A tight upper bound on the number of nonzero weights of a quasi-cyclic code *

Xiaoxiao Li¹, Minjia Shi¹, San Ling²

¹School of Mathematical Sciences, Anhui University, Hefei, 230601, China
²School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

Abstract

Let \( C \) be a quasi-cyclic code of index \( l (l \geq 2) \). Let \( G \) be the subgroup of the automorphism group of \( C \) generated by \( \rho^l \) and the scalar multiplications of \( C \), where \( \rho \) denotes the standard cyclic shift. In this paper, we find an explicit formula of orbits of \( G \) on \( C \setminus \{0\} \). Consequently, an explicit upper bound on the number of nonzero weights of \( C \) is immediately derived and a necessary and sufficient condition for codes meeting the bound is exhibited. If \( C \) is a one-generator quasi-cyclic code, a tighter upper bound on the number of nonzero weights of \( C \) is obtained by considering a larger automorphism subgroup which is generated by the multiplier, \( \rho^l \) and the scalar multiplications of \( C \). In particular, we list some examples to show the bounds are tight. Our main result improves and generalizes some of the results in [25].

Keywords: Quasi-cyclic code, Hamming weight, upper bound, group action

1 Introduction

In 1973, Delsarte studied the for a given code \( C \), the relations between the number of distinct distances for \( C \), the number of distinct distances for the dual code \( C^\perp \),

*This research is supported by Natural Science Foundation of China under Grant 12071001. The work of Xiaoxiao Li is supported by the China Scholarship Council under Grant 202306500025.
and the minimum distances of $C$ and $C^\perp$, see [9]. In that paper, some interesting results on the weight distributions of cosets of a code are obtained, which show the importance of the number of distinct distances in the code. It is easy to see that when one restricts the study to linear codes, then the number of distinct distances coincides with the number of nonzero weights. The early researches on determining the number of weights of a given nonzero linear code can be seen in [1–3, 12, 13, 21].

For a general linear code, it seems very difficult to obtain an explicit formula for the number of nonzero weights of the code. A more modest goal is to find acceptable bounds on the number of nonzero weights of a linear code. Indeed, there have been several recent works investigating lower and upper bounds on the number of nonzero weights of linear codes. Alderson [1] determined necessary and sufficient conditions for the existence of full weight spectrum codes, i.e., codes containing codewords of each weight up to the code length. Shi et al. in a series of papers [24–26] studied the number of nonzero weights of linear codes. Shi, Li, Neri and Sole [21] derived upper and lower bounds on the number of nonzero weights of cyclic codes. Chen and Zhang [8] obtained the explicit upper bound on the number of nonzero weights of a simple-root cyclic code and exhibit a necessary and sufficient condition for cyclic codes meeting the bound. Moreover, in [8], their results improves and generalizes some of the results in [24]. Recently, Chen et al. [7] improved the upper bound in [8] with larger subgroups of the automorphism groups of the codes.

Motivated by the work [8, 7] and [25], the objective of this paper is to establish a tight upper bound on the number of nonzero weights of a quasi-cyclic code of index $l(l \geq 2)$ with simple root. In [8] and [7], Chen et al. pointed out the number of nonzero weights of a linear code is bounded from above by the number of orbits of the automorphism group acting on the code. Let $C$ be a quasi-cyclic code of length $lm$ and index $l$ (co-index $m$). Let $G$ be the subgroup of $\text{Aut}(C)$ (the automorphism group of $C$) generated by $\rho^l$ and the scalar multiplications of $C$, where $\rho$ denotes the standard cyclic shift. The problem is therefore converted to finding the number of orbits of $G$ on $C^* \setminus \{0\}$. An explicit formula for the number of orbits of $G$ on $C^*$ is obtained. Consequently, an explicit upper bound on the number of nonzero weights of $C$ is immediately derived and a necessary and sufficient condition for quasi-cyclic codes meeting the bound is exhibited. If $C$ is a one-generator quasi-cyclic code, we consider a larger automorphism subgroup which is generated by the multiplier, $\rho^l$ and the scalar multiplications of $C$ and obtain a tighter upper bound on the number of nonzero weights. We also note that [25, Section III] gave some upper bounds on
the number of nonzero weights of a special class of strongly quasi-cyclic code, i.e., a quasi-cyclic code of co-index $m$ such that all its nonzero codewords have period $m$. Comparing our results with those in [25, Section III], our results remove the constrain “strongly” and characterize a necessary and sufficient condition for the codes meeting the bounds.

The material is arranged as follows. Section 2 contains the necessary terminology and definitions on linear codes, quasi-cyclic codes and group actions. Section 3 presents the main results (see Theorems 1, 2 and 3), which give the tight upper bounds on the number of weights that a quasi-cyclic code can have. Section 4 gives the proofs of Theorems 1, 2 and 3 by counting the number of orbits of $G$ on $C^*$. Several examples in Section 5 show our bound is tight. Finally, we share our conclusions and some open problems in Section 6.

2 Background material

Let $F_q$ be the finite field with $q$ elements and let $F_q^* = F_q \setminus \{0\}$ be the multiplicative group of the finite field $F_q$. In this section, we review some previously known facts about linear codes, automorphism group of a linear code, and recall some notions and results about quasi-cyclic codes.

2.1 Linear codes and group actions

Let $F_q^n$ be the set of all $n$-tuples whose coordinates belong to $F_q$. A linear code $C$ of length $n$ over $F_q$ is a vector subspace of $F_q^n$ over $F_q$. The dimension of the code is its dimension as an $F_q$-vector space, and is denoted by $k$. A linear code of length $n$ and dimension $k$ over $F_q$ will be denoted for brevity by $[n,k]$ code. The elements of $C$ are called codewords.

The Hamming weight of $x \in F_q^n$ is the number of indices $i$ where $x_i \neq 0$, and it is denoted by $\text{wt}_H(x)$. The set of weights of a linear code $C$ (including the 0) is denoted by $\text{wt}(C)$, and the number of nonzero weights of $C$ by $s(C)$, i.e. $\text{wt}(C) = \{ \text{wt}_H(c) | c \in C \}$ and $s(C) = |\text{wt}(C) \setminus \{0\}| = |\text{wt}(C)| - 1$.

