AIMS Mathematics, 11(4): 10049–10078.
DOI: 10.3934/math.2026415
Received: 19 December 2025
Revised: 08 March 2026
Accepted: 18 March 2026
Published: 14 April 2026

https://www.aimspress.com/journal/Math

Research article

Cyclotomy, cyclotomic cosets and arithmetic properties of some families in $\frac{\mathbb{F}_l[x]}{\langle x^{p^s q^t}-1\rangle}$

Juncheng Zhou and Hongfeng Wu*

College of Science, North China University of Technology, Beijing 100144, China

* **Correspondence:** Email: whfmath@ncut.edu.cn.

Abstract: Arithmetic properties of some families in $\mathbb{F}_l[x]/\langle x^{p^s q^t}-1\rangle$ were obtained by using the cyclotomic classes of order 2 with respect to $n = p^s q^t$, where $p \equiv 3 \bmod 4$, $\gcd(\phi(p^s), \phi(q^t)) = 2$, l is a primitive root modulo q^t, and $\mathrm{ord}_{p^s}(l) = \phi(p^s)/2$. The form of these cyclotomic classes enabled us to further generalize the results obtained in [1]. The explicit expressions of primitive idempotents of minimal ideals in $\mathbb{F}_l[x]/\langle x^{p^s q^t}-1\rangle$ were also obtained.

Keywords: cyclotomy; cyclotomic cosets; cyclotomic numbers; cyclic codes; finite fields
Mathematics Subject Classification: 11T71, 11T23, 94B15

1. Introduction

The theory of cyclotomy is a significant tool in the research of codes. Classical cyclotomy is cyclotomy with respect to an odd prime. C. Ding and T. Helleseth [2] introduced a generalized cyclotomy of order 2 with respect to a composite number n and includes classical cyclotomy as a special case. The last two decades have witnessed a lot of research on cyclic codes by using the theory of cyclotomy [3].

Let $\mathbb{F}_l$ be a finite field of order l, where l is a prime. A cyclic code of length n over $\mathbb{F}_l$ is viewed as an ideal in the ring $\mathbb{F}_l[x]/\langle x^n-1\rangle$, where $\gcd(n, l) = 1$. It is well known that an ideal in $\frac{\mathbb{F}_l[x]}{\langle x^n-1\rangle}$ can be written as a direct sum of minimal ideals. Further, each minimal ideal (minimal cyclic code) is generated by a primitive idempotent. Thus it is useful to obtain the explicit expressions for primitive idempotents in $\mathbb{F}_l[x]/\langle x^n-1\rangle$.

A lot of papers have investigated cyclic codes and their primitive idempotents by using the theory of cyclotomy. In [2], generalized cyclotomy of order 2 was applied for constructing codes of length $n = p_1^{e_1} \cdots p_t^{e_t}$ with each p_i being an odd prime. In [4], Ding studied the codes of length pq over $\mathbb{F}_l$ by using generalized cyclotomy, where l is a quadratic residue modulo with both p and q.

In [5], R. Singh and M. Prunthi obtain the explicit expressions of the primitive of the irreducible quadratic residue cyclic codes of length p^sq^t and $\text{ord}_{p^s}(l) = \phi(p^s)/2$, $\text{ord}_{q^t}(l) = \phi(q^t)/2$, which in fact generalizes C. Ding's results. In [6], F. Li and Q. Yue investigated irreducible cyclic codes of length $n = p^sq^t$ over $\mathbb{F}_l$ with $pq \mid l-1$. In [7], Z. Shi and F. Fu found the primitive idempotents of irreducible constacyclic codes and Linear codes with complementary-duals(LCD) cyclic codes of length $n = p^sq^t$ over $\mathbb{F}_l$ with $\gcd(pq, l(l-1)) = 1$. In [8], G.K. Backshi and M. Raka obtained minimal cyclic codes of length p^sq, where l is a primitive root of both p^s and q, and $\gcd(\phi(p)/2, \phi(q)/2) = 1$. In [9], A. Sahni and P.T. Sehgal also investigated minimal cyclic codes of length p^sq, where l is a primitive root of both p^s and q, and $\gcd(\phi(p), \phi(q)) = d$.

S. Jain, S. Betra, and K. Kmar considered a case different from all of the research above. In [1, 10, 11], p, q are distinct odd primes, $p \equiv 3 \pmod 4$, and $\gcd(\phi(p^s), \phi(q^t)) = 2$. l is a primitive root modulo q and $\text{ord}_{p^s}(l) = \phi(p^s)/2$. However, S. Jain et al. only investigated primitive idempotents when $n = pq$. Arithmetic properties of some families and primitive idempotents in $\frac{\mathbb{F}_l[x]}{\langle x^{p^sq^t}-1\rangle}$, where l is a primitive root modulo q^t and $\text{ord}_{p^s}(l) = \phi(p^s)/2$, were unstudied.

In this paper, we first generalize the results of S. Jain et al. and obtained the arithmetic properties of some families in $\frac{\mathbb{F}_l[x]}{\langle x^{p^sq^t}-1\rangle}$, where p, q are distinct odd primes, $p \equiv 3 \bmod 4$, $\gcd(\phi(p^s), \phi(q^t)) = 2$, $\text{ord}_{p^s}(l) = \phi(p^s)/2$, and $\text{ord}_{q^t}(l) = \phi(q^t)$. In Section 2, we give the cyclotomic classes of order 2 and write l-cyclotomic cosets modulo p^sq^t in an additive form in order to facilitate the following study. In Section 3, we calculate the cyclotomic number of order 2 and investigate relationships between cyclotomic cosets.

In Section 4, we investigate arithmetic properties of the polynomials in the ring $\frac{\mathbb{F}_l[x]}{\langle x^{p^sq^t}-1\rangle}$ that have the form

$$\chi_\gamma = \sum_{i \in C_\gamma} x^i,$$

where C_γ is the cyclotomic coset containing γ. The results in Section 3 will be used to prove the theorems in Section 4. For convenience, the lemmas in Section 3 and theorems in Section 4 are one-to-one, that is, Lemma 3. $(X+1) \to$ Theorem 4. X, for $1 \leqslant X \leqslant 16$.

In Section 5, we calculate the explicit expressions of primitive idempotents. Theorem 6 in Chapter 8 of [12] gives the expressions over $\mathbb{F}_2$, and G.K. Bassi and M. Raka [8] generalized it into $\mathbb{F}_l$ for any primes. By classifying the p^sq^t-th roots of a unit, we can see that primitive idempotents can be written in the form of a linear combination of χ_γ, which is defined in Section 4. We then obtain the explicit expressions of primitive idempotents of minimal ideals in $\frac{\mathbb{F}_l[x]}{\langle x^{p^sq^t}-1\rangle}$.

The terminology and assumptions throughout this paper are as follows:

(1) p, q, l are three distinct primes with p and q odd and $p \equiv 3 \pmod 4$.

(2) $\mathbb{Z}_m^*$ denotes the set of units modulo m, for any positive integer m.

(3) $\text{ord}_m(k)$ denotes the multiplicative order of k modulo m and $\phi(\cdot)$ denotes Euler's phi function.

(4) $\text{ord}_{p^s}(l) = \phi(p^s)/2$, $\text{ord}_{q^t}(l) = \phi(q^t)$, and $\gcd(\phi(p^s), \phi(q^t)) = 2$.

(5) R_k denotes the set of quadratic residues in $\mathbb{Z}_{p^k}^*$ and N_k denotes the set of quadratic nonresidues in $\mathbb{Z}_{p^k}^*$. It is easy to find that

$$R_k = \{x + p\lambda : x \in R_1, 0 \leqslant \lambda \leqslant p^{k-1} - 1\}$$

and

$$N_k = \{x + p\lambda : x \in N_1, 0 \leqslant \lambda \leqslant p^{k-1} - 1\}.$$

2. Cyclotomic classes of order 2 and l-cyclotomic cosets modulo $p^s q^t$

2.1. l-cyclotomic cosets

In this section, we obtain all the l-cyclotomic cosets modulo $n = p^s q^t$, when $\text{ord}_{p^s}(l) = \phi(p^s)/2$, $\text{ord}_{q^t}(l) = \phi(q^t)$, and $\gcd(\phi(p^s), \phi(q^t)) = 2$. To obtain these cosets, we first prove some results.

Definition 2.1. *The l-cyclotomic coset modulo n containing γ denoted by C_γ is defined as*

$$C_\gamma = \{\gamma l^i \bmod n : i = 0, 1, \cdots, \tau - 1\},$$

where τ is the least positive integer such that

$$\gamma l^\tau \equiv \gamma \bmod n.$$

We know that these cyclotomic cosets partition the set $\{0, 1, \cdots, n-1\}$. A subset $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ of $\mathbb{Z}_n$ is said to be a complete set of representative l-cyclotomic cosets modulo n if $C_{\gamma_1}, C_{\gamma_2}, \cdots, C_{\gamma_m}$ are distinct and

$$\bigcup_{i=1}^{m} C_{\gamma_i} = \mathbb{Z}_n.$$

Lemma 2.2 ([1], Lemma 2.1, p. 3)**.** $\text{ord}_n(l) = \phi(n)/2$.

Lemma 2.3 ([1], Lemma 2.2, p. 3)**.** *If g is a primitive root modulo q^t, then g is also a primitive root modulo q^{t-j} with $0 \leqslant j < t$.*

Lemma 2.4 ([1], Lemma 2.3, p. 3)**.** *If $\text{ord}_{p^s}(l) = \phi(p^s)/2$, then $\text{ord}_{p^{s-i}}(l) = \phi(p^{s-i})/2$ with $0 \leqslant i < s$.*

Now we will find all the l-cyclotomic cosets modulo $p^s q^t$ using the results above.

Theorem 2.5. *There are $(2s + 1)(t + 1)$ l-cyclotomic cosets modulo $p^s q^t$, which are given as follows:*

$$\begin{aligned}
&C_0 = \{0\};\\
&C_{p^s q^j} = \{p^s q^j l^m : 0 \leqslant m \leqslant \phi(q^{t-j}) - 1\}, \quad 0 \leqslant j \leqslant t - 1;\\
&C_{p^i q^j} = \{p^i q^j l^m : 0 \leqslant m \leqslant \phi(p^{s-i} q^{t-j})/2 - 1\}, \quad 0 \leqslant i \leqslant s - 1, 0 \leqslant j \leqslant t;\\
&C_{p^i q^j g} = \{p^i q^j g l^m : 0 \leqslant m \leqslant \phi(p^{s-i} q^{t-j})/2 - 1\}, \quad 0 \leqslant i \leqslant s - 1, 0 \leqslant j \leqslant t,
\end{aligned}$$

where g is a common primitive root of both p^s and q^t.

Proof. Obviously, the sets given above are distinct. Also,

$$\#C_0 + \sum_{j=0}^{t-1} \#C_{p^s q^j} + \sum_{i=0}^{s-1} \sum_{j=0}^{t} \#C_{p^i q^j} + \sum_{i=0}^{s-1} \sum_{j=0}^{t} \#C_{p^i q^j g} = n,$$

which implies that these are all the l-cyclotomic cosets modulo n, and hence this proves the results. □

2.2. Cyclotomic classes of order 2

In this section, we will try to write l-cyclotomic cosets in Theorem 2.5 in an addictive form, which will make our subsequent calculations more convenient.

Lemma 2.6 ([13], Theorem 8.10, p. 162)**.** *An integer $n > 1$ has a primitive root if and only if $n = 2, 4, p^s$, or $2p^s$ for some odd prime p.*

Let g_1 and g_2 be the primitive roots modulo p^s and q^t, respectively, and g be the solution of simultaneous congruences

$$g \equiv g_1 \bmod p^s,$$
$$g \equiv g_2 \bmod q^t.$$

Then the existence of g is guaranteed by the Chinese remainder theorem. g is a common primitive root of both p^s and q^t.

