$.

Theorem 2.4.3. Each $\mathcal{C}_{2g^k p^j}$ for $0 \leq j \leq n-1$ and $0 \leq k \leq d-1$ are equivalent codes of length $2p^n$ and minimum distance at least $4p^j$.

Proof. We observe that,

$$\prod_{k=0}^{d-1} M^{2g^k p^j}(x) = (1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \cdots + x^{(p-1)p^{n-j-1}}).$$

Also, $x^{2p^n} - 1 = \left(x^{p^{n-j}} - 1\right)(1 + x^{p^{n-j}} + x^{2p^{n-j}} + \cdots + x^{(2p^j-1)p^{n-j}})$

$= \left(x^{p^{n-j-1}} - 1\right)(1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \cdots + x^{(p-1)p^{n-j-1}})(1 + x^{p^{n-j}} + x^{2p^{n-j}} + \cdots + x^{(2p^j-1)p^{n-j}})$.

Therefore, we have

$$\frac{x^{2p^n}-1}{\prod_{k=0}^{d-1} M^{2g^k p^j}(x)} = \left(x^{p^{n-j-1}} - 1\right)\left(1 + x^{p^{n-j}} + x^{2p^{n-j}} + \cdots + x^{(2p^j-1)p^{n-j}}\right).$$

Let χ_j be the code of length p^{n-j} over F_l generated by $\left(x^{p^{n-j-1}} - 1\right)$. Then the minimum distance of χ_j is 2. By definition 1.4.24, Sahni and Sehgal [95], we have a multiplier mapping μ_g such that $\theta_{2g^{k+1}p^j}(x) = \mu_{g^{-1}}(\theta_{2g^k p^j}(x))$ i.e. $\mu_g\left(\theta_{2g^{k+1}p^j}(x)\right) = \theta_{2g^k p^j}(x)$.

Thus, $\mu_{g^m}\left(\theta_{2g^{k+m}p^j}(x)\right) = \theta_{2g^k p^j}(x)$ for all $k, m, 0 \leq k, m \leq d-1$. Therefore, for a fixed j, the generating idempotents $\theta_{2g^k p^j}(x)$, $0 \leq k \leq d-1$, are images of each other under the multiplier μ_g proving that the minimal codes $\mathcal{C}_{2g^k p^j}$, $0 \leq k \leq d-1$, are all permutation equivalent codes by using Theorem 1.4.23.

Also as the minimum distance of permutation equivalent codes is the same, the minimal codes $\mathcal{C}_{2g^k p^j}$, $0 \leq k \leq d-1$, have equal minimum distance.

Let χ_j^* be the cyclic code of length $2p^n$, generated by $\frac{x^{2p^n}-1}{\prod_{k=0}^{d-1} M^{2g^k p^j}(x)}$.

Then χ_j^* is a repetition code of χ_j repeated $2p^j$ times and by Lemma 2.4.1, its minimum distance is $4p^j$. Further, $\chi_j^* = \bigoplus_{k=0}^{d-1} \mathcal{C}_{2g^k p^j}$. The minimal cyclic codes $\mathcal{C}_{2g^k p^j}$ being sub codes of χ_j^* have minimum distance at least $4p^j$.

Theorem 2.4.4. Each $\mathcal{C}_{g^k p^j}$, for $0 \leq j \leq n-1$ and $0 \leq k \leq d-1$ are equivalent codes of length $2p^n$ and minimum distance at least $4p^j$.

Proof. Similar as Theorem 2.4.3.

2.5 Some Examples

Example 2.5.1. Let $p = 11$, $n = 1$, $l = 3$. Then length of the cyclic code is 22, $g = 7$ and $d = 2$.

The cyclotomic cosets modulo 22 are given by:

$$C_0 = \{0\}, \quad C_{11} = \{11\}, \quad C_1 = \{1,3,5,9,15\}, \quad C_2 = \{2,6,8,10,18\}$$
$$C_7 = \{7,13,17,19,21\}, \quad C_{14} = \{4,12,14,16,20\}.$$

Explicit expressions for the primitive idempotents of the irreducible cyclic code of length 22 are given by:

$$\theta_0(x) = 1 + x + x^2 + \cdots + x^{21}$$
$$\theta_1(x) = 2 + \sigma_1(x) + \sigma_{11}(x) - \sigma_{14}(x)$$
$$\theta_2(x) = 2 - \sigma_7(x) - \sigma_{11}(x) - \sigma_{14}(x)$$
$$\theta_7(x) = 2 - \sigma_2(x) + \sigma_7(x) + \sigma_{11}(x)$$
$$\theta_{11}(x) = 1 - \sigma_1(x) + \sigma_2(x) - \sigma_7(x) - \sigma_{11}(x) - \sigma_{14}(x)$$
$$\theta_{14}(x) = 2 - \sigma_1(x) - \sigma_2(x) - \sigma_{11}(x)$$

The minimal ternary cyclic codes of length 22 have the following parameters:

Code	Dimension	Minimum Distance	Generating Polynomial
$\mathcal{C}_0$	1	22	$1 + x + x^2 + \ldots + x^{21}$
$\mathcal{C}_{11}$	1	22	$1 - x + x^2 - \ldots + x^{21}$

χ_j^*	10	4	$(x-1)(1+x^{11})$
χ_j^{**}	10	4	$(x-1)(1-x^{11})$

Note that $\mathcal{C}_2$, $\mathcal{C}_{14}$ and $\mathcal{C}_1$, $\mathcal{C}_7$ are sub codes of χ_j^* and χ_j^{**} respectively.