**Definition 1.** Let $C$ be a linear code of length $n$ over $F_q$. The automorphism group of $C$, denoted by $\text{Aut}(C)$, consists of all $n \times n$ monomial matrices $A$ over $F_q$ such that $cA \in C$ for all $c \in C$. 
Now we recall the result which is the number of nonzero weights of $C$ is bounded from the number of $G$-orbits, where $G$ is a subgroup of $\text{Aut}(C)$, see [8, 23].

**Proposition 1.** [8] Let $C$ be a linear code of length $n$ over $\mathbb{F}_q$ with $s(C)$ nonzero weights and let $\text{Aut}(C)$ be the automorphism group of $C$. Suppose that $G$ is a subgroup of $\text{Aut}(C)$. If the number of orbits of $G$ on $C^* = C \setminus \{0\}$ is equal to $N$, then $s(C) \leq N$. Moreover, the equality holds if and only if for any two nonzero codewords $c_1, c_2 \in C^*$ with the same weight, there exists an automorphism $A \in G$ such that $c_1A = c_2$.

In order to determine the number of orbits of $G$ on $C^*$, we need two important lemmas from [8, 14].

**Lemma 1.** [14] Let $C$ be a linear code of length $n$ over $\mathbb{F}_q$ and let $\text{Aut}(C)$ be the automorphism group of $C$. Suppose that $G$ is a subgroup of $\text{Aut}(C)$. Then, the cardinality of $G \setminus C^*$ (the set of all the orbits of $G$ on $C^*$) is equal to

$$|G \setminus C^*| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|,$$

where $\text{Fix}(g) = \{ c \in C | gc = c \}$.

**Lemma 2.** [8] Let $G$ be a finite group acting on a finite set $X$ and let $H$ be a normal subgroup of $G$. It is clear that $H$ naturally acts on $X$. Suppose the set of $H$-orbits are denoted by $H \setminus X = \{ Hx | x \in X \}$. Then the factor group $G/H$ acts on $H \setminus X$ and

$$|G \setminus X| = |(G/H) \setminus (H \setminus X)|.$$

### 2.2 Quasi-cyclic codes

In this subsection, we recall some definitions and results about quasi-cyclic codes. For more detailed information about cyclic codes and quasi-cyclic codes, readers may refer to [5, 6, 10, 11, 15–20, 22].

Let $a_1, a_2, \ldots, a_r$ be integers, where $r \geq 2$ is a positive integer. Let $\text{gcd}(a_1, a_2, \ldots, a_r)$ be the greatest common divisor of $a_1, a_2, \ldots, a_r$. Let $m$ be a positive integer with $\text{gcd}(m, q) = 1$. Let $\mathbb{F}_q[x]$ denote the polynomials in the indeterminate $x$ with coefficients in $\mathbb{F}_q$. Let $\langle x^m - 1 \rangle$ denote the ideal generated by $x^m - 1$ in $\mathbb{F}_q[x]$. Then, we have the quotient ring $R_m = \mathbb{F}_q[x]/\langle x^m - 1 \rangle$. 

4
We denote by $\rho$ the standard shift operator on $\mathbb{F}_q^n$. A linear code is said to be quasi-cyclic of index $l$ or $l$-quasi-cyclic code if and only if it is invariant under $\rho^l$. Let $C$ be a quasi-cyclic code over $\mathbb{F}_q$ of length $n = lm$ and index $l$. Let $c = (c_{00}, c_{01}, \ldots, c_{0,l-1}, c_{10}, c_{11}, \ldots, c_{1,l-1}, \ldots, c_{m-1,0}, c_{m-1,1}, \ldots, c_{m-1,l-1})$ denote a codeword in $C$.

Define a map $\phi : \mathbb{F}_{qlm} \rightarrow R_l^m$ by

$$\phi(c) = (c_0(x), c_1(x), \ldots, c_{l-1}(x)) \in R_l^m,$$

where $c_j(x) = \sum_{i=0}^{m-1} c_{ij}x^i \in R_m$. It is known (cf. [15], for instance) that $\phi$ induces a one-to-one correspondence between quasi-cyclic codes over $\mathbb{F}_q$ of index $l$ and length $lm$ and linear codes over $R_m$ of length $l$.

It is well known that every minimal ideal of $R_m$ is generated uniquely by a primitive idempotent of $R_m$, see [11]. There is a one-to-one correspondence between the primitive idempotents of $R_m$ and the $q$-cyclotomic cosets modulo $m$. Let $m'$ be the order of $q$ modulo $m$, i.e., $m'$ is the least positive integer such that $m$ is a divisor of $q^{m'} - 1$. Suppose $\zeta$ is a primitive $m$-th root of unity in $\mathbb{F}_{q^{m'}}$ and there are $s + 1$ distinct $q$-cyclotomic cosets $\{\Gamma_j\}_{j=0}^s$ modulo $m$ with $\Gamma_0 = \{i_0 = 0\}$ and $\Gamma_t = \{i_t, i_tq, i_tq^2, \ldots, i_tq^{k_t-1}\}$ for $1 \leq t \leq s$, where $k_t$ is the cardinality of the $q$-cyclotomic coset $\Gamma_t$ for $0 \leq t \leq s$. Then the quotient ring $\mathbb{F}_{q^{m'}}[x]/\langle x^m - 1 \rangle$ has exactly $m$ primitive idempotents given by

$$e_i = \frac{1}{m} \sum_{j=0}^{m-1} \zeta^{-ij}x^j \quad \text{for } 0 \leq i \leq m - 1,$$

see [6]. Moreover, $R_m = \mathbb{F}_q[x]/\langle x^m - 1 \rangle$ has exactly $s$ primitive idempotents given by

$$\varepsilon_t = \sum_{j \in \Gamma_t} e_j \quad \text{for } 0 \leq t \leq s.$$

According to [11] Theorem 4.3.8, $R_m$ is the vector space direct sum of the minimal ideals $R_m \varepsilon_t$ for $0 \leq t \leq s$, in symbols,

$$R_m = R_m \varepsilon_0 \oplus R_m \varepsilon_1 \oplus \cdots \oplus R_m \varepsilon_s.$$