Further, let v be the solution of simultaneous congruences

$$v \equiv 1 \bmod p^s,$$
$$v \equiv g \bmod q^t.$$

Then the cyclotomic classes of order 2 with respect to $p^s q^t$ are given by

$$D_0^{p^s q^t} = \left\{ g^{2i} : i = 0, 1, \cdots, \frac{\phi(p^s q^t)}{4} - 1 \right\} \cup \left\{ g^{2i} v : i = 0, 1, \cdots, \frac{\phi(p^s q^t)}{4} - 1 \right\},$$

and

$$D_1^{p^s q^t} = g D_0^{p^s q^t}.$$

Lemma 2.7 ([14], Theorem 83)**.** *An integer a is a quadratic residue modulo with an odd prime p if and only if $a^{\phi(p)/2} \equiv 1 \bmod p$.*

Lemma 2.8. *Let p be an odd prime and a be an integer coprime with p, Then a is a quadratic residue modulo p^s if and only if a is a quadratic residue modulo p.*

Proof. Obviously, a is a quadratic residue modulo p if a is a quadratic residue modulo p^s. If a is an quadratic residue modulo p^i, there exists an integer b such that $b^2 \equiv a \bmod p^i$. We claim that there exists an integer $k \in \{0, 1, \cdots, p-1\}$ such that $(b + kp^i)^2 \equiv a \bmod p^{i+1}$ for $(2, p) = 1$, and hence this proves the result. □

Lemma 2.9. *Let p and q be two distinct odd primes. If x runs through reduced residue system modulo q^t and y runs through reduced residue system modulo p^s, then the set $\{p^s x + q^t y\}$ containing $\phi(p^s)\phi(q^t)$ number of integers forms the reduced residue system modulo $p^s q^t$.*

Proof. Obviously, elements in the set $\{p^s x + q^t y\}$ are coprime with both p and q. If $p^s x + q^t y = p^s x' + q^t y'$, then $p^s(x - x') = -q^t(y - y')$. For p, q to be distinct, $x \equiv x' \bmod q^t$ and $y \equiv y' \bmod p^s$. Also, since there are exactly $\phi(p^s)\phi(q^t)$ elements in the reduced residue system modulo $p^s q^t$, the result is proved. □

Theorem 2.10. *Let $v \equiv 1 \bmod p^s$ and $v \equiv g \bmod q^t$, and then:*

(i) If q is a quadratic residue modulo p, then

$$D_0^{p^s q^t} = \left\{q^t x + p^s y : x \in R_s, y \in \mathbb{Z}_{q^t}^*\right\}$$

and

$$D_1^{p^s q^t} = \left\{q^t x + p^s y : x \in N_s, y \in \mathbb{Z}_{q^t}^*\right\}.$$

(ii) If q is a quadratic nonresidue modulo p, then

$$D_0^{p^s q^t} = \left\{q^t x + p^s y : x \in N_s, y \in \mathbb{Z}_{q^t}^*\right\},$$
$$D_1^{p^s q^t} = \left\{q^t x + p^s y : x \in R_s, y \in \mathbb{Z}_{q^t}^*\right\},$$

if $2 \nmid t$ and

$$D_0^{p^s q^t} = \left\{q^t x + p^s y : x \in R_s, y \in \mathbb{Z}_{q^t}^*\right\},$$
$$D_1^{p^s q^t} = \left\{q^t x + p^s y : x \in N_s, y \in \mathbb{Z}_{q^t}^*\right\},$$

if $2 \mid t$.

Proof. We only prove the first result, and the second result can be proved similarly. By the definition of $D_0^{p^s q^t}$, elements in $D_0^{p^s q^t}$ are all quadratic residue modulo p^s and $D_0^{p^s q^t} (\mathrm{mod}\, p^s)$ contains $\phi(q^t)$ copies of R_s. Similarly, $D_1^{p^s q^t} (\mathrm{mod}\, p^s)$ contains $\phi(q^t)$ copies of N_s.

Let $\omega_r = \{q^t x + p^s y : x \in R_s, y \in \mathbb{Z}_{q^t}^*\}$ and $\omega_n = \{q^t x + p^s y : x \in N_s, y \in \mathbb{Z}_{q^t}^*\}$, and then by Lemma 2.9, $\omega_r \sqcup \omega_g = \mathbb{Z}_{p^s q^t}^*$. If q is a quadratic residue modulo p, then $\omega_r (\mathrm{mod} p^s)$ contains $\phi(q^t)$ copies of R_s and $\omega_n (\mathrm{mod} p^s)$ contains $\phi(q^t)$ copies of N_s. So $\omega_r = D_0^{p^s q^t}$ and $\omega_n = D_1^{p^s q^t}$. □

Lemma 2.11. *$C_1 = D_0^{p^s q^t}$ and $C_g = D_1^{p^s q^t}$.*

Proof. By Lemma 2.7, l is a quadratic residue modulo p. Since $\mathrm{ord}_{p^s q^t} = \phi(p^s q^t)/2$, we can see that $C_1 (\mathrm{mod} p^s)$ contains $\phi(q^t)$ copies of R_s and $C_g (\mathrm{mod} p^s)$ contains $\phi(q^t)$ copies of N_s. Also, $C_1 \sqcup C_g = \mathbb{Z}_{p^s q^t}^*$, so we have $C_1 = D_0^{p^s q^t}$ and $C_g = D_1^{p^s q^t}$. □

Now we can give the main result of this setion below.

Theorem 2.12. *The l-cyclotomic coset obtained in Theorem 2.5 can also be represented as follows:*

(i) If q is a quadratic residue modulo p, then

$$\begin{aligned}
&C_0 = \{0\};\\
&C_{p^i q^j} = \left\{p^i q^t x + p^s q^j y : x \in R_{s-i}, q \in \mathbb{Z}_{q^{t-j}}^*\right\}, \quad 0 \leqslant i \leqslant s-1, 0 \leqslant j \leqslant t-1;\\
&C_{p^i q^t} = \left\{p^i q^t x : x \in R_{s-i}\right\}, \quad 0 \leqslant i \leqslant s-1;\\
&C_{p^i q^j g} = \left\{p^i q^t x + p^s q^j y : x \in N_{s-i}, q \in \mathbb{Z}_{q^{t-j}}^*\right\}, \quad 0 \leqslant i \leqslant s-1, 0 \leqslant j \leqslant t-1;\\
&C_{p^i q^t g} = \left\{p^i q^t x : x \in N_{s-i}\right\}, \quad 0 \leqslant i \leqslant s-1;\\
&C_{p^s q^j} = \left\{p^s q^j y : y \in \mathbb{Z}_{q^{t-j}}^*\right\}, \quad 0 \leqslant j \leqslant t-1.
\end{aligned}$$

(ii) If q is a quadratic nonresidue modulo p, then

$$\begin{aligned}
&C_0 = \{0\};\\
&C_{p^iq^j} = \left\{p^iq^tx + p^sq^jy : x \in N_{s-i}, q \in \mathbb{Z}^*_{q^{t-j}}\right\}, \quad 0 \leqslant i \leqslant s-1, 0 \leqslant j \leqslant t-1, 2 \nmid t-j;\\
&C_{p^iq^j} = \left\{p^iq^tx + p^sq^jy : x \in R_{s-i}, q \in \mathbb{Z}^*_{q^{t-j}}\right\}, \quad 0 \leqslant i \leqslant s-1, 0 \leqslant j \leqslant t-1, 2 \mid t-j;\\
&C_{p^iq^t} = \left\{p^iq^tx : x \in R_{s-i}\right\}, \quad 0 \leqslant i \leqslant s-1;\\
&C_{p^iq^jg} = \left\{p^iq^tx + p^sq^jy : x \in R_{s-i}, q \in \mathbb{Z}^*_{q^{t-j}}\right\}, \quad 0 \leqslant i \leqslant s-1, 0 \leqslant j \leqslant t-1, 2 \nmid t-j;\\
&C_{p^iq^jg} = \left\{p^iq^tx + p^sq^jy : x \in N_{s-i}, q \in \mathbb{Z}^*_{q^{t-j}}\right\}, \quad 0 \leqslant i \leqslant s-1, 0 \leqslant j \leqslant t-1, 2 \mid t-j;\\
&C_{p^iq^tg} = \left\{p^iq^tx : x \in N_{s-i}\right\}, \quad 0 \leqslant i \leqslant s-1;\\
&C_{p^sq^j} = \left\{p^sq^jy : y \in \mathbb{Z}^*_{q^{t-j}}\right\}, \quad 0 \leqslant j \leqslant t-1.
\end{aligned}$$

Proof. Note that

$$C_{p^iq^j} = p^iq^jD_0^{p^{s-i}q^{t-j}} \text{ and } C_{p^iq^jg} = p^iq^jD_1^{p^{s-i}q^{t-j}},$$

and then it can be proved easily using Lemma 2.11. □

3. Cyclotomic number of order 2

Lemma 3.1. *Let p be a prime of the form $4k-1$, and then*

(i) For any $r \in R_s$, we have

$$\#(r+R_s)\cap R_s = \#(r+N_s)\cap R_s = \#(r+N_s)\cap N_s = \frac{p-3}{4}p^{s-1},$$

and

$$\#(r+R_s)\cap N_s = \frac{p+1}{4}p^{s-1}.$$

(ii) For any $n \in N_s$, we have

$$\#(n+N_s)\cap N_s = \#(n+R_s)\cap R_s = \#(n+R_s)\cap N_s = \frac{p-3}{4}p^{s-1},$$

and

$$\#(n+N_s)\cap R_s = \frac{p+1}{4}p^{s-1}.$$

Proof. We only prove the first result, and the second one can be proved similarly. By Lemma 2.7, -1 is a quadratic nonresidue modulo p, so there is no element in $(r+R_s)\cap p\mathbb{Z}_{p^s}$. Then

$$\#(r+R_s)\cap R_s + (r+R_s)\cap N_s = \#(r+R_s)\cap \mathbb{Z}_{p^s} - \#(r+R_s)\cap p\mathbb{Z}_{p^s} = \frac{p-1}{2}p^{s-1}.$$

Since $-r$ is nonresidue modulo p, there are p^{s-1} elements in $(r+N_s)\cap p\mathbb{Z}_{p^s}$, and then

$$\#(r+N_s)\cap R_s + (r+N_s)\cap N_s = \#(r+N_s)\cap \mathbb{Z}_{p^s} - \#(r+N_s)\cap p\mathbb{Z}_{p^s} = \frac{p-3}{2}p^{s-1}.$$

Also, since $r + p\mathbb{Z}_{p^s} \subset R_s$,

$$\#(r + R_s) \cap R_s + \#(r + N_s) \cap R_s = \#R_s - \#(r + p\mathbb{Z}_{p^s}) \cap R_s = \frac{p-3}{2} p^{s-1}$$

and

$$\#(r + R_s) \cap N_s + \#(r + N_s) \cap N_s = \#N_s - \#(r + p\mathbb{Z}_{p^s}) \cap N_s = \frac{p-1}{2} p^{s-1}.$$

By the four equations above, we have

$$\#(r + R_s) \cap R_s = \#(r + N_s) \cap R_s = \#(r + N_s) \cap N_s = \frac{p-3}{4} p^{s-1},$$

and

$$\#(r + R_s) \cap N_s = \frac{p+1}{4} p^{s-1}.$$

□

For simplicity, we denote $C_{ij} = C_{p^i q^j}$ and $C^*_{ij} = C_{p^i q^j g}$. In particular, $C_{ij} = C^*_{ij}$ if $i = s$ and $C_{st} = C_0$. Then by Theorem 2.12 and Lemma 3.1 , we can calculate the size of the intersections of cyclotomic cosets and their translations.

Lemmas 3.2–3.6 give the size of the intersections when two cosets have the same i and j.

Lemma 3.2. *Let $a \in C_{ij}$ with $0 \leqslant i \leqslant s-1$ and $0 \leqslant j \leqslant t-1$, then*

(i) $\#(a + C_{ij}) \cap C_{ij} = \frac{p-3}{4} p^{s-i-1}(q-2)q^{t-j-1}$;

(ii) $\#(a + C_{ij}) \cap C^*_{ij} = \frac{p+1}{4} p^{s-i-1}(q-2)q^{t-j-1}$;

(iii) If q is a quadratic residue modulo p, then for $j < m \leqslant t$,

$$\#(a + C_{ij}) \cap C_{im} = \frac{p-3}{4} p^{s-i-1}\phi(q^{t-m})$$

and

$$\#(a + C_{ij}) \cap C^*_{im} = \frac{p+1}{4} p^{s-i-1}\phi(q^{t-m});$$

(iv) If q is a quadratic nonresidue modulo p, then for $j < m \leqslant t$,

$$\#(a + C_{ij}) \cap C_{im} = \begin{cases} \frac{p+1}{4} p^{s-i-1}\phi(q^{t-m}), & 2 \nmid m-j, \\ \frac{p-3}{4} p^{s-i-1}\phi(q^{t-m}), & 2 \mid m-j, \end{cases}$$

and

$$\#(a + C_{ij}) \cap C^*_{im} = \begin{cases} \frac{p-3}{4} p^{s-i-1}\phi(q^{t-k}), & 2 \nmid m-j, \\ \frac{p+1}{4} p^{s-i-1}\phi(q^{t-m}), & 2 \mid m-j. \end{cases}$$

Lemma 3.3. *Let $a^* \in C^*_{ij}$ with $0 \leqslant i \leqslant s-1$ and $0 \leqslant j \leqslant t-1$, and then*

(i) $\#(a^* + C^*_{ij}) \cap C_{ij} = \frac{p+1}{4} p^{s-i-1}(q-2)q^{t-j-1}$;

(ii) $\#(a^* + C^*_{ij}) \cap C^*_{ij} = \frac{p-3}{4} p^{s-i-1}(q-2)q^{t-j-1}$;

(iii) If q is a quadratic residue modulo p, then for $j < m \leqslant t$,

$$\#(a^* + C_{ij}^*) \cap C_{im} = \frac{p+1}{4} p^{s-i-1} \phi(q^{t-m})$$

and

$$\#(a^* + C_{ij}^*) \cap C_{im}^* = \frac{p-3}{4} p^{s-i-1} \phi(q^{t-m});$$

(iv) If q is a quadratic nonresidue modulo p, then for $j < m \leqslant t$,

$$\#(a^* + C_{ij}^*) \cap C_{im} = \begin{cases} \frac{p-3}{4} p^{s-i-1} \phi(q^{t-m}), & 2 \nmid m-j, \\ \frac{p+1}{4} p^{s-i-1} \phi(q^{t-m}), & 2 \mid m-j, \end{cases}$$

and

$$\#(a^* + C_{ij}^*) \cap C_{im}^* = \begin{cases} \frac{p+1}{4} p^{s-i-1} \phi(q^{t-k}), & 2 \nmid m-j, \\ \frac{p-3}{4} p^{s-i-1} \phi(q^{t-m}), & 2 \mid m-j. \end{cases}$$

Lemma 3.4. *Let $a \in C_{ij}$, $0 \leqslant i \leqslant s-1$, and $0 \leqslant j \leqslant t-1$. Then*

(i) $\#(a + C_{ij}^*) \cap C_{ij} = \#(a + C_{ij}^*) \cap C_{ij}^* = \frac{p-3}{4} p^{s-i-1}(q-2) q^{t-j-1}$.