Example 2.5.2.

Let $p = 13$, $n = 1$, $l = 5$. Then length of the minimal cyclic code is 26, $g = 7$, $A_0^{(0)} = 4, B_0^{(0)} = 3$, $A_0^{(1)} = 3, B_0^{(1)} = 2$, $A_0^{(2)} = 2, B_0^{(2)} = 1$ and $d = 3$.

The cyclotomic cosets modulo 26 are given by:

$C_0 = \{0\}$, $C_{13} = \{13\}$, $C_1 = \{1, 5, 25, 8\}$,

$C_2 = \{2, 10, 24, 16\}$, $C_{23} = \{3, 15, 23, 11\}$,

$C_7 = \{9, 19, 17, 7\}$, $C_{20} = \{6, 4, 20, 22\}$,

$C_{14} = \{18, 12, 8, 14\}$.

Explicit expressions for the primitive idempotents of the irreducible (minimal) cyclic code of length 26 are given by:

$\theta_0(x) = 1 + x + x^2 + \cdots + x^{25}$.

$\theta_{13}(x) = 1 + 4\,\sigma_{13}(x) + \sigma_2(x) + 4\sigma_1(x) + \sigma_{14}(x) + 4\sigma_7(x) + \sigma_{20}(x) + 4\sigma_{23}(x)$.

$\theta_1(x) = 1 + 4\,\sigma_{13}(x) + \sigma_2(x) + 4\sigma_1(x) + \sigma_{14}(x) + 4\sigma_7(x) + \sigma_{20}(x) + 4\sigma_{23}(x) + \sum_{h=0}^{2}(B_0^{(h)}\,\sigma_{7^h}(x) + A_0^{(h)}\,\sigma_{2.7^h}(x))$.

$\theta_7(x) = 1 + 4\,\sigma_{13}(x) + \sigma_2(x) + 4\sigma_1(x) + \sigma_{14}(x) + 4\sigma_7(x) + \sigma_{20}(x) + 4\sigma_{23}(x) + \sum_{h=0}^{2}(B_0^{(1+h)}\,\sigma_{7^h}(x) + A_0^{(1+h)}\,\sigma_{2.7^h}(x))$.

$\theta_{23}(x) = 1 + 4\,\sigma_{13}(x) + \sigma_2(x) + 4\sigma_1(x) + \sigma_{14}(x) + 4\sigma_7(x) + \sigma_{20}(x) + 4\sigma_{23}(x) + \sum_{h=0}^{2}(B_0^{(2+h)}\,\sigma_{7^h}(x) + A_0^{(2+h)}\,\sigma_{2.7^h}(x))$.

$\theta_2(x) = 1 + \sigma_1(x) + \sigma_{13}(x) + \sigma_2(x) + \sigma_7(x) + \sigma_{14}(x) + \sigma_{20}(x) + \sigma_{23}(x) + \sum_{h=0}^{2} A_0^{(h)}\,(\sigma_{7^h}(x) + \sigma_{2.7^h}(x))$.

$\theta_{14}(x) = 1 + \sigma_1(x) + \sigma_{13}(x) + \sigma_2(x) + \sigma_7(x) + \sigma_{14}(x) + \sigma_{20}(x) + \sigma_{23}(x) + \sum_{h=0}^{2} A_0^{(h+1)}\,(\sigma_{7^h}(x) + \sigma_{2.7^h}(x))$.

$\theta_{20}(x) = 1 + \sigma_1(x) + \sigma_{13}(x) + \sigma_2(x) + \sigma_7(x) + \sigma_{14}(x) + \sigma_{20}(x) + \sigma_{23}(x)$

$+ \sum_{h=0}^{2} A_0^{(h+2)} (\sigma_{7^h}(x) + \sigma_{2.7^h}(x))$.

The minimal cyclic codes of length 26 have the following parameters:

Code	Dimension	Minimum Distance	Generating Polynomial
$\mathcal{C}_0$	1	26	$1 + x + x^2 + \cdots + x^{25}$
$\mathcal{C}_{13}$	1	26	$1 - x + x^2 - \cdots + x^{25}$
χ_j^*	12	4	$(x-1)(1+x^{13})$
χ_j^{**}	12	4	$(x-1)(1-x^{13})$

Since $\mathcal{C}_2$, $\mathcal{C}_{14}, \mathcal{C}_{20}$ and $\mathcal{C}_1$, $\mathcal{C}_7, \mathcal{C}_{23}$ are sub codes of χ_j^* and χ_j^{**} respectively, therefore, their minimum distance is at least 4.