Using the Discrete Fourier Transform, we have, for each $0 \leq t \leq s$,

$$R_m \varepsilon_t = \left\{ \sum_{j=0}^{k_t-1} \left( \sum_{u=0}^{k_t-1} c_u \zeta^{ju}q^{j} \right)e_{iuq^j} | c_j \in \mathbb{F}_q \right\}.$$

(1)
Therefore, $R_m^t$ is the direct sum of $(R_m \varepsilon_t)^l$ for $0 \leq t \leq s$, in symbols,

$$(R_m)^l = (R_m \varepsilon_0)^l \oplus (R_m \varepsilon_1)^l \oplus \cdots \oplus (R_m \varepsilon_s)^l.$$ 

It follows that every $R_m$-linear code $\phi(C)$ of length $l$ can be decomposed as the direct sum

$$\phi(C) = C_0 \oplus C_1 \oplus \cdots \oplus C_s,$$

where $C_t$ is a linear code over $R_m \varepsilon_t$ of length $l$ for $0 \leq t \leq s$ and $C$ is a quasi-cyclic code over $\mathbb{F}_q$ of length $n = lm$ and index $l$. Actually, for each $1 \leq t \leq s$, $C_t$ is a subset of $(R_m \varepsilon_t)^l$. A quasi-cyclic code $C$ is one-generator if and only if its generator matrix over $R_m$ contains only one row, see [19].

3 Statement of main results

In this section we give a tight upper bound on $s(C)$ which is the number of nonzero weights of a quasi-cyclic code $C$. For a general quasi-cyclic code $C$, we consider two obvious automorphisms: one is the cyclic shift $\rho^l$ whose $\rho$ is the standard shift operator and $l$ is the index of $C$, and the other is the scalar multiplication. For a one-generator quasi-cyclic code $C$, apart from the cyclic shift and the scalar multiplications, we consider that the multiplier $\mu$ is also an automorphism of $C$. According to Proposition 1 if the number of the orbits of the group generated by these three automorphisms on $C$ can be figured out, then we have a upper bound of $s(C)$, naturally.

The main results of this paper are given below.

Theorem 1. Let $C$ be a quasi-cyclic code of length $lm$ and index $l$ over $\mathbb{F}_q$. Suppose that

$$C = C_{t_1} \oplus C_{t_2} \oplus \cdots \oplus C_{t_U},$$

where $0 \leq t_1 < t_2 < \cdots < t_U \leq s$, $C_{t_j}$ is a linear code over $R_m \varepsilon_{t_j}$ of length $l$ and also is a $[n = lm, K_{t_j}]$ quasi-cyclic code over $\mathbb{F}_q$ for $1 \leq j \leq U$. Suppose that the primitive idempotent $\varepsilon_{t_j}$ corresponds to the $q$-cyclotomic coset $\{i_{t_j}, i_{t_j}q, \ldots, i_{t_j}q^{K_{t_j}-1}\}$ for each $1 \leq j \leq U$. Then the number of orbits of $\langle \rho^l \rangle$ on $C^* = C \setminus \{0\}$ is equal to

$$\sum_{\{j_1, j_2, \ldots, j_u\} \subseteq \{1, 2, \ldots, U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} \frac{\gcd(m, i_{t_{j_1}}, i_{t_{j_2}}, \ldots, i_{t_{j_u}})}{m} \prod_{v=1}^{u} (q^{K_{t_{j_v}}} - 1),$$

which is denoted by $N$. In particular,

$$s(C) \leq N.$$
with equality if and only if for any codewords \( c_1, c_2 \in C^* \) with the same weight, there exists an integer \( i \) such that \( \rho^i(c_1) = c_2 \).

Let \( U = 2 \), then the formula in Theorem 1 can be concise and clear. As a direct application of Theorem 1, we immediately obtain the following corollary.

**Corollary 1.** Let \( C \) be a quasi-cyclic code of length \( lm \) and index \( l \) over \( \mathbb{F}_q \). Suppose that

\[
C = C_{t_1} \oplus C_{t_2},
\]

where \( 0 \leq t_1 < t_2 \leq s \), \( C_{t_j} \) is a linear code over \( R_{m\varepsilon_{t_j}} \) of length \( l \) and is also a \([n = lm, K_{t_j}]\) quasi-cyclic code over \( \mathbb{F}_q \) for \( 1 \leq j \leq 2 \). Suppose that the primitive idempotent \( \varepsilon_{t_j} \) corresponds to the \( q \)-cyclotomic coset \( \{i_{t_j}, i_{t_j}q, \ldots, i_{t_j}q^{K_{t_j} - 1}\} \) for each \( 1 \leq j \leq 2 \). Then the number of orbits of \( \langle \rho, M \rangle \) on \( C^* = C \setminus \{0\} \) is equal to

\[
\frac{\gcd(m, i_{t_1}, i_{t_2}) (q^{K_{t_1}} - 1)(q^{K_{t_2}} - 1)}{m} + \frac{\gcd(m, i_{t_1}) (q^{K_{t_1}} - 1)}{m} + \frac{\gcd(m, i_{t_2}) (q^{K_{t_2}} - 1)}{m}.
\]

Next, we turn to study the action of \( \langle \rho', M \rangle \) on \( C^* \), where \( \rho \) is the standard shift operator and \( l \) is the index of \( C \), and \( M = \{\sigma a | a \in \mathbb{F}_q^*\} \) consists of the scalar multiplications on \( C \). It is easy to check that \( \sigma a \rho' = \rho' \sigma a \) for any \( a \in \mathbb{F}_q^* \). According to the definitions of \( \rho' \) and \( M \), we immediately get the following results.

**Lemma 3.** The subgroup \( \langle \rho', M \rangle \) of \( \text{Aut}(C) \) is the direct product of \( \rho' \) and \( M \), that is

\[
\langle \rho', M \rangle = \langle \rho' \rangle \times M.
\]

In particular, \( \langle \rho', M \rangle \) is of order \( m(q - 1) \).