(ii) For $j < m \leqslant t$, we have

$$\#(a + C_{ij}^*) \cap C_{im} = \#(a + C_{ij}^*) \cap C_{im}^* = \frac{p-3}{4} p^{s-i-1} \phi(q^{t-m}).$$

(iii) For $i < k \leqslant s-1$ and $j < m \leqslant t$, we have

$$\#(a + C_{ij}^*) \cap C_{km} = \#(a + C_{ij}^*) \cap C_{km}^* = \phi(p^{s-k}) \phi(q^{t-m})/2.$$

(iv) $\#(a + C_{ij}^*) \cap C_{sj} = (q-2) q^{t-j-1}$.

(v) For $j < m \leqslant t$, we have

$$\#(a + C_{ij}^*) \cap C_{sm} = \phi(q^{t-m}).$$

(vi) For $i < k \leqslant s-1$, we have

$$\#(a + C_{ij}^*) \cap C_{kj} = \#(a + C_{ij}^*) \cap C_{kj}^* = \phi(p^{s-k})(q-2) q^{t-j-1}/2.$$

Lemma 3.5. *Let $a \in C_{sj}$ and $0 \leqslant j \leqslant t-1$, and then*

(i) $\#(a + C_{sj}) \cap C_{sj} = (q-2) q^{t-j-1}$.

(ii) For $j < m \leqslant t$, we have $\#(a + C_{sj}) \cap C_{sm} = \phi(q^{t-m})$.

Lemma 3.6. *Let $a \in C_{it}$, $a^* \in C_{it}^*$, and $0 \leqslant i \leqslant s-1$, and then*

(i) $\#(a + C_{it}) \cap C_{it} = \#(a^* + C_{it}^*) \cap C_{it}^* = \frac{p-3}{4} p^{s-i-1}$.

(ii) $\#(a + C_{it}) \cap C_{it}^* = \#(a^* + C_{it}^*) \cap C_{it} = \frac{p+1}{4} p^{s-i-1}$.

(iii) $\#(a + C_{it}^*) \cap C_{it} = \#(a + C_{it}^*) \cap C_{it}^* = \frac{p-3}{4} p^{s-i-1}$.

(iv) For $i < k \leqslant s-1$, we have

$$\#(a + C_{it}^*) \cap C_{kt} = (a + C_{it}^*) \cap C_{kt}^* = \frac{\phi(p^{s-k})}{2}.$$

(v) $\#(a + C_{it}^*) \cap C_0 = 1$.

Lemmas 3.7 and 3.8 give the size of the intersections when i and j are both different.

Lemma 3.7. *Let $a \in C_{ij}$, $a^* \in C_{ij}$, $0 \leqslant i < i' \leqslant s-1$, and $0 \leqslant j < j' \leqslant t$, and then*

(i) $\#(a + C_{i'j'}) \cap C_{ij} = \#(a + C_{i'j'}^*) \cap C_{ij} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j'})$.

(ii) $\#(a^* + C_{i'j'}) \cap C_{ij}^* = \#(a^* + C_{i'j'}^*) \cap C_{ij}^* = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j'})$.

Lemma 3.8. *Let $a \in C_{ij}$, $a^* \in C_{ij}$, $0 \leqslant i < i' \leqslant s-1$, and $0 \leqslant j' < j \leqslant t$, and then*

(i) $\#(a + C_{i'j'}) \cap C_{ij'} = \#(a + C_{i'j'}^*) \cap C_{ij'} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})$.

(ii) $\#(a^* + C_{i'j'}) \cap C_{ij'}^*) = \#(a^* + C_{i'j'}^*) \cap C_{ij'}^*) = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})$.

Lemmas 3.9–3.13 give the size of the intersections when two cosets have the same i but different j.

Lemma 3.9. *Let $a \in C_{ij}$, $0 \leqslant i \leqslant s-1$, and $0 \leqslant j < j' \leqslant t$, and then*

(i) $\#(a + C_{ij'}) \cap C_{ij} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})$.

(ii) Suppose q is a quadratic residue modulo p. Then

$$\#(a + C_{ij'}) \cap C_{ij}^* = \frac{p+1}{4}p^{s-i-1}\phi(q^{t-j'}).$$

(iii) If q is a quadratic nonresidue modulo p and $2 \mid j' - j$, then

$$\#(a + C_{ij'}) \cap C_{ij}^* = \frac{p+1}{4}p^{s-i-1}\phi(q^{t-j'}).$$

(iv) If q is a quadratic nonresidue modulo p and $2 \nmid j' - j$, then

$$\#(a + C_{ij'}) \cap C_{ij}^* = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'}).$$

Also, for $i < k \leqslant s-1$,

$$\#(a + C_{ij'}) \cap C_{kj} = \#(a + C_{ij'}) \cap C_{kj}^* = \frac{\phi(p^{s-k})}{2}\phi(q^{t-j'}),$$

and

$$\#(a + C_{ij'}) \cap C_{sj} = \phi(q^{t-j'}).$$

Lemma 3.10. *Let $a^* \in C^*_{ij}$, $0 \leqslant i \leqslant s-1$, and $0 \leqslant j < j' \leqslant t$. Then*

(i) $\#(a^* + C^*_{ij'}) \cap C^*_{ij} = \frac{p-3}{4} p^{s-i-1}\phi(q^{t-j'})$.

(ii) Suppose q is a quadratic residue modulo p. Then

$$\#(a^* + C^*_{ij'}) \cap C_{ij} = \frac{p+1}{4} p^{s-i-1}\phi(q^{t-j'}).$$

(iii) If q is a quadratic nonresidue modulo p and $2 \mid j' - j$, then

$$\#(a^* + C^*_{ij'}) \cap C_{ij} = \frac{p+1}{4} p^{s-i-1}\phi(q^{t-j'}).$$

(iv) If q is a quadratic nonresidue modulo p and $2 \nmid j' - j$, then

$$\#(a^* + C^*_{ij'}) \cap C_{ij} = \frac{p-3}{4} p^{s-i-1}\phi(q^{t-j'}).$$

Also, for $i < k \leqslant s-1$,

$$\#(a^* + C^*_{ij'}) \cap C_{kj} = \#(a + C_{ij'}) \cap C^*_{kj} = \frac{\phi(p^{s-k})}{2}\phi(q^{t-j'}),$$

and

$$\#(a^* + C^*_{ij'}) \cap C_{sj} = \phi(q^{t-j'}).$$

Lemma 3.11. *Let $a \in C_{ij}$, $0 \leqslant i \leqslant s-1$, and $0 \leqslant j < j' \leqslant t$. Then*

(i) If q is a quadratic residue modulo p, then

$$\#(a + C^*_{ij'}) \cap C_{ij} = (a + C^*_{ij'}) \cap C^*_{ij} = \frac{p-3}{4} p^{s-i-1}\phi(q^{t-j'}).$$

Also, for $i < k \leqslant s-1$,

$$\#(a + C^*_{ij'}) \cap C_{kj} = \#(a + C^*_{ij'}) \cap C^*_{kj} = \frac{\phi(p^{s-k})}{2}\phi(q^{t-j'}),$$

and

$$\#(a + C^*_{ij'}) \cap C_{sj} = \phi(q^{t-j'}).$$

(ii) If q is a quadratic nonresidue modulo p and $2 \nmid j' - j$, then

$$\#(a + C^*_{ij'}) \cap C_{ij} = \frac{p-3}{4} p^{s-i-1}\phi(q^{t-j'})$$

and

$$\#(a + C^*_{ij'}) \cap C^*_{ij} = \frac{p+1}{4} p^{s-i-1}\phi(q^{t-j'}).$$

(iii) If q is a quadratic nonresidue modulo p and $2 \mid j' - j$, then

$$\#(a + C_{ij'}^*) \cap C_{ij} = (a + C_{ij'}^*) \cap C_{ij}^* = \frac{p-3}{4} p^{s-i-1} \phi(q^{t-j'}).$$

Also, for $i < k \leqslant s-1$,

$$\#(a + C_{ij'}^*) \cap C_{kj} = \#(a + C_{ij'}^*) \cap C_{kj}^* = \frac{\phi(p^{s-k})}{2} \phi(q^{t-j'}),$$

and

$$\#(a + C_{ij'}^*) \cap C_{sj} = \phi(q^{t-j'}).$$

Lemma 3.12. *Let $a^* \in C_{ij}^*$, $0 \leqslant i \leqslant s-1$, and $0 \leqslant j < j' \leqslant t$. Then*

(i) If q is a quadratic residue modulo p, then

$$\#(a^* + C_{ij'}) \cap C_{ij} = (a^* + C_{ij'}) \cap C_{ij}^* = \frac{p-3}{4} p^{s-i-1} \phi(q^{t-j'}).$$

Also, for $i < k \leqslant s-1$,

$$\#(a^* + C_{ij'}) \cap C_{kj} = \#(a^* + C_{ij'}) \cap C_{kj}^* = \frac{\phi(p^{s-k})}{2} \phi(q^{t-j'}),$$

and

$$\#(a^* + C_{ij'}) \cap C_{sj} = \phi(q^{t-j'}).$$

(ii) If q is a quadratic nonresidue modulo p and $2 \nmid j' - j$, then

$$\#(a^* + C_{ij'}) \cap C_{ij} = \frac{p+1}{4} p^{s-i-1} \phi(q^{t-j'})$$

and

$$\#(a^* + C_{ij'}) \cap C_{ij}^* = \frac{p-3}{4} p^{s-i-1} \phi(q^{t-j'}).$$

(iii) If q is a quadratic nonresidue modulo p and $2 \mid j' - j$, then

$$\#(a^* + C_{ij'}) \cap C_{ij} = (a^* + C_{ij'}) \cap C_{ij}^* = \frac{p-3}{4} p^{s-i-1} \phi(q^{t-j'}).$$

Also, for $i < k \leqslant s-1$,

$$\#(a^* + C_{ij'}) \cap C_{kj} = \#(a^* + C_{ij'}) \cap C_{kj}^* = \frac{\phi(p^{s-k})}{2} \phi(q^{t-j'}),$$

and

$$\#(a^* + C_{ij'}) \cap C_{sj} = \phi(q^{t-j'}).$$

Lemma 3.13. *(i) Let $a \in C_{sj}$ and $0 \leqslant j < j' \leqslant t$. Then $\#(a + C_{sj'}) \cap C_{sj} = \phi(q^{t-j'})$.*

(ii) Let $a \in C_{ij}$, $0 \leqslant i \leqslant s-1$, and $0 \leqslant j < j' \leqslant t$. Then $\#(a + C_{sj'}) \cap C_{ij} = \phi(q^{t-j'})$.

(iii) *Let* $a^* \in C_{ij}^*$, $0 \leqslant i \leqslant s-1$, *and* $0 \leqslant j < j' \leqslant t$. *Then* $\#(a^* + C_{sj'}) \cap C_{ij}^* = \phi(q^{t-j'})$.

(iv) *Let* $a \in C_{ij}$, $0 \leqslant i \leqslant s-1$, *and* $0 \leqslant j' < j \leqslant t$. *Then* $\#(a + C_{sj'}) \cap C_{ij'} = \phi(q^{t-j})$.