**Theorem 2.** Let \( C \) be a quasi-cyclic code of length \( lm \) and index \( l \) over \( \mathbb{F}_q \). Suppose that

\[
C = C_{t_1} \oplus C_{t_2} \oplus \cdots \oplus C_{t_U},
\]

where \( 0 \leq t_1 < t_2 < \cdots < t_U \leq s \), \( C_{t_j} \) is a linear code over \( R_{m\varepsilon_{t_j}} \) of length \( l \) and is also a \([n = lm, K_{t_j}]\) quasi-cyclic code over \( \mathbb{F}_q \) for \( 1 \leq j \leq U \). Suppose that the primitive idempotent \( \varepsilon_{t_j} \) corresponds to the \( q \)-cyclotomic coset \( \{i_{t_j}, i_{t_j}q, \ldots, i_{t_j}q^{K_{t_j} - 1}\} \) for each \( 1 \leq j \leq U \). Then the number of orbits of \( \langle \rho', M \rangle \) on \( C^* = C \setminus \{0\} \) is equal to

\[
\sum_{\{j_1, j_2, \ldots, j_U\} \subseteq \{1, 2, \ldots, U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} \frac{\gcd(m, i_{j_1}, i_{j_2}, \ldots, i_{j_u}) \prod_{v=1}^{u} (q^{K_{j_v}} - 1)}{m(q - 1)}.
\]
gcd \left( q - 1, \frac{m}{\gcd(m, i_{t_1})}, \ldots, \frac{m}{\gcd(m, i_{t_u})} \right),

which is denoted by N. In particular,

\[ s(C) \leq N, \]

with equality if and only if for any codewords \( c_1, c_2 \in C^* \) with the same weight, there exists an integer \( i \) and an element \( a \in \mathbb{F}_q^* \) such that \( \rho^i(a c_1) = c_2 \).

By virtue of Theorem 2, we immediately obtain the following corollary.

**Corollary 2.** Let \( C \) be a quasi-cyclic code of length \( lm \) and index \( l \) over \( \mathbb{F}_q \). Suppose that

\[ C = C_{t_1} \oplus C_{t_2}, \]

where \( 0 \leq t_1 < t_2 \leq s \), \( C_{t_j} \) is a linear code over \( R_{m} \varepsilon_{t_j} \) of length \( l \) and is also a \([n = lm, K_{t_j}]\) quasi-cyclic code over \( \mathbb{F}_q \) for \( 1 \leq j \leq 2 \). Suppose that the primitive idempotent \( \varepsilon_{t_j} \) corresponds to the \( q \)-cyclotomic coset \( \{i_{t_j}, i_{t_j}q, \ldots, i_{t_j}q^{K_{t_j} - 1}\} \) for each \( 1 \leq j \leq 2 \). Then the number of orbits of \( \langle \rho^l, M \rangle \) on \( C^* = C \setminus \{0\} \) is equal to

\[
\frac{\gcd(m, i_{t_1}, i_{t_2})(q^{K_{t_1}} - 1)(q^{K_{t_2}} - 1)}{m(q - 1)} \cdot \gcd \left( q - 1, \frac{m}{\gcd(m, i_{t_1})}, \frac{m}{\gcd(m, i_{t_2})} \right) \\
+ \frac{\gcd(m, i_{t_1})(q^{K_{t_1}} - 1)}{m(q - 1)} \cdot \gcd \left( q - 1, \frac{m}{\gcd(m, i_{t_1})} \right) \\
+ \frac{\gcd(m, i_{t_2})(q^{K_{t_2}} - 1)}{m(q - 1)} \cdot \gcd \left( q - 1, \frac{m}{\gcd(m, i_{t_2})} \right).
\]

The map \( \mu_q : x \mapsto x^q \) is a ring isomorphism from \( R_m \) onto itself. It can be extended to \( R_{m}^l \) componentwise. Then, we turn to study the action of \( \langle \mu_q, \rho^l, M \rangle \) on \( C^* \).

**Theorem 3.** Suppose that \( f_1(x), f_2(x), \ldots, f_U(x) \in R_m \). Let \( C \) be a one-generator quasi-cyclic code of length \( lm \) and index \( l \) over \( \mathbb{F}_q \). Suppose that

\[ C = C_{t_1} \oplus C_{t_2} \oplus \cdots \oplus C_{t_U}, \]

where \( 0 \leq t_1 < t_2 < \cdots < t_U \leq s \), \( C_{t_j} \) is a linear code over \( R_{m} \varepsilon_{t_j} \) of dimension 1 and length \( l \) with generator matrix \([a_{j,0}(x), a_{j,1}(x), \ldots, a_{j,l-1}(x)]\) over \( R_{m} \varepsilon_{t_j} \), where \( a_{j,v} \in \{0, f_j(x)\} \) for \( 0 \leq v \leq l - 1 \), and is also a \([n = lm, K_{t_j}]\) quasi-cyclic code over \( \mathbb{F}_q \) for \( 1 \leq j \leq U \). Suppose that the primitive idempotent \( \varepsilon_{t_j} \) corresponds to the
corollary \{i_t, i_t q, \ldots, i_t q^{k_{j-1}}\} for each \(1 \leq j \leq U\). Then the number of orbits of \(\langle \mu_q, \rho^j, M \rangle\) on \(C^* = C \setminus \{0\}\) is equal to

\[
\sum_{\{j_1, j_2, \ldots, j_u\} \subseteq \{1, 2, \ldots, U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} N_{j_1, j_2, \ldots, j_u},
\]

where

\[
N_{j_1, j_2, \ldots, j_u} = \frac{1}{m' m (q - 1)} \sum_{r=0}^{m' - 1} \gcd\left( m, \frac{i_{t_1} I_{t_1}}{\gcd(I, I_{t_1})}, \ldots, \frac{i_{t_m} I_{t_m}}{\gcd(I, I_{t_m})}, \frac{(i_{t_{j_2}} - i_{t_{j_1}}) I_{t_{j_1}} I_{t_{j_2}}}{\gcd(I_{t_{j_1}}, I_{t_{j_2}})}, \ldots, \frac{(i_{t_{j_u}} - i_{t_{j_{u-1}}}) I_{t_{j_{u-1}}} I_{t_{j_u}}}{\gcd(I_{t_{j_{u-1}}}, I_{t_{j_u}})} \right) \gcd(I, I_{t_{j_1}}, \ldots, I_{t_{j_u}}) \cdot \prod_{v=1}^{u} (q^{\gcd(k_{j_v}, r)} - 1)
\]

with \(I = q - 1\) and \(I_{t_v} = \frac{q^{k_{j_v} - 1}}{q^{\gcd(k_{j_v}, r)} - 1}\) for \(v = 1, 2, \ldots, u\).

In particular, the number of non-zero weights of \(C\) is less than or equal to the number of orbits of \(\langle \mu_q, \rho^j, M \rangle\) on \(C^*\).

By virtue of Theorem 3 we immediately obtain the following corollary.

**Corollary 3.** Suppose that \(f_1(x), f_2(x) \in R_m\). Let \(C\) be a one-generator quasi-cyclic code of length \(lm\) and index \(l\) over \(F_q\). Suppose that

\[
C = C_{t_1} \oplus C_{t_2},
\]

where \(0 \leq t_1 < t_2 \leq s\), \(C_{t_j}\) is a linear code over \(R_m \varepsilon_{t_j}\) of dimension 1 and length \(l\) with generator matrix \([a_{j,0}(x), a_{j,1}(x), \ldots, a_{j,l-1}(x)]\) over \(R_m \varepsilon_{t_j}\), where \(a_{j,v} \in \{0, f_j(x)\}\) for \(0 \leq v \leq l - 1\), and is also a \([n = lm, k_j]\) quasi-cyclic code over \(F_q\) for \(1 \leq j \leq 2\). Suppose that the primitive idempotent \(\varepsilon_{t_j}\) corresponds to the \(q\)-cyclotomic coset \(\{i_{t_j}, i_{t_j} q, \ldots, i_{t_j} q^{k_{j-1}}\}\) for each \(1 \leq j \leq 2\). Suppose \(k_{t_1}|k_{t_2}\) then the number of orbits of \(\langle \mu_q, \rho^j, M \rangle\) on \(C^* = C \setminus \{0\}\) is equal to

\[
s_{t_1} + s_{t_2} + s_{t_1, t_2},
\]

where

\[
s_{t_v} = \frac{1}{k_{t_v}} \sum_{r|k_{t_v}} \varphi\left(\frac{k_{t_v}}{r}\right) \gcd(q^r - 1, \frac{q^{k_{t_v}} - 1}{q - 1}, \frac{i_{t_v} (q^{k_{t_v}} - 1)}{m}) \quad \text{for} \quad v = 1, 2,
\]
and
\[ s_{t_1,t_2} = \frac{1}{m'} \sum_{r=0}^{m'-1} \gcd\left( (q^{\gcd(k_1,r)} - 1) \gcd(q^{\gcd(k_2,r)} - 1), \frac{(q^{k_1} - 1)(q^{\gcd(k_2,r)} - 1)}{(q - 1)(q^{\gcd(k_1,r)} - 1)} \right) \frac{i_{t_1}(q^{k_1} - 1)}{m(q^{\gcd(k_1,r)} - 1)}, \frac{i_{t_2}(q^{k_2} - 1)}{m(q^{\gcd(k_1,r)} - 1)}, (i_{t_2} - i_{t_1})(q^{k_1} - 1)(q^{k_2} - 1) ) \].

In particular, the number of non-zero weights of \( C \) is less than or equal to the number of orbits of \( \langle \mu_q, \rho^l, M \rangle \) on \( C^* \).

4 Proofs of main results

This section is divided into four parts. First, we give the statement of some lemmas. Next, we present the proofs of the main results.

4.1 Statement of some lemmas

Recall that \( R_m = \mathbb{F}_q[x]/(x^m - 1) \). We have the following two \( \mathbb{F}_q \)-linear maps on \( R_m \), denoted by \( \rho^l \) and \( \sigma_a \), respectively:

\[ \rho^l : R_m^l \rightarrow R_m^l \]

\[ \rho^l \left( \sum_{i=0}^{m-1} c_0 x^i, \sum_{i=0}^{m-1} c_1 x^i, \ldots, \sum_{i=0}^{m-1} c_{l-1} x^i \right) = \left( \sum_{i=0}^{m-1} c_0 x^{i+1}, \sum_{i=0}^{m-1} c_1 x^{i+1}, \ldots, \sum_{i=0}^{m-1} c_{l-1} x^{i+1} \right) \]

is a \( \mathbb{F}_q \)-vector space isomorphism of \( R_m^l \), and for any fixed element \( a \in \mathbb{F}_q^* \),

\[ \sigma_a : R_m^l \rightarrow R_m^l \]

\[ \sigma_a \left( \sum_{i=0}^{m-1} c_0 x^i, \sum_{i=0}^{m-1} c_1 x^i, \ldots, \sum_{i=0}^{m-1} c_{l-1} x^i \right) = \left( \sum_{i=0}^{m-1} ac_0 x^i, \sum_{i=0}^{m-1} ac_1 x^i, \ldots, \sum_{i=0}^{m-1} ac_{l-1} x^i \right) \]

is a \( \mathbb{F}_q \)-vector space isomorphism of \( R_m^l \). Both \( \rho^l \) and \( \sigma_a \) are also linear maps on \( \mathbb{F}_q^n \) with \( n = lm \), which satisfy that for any element \( c \) of \( \mathbb{F}_q^m \) and

\[ c = (c_0, c_0, \ldots, c_0, c_{l-1}, c_{10}, c_{11}, \ldots, c_{1,l-1}, \ldots, c_{m-1,0}, c_{m-1,1}, \ldots, c_{m-1,l-1}) \]

then

\[ \rho^l(c) = (c_{10}, c_{11}, \ldots, c_{1,l-1}, c_{20}, c_{21}, \ldots, c_{2,l-1}, \ldots, c_{00}, c_{01}, \ldots, c_{0,l-1}) \]
The map $\mu_q : x \mapsto x^q$ is a ring isomorphism from $R_m$ onto itself. It can be extended to $R^l_m$ componentwise. Specifically, the multiplier $\mu_q$ defined on $R^l_m$ by

$$\mu_q : R^l_m \to R^l_m$$

$$\mu_q \left( \sum_{i=0}^{m-1} c_{i0} x^i, \ldots, \sum_{i=0}^{m-1} c_{i,l-1} x^i \right) = \left( \sum_{i=0}^{m-1} c_{i0} x^{qi}, \ldots, \sum_{i=0}^{m-1} c_{i,l-1} x^{qi} \right) \mod (x^m - 1)$$

is a ring automorphism of $R^l_m$. Since $\gcd(m, q) = 1$, the map $\mu_q$ induces a permutation of the coefficients of any polynomial in $R_m$.