(v) *Let* $a^* \in C_{ij}^*$, $0 \leqslant i \leqslant s-1$, *and* $0 \leqslant j' < j \leqslant t$. *Then* $\#(a^* + C_{sj'}) \cap C_{ij'}^* = \phi(q^{t-j})$.

Lemmas 3.14–3.17 give the size of the intersections when two cosets have the same j but different i.

Lemma 3.14. *Let* $a \in C_{ij}$, $0 \leqslant i < i' \leqslant s-1$, *and* $0 \leqslant j \leqslant t-1$. *Then*

(i) $\#(a + C_{i'j}) \cap C_{ij} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}$.

(ii) *If* q *is a quadratic residue modulo* p, *then for* $j < m \leqslant t$, *we have*

$$\#(a + C_{i'j}) \cap C_{im} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

(iii) *If* q *is a quadratic nonresidue modulo* p, *then for* $j < m \leqslant t$ *and* $2 \nmid m-j$, *we have*

$$\#(a + C_{i'j}) \cap C_{im}^* = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

For $j < m \leqslant t$ *and* $2 \mid m-j$, *we have*

$$\#(a + C_{i'j}) \cap C_{im} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

Lemma 3.15. *Let* $a^* \in C_{ij}^*$, $0 \leqslant i < i' \leqslant s-1$, *and* $0 \leqslant j \leqslant t-1$. *Then*

(i) $\#(a^* + C_{i'j}^*) \cap C_{ij}^* = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}$.

(ii) *If* q *is a quadratic residue modulo* p, *then for* $j < m \leqslant t$, *we have*

$$\#(a^* + C_{i'j}^*) \cap C_{im}^* = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

(iii) *If* q *is a quadratic nonresidue modulo* p, *then for* $j < m \leqslant t$ *and* $2 \nmid m-j$, *we have*

$$\#(a^* + C_{i'j}^*) \cap C_{im} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

For $j < m \leqslant t$ *and* $2 \mid m-j$, *we have*

$$\#(a^* + C_{i'j}^*) \cap C_{im}^* = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

Lemma 3.16. *Let* $a \in C_{ij}$, $0 \leqslant i < i' \leqslant s-1$, *and* $0 \leqslant j \leqslant t-1$. *Then*

(i) $\#(a + C_{i'j}^*) \cap C_{ij} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}$.

(ii) If q is a quadratic residue modulo p, then for $j < m \leqslant t$, we have

$$\#(a + C^*_{i'j}) \cap C_{im} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

(iii) If q is a quadratic nonresidue modulo p, then for $j < m \leqslant t$ and $2 \nmid m - j$, we have

$$\#(a + C^*_{i'j}) \cap C^*_{im} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

For $j < m \leqslant t$ and $2 \mid m - j$, we have

$$\#(a + C^*_{i'j}) \cap C_{im} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

Lemma 3.17. *Let $a^* \in C^*_{ij}$, $0 \leqslant i < i' \leqslant s - 1$, and $0 \leqslant j \leqslant t - 1$. Then*

(i) $\#(a^* + C_{i'j}) \cap C^*_{ij} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}$.

(ii) If q is a quadratic residue modulo p, then for $j < m \leqslant t$, we have

$$\#(a^* + C^*_{i'j}) \cap C^*_{im} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

(iii) If q is a quadratic nonresidue modulo p, then for $j < m \leqslant t$ and $2 \nmid m - j$, we have

$$\#(a^* + C_{i'j}) \cap C_{im} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

For $j < m \leqslant t$ and $2 \mid m - j$, we have

$$\#(a^* + C_{i'j}) \cap C^*_{im} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-m}).$$

These results will be used to study arithmetic of some specific families of polynomials in the next section.

4. Arithmetic properties

In this section, we will study arithmetic properties of some families in the ring $\mathbb{F}_l[x]/\langle x^{p^s q^t - 1}\rangle$. For that, let us define

$$\chi_{ij} = \sum_{\alpha \in C_{ij}} x^\alpha$$

and

$$\chi^*_{ij} = \sum_{\alpha \in C^*_{ij}} x^\alpha.$$

In particular, $\chi_{sj} = \chi^*_{sj}$ for $0 \leqslant j \leqslant t$ and $\chi_{st} = 1$.

They look like "some kind of characteristics". In fact, primitive idempotents in the ring $\mathbb{F}_l[x]/\langle x^{p^s q^t - 1}\rangle$ can be written in the form of a linear combination of these polynomials. So it is necessary to study them.

In this section, the proof of Theorem 4. X needs the results in Lemma 3. $(X + 1)$.

Theorem 4.1. *Let* $0 \leqslant i \leqslant s-1$ *and* $0 \leqslant j \leqslant t-1$, *and then*

(i) If q is a quadratic residue modulo p, then

$$\chi_{ij}^2 = \frac{p-3}{4}p^{s-i-1}\left((q-2)\,q^{t-j-1}\chi_{ij} + \phi(q^{t-j})\sum_{j<m\leqslant t}\chi_{im}\right) + \frac{p+1}{4}p^{s-i-1}\left((q-2)\,q^{t-j-1}\chi_{ij}^* + \phi(q^{t-j})\sum_{j<m\leqslant t}\chi_{im}^*\right).$$

(ii) If q is a quadratic nonresidue modulo p, then

$$\chi_{ij}^2 = \frac{p-3}{4}p^{s-i-1}\left((q-2)\,q^{t-j-1}\chi_{ij} + \phi(q^{t-j})\left(\sum_{\substack{j<m\leqslant t\\ 2\nmid m-j}}\chi_{im}^* + \sum_{\substack{j<m\leqslant t\\ 2\mid m-j}}\chi_{im}\right)\right) + \frac{p+1}{4}p^{s-i-1}\left((q-2)\,q^{t-j-1}\chi_{ij}^* + \phi(q^{t-j})\left(\sum_{\substack{j<m\leqslant t\\ 2\nmid m-j}}\chi_{im} + \sum_{\substack{j<m\leqslant t\\ 2\mid m-j}}\chi_{im}^*\right)\right).$$

Proof. We will only prove result (i). Let $a \in C_{ij}$, and then by Lemma 3.2, we obtain

$$\#(a+C_{ij})\cap C_{im} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-m}), \quad j<m\leqslant t. \tag{4.1}$$

We can choose $b \in C_{ij}$ such that $a+b=c$, where $c \in C_{im}$. So we get $l^k a + l^k b = l^k c$ for $0 \leqslant k \leqslant \frac{\phi(p^{s-i})}{2}\phi(q^{t-j})-1$. When $l^k a$ runs through C_{ij}, for $\#C_{im} = \frac{p^{s-i}}{2}\phi(q^{t-m})$, $l^k c$ runs through C_{im} exactly $\#C_{ij}/\#C_{im} = \phi(q^{t-j})/\phi(q^{t-m})$ times. So by (4.1), we obtain that the multiset $C_{ij}+C_{ij}$ contains $\frac{p-3}{4}p^{s-i-1}\phi(q^{t-j})$ copies of C_{im}. By a similar argument and by Lemma 3.2, we obtain that the multiset $C_{ij}+C_{ij}$ contains $\frac{p-3}{4}p^{s-i-1}(q-2)q^{t-j-1}$ copies of C_{ij}, $\frac{p+1}{4}p^{s-i-1}(q-2)q^{t-j-1}$ copies of C_{ij}^*, and $\frac{p+1}{4}p^{s-i-1}\phi(q^{t-j})$ copies of C_{im}^* for $j<m\leqslant t$.

Further it is easy to verify that the coefficients of the terms on the both sides in result (i) are equal. This together with the argument above proves the result (i). □

In a similar way to the proof of Theorem 4.1, we can prove the results in Theorems 4.2–4.6.

Theorem 4.2. *Let* $0 \leqslant i \leqslant s-1$ *and* $0 \leqslant j \leqslant t-1$, *and then*

(i) If q is a quadratic residue modulo p, then

$$\left(\chi_{ij}^*\right)^2 = \frac{p-3}{4}p^{s-i-1}\left((q-2)\,q^{t-j-1}\chi_{ij}^* + \phi(q^{t-j})\sum_{j<m\leqslant t}\chi_{im}^*\right) + \frac{p+1}{4}p^{s-i-1}\left((q-2)\,q^{t-j-1}\chi_{ij} + \phi(q^{t-j})\sum_{j<m\leqslant t}\chi_{im}\right).$$

(ii) If q is a quadratic nonresidue modulo p, then

$$\left(\chi_{ij}^*\right)^2 = \frac{p-3}{4}p^{s-i-1}\left((q-2)\,q^{t-j-1}\chi_{ij}^* + \phi(q^{t-j})\left(\sum_{\substack{j<m\leqslant t\\ 2\nmid m-j}}\chi_{im} + \sum_{\substack{j<m\leqslant t\\ 2\mid m-j}}\chi_{im}^*\right)\right)$$
$$+ \frac{p+1}{4}p^{s-i-1}\left((q-2)\,q^{t-j-1}\chi_{ij} + \phi(q^{t-j})\left(\sum_{\substack{j<m\leqslant t\\ 2\nmid m-j}}\chi_{im}^* + \sum_{\substack{j<m\leqslant t\\ 2\mid m-j}}\chi_{im}\right)\right).$$

Theorem 4.3. *Let $0 \leqslant i \leqslant s-1$ and $0 \leqslant j \leqslant t-1$, and then*

$$\chi_{ij}\chi_{ij}^* = \frac{p-3}{4}p^{s-i-1}(q-2)q^{t-j-1}(\chi_{ij}+\chi_{ij}^*) + \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j})\sum_{j<m\leqslant t}(\chi_{im}+\chi_{im}^*)$$
$$+ \frac{\phi(p^{s-i})}{2}\phi(q^{t-j})\sum_{\substack{i<k\leqslant s-1\\ j<m\leqslant t}}(\chi_{km}+\chi_{km}^*) + \frac{\phi(p^{s-i})}{2}(q-2)q^{t-j-1}\chi_{sj}$$
$$+ \frac{\phi(q^{s-i})}{2}\phi(q^{t-j})\sum_{j<m\leqslant t}\chi_{sm} + \frac{\phi(p^{s-i})}{2}(q-2)q^{t-j-1}\sum_{i<k\leqslant s-1}(\chi_{kj}+\chi_{kj}^*).$$

Theorem 4.4. *Let $0 \leqslant j \leqslant t-1$, and then $\chi_{sj}^2 = (q-2)q^{t-j-1}\chi_{sj} + \phi(q^{t-j})\sum\limits_{j<m\leqslant t}\chi_{sm}$.*

Theorem 4.5. *Let $0 \leqslant i \leqslant s-1$, and then*

(i) $\chi_{it}^2 = \frac{p-3}{4}p^{s-i-1}\chi_{it} + \frac{p+1}{4}p^{s-i-1}\chi_{it}^*$.

(ii) $\left(\chi_{it}^*\right)^2 = \frac{p-3}{4}p^{s-i-1}\chi_{it}^* + \frac{p+1}{4}p^{s-i-1}\chi_{it}$.

(iii) $\chi_{it}\chi_{it}^* = \frac{p-3}{4}p^{s-i-1}\left(\chi_{it}+\chi_{it}^*\right) + \frac{\phi(p^{s-i})}{2}\left(\sum\limits_{i<k\leqslant s-1}\left(\chi_{kt}+\chi_{kt}^*\right)+1\right)$.

Theorem 4.6. *Let $0 \leqslant i < i' \leqslant s-1$ and $0 \leqslant j < j' \leqslant t$, and then*

(i) $\chi_{ij}\chi_{i'j'} = \chi_{ij}\chi_{i'j'}^* = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j'})\chi_{ij}$.

(ii) $\chi_{ij}^*\chi_{i'j'} = \chi_{ij}^*\chi_{i'j'}^* = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j'})\chi_{ij}^*$.

Theorem 4.7. *Let $0 \leqslant i < i' \leqslant s-1$ and $0 \leqslant j' < j \leqslant t$, and then*

(i) $\chi_{ij}\chi_{i'j'} = \chi_{ij}\chi_{i'j'}^* = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\chi_{ij'}$.

(ii) $\chi_{ij}^*\chi_{i'j'} = \chi_{ij}^*\chi_{i'j'}^* = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\chi_{ij'}^*$.

Proof. We will prove the first part of result (i) for the case where q is a quadratic residue modulo p. That means, we need to show that, in the multiset

$$p^i q^{j'}\left(\{q^{t-j'}x + p^{s-i}q^{j-j'}y : x \in R_{s-i}, y \in \mathbb{Z}^*_{q^{t-j}}\} + \{p^{i'-i}q^{t-j'}x' + p^{s-i}y' : x' \in R_{s-i'}, y' \in \mathbb{Z}^*_{q^{t-j'}}\}\right),$$

every element appears exactly $\frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})$ times.

Note that

$$C_{ij'} = p^i q^{j'}\{q^{t-j'}x + p^{s-i}y' : x \in R_{s-i}, y' \in \mathbb{Z}^*_{q^{t-j'}}\}.$$

Let $x_0 \in R_{s-i}$, since $i > i$, for any $x' \in R_{s-i'}$, and there is exactly one $x \in R_{s-i}$ such that $x_0 \equiv p^{i'-i}x' + x \bmod p^{s-i}$. Also, let $y_0 \in \mathbb{Z}^*_{q^{t-j}}$, for any $y \in \mathbb{Z}^*_{q^{t-j}}$, and there is exactly one $y' \in \mathbb{Z}^*_{q^{t-j'}}$ such that $y_0 \equiv q^{j-j'}y + y' \bmod q^{t-j'}$. Hence every element appears

$$\#R_{s-i'} \cdot \#\mathbb{Z}^*_{q^{t-j}} = \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})$$

times. The result is proved. □

The results in Theorems 4.8–4.16 can be proved by using the methods in the proof of Theorem 4.1 or Theorem 4.7.

Theorem 4.8. *Let $0 \leqslant i \leqslant s-1$ and $0 \leqslant j < j' \leqslant t$, and then*

(i) If q is a quadratic residue modulo p, then

$$\chi_{ij}\chi_{ij'} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\chi_{ij} + \frac{p+1}{4}p^{s-i-1}\phi(q^{t-j'})\chi^*_{ij}.$$

(ii) If q is a quadratic nonresidue modulo p and $2 \mid j'-j$, then

$$\chi_{ij}\chi_{ij'} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\chi_{ij} + \frac{p+1}{4}p^{s-i-1}\phi(q^{t-j'})\chi^*_{ij}.$$

(iii) If q is a quadratic nonresidue modulo p and $2 \nmid j'-j$, then

$$\chi_{ij}\chi_{ij'} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\left(\chi_{ij} + \chi^*_{ij}\right) + \frac{\phi(p^{s-i})}{2}\phi(q^{t-j'})\left(\sum_{i<k\leqslant s-1}\left(\chi_{kj} + \chi^*_{kj}\right) + \chi_{sj}\right).$$

Theorem 4.9. *Let $0 \leqslant i \leqslant s-1$ and $0 \leqslant j < j' \leqslant t$, and then*

(i) If q is a quadratic residue modulo p, then

$$\chi^*_{ij}\chi^*_{ij'} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\chi^*_{ij} + \frac{p+1}{4}p^{s-i-1}\phi(q^{t-j'})\chi_{ij}.$$

(ii) If q is a quadratic nonresidue modulo p and $2 \mid j'-j$, then

$$\chi^*_{ij}\chi^*_{ij'} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\chi^*_{ij} + \frac{p+1}{4}p^{s-i-1}\phi(q^{t-j'})\chi_{ij}.$$

(iii) If q is a quadratic nonresidue modulo p and $2 \nmid j' - j$, then

$$\chi_{ij}^{*}\chi_{ij'}^{*} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\left(\chi_{ij}+\chi_{ij}^{*}\right)+\frac{\phi(p^{s-i})}{2}\phi(q^{t-j'})\left(\sum_{i<k\leqslant s-1}\left(\chi_{kj}+\chi_{kj}^{*}\right)+\chi_{sj}\right).$$

Theorem 4.10. *Let $0 \leqslant i \leqslant s-1$ and $0 \leqslant j < j' \leqslant t$, and then*

(i) If q is a quadratic residue modulo p, then

$$\chi_{ij}\chi_{ij'}^{*} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\left(\chi_{ij}+\chi_{ij}^{*}\right)+\frac{\phi(p^{s-i})}{2}\phi(q^{t-j'})\left(\sum_{i<k\leqslant s-1}\left(\chi_{kj}+\chi_{kj}^{*}\right)+\chi_{sj}\right).$$

(ii) If q is a quadratic nonresidue modulo p and $2 \nmid j' - j$, then

$$\chi_{ij}\chi_{ij'}^{*} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\chi_{ij}+\frac{p+1}{4}p^{s-i-1}\phi(q^{t-j'})\chi_{ij}^{*}.$$

(iii) If q is a quadratic nonresidue modulo p and $2 \mid j' - j$, then

$$\chi_{ij}\chi_{ij'}^{*} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\left(\chi_{ij}+\chi_{ij}^{*}\right)+\frac{\phi(p^{s-i})}{2}\phi(q^{t-j'})\left(\sum_{i<k\leqslant s-1}\left(\chi_{kj}+\chi_{kj}^{*}\right)+\chi_{sj}\right).$$

Theorem 4.11. *Let $0 \leqslant i \leqslant s-1$ and $0 \leqslant j < j' \leqslant t$, and then*

(i) If q is a quadratic residue modulo p, then

$$\chi_{ij}^{*}\chi_{ij'} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\left(\chi_{ij}+\chi_{ij}^{*}\right)+\frac{\phi(p^{s-i})}{2}\phi(q^{t-j'})\left(\sum_{i<k\leqslant s-1}\left(\chi_{kj}+\chi_{kj}^{*}\right)+\chi_{sj}\right).$$

(ii) If q is a quadratic nonresidue modulo p and $2 \nmid j' - j$, then

$$\chi_{ij}^{*}\chi_{ij'} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\chi_{ij}^{*}+\frac{p+1}{4}p^{s-i-1}\phi(q^{t-j'})\chi_{ij}.$$

(iii) If q is a quadratic nonresidue modulo p and $2 \mid j' - j$, then

$$\chi_{ij}^{*}\chi_{ij'} = \frac{p-3}{4}p^{s-i-1}\phi(q^{t-j'})\left(\chi_{ij}+\chi_{ij}^{*}\right)+\frac{\phi(p^{s-i})}{2}\phi(q^{t-j'})\left(\sum_{i<k\leqslant s-1}\left(\chi_{kj}+\chi_{kj}^{*}\right)+\chi_{sj}\right).$$

Theorem 4.12. *(i) Let $0 \leqslant j < j' \leqslant t$, and then $\chi_{sj}\chi_{sj'} = \phi(q^{t-j'})\chi_{sj}$.*

(ii) Let $0 \leqslant i \leqslant s-1$ and $0 \leqslant j < j' \leqslant t$, and then

$$\chi_{ij}\chi_{sj'} = \phi(q^{t-j'})\chi_{ij}$$

and

$$\chi_{ij}^{*}\chi_{sj'} = \phi(q^{t-j'})\chi_{ij}^{*}.$$

(iii) Let $0 \leqslant i \leqslant s-1$ *and* $0 \leqslant j' < j \leqslant t$, *and then*

$$\chi_{ij}\chi_{sj'} = \phi(q^{t-j})\chi_{ij'}$$

and

$$\chi^*_{ij}\chi_{sj'} = \phi(q^{t-j})\chi^*_{ij'}.$$

Theorem 4.13. *Let* $0 \leqslant i < i' \leqslant s-1$ *and* $0 \leqslant j \leqslant t-1$, *and then*

(i) If q is a quadratic residue modulo p, then

$$\chi_{ij}\chi_{i'j} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}\chi_{ij} + \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\sum_{j<m\leqslant t}\chi_{im}.$$

(ii) If q is a quadratic nonresidue modulo p, then

$$\chi_{ij}\chi_{i'j} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}\chi_{ij} + \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\left(\sum_{\substack{j<m\leqslant t\\ 2\nmid m-j}}\chi^*_{im} + \sum_{\substack{j<m\leqslant t\\ 2\mid m-j}}\chi_{im}\right).$$

Theorem 4.14. *Let* $0 \leqslant i < i' \leqslant s-1$ *and* $0 \leqslant j \leqslant t-1$, *and then*

(i) If q is a quadratic residue modulo p, then

$$\chi^*_{ij}\chi^*_{i'j} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}\chi^*_{ij} + \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\sum_{j<m\leqslant t}\chi^*_{im}.$$

(ii) If q is a quadratic nonresidue modulo p, then

$$\chi^*_{ij}\chi^*_{i'j} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}\chi^*_{ij} + \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\left(\sum_{\substack{j<m\leqslant t\\ 2\nmid m-j}}\chi_{im} + \sum_{\substack{j<m\leqslant t\\ 2\mid m-j}}\chi^*_{im}\right).$$

Theorem 4.15. *Let* $0 \leqslant i < i' \leqslant s-1$ *and* $0 \leqslant j \leqslant t-1$, *and then*

(i) If q is a quadratic residue modulo p, then

$$\chi_{ij}\chi^*_{i'j} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}\chi_{ij} + \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\sum_{j<m\leqslant t}\chi_{im}.$$

(ii) If q is a quadratic nonresidue modulo p, then

$$\chi_{ij}\chi^*_{i'j} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}\chi_{ij} + \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\left(\sum_{\substack{j<m\leqslant t\\ 2\nmid m-j}}\chi^*_{im} + \sum_{\substack{j<m\leqslant t\\ 2\mid m-j}}\chi_{im}\right).$$

Theorem 4.16. *Let* $0 \leqslant i < i' \leqslant s-1$ *and* $0 \leqslant j \leqslant t-1$, *and then*

(i) If q is a quadratic residue modulo p, then

$$\chi^*_{ij}\chi_{i'j} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}\chi^*_{ij} + \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\sum_{j<m\leqslant t}\chi^*_{im}.$$

(ii) If q is a quadratic nonresidue modulo p, then

$$\chi^*_{ij}\chi_{i'j} = \frac{\phi(p^{s-i'})}{2}(q-2)q^{t-j-1}\chi^*_{ij} + \frac{\phi(p^{s-i'})}{2}\phi(q^{t-j})\left(\sum_{\substack{j<m\leqslant t\\ 2\nmid m-j}}\chi_{im} + \sum_{\substack{j<m\leqslant t\\ 2\mid m-j}}\chi^*_{im}\right).$$

Corollary 4.17. *Let* $0 \leqslant i < i' \leqslant s-1$ *and* $0 \leqslant j \leqslant t-1$, *and then*

$$\chi_{ij}\chi_{i'j} = \chi_{ij}\chi^*_{i'j}$$

and

$$\chi^*_{ij}\chi_{i'j} = \chi^*_{ij}\chi^*_{i'j}.$$

5. Primitive idempotents in the ring $\mathbb{F}_l[x]/\langle x^{p^sq^t-1}\rangle$

Let α be a fixed primitive nth root of unit in some extension field of $\mathbb{F}_l$. Then the polynomial

$$M_\gamma(x) = \prod_{i\in C_\gamma}(x-\alpha^i)$$

is the minimal polynomial of α^γ over $\mathbb{F}_l$. Let $\mathscr{M}_\gamma$ be the minimal ideal in $\mathbb{F}_l[x]/\langle x^n-1\rangle$ generated by $(x^n-1)/M_\gamma(x)$ and $\theta_\gamma(x)$ be the primitive idempotent of $\mathscr{M}_\gamma$, that is,

$$\theta_\gamma(\alpha^u) = \begin{cases} 1, & u \in C_\gamma; \\ 0, & u \notin C_\gamma. \end{cases}$$

Lemma 5.1 ([8], Theorem 1, p. 433)**.**

$$\theta_\gamma(x) = \sum_{0\leqslant u<n}\epsilon_u x^u$$

where

$$\epsilon_u = 1/n\sum_{j\in C_\gamma}\alpha^{-uj}, \quad u \geqslant 0.$$

In this section, let α be a fixed primitive p^sq^t-th root of the unit in some extension field of $\mathbb{F}_l$. Also, for simplicity, we denote

$$\theta_{ij} = \theta_{p^iq^j}$$

and

$$\theta^*_{ij} = \theta_{p^iq^jg}.$$

In particular, $\theta_{ij} = \theta^*_{ij}$ when $i = s$ and $\theta_{st} = \theta_0$.