For any quasi-cyclic code $C$ of length $n = lm$ and index $l$, it is readily seen that all $\mu_q$, $\rho^j$ and $\sigma_a$ belong to $\text{Aut}(C)$. We know that $M = \{ \sigma_a | a \in \mathbb{F}_q^* \}$ is a subgroup of $\text{Aut}(C)$. Clearly, the subgroup $M$ is cyclic with order $q - 1$. Since $\gcd(l, n) = \gcd(l, lm) = l$, $\langle \rho^l \rangle$ is of order $m$. Let $m'$ be the order of $q$ modulo $m$. Therefore, $\langle \mu_q \rangle = \{ \mu_q^i | 0 \leq i \leq m' - 1 \}$, i.e., $\langle \mu_q \rangle$ is of order $m'$. The proof of the following Lemma is similar to that in [7, Lemma 2.2], so we omit it.

**Lemma 4.** The subgroup $\langle \mu_q, \rho^l, M \rangle$ of $\text{Aut}(C)$ is of order $m'm(q - 1)$, and each element of $\langle \mu_q, \rho^l, M \rangle$ can be written uniquely as a product $\mu_q^{i_1} \rho^{i_2} \sigma_a$ for some $0 \leq r_1 \leq m' - 1$, $0 \leq r_2 \leq m - 1$ and $a \in \mathbb{F}_q^*$.

Firstly, we consider the action of $\rho^l$ on $C^*$. For each integer $i$ with $0 \leq i \leq m - 1$, it is easy to check that $|\text{Fix}(\rho^{il})| = |\text{Fix}(\rho^{\gcd(i, m)})| = |\text{Fix}(\rho^{\gcd(i, m)l})|$, where

$$\text{Fix}(\rho^{il}) = \{ c \in C^* | \rho^{il}(c) = c \}.$$ 

For an integer $r$ with $r|m$, the number of integers $i$ satisfying $0 \leq i \leq m - 1$ and $\gcd(i, m) = r$ is equal to $\varphi(m)$, where $\varphi$ is Euler’s totient function. By Lemma 4, one has

$$|\langle \rho^l \rangle \setminus C^*| = \frac{1}{m} \sum_{i=0}^{m-1} |\text{Fix}(\rho^{il})| = \frac{1}{m} \sum_{r|m} \varphi(m) |\text{Fix}(\rho^{rl})|. \quad (3)$$

**Lemma 5.** Let $C$ be a $[n = lm, K]$ quasi-cyclic code over $\mathbb{F}_q$ which is a linear code over $R_m \varepsilon_t$. Suppose that the primitive idempotent $\varepsilon_t$ corresponds to the $q$-cyclotomic
coset \{i_t, i_tq, \ldots, i_tq^{k-1}\}. Then the number of orbits of \langle \rho^j \rangle on \mathcal{C}^* = \mathcal{C} \setminus \{0\} is equal to 
\[
\frac{\gcd(m, i_t)(q^K - 1)}{m}
\]
In particular,
\[
s(\mathcal{C}) \leq \frac{\gcd(m, i_t)(q^K - 1)}{m},
\]
with equality if and only if for any codewords \(c_1, c_2 \in \mathcal{C}^*\) with the same weight, there exists an integer \(i\) such that \(\rho^i(c_1) = c_2\).

**Proof.** By Proposition 11, it is enough to count the number of orbits of \langle \rho^j \rangle on \mathcal{C}^*. By Eq. (3), we aim to find the value of \(|\text{Fix}(\rho^j)|\), for each divisor \(r\) of \(m\). To this end, let \(r\) be a divisor of \(m\) and take a typical nonzero element
\[
c = (c_0(x), c_1(x), \ldots, c_{l-1}(x)) \in \mathcal{C}^*,
\]
where \(c_u(x) \in R_m \varepsilon_t\) for \(0 \leq u \leq l - 1\). By Eq. (11), for each \(0 \leq u \leq l - 1\),
\[
c_u(x) = \sum_{j=0}^{k-1} (c_{u0} + c_{u1} \zeta^{ijq^j} + \cdots + c_{u,k-1} \zeta^{(k-1)ijq^j})e_{iq^j} \in R_m \varepsilon_t.
\]
Note that \(e_{iq^j} = \frac{1}{m} \sum_{v=0}^{m-1} \zeta^{-iq^j v} x^v\), and thus
\[
x^r e_{iq^j} = \frac{1}{m} \sum_{v=0}^{m-1} \zeta^{-iq^j v} x^{v+r}
\]
\[
= \zeta^{iq^j r} \frac{1}{m} \sum_{v=0}^{m-1} \zeta^{-iq^j (v+r)} x^{v+r}
\]
\[
= \zeta^{iq^j r} e_{iq^j}.
\]
Since \(\rho^j(c) = (xc_0(x), xc_1(x), \ldots, xc_{l-1}(x))\), then we have
\[
\rho^j(c) = (x^r c_0(x), x^r c_1(x), \ldots, x^r c_{l-1}(x))
\]
and
\[
x^r c_u(x) = x^r \left( \sum_{j=0}^{k-1} (c_{u0} + c_{u1} \zeta^{ijq^j} + \cdots + c_{u,k-1} \zeta^{(k-1)ijq^j}) e_{iq^j} \right)
\]
\[
= \sum_{j=0}^{k-1} (c_{u0} + c_{u1} \zeta^{ijq^j} + \cdots + c_{u,k-1} \zeta^{(k-1)ijq^j}) x^r e_{iq^j}
\]
\[
= \sum_{j=0}^{k-1} \zeta^{iq^j r} (c_{u0} + c_{u1} \zeta^{ijq^j} + \cdots + c_{u,k-1} \zeta^{(k-1)ijq^j}) e_{iq^j},
\]