Case 1: q is a quadratic residue modulo p

We first calculate $\chi_{ij}(\alpha^u)$, $0 \leqslant i \leqslant s-1, 0 \leqslant j \leqslant t$. By Theorem 2.12, we get

$$\chi_{ij}(\alpha^u) = \sum_{x\in R_{s-i}} \sum_{y\in\mathbb{Z}^*_{q^{t-j}}} \alpha^{up^iq^j(q^{t-j}x+p^{s-i}y)} = \sum_{x\in Rs-i} \alpha^{up^iq^tx} \sum_{y\in\mathbb{Z}^*_{q^{t-j}}} \alpha^{up^sq^jy}$$
$$= \sum_{x\in R_1} \alpha^{up^iq^tx} \sum_{0\leqslant\lambda<p^{s-i-1}} \alpha^{up^{i+1}q^t\lambda} \sum_{y\in\mathbb{Z}^*_{q^{t-j}}} \alpha^{up^sq^jy}.$$

Similarly, we have

$$\chi^*_{ij}(\alpha^u) = \sum_{x\in N_1} \alpha^{up^iq^tx} \sum_{0\leqslant\lambda<p^{s-i-1}} \alpha^{up^{i+1}q^t\lambda} \sum_{y\in\mathbb{Z}^*_{q^{t-j}}} \alpha^{up^sq^jy}.$$

The results below are obvious:

Lemma 5.2. *If $p^{s-i}q^{t-j} \mid u$, then $\chi_{ij}(\alpha^u) = \chi^*_{ij}(\alpha^u) = \frac{\phi(p^{s-i})}{2}\phi(q^{t-j})$.*

Lemma 5.3. *If $p^{s-i-1} \nmid u$ or $q^{t-j-1} \nmid u$, then $\chi_{ij}(\alpha^u) = \chi^*_{ij}(\alpha^u) = 0$.*

Lemma 5.4. *If q^{t-j-1} exactly divides u, then*

$$\sum_{y\in\mathbb{Z}^*_{q^{t-j}}} \alpha^{up^sq^jy} = -q^{t-j-1}.$$

Let $\beta = \alpha^{p^{s-1}q^t}$, and then β is a pth root of the unit. We denote

$$\mathscr{R} = \sum_{x\in R_1} \beta^x$$

and

$$\mathscr{N} = \sum_{x\in N_1} \beta^x,$$

and then

$$\mathscr{R} + \mathscr{N} = -1 \quad \text{and} \quad \mathscr{R}\mathscr{N} = \frac{p+1}{4}.$$

So $\mathscr{R}, \mathscr{N}$ are two roots of the equation

$$x^2 + x + \frac{p+1}{4} = 0.$$

If $l = 2$, then $p \equiv -1 \bmod 8$ for $2 \in R_1$. Without loss of generality, we may suppose

$$\mathscr{R} = 1, \quad \mathscr{N} = 0.$$

If l is an odd prime, then

$$\mathscr{R} = \frac{-1+\delta}{2}, \quad \mathscr{N} = \frac{-1-\delta}{2},$$

where $\delta \in \mathbb{F}_l$ such that $\delta^2 = -p$. Note that, by quadratic reciprocity law,

$$\left(\frac{-p}{l}\right) = \left(\frac{l}{p}\right) = 1,$$

so δ is well defined.

Lemma 5.5. *Let q be a quadratic residue modulo p.*

(i) If $u \in C_{s-i-1,t-j-1}$, then

$$\chi_{ij}(\alpha^u) = -\mathscr{R}p^{s-i-1}q^{t-j-1}$$

and

$$\chi^*_{ij}(\alpha^u) = -\mathscr{N}p^{s-i-1}q^{t-j-1}.$$

(ii) If $u \in C^*_{s-i-1,t-j-1}$, then

$$\chi_{ij}(\alpha^u) = -\mathscr{N}p^{s-i-1}q^{t-j-1}$$

and

$$\chi^*_{ij}(\alpha^u) = -\mathscr{R}p^{s-i-1}q^{t-j-1}.$$

Lemma 5.6. *Let q be a quadratic residue modulo p and $t - j \leqslant m \leqslant t$.*

(i) If $u \in C_{s-i-1,m}$, then

$$\chi_{ij}(\alpha^u) = \mathscr{R}p^{s-i-1}\phi(q^{t-j})$$

and

$$\chi^*_{ij}(\alpha^u) = \mathscr{N}p^{s-i-1}\phi(q^{t-j}).$$

(ii) If $u \in C^*_{s-i-1,m}$, then

$$\chi_{ij}(\alpha^u) = \mathscr{N}p^{s-i-1}\phi(q^{t-j})$$

and

$$\chi^*_{ij}(\alpha^u) = \mathscr{R}p^{s-i-1}\phi(q^{t-j}).$$

If $i = s$, then

$$\chi_{sj}(\alpha^u) = \sum_{y\in\mathbb{Z}^*_{q^{t-j}}} \alpha^{up^sq^jy},$$

where these values are easy to calculate.

Now we consider the explicit expressions for primitive idempotents. Note that if u and u' are in the same cyclotomic coset, then $\epsilon_u = \epsilon_{u'}$. So we can evaluate, for example, θ_{ij} by classifying u according to different cyclotomic cosets, that is,

$$\theta_{ij} = \sum_{\gamma\in\Gamma} a_\gamma\chi_\gamma, \tag{5.1}$$

where Γ is the set of the representatives of all cyclotomic cosets. By Lemma 5.1, we know that

$$a_\gamma = \frac{1}{n}\chi_{ij}(\alpha^{-u}),\ -u \in C_\gamma,$$

and then by the argument above, we can get the results below.

Theorem 5.7. *Let q be a quadratic residue modulo p.*

(i) For $i = 0$ and $j = t$,

$$\theta_{0t}(x) = \frac{1}{pq^t}\left(\frac{p-1}{2}\sum_{0\leqslant m\leqslant t}\chi_{sm}(x) + \mathscr{N}\sum_{0\leqslant m\leqslant t}\chi_{s-1,m}(x) + \mathscr{R}\sum_{0\leqslant m\leqslant t}\chi^*_{s-1,m}(x)\right),$$

and

$$\theta^*_{0t}(x) = \frac{1}{pq^t}\left(\frac{p-1}{2}\sum_{0\leqslant m\leqslant t}\chi_{sm}(x) + \mathscr{R}\sum_{0\leqslant m\leqslant t}\chi_{s-1,m}(x) + \mathscr{N}\sum_{0\leqslant m\leqslant t}\chi^*_{s-1,m}(x)\right).$$

(ii) For $i = 0$ and $0 \leqslant j \leqslant t-1$,

$$\begin{aligned}\theta_{0j}(x) \;=\; & \frac{1}{pq^{j+1}}\Bigg(\frac{(p-1)}{2}(q-1)\sum_{t-j\leqslant m\leqslant t}\chi_{sm}(x)\\ & + (q-1)\Bigg(\mathscr{N}\sum_{t-j\leqslant m\leqslant t}\chi_{s-1,m}(x) + \mathscr{R}\sum_{t-j\leqslant m\leqslant m}\chi^*_{s-1,m}(x)\Bigg)\\ & - \Big(\mathscr{N}\chi_{s-1,t-j-1}(x) + \mathscr{R}\chi^*_{s-1,t-j-1}(x)\Big) - \frac{p-1}{2}\chi_{s,t-j-1}(x)\Bigg),\end{aligned}$$

and

$$\begin{aligned}\theta^*_{0j}(x) \;=\; & \frac{1}{pq^{j+1}}\Bigg(\frac{(p-1)}{2}(q-1)\sum_{t-j\leqslant m\leqslant t}\chi_{sm}(x)\\ & + (q-1)\Bigg(\mathscr{R}\sum_{t-j\leqslant m\leqslant t}\chi_{s-1,m}(x) + \mathscr{N}\sum_{t-j\leqslant m\leqslant m}\chi^*_{s-1,m}(x)\Bigg)\\ & - \Big(\mathscr{R}\chi_{s-1,t-j-1}(x) + \mathscr{N}\chi^*_{s-1,t-j-1}(x)\Big) - \frac{p-1}{2}\chi_{s,t-j-1}(x)\Bigg).\end{aligned}$$

(iii) For $1 \leqslant i \leqslant s-1$ and $0 \leqslant j \leqslant t-1$,

$$\begin{aligned}\theta_{ij}(x) \;=\; & \frac{1}{p^{i+1}q^{j+1}}\Bigg(\frac{(p-1)}{2}(q-1)\Bigg(\sum_{\substack{s-i\leqslant k\leqslant s-1\\ t-j\leqslant m\leqslant t}}(\chi_{km}(x)+\chi^*_{km}(x)) + \sum_{t-j\leqslant m\leqslant t}\chi_{sm}(x)\Bigg)\\ & + (q-1)\Bigg(\mathscr{N}\sum_{t-j\leqslant m\leqslant t}\chi_{s-i-1,m}(x) + \mathscr{R}\sum_{t-j\leqslant m\leqslant m}\chi^*_{s-i-1,m}(x)\Bigg)\\ & - \Big(\mathscr{N}\chi_{s-i-1,t-j-1}(x) + \mathscr{R}\chi^*_{s-i-1,t-j-1}(x)\Big) - \frac{p-1}{2}\Big(\chi_{s-i,t-j-1}(x) + \chi^*_{s-i,t-j-1}(x)\Big)\Bigg),\end{aligned}$$

and

$$\begin{aligned}\theta^*_{ij}(x) \;=\; & \frac{1}{p^{i+1}q^{j+1}}\Bigg(\frac{(p-1)}{2}(q-1)\Bigg(\sum_{\substack{s-i\leqslant k\leqslant s-1\\ t-j\leqslant m\leqslant t}}(\chi_{km}(x)+\chi^*_{km}(x)) + \sum_{t-j\leqslant m\leqslant t}\chi_{sm}(x)\Bigg)\\ & + (q-1)\Bigg(\mathscr{R}\sum_{t-j\leqslant m\leqslant t}\chi_{s-i-1,m}(x) + \mathscr{N}\sum_{t-j\leqslant m\leqslant m}\chi^*_{s-i-1,m}(x)\Bigg)\\ & - \Big(\mathscr{R}\chi_{s-i-1,t-j-1}(x) + \mathscr{N}\chi^*_{s-i-1,t-j-1}(x)\Big) - \frac{p-1}{2}\Big(\chi_{s-i,t-j-1}(x) + \chi^*_{s-i,t-j-1}(x)\Big)\Bigg).\end{aligned}$$

(iv) For $1 \leqslant i \leqslant s-1$ *and* $j = t$,

$$\theta_{it}(x) = \frac{1}{p^{i+1}q^t}\Bigg(\frac{p-1}{2}\sum_{\substack{s-i\leqslant k\leqslant s-1\\ 0\leqslant m\leqslant t}}(\chi_{km}(x)+\chi^*_{km}(x)) + \frac{p-1}{2}\sum_{0\leqslant m\leqslant t}\chi_{sm}(x) + \mathscr{N}\sum_{0\leqslant m\leqslant t}\chi_{s-i-1,m}(x) + \mathscr{R}\sum_{0\leqslant m\leqslant t}\chi^*_{s-i-1,m}(x)\Bigg),$$

and

$$\theta^*_{it}(x) = \frac{1}{p^{i+1}q^t}\Bigg(\frac{p-1}{2}\sum_{\substack{s-i\leqslant k\leqslant s-1\\ 0\leqslant m\leqslant t}}(\chi_{km}(x)+\chi^*_{km}(x)) + \frac{p-1}{2}\sum_{0\leqslant m\leqslant t}\chi_{sm}(x) + \mathscr{R}\sum_{0\leqslant m\leqslant t}\chi_{s-i-1,m}(x) + \mathscr{N}\sum_{0\leqslant m\leqslant t}\chi^*_{s-i-1,m}(x)\Bigg).$$

(v) For $i = s$ *and* $0 \leqslant j \leqslant t-1$,

$$\theta_{sj}(x) = \frac{1}{p^s q^{j+1}}\Bigg((q-1)\Bigg(\sum_{\substack{0\leqslant k\leqslant s-1\\ t-j\leqslant m\leqslant t}}(\chi_{km}(x)+\chi^*_{km}(x)) + \sum_{t-j\leqslant m\leqslant t}\chi_{sm}(x)\Bigg) - \Bigg(\sum_{0\leqslant k\leqslant s-1}(\chi_{k,t-j-1}(x)+\chi^*_{k,t-j-1}(x)) + \chi_{s,t-j-1}(x)\Bigg)\Bigg).$$

(vi) For $i = s$ *and* $j = t$,

$$\theta_{st}(x) = \frac{1}{p^s q^t}\Bigg(\sum_{\substack{0\leqslant k\leqslant s-1\\ 0\leqslant m\leqslant t}}(\chi_{ij}(x)+\chi^*_{ij}(x)) + \sum_{0\leqslant m\leqslant t}\chi_{sj}(x)\Bigg) = \frac{1}{p^s q^t}\sum_{0\leqslant u<p^s q^t} x^u.$$

Case 2: q is a quadratic nonresidue modulo p

Let q be a quadratic nonresidue modulo p and $u \in C_{km}$ or C^*_{km}. If $k < i-1$ or $k \geqslant i$, then we can evaluate $\chi_{ij}(\alpha^{-u})$ in a similar way as in Case 1, for whether u is a quadratic residue modulo p does not influence the coefficient of χ_{km} or χ^*_{km}. However, if $k = i-1$, by theorem 2.12, whether the coefficient of χ_{km} (or χ^*_{km}) is a multiple of $\mathscr{R}$ or $\mathscr{N}$ depends on $j - m \bmod 2$. Then by (5.1), we can archive the results below.

Theorem 5.8. *Let q be a quadratic nonresidue modulo p.*

(i) For $i = 0$ *and* $j = t$,

$$\theta_{0t}(x) = \frac{1}{pq^t}\Bigg(\frac{p-1}{2}\sum_{0\leqslant m\leqslant t}\chi_{sm}(x) + \mathscr{N}\Bigg(\sum_{\substack{0\leqslant m\leqslant t\\ 2|t-m}}\chi_{s-1,m}(x) + \sum_{\substack{0\leqslant m\leqslant t\\ 2\nmid t-m}}\chi^*_{s-1,m}(x)\Bigg) + \mathscr{R}\Bigg(\sum_{\substack{0\leqslant m\leqslant t\\ 2|t-m}}\chi^*_{s-1,m}(x) + \sum_{\substack{0\leqslant m\leqslant t\\ 2\nmid t-m}}\chi_{s-1,m}(x)\Bigg)\Bigg),$$

and

$$\theta^*_{0t}(x) = \frac{1}{pq^t}\Bigg(\frac{p-1}{2}\sum_{0\leqslant m\leqslant t}\chi_{sm}(x) + \mathscr{R}\Bigg(\sum_{\substack{0\leqslant m\leqslant t\\ 2|t-m}}\chi_{s-1,m}(x) + \sum_{\substack{0\leqslant m\leqslant t\\ 2\nmid t-m}}\chi^*_{s-1,m}(x)\Bigg)$$
$$+ \mathscr{N}\Bigg(\sum_{\substack{0\leqslant m\leqslant t\\ 2|t-m}}\chi^*_{s-1,m}(x) + \sum_{\substack{0\leqslant m\leqslant t\\ 2\nmid t-m}}\chi_{s-1,m}(x)\Bigg)\Bigg).$$

(ii) For $i = 0$ and $0 \leqslant j \leqslant t-1$,

$$\begin{aligned}\theta_{0j}(x) \;=\; &\frac{1}{pq^{j+1}}\Bigg(\frac{(p-1)}{2}(q-1)\sum_{t-j\leqslant m\leqslant t}\chi_{sm}(x)\\ &+ (q-1)\mathscr{N}\Bigg(\sum_{\substack{t-j\leqslant m\leqslant t\\ 2|m-j}}\chi_{s-1,m}(x) + \sum_{\substack{t-j\leqslant m\leqslant t\\ 2\nmid m-j}}\chi^*_{s-1,m}(x)\Bigg)\\ &+ (q-1)\mathscr{R}\Bigg(\sum_{\substack{t-j\leqslant m\leqslant m\\ 2|m-j}}\chi^*_{s-1,m}(x) + \sum_{\substack{t-j\leqslant m\leqslant m\\ 2\nmid m-j}}\chi_{s-1,m}(x)\Bigg)\\ &- \Bigg(\frac{-1+(-1)^t\delta}{2}\chi_{s-1,t-j-1}(x) + \frac{-1-(-1)^t\delta}{2}\chi^*_{s-1,t-j-1}(x)\Bigg) - \frac{p-1}{2}\chi_{s,t-j-1}(x)\Bigg),\end{aligned}$$

and

$$\begin{aligned}\theta_{0j}(x)^* \;=\; &\frac{1}{pq^{j+1}}\Bigg(\frac{(p-1)}{2}(q-1)\sum_{t-j\leqslant m\leqslant t}\chi_{sm}(x)\\ &+ (q-1)\mathscr{R}\Bigg(\sum_{\substack{t-j\leqslant m\leqslant t\\ 2|m-j}}\chi_{s-1,m}(x) + \sum_{\substack{t-j\leqslant m\leqslant t\\ 2\nmid m-j}}\chi^*_{s-1,m}(x)\Bigg)\\ &+ (q-1)\mathscr{N}\Bigg(\sum_{\substack{t-j\leqslant m\leqslant m\\ 2|m-j}}\chi^*_{s-1,m}(x) + \sum_{\substack{t-j\leqslant m\leqslant m\\ 2\nmid m-j}}\chi_{s-1,m}(x)\Bigg)\\ &- \Bigg(\frac{-1-(-1)^t\delta}{2}\chi_{s-1,t-j-1}(x) + \frac{-1+(-1)^t\delta}{2}\chi^*_{s-1,t-j-1}(x)\Bigg) - \frac{p-1}{2}\chi_{s,t-j-1}(x)\Bigg).\end{aligned}$$

(iii) For $1 \leqslant i \leqslant s-1$ and $0 \leqslant j \leqslant t-1$,

$$\begin{aligned}\theta_{ij}(x) \;=\; &\frac{1}{p^{i+1}q^{j+1}}\Bigg(\frac{(p-1)}{2}(q-1)\Bigg(\sum_{\substack{s-i\leqslant k\leqslant s-1\\ t-j\leqslant m\leqslant t}}(\chi_{km}(x)+\chi^*_{km}(x)) + \sum_{t-j\leqslant m\leqslant t}\chi_{sm}(x)\Bigg)\\ &+ (q-1)\mathscr{N}\Bigg(\sum_{\substack{t-j\leqslant m\leqslant t\\ 2|m-j}}\chi_{s-i-1,m}(x) + \sum_{\substack{t-j\leqslant m\leqslant t\\ 2\nmid m-j}}\chi^*_{s-1,m}(x)\Bigg)\\ &+ (q-1)\mathscr{R}\Bigg(\sum_{\substack{t-j\leqslant m\leqslant m\\ 2|m-j}}\chi^*_{s-i-1,m}(x) + \sum_{\substack{t-j\leqslant m\leqslant m\\ 2\nmid m-j}}\chi_{s-1,m}(x)\Bigg)\end{aligned}$$

$$- \Big(\frac{-1+(-1)^t\delta}{2} \chi_{s-i-1,t-j-1}(x) + \frac{-1-(-1)^t\delta}{2} \chi^*_{s-i-1,t-j-1}(x) \Big)$$
$$- \frac{p-1}{2} \Big(\chi_{s-i,t-j-1}(x) + \chi^*_{s-i,t-j-1}(x) \Big) \Big),$$

and

$$\theta^*_{ij}(x) = \frac{1}{p^{i+1}q^{j+1}} \Bigg(\frac{(p-1)}{2}(q-1) \Big(\sum_{\substack{s-i\leqslant k\leqslant s-1 \\ t-j\leqslant m\leqslant t}} (\chi_{km}(x) + \chi^*_{km}(x)) + \sum_{t-j\leqslant m\leqslant t} \chi_{sm}(x) \Big)$$
$$+ (q-1)\mathscr{R}\Big(\sum_{\substack{t-j\leqslant m\leqslant t \\ 2|m-j}} \chi_{s-i-1,m}(x) + \sum_{\substack{t-j\leqslant m\leqslant t \\ 2\nmid m-j}} \chi^*_{s-1,m}(x) \Big)$$
$$+ (q-1)\mathscr{N}\Big(\sum_{\substack{t-j\leqslant m\leqslant m \\ 2|m-j}} \chi^*_{s-i-1,m}(x) + \sum_{\substack{t-j\leqslant m\leqslant m \\ 2\nmid m-j}} \chi_{s-1,m}(x) \Big)$$
$$- \Big(\frac{-1-(-1)^t\delta}{2} \chi_{s-i-1,t-j-1}(x) + \frac{-1+(-1)^t\delta}{2} \chi^*_{s-i-1,t-j-1}(x) \Big)$$
$$- \frac{p-1}{2} \Big(\chi_{s-i,t-j-1}(x) + \chi^*_{s-i,t-j-1}(x) \Big) \Bigg).$$

(iv) For $1 \leqslant i \leqslant s-1$ and $j = t$,

$$\theta_{it}(x) = \frac{1}{p^{i+1}q^t} \Bigg(\frac{p-1}{2} \sum_{\substack{s-i\leqslant k\leqslant s-1 \\ 0\leqslant m\leqslant t}} (\chi_{km}(x) + \chi^*_{km}(x)) + \frac{p-1}{2} \sum_{0\leqslant m\leqslant t} \chi_{sm}(x)$$
$$+ \mathscr{N}\Big(\sum_{\substack{0\leqslant m\leqslant t \\ 2|t-m}} \chi_{s-i-1,m}(x) + \sum_{\substack{0\leqslant m\leqslant t \\ 2\nmid t-m}} \chi^*_{s-i-1,m}(x) \Big) + \mathscr{R}\Big(\sum_{\substack{0\leqslant m\leqslant t \\ 2|t-m}} \chi^*_{s-i-1,m}(x) + \sum_{\substack{0\leqslant m\leqslant t \\ 2\nmid t-m}} \chi_{s-i-1,m}(x) \Big) \Bigg),$$

and

$$\theta_{it}(x) = \frac{1}{p^{i+1}q^t} \Bigg(\frac{p-1}{2} \sum_{\substack{s-i\leqslant k\leqslant s-1 \\ 0\leqslant m\leqslant t}} (\chi_{km}(x) + \chi^*_{km}(x)) + \frac{p-1}{2} \sum_{0\leqslant m\leqslant t} \chi_{sm}(x)$$
$$+ \mathscr{R}\Big(\sum_{\substack{0\leqslant m\leqslant t \\ 2|t-m}} \chi_{s-i-1,m}(x) + \sum_{\substack{0\leqslant m\leqslant t \\ 2\nmid t-m}} \chi^*_{s-i-1,m}(x) \Big) + \mathscr{N}\Big(\sum_{\substack{0\leqslant m\leqslant t \\ 2|t-m}} \chi^*_{s-i-1,m}(x) + \sum_{\substack{0\leqslant m\leqslant t \\ 2\nmid t-m}} \chi_{s-i-1,m}(x) \Big) \Bigg).$$

(v) For $i = s$ and $0 \leqslant j \leqslant t-1$,

$$\theta_{sj}(x) = \frac{1}{p^s q^{j+1}} \Bigg((q-1) \Big(\sum_{\substack{0\leqslant k\leqslant s-1 \\ t-j\leqslant m\leqslant t}} (\chi_{km}(x) + \chi^*_{km}(x)) + \sum_{t-j\leqslant m\leqslant t} \chi_{sm}(x) \Big)$$
$$- \Big(\sum_{0\leqslant k\leqslant s-1} (\chi_{k,t-j-1}(x) + \chi^*_{k,t-j-1}(x)) + \chi_{s,t-j-1}(x) \Big) \Bigg).$$

(vi) For $i = s$ and $j = t$,

$$\theta_{st}(x) = \frac{1}{p^s q^t}\Bigg(\sum_{\substack{0\leqslant k\leqslant s-1\\ 0\leqslant m\leqslant t}} (\chi_{ij}(x) + \chi^*_{ij}(x)) + \sum_{0\leqslant m\leqslant t} \chi_{sj}(x)\Bigg) = \frac{1}{p^s q^t}\sum_{0\leqslant u<p^s q^t} x^u.$$

Remark 5.9. *In Theorem 5.8, if $l = 2$, we set*

$$\frac{-1+\delta}{2} = \mathscr{R} = 1 \quad \textit{and} \quad \frac{-1-\delta}{2} = \mathscr{N} = 0,$$

are, respectively, the definitions of $\mathscr{R}$ and $\mathscr{N}$ above.