12
for $0 \leq u \leq l - 1$. It follows that $\rho^{il}(c) = c$ if and only if $x^r c_u(x) = c_u(x)$ for all $0 \leq u \leq l - 1$ if and only if $\zeta^{uq^ir} = 1$ for all $0 \leq j \leq k - 1$. Since $\zeta$ is a primitive $m$-th root of unity and $\gcd(m, q) = 1$, $\zeta^{uq^ir} = 1$ precisely when $m$ is a divisor of $uq^r$ (equivalently, $\frac{m}{r}$ is a divisor of $u$). This leads to

$$|\text{Fix}(\rho^l)| = \begin{cases} q^K - 1, & \text{if } \frac{m}{r} | i_t; \\ 0, & \text{if } \frac{m}{r} \nmid i_t. \end{cases}$$

By Eq. (3), the number of orbits of $\langle \rho^l \rangle$ on $C^*$ is equal to

$$\frac{1}{m} \sum_{i=0}^{m-1} |\text{Fix}(\rho^i)| = \frac{1}{m} \sum_{r|m} \varphi\left(\frac{m}{r}\right) |\text{Fix}(\rho^l)|$$

$$= \frac{q^K - 1}{m} \sum_{r|m, \frac{m}{r} | i_t} \varphi\left(\frac{m}{r}\right)$$

$$= \gcd(m, i_t)(q^K - 1)/m.$$ 

The proof is completed. \hfill \square

Based on Lemma 3, we use the method provided in Lemma 2 to determine the number of orbits of the group $\langle \rho^l, M \rangle$ acting on the quasi-cyclic code.

**Lemma 6.** Let $C$ be a $[n = lm, K]$ quasi-cyclic code over $F_q$ which is a linear code over $R_m \mathbb{E}_i$. Suppose that the primitive idempotent $\mathbb{E}_i$ corresponds to the $q$-cyclotomic coset $\{i_t, i_t q, \ldots, i_t q^{k-1}\}$. Then the number of orbits of $\langle \rho^l, M \rangle$ on $C^* = C \setminus \{0\}$ is equal to

$$\gcd\left(m, (q - 1)i_t\right)(q^K - 1)/m(q - 1).$$

In particular,

$$s(C) \leq \frac{\gcd\left(m, (q - 1)i_t\right)(q^K - 1)}{m(q - 1)},$$

with equality if and only if for any codewords $c_1, c_2 \in C^*$ with the same weight, there exists an integer $i$ and an element $a \in F_q^*$ such that $\rho^i(a c_1) = c_2$.

**Proof.** It is readily seen that the multiplicative cyclic group $F_q^*$ is isomorphic to $M$; consequently, $M$ is a cyclic group of order $q - 1$. In particular, if $\xi$ is a primitive element of $F_q$ (namely, the cyclic group $F_q^*$ is generated by $\xi$), then $\sigma_\xi$ is a generator of $M$. Recall that $\langle \rho^l \rangle \setminus C^* = \{\langle \rho^l \rangle(c) | c \in C^*\}$ denotes the set of orbits of $\langle \rho^l \rangle$ on
\(C^* = C \setminus \{0\}\), where \(\langle \rho^i \rangle(c) = \{\rho^i(c)|0 \leq i \leq m-1\}\). Then \(M\) acts on \(\langle \rho^i \rangle \setminus C^*\) in the following natural way:
\[
M \times \langle \rho^i \rangle \setminus C^* \rightarrow \langle \rho^i \rangle \setminus C^*
\]
\[
(\sigma, \langle \rho^i \rangle(c)) \mapsto \langle \rho^i \rangle(ac).
\]
By Lemma 2, the number of orbits of \(M\) on \(C^*\) is equal to the number of orbits of \(M\) on \(\langle \rho^i \rangle \setminus C^*\), where the latter is equal to
\[
|\langle (\rho^i, M) \setminus C^* \rangle| = \frac{1}{q-1} \sum_{r|q-1} \varphi \left( \frac{q-1}{r} \right) |\text{Fix}(\sigma^*_\xi)|
\]
with \(\text{Fix}(\sigma^*_\xi) = \{\langle \rho^i \rangle(c) \in \langle \rho^i \rangle \setminus C^*|\langle \rho^i \rangle(c) = \langle \rho^i \rangle(\xi^* \cdot c)\}\). Therefore, our ultimate goal is to calculate the value of \(|\text{Fix}(\sigma^*_\xi)|\). To this end, as we did in the proof of Lemma 5, let \(r\) be a divisor of \(q-1\) and take a typical nonzero element
\[
c = (c_0(x), c_1(x), \ldots, c_{l-1}(x)) \in C^*,
\]
where \(c_u(x) \in R_m \varepsilon_t\) for \(0 \leq u \leq l-1\). By Eq. (1), for each \(0 \leq u \leq l-1\),
\[
c_u(x) = \sum_{j=0}^{k-1} (c_{u0} + c_{u1} \zeta^{iq^j} + \cdots + c_{u,k-1} \zeta^{(k-1)iq^j}e_{i,q^j}) \in R_m \varepsilon_t.
\]
The condition \(\langle \rho^z \rangle(c) = \langle \rho^z \rangle(\xi^* \cdot c)\) is equivalent to requiring that there exists an integer \(z \geq 0\) such that \(\rho^z(c) = \xi^* \cdot c\). Simple algebraic calculations show that
\[
\rho^z(c) = (x^z c_0(x), x^z c_1(x), \ldots, x^z c_{l-1}(x))
\]
and
\[
\xi^* \cdot c = (\xi^* c_0(x), \xi^* c_1(x), \ldots, \xi^* c_{l-1}(x)),
\]
where for each \(0 \leq u \leq l-1\),
\[
x^z c_u(x) = \sum_{j=0}^{k-1} \zeta^{iq^j} (c_{u0} + c_{u1} \zeta^{iq^j} + \cdots + c_{u,k-1} \zeta^{(k-1)iq^j}) \in R_m \varepsilon_t
\]
and
\[
\xi^* c_u(x) = \sum_{j=0}^{k-1} \xi^*(c_{u0} + c_{u1} \zeta^{iq^j} + \cdots + c_{u,k-1} \zeta^{(k-1)iq^j}) \in R_m \varepsilon_t.
\]
Therefore, \(\rho^z(c) = \xi^* c\) if and only if \(x^z c_u(x) = \xi^* c_u(x)\) for \(0 \leq u \leq l-1\) if and only if there exists an integer \(z \geq 0\) such that \(\zeta^{iq^j} = \xi^*\) for \(0 \leq j \leq k-1\). Since \(\xi \in \mathbb{F}_q\),
there exists an integer \( z \geq 0 \) such that \( \zeta^{i_{j}q_{j}z} = \xi^r \) for \( 0 \leq j \leq k-1 \) if and only if there exists an integer \( z \geq 0 \) such that \( \zeta^{i_{z}} = \xi^r \).