Example 5.10. *Set $p = 11$, $q = 5$, $s = t = 1$, $g = 2$, and $l = 3$. Then $n = 55$. 3 is a primitive of 5 and* $\mathrm{ord}_{11}(3) = 5$. *$R_1 = \{1, 3, 4, 5, 9, \}$ and $N_1 = \{2, 6, 7, 8, 10\}$. Note that 5 is a quadratic residue modulo 11, by Theorem 2.12, and the 3-ary cyclotomic cosets modulo 55 are given below:*

$$\begin{aligned}
&C_0 = \{0\},\\
&C_1 = \{5x + 11y : x \in R_1, y \in \mathbb{Z}_5^*\}\\
&\quad = \{1, 3, 4, 9, 12, 14, 16, 23, 26, 27, 31, 34, 36, 37, 38, 42, 47, 48, 49, 53\},\\
&C_2 = \{5x + 11y : x \in N_1, y \in \mathbb{Z}_5^*\}\\
&\quad = \{2, 6, 7, 8, 13, 17, 18, 19, 21, 24, 28, 29, 32, 39, 41, 43, 46, 51, 52, 54\},\\
&C_5 = \{5x : x \in R_1\} = \{5, 15, 20, 25, 45\},\\
&C_{10} = \{5x : x \in N_1\} = \{10, 30, 35, 40, 50\},\\
&C_{11} = \{11y : y \in \mathbb{Z}_5^*\} = \{11, 22, 33, 44\}.
\end{aligned}$$

Set $\delta = 2 \in \mathbb{F}_3$. Let α be a 55-th root of the unit such that $\mathscr{R} = 2$ and $\mathscr{N} = 0$. Note that $11^{-1} = 5^{-1} = 2$ in $\mathbb{F}_3$, by Theorem 5.7, and the six primitive idempotents are given below.

$$\begin{aligned}
&\theta_0(x) = 1 + x + \cdots + x^{54},\\
&\theta_1(x) = 2 + 2\chi_{10}(x) + \chi_2(x) + \chi_{11}(x),\\
&\theta_2(x) = 2 + 2\chi_5(x) + \chi_1(x) + \chi_{11}(x),\\
&\theta_5(x) = 2 + 2\chi_2(x) + 2\chi_{10}(x) + 2\chi_{11}(x),\\
&\theta_{10}(x) = 2 + 2\chi_1(x) + 2\chi_5(x) + 2\chi_{11}(x),\\
&\theta_{11}(x) = 1 + 2\chi_1(x) + 2\chi_2(x) + \chi_5(x) + \chi_1 0(x) + 2\chi_{11}(x).
\end{aligned}$$

Example 5.11. *Set $p = 7$, $q = 5$, $s = t = 1$, $g = 3$, and $l = 2$. Then $n = 35$. 2 is a primitive root of 5 and* $\mathrm{ord}_7(2) = 3$. *$R_1 = \{1, 2, 4\}$ and $N_1 = \{3, 5, 6\}$. Note that 5 is a quadratic nonresidue modulo 7, by Theorem 2.12, and the 2-ary cyclotomic cosets modulo 35 are given below:*

$$\begin{aligned}
&C_0 = \{0\},\\
&C_1 = \{5x + 7y : x \in N_1, y \in \mathbb{Z}_5^*\} = \{1, 2, 4, 8, 9, 11, 16, 18, 22, 23, 29, 32\},\\
&C_3 = \{5x + 7y : x \in R_1, y \in \mathbb{Z}_5^*\} = \{3, 6, 12, 13, 17, 19, 24, 26, 27, 31, 33\},\\
&C_5 = \{5x : x \in R_1\} = \{5, 10, 20\},
\end{aligned}$$

$$C_{15} = \{5x : x \in N_1\} = \{15, 25, 30\},$$
$$C_7 = \{7y : y \in \mathbb{Z}_5^*\} = \{7, 14, 21, 28\}.$$

Let α be a 35-th root of the unit such that $\mathscr{R} = 1$ and $\mathscr{N} = 0$. Note that $7^{-1} = 5^{-1} = 1$ in $\mathbb{F}_2$, by Theorem 5.8, and the six primitive idempotents are given below.

$$\theta_0(x) = 1 + x + \cdots + x^{34},$$
$$\theta_1(x) = \chi_3(x) + \chi_7(x),$$
$$\theta_3(x) = \chi_1(x) + \chi_7(x),$$
$$\theta_5(x) = 1 + \chi_3(x) + \chi_5(x) + \chi_7(x),$$
$$\theta_{15}(x) = 1 + \chi_1(x) + \chi_7(x) + \chi_{15}(x),$$
$$\theta_7(x) = \chi_1(x) + \chi_3(x) + \chi_7(x).$$

6. Parameters of some cyclic codes of length $p^s q^t$

The dimension of the minimal code $\mathscr{M}_\gamma$ is the number of non-zeros of the generating idempotent, which is the cardinality of the class C_γ.

Lemma 6.1 ([8], Lemma 10, p. 446)**.** *If $\mathscr{C}$ is a cyclic code of length n generated by $g(x)$ and is of minimum distance d, then the code $\hat{\mathscr{C}}$ of length nk generated by $g(x)(1 + x^n + \cdots + x^{(k-1)m})$ is a repetition code of $\mathscr{C}$ repeated k times and its minimum distance is dk.*

Proposotion 6.1. *The generating polynomials of the code $\mathscr{M}_0$ are clearly*

$$\frac{x^{p^s q^t} - 1}{x - 1} = 1 + x + \cdots + x^{p^s q^t - 1}$$

and its minimum distance is $p^s q^t$.

Proposotion 6.2. *For $0 \leqslant j \leqslant t - 1$,*

$$x^{p^s q^t} - 1 = (1 + x^{q^{t-j-1}} + \cdots + x^{(q-1)q^{t-j-1}})(x^{q^{t-j-1}} - 1)(1 + x^{q^{t-j}} + \cdots + x^{(p^s q^j - 1)q^{t-j}}).$$

The minimal polynomial of $\alpha^{p^s q^j}$ is

$$M_{p^s q^j}(x) = 1 + x^{q^{t-j-1}} + \cdots + x^{(q-1)q^{t-j-1}},$$

and therefore the generating polynomial of $\mathscr{M}_{p^s q^j}$ is

$$(x^{q^{t-j-1}} - 1)(1 + x^{q^{t-j}} + \cdots + x^{(p^s q^j - 1)q^{t-j}}).$$

Let $\mathscr{C}_j$ be the code of length q^{t-j} generated by $x^{q^{t-j-1}} - 1$, and then by Lemma 6.1, the code $\mathscr{M}_{p^s q^j}$ is the repetition code of $\mathscr{C}_j$ and its minimum distance is $2p^s q^j$.

Proposotion 6.3. *For $0 \leqslant i \leqslant s - 1$ and $0 \leqslant j \leqslant t$, we denote $d_{ij}^{(0)}(x) = M_{p^i q^j}(x)$ and $d_{ij}^{(1)}(x) = M_{p^i q^j g}(x)$. Let $A = (a_{ij}) \in \mathbb{F}_2^{s \times (t+1)}$. Let $\mathscr{C}_A$ be the code of length $p^s q^t$ generated by*

$$g_A(x) = \prod_{\substack{0 \leqslant i \leqslant s-1 \\ 0 \leqslant j \leqslant t}} d_{ij}^{(a_{ij})}(x),$$

and then $\mathscr{C}_A$ is a $[p^sq^t, \frac{(p^s+1)q^t}{2}]$ code with minimum odd-like weight $d \geqslant p^{s/2}$. In fact, let $A' = (1 - a_{ij})_{s\times(t+1)}$ and $\mathscr{C}_{A'}$ be the codes generated by

$$g_{A'}(x) = \prod_{\substack{0\leqslant i\leqslant s-1\\ 0\leqslant j\leqslant t}} d_{ij}^{(1-a_{ij})}(x).$$

Suppose $a(x)$ is a codeword of minimum odd-like weight d of $\mathscr{C}_A$. Then the polynomial

$$b(x) = a(x)a(x^g) \bmod (x^{p^sq^t} - 1)$$

is a codeword with odd-like weight of both $\mathscr{C}_A$ and $\mathscr{C}_{A'}$. It follows that $b(x)$ is a multiple of

$$g_A(x)g_{A'}(x) = \frac{x^{p^sq^t} - 1}{\prod\limits_{0\leqslant j\leqslant t} M_{p^sq^j}(x)} = \frac{x^{p^sq^t-1}}{x^{q^t} - 1} = 1 + x^{q^t} + \cdots + x^{(p^s-1)q^t}.$$

Since there are at most d^2 terms in $b(x)$, we have $d^2 \geqslant p^s$.

Proposotion 6.4. *Suppose $0 \leqslant i \leqslant s - 1$ and $0 \leqslant j \leqslant t$. Let $A = (a_{km}) \in \mathbb{F}_2^{(s-1)\times(t+1-j)}$. We define*

$$g_A(x) = \prod_{\substack{i\leqslant k\leqslant s-1\\ j\leqslant m\leqslant t}} d_{km}^{(a_{km})}(x),$$

and let $\mathscr{C}_A$ be the code generated by

$$g_A(x)(1 + x^{p^{s-i}q^{t-j}} + \cdots + x^{(p^iq^j-1)p^{s-i}q^{t-j}}).$$

Then $\mathscr{C}_A$ is a $[p^sq^t, \frac{(p^{s-i}+1)q^{t-j}}{2}]$ code with minimum odd-like weight $d \geqslant p^{(s+i)/2}q^j$. In fact, let $\bar{\mathscr{C}}_A$ be the code of length $p^{s-i}q^{t-j}$ with the generator polynomial $g_A(x)$. We also define $A' = (1 - a_{ij})_{(s-i)\times(t+1-j)}$ and $\bar{\mathscr{C}}_{A'}$ is the code of length $p^{s-i}q^{t-j}$ with the generator polynomial

$$g_{A'}(x) = \prod_{\substack{i\leqslant k\leqslant s-1\\ j\leqslant m\leqslant t}} d_{km}^{(1-a_{km})}(x).$$

Suppose $a(x)$ is a codeword of minimum odd-like weight d_0 of $\bar{\mathscr{C}}_A$. Then the polynomial

$$b(x) = a(x)a(x^g) \bmod (x^{p^{s-i}q^{t-j}} - 1)$$

is a codeword with odd-like weight of both $\bar{\mathscr{C}}_A$ and $\bar{\mathscr{C}}_{A'}$. It follows that $b(x)$ is a multiple of

$$g_A(x)g_{A'}(x) = \frac{x^{p^{s-i}q^{t-j}} - 1}{\prod\limits_{j\leqslant m\leqslant t} M_{p^sq^m}(x)} = \frac{x^{p^{s-i}q^{t-j}} - 1}{x^{q^{t-j}} - 1} = 1 + x^{q^{t-j}} + \cdots + x^{(p^{s-i}-1)q^{t-j}}.$$

Since there are at most d_0^2 terms in $b(x)$, we have $d_0^2 \geqslant p^{s-i}$. Then by Lemma 6.1, we have

$$d = p^iq^jd_0 \geqslant p^{(s+i)/2}q^j.$$

Author contributions

All authors contributed equally to the writing and review of this manuscript. All authors have read and approved the final version of the manuscript for publication.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was supported by Natural Science Foundation of Beijing Municipal (M23017).

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. K. Kumar, S. Betra, Cyclotomy, cyclotomic cosets and arithmetic properties of some families in $\frac{\mathbb{F}_l[x]}{\langle x^{p^l q}-1\rangle}$, *Asian-Eur. J. Math.*, **2** (2023), 2350023. https://doi.org/10.1142/S1793557123500237
2. C. Ding, T. Helleseth, New generalized cyclotomy and its applications, *Finite Fields Appl.*, **4** (1998), 140–166. https://doi.org/10.1006/ffta.1998.0207
3. F. Li, Q. Yue, The primitive idempotents and weight distributions of irreducible constacyclix codes, *Des. Codes Cryptogr.*, **86** (2018), 771–784. https://doi.org/10.1007/s10623-017-0356-2
4. C. Ding, Cyclotomic constructions of cyclic codes with length being the product of two primes, *IEEE Trans. Inform. Theory*, **58** (2012), 2231–2236. https://doi.org/10.1109/TIT.2011.2176915
5. R. Singh, M. Pruthi, Primitive idempotents of irreducible quadratic residue cyclic codes of length $p^n q^m$, *Int. J. Algrbra*, **5** (2011), 285–294.
6. F. Li, Q. Yue, The minimum Hamming distances of irreducible cyclic codes, *Finite Fields Appl.*, **29** (2014), 225–242. https://doi.org/10.1016/j.ffa.2014.05.003
7. Z. Shi, F. Fu, The primitive idempotents of irreducible constacyclic codes and LCD cyclic codes, *Cryptogr. Commun.*, **12** (2020), 29–52. https://doi.org/10.1007/s12095-019-00362-w
8. G. K. Bakshi, M. Raka, Minimal cyclic codes of length $p^n q$, *Finite Fields Appl.*, **9** (2003), 432–448. https://doi.org/10.1016/S1071-5797(03)00023-6
9. A. Sahni, P. T. Sehgal, Minimal cyclic codes of length $p^n q$, *Finite Fields Appl.*, **18** (2012), 1017–1036. https://doi.org/10.1016/j.ffa.2012.07.003
10. S. Jain, S. Betra, Cyclotomy and arithmetic properties of some families in $\mathbb{Z}[x]/\langle x^{pq}-1\rangle$, *Asian-Eur. J. Math.*, **13** (2020), 2050077. https://doi.org/10.1142/S1793557120500771
11. S. Jain, S. Batra, Cyclic self dual codes of length pq over $\mathbb{Z}_4$, *J. Discr. Math. Sci. Cryptogr.*, **15** (2022), 2305–2319. https://doi.org/10.1080/09720529.2020.1823680

12. F. J. MacWilliams, N. J. Z. Sloane, *Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.

13. D. M. Burton, *Elementary Number Theory*, New Delhi: Tate McGra-Hill Publishers, 2007.

14. G. Hardy, E. Wright, *An Introduction to the Theory of Numbers*, 5Eds., Oxford: Clarendon Press, 1984.

AIMS Press