In the following we transform the equality \( \zeta^{i_{z}} = \xi^r \) into numerical conditions. Suppose that \( \omega \) is a primitive element of \( \mathbb{F}_{q^m'} \), where \( m' \) is the least positive integer such that \( m' \) is a divisor of \( q^{m'} - 1 \). Denote by \( \text{ord}(\alpha) \) the order of the element \( \alpha \in \mathbb{F}_{q^m'} \).

Note that \( \zeta \) is a primitive \( m \)-th root of unity, \( \xi \) is a primitive \( (q-1) \)-th root of unity and \( r \) is a divisor \( q-1 \). Setting \( \zeta = \omega^{\frac{q^{m'}-1}{m}} \) and \( \xi = \omega^{\frac{q^{m'}-1}{q-1}} \), we have

\[
\zeta^{i_{z}} = \xi^r \iff \omega^{\frac{(q^{m'}-1)i_{z}}{m}} = \omega^{\frac{(q^{m'}-1)i_{z}}{q-1}} \\
\iff \langle \omega^{\frac{(q^{m'}-1)i_{z}}{q-1}} \rangle \subseteq \langle \omega^{\frac{(q^{m'}-1)i_{z}}{q-1}} \rangle \\
\iff \text{ord}(\omega^{\frac{(q^{m'}-1)i_{z}}{q-1}}) | \text{ord}(\omega^{\frac{(q^{m'}-1)i_{z}}{q-1}}) \\
\iff \text{gcd}(q^{m'}-1, \frac{(q^{m'}-1)i_{z}}{m}) \mid \frac{(q^{m'}-1)i_{z}}{q-1} \\
\iff \frac{(q^{m'}-1) \text{gcd}(m, i_{z})}{m} \mid \frac{(q^{m'}-1)i_{z}}{q-1} \\
\iff \frac{q-1}{r} \mid \frac{m}{\text{gcd}(m, i_{z})},
\]

where \( \langle \omega^{\frac{(q^{m'}-1)i_{z}}{q-1}} \rangle \) and \( \langle \omega^{\frac{(q^{m'}-1)i_{z}}{q-1}} \rangle \) denote the cyclic subgroups of \( \mathbb{F}_{q^m'}^{\times} \) generated by \( \omega^{\frac{(q^{m'}-1)i_{z}}{q-1}} \) and \( \omega^{\frac{(q^{m'}-1)i_{z}}{q-1}} \), respectively. It follows that there exists an integer \( z \geq 0 \) such that \( \zeta^{i_{z}} = \xi^r \) if and only if \( \frac{q-1}{r} \) is a divisor of \( \frac{m}{\text{gcd}(m, i_{z})} \). By Lemma 5, \( \langle \rho' \rangle \setminus C^\ast \) has size \( \frac{\text{gcd}(m, i_{z})(q^{K}-1)}{m} \); then we have

\[
|\text{Fix}(\sigma_{\xi})| = \begin{cases} 
\frac{\text{gcd}(m, i_{z})(q^{K}-1)}{m}, & \text{if } \frac{q-1}{r} \mid \frac{m}{\text{gcd}(m, i_{z})}; \\
0, & \text{if } \frac{q-1}{r} \nmid \frac{m}{\text{gcd}(m, i_{z})}.
\end{cases}
\]
Returning to Eq. (11), the number of orbits of \( \langle \rho^l, M \rangle \) on \( C^* \) is equal to
\[
|\langle \rho^l, M \rangle \setminus C^*| = \frac{1}{q - 1} \sum_{r | (q - 1)} \varphi\left( \frac{q - 1}{r} \right) |\text{Fix}(\sigma_{\xi}^r)|
\]
\[
= \frac{1}{q - 1} \sum_{r | (q - 1)} \varphi(r) |\text{Fix}(\sigma_{\xi}^r)|
\]
\[
= \frac{1}{q - 1} \sum_{r | (q - 1), r | \gcd(m, \sigma_{\xi}^r)} \varphi(r) \frac{\gcd(m, \sigma_{\xi}^r)(q^K - 1)}{m}
\]
\[
= \frac{\gcd(m, i^q_l)(q^K - 1)}{m(q - 1)} \sum_{r | (q - 1), r | \gcd(m, \sigma_{\xi}^r)} \varphi(r)
\]
\[
= \frac{\gcd(m, (q - 1)i^q_l)(q^K - 1)}{m(q - 1)}
\]
The proof is completed. \(\square\)

Next, we consider the action of \( \langle \mu^q, \rho^l, M \rangle \) on \( C^* \), where \( C \) is a one-generator quasi-cyclic code.

**Lemma 7.** Suppose that \( f(x) \in R_m \). Let \( C \) be a one-generator quasi-cyclic code over \( \mathbb{F}_q \) which is a \([l, 1]\)-linear code over \( R_m \varepsilon_i \) with generator matrix \([a_0(x), a_1(x), \ldots, a_{l-1}(x)]\) over \( R_m \varepsilon_i \), where \( a_v \in \{0, f(x)\} \) for \( 0 \leq v \leq l - 1 \). Suppose that the primitive idempotent \( \varepsilon_i \) corresponds to the \( q \)-cyclotomic coset \( \{i^q_l, i^q_lq, \ldots, i^q_lq^{k-1}\} \). Then the number of orbits of \( \langle \mu^q, \rho^l, M \rangle \) on \( C^* = C \setminus \{0\} \) is equal to
\[
\frac{1}{k} \sum_{r | k} \varphi\left( \frac{k}{r} \right) \gcd\left( q^r - 1, \frac{q^k - 1}{q - 1}, \frac{i^q_{i}q^{k-1} - 1}{m} \right).
\]
In particular,
\[
s(C) \leq \frac{1}{k} \sum_{r | k} \varphi\left( \frac{k}{r} \right) \gcd\left( q^r - 1, \frac{q^k - 1}{q - 1}, \frac{i^q_{i}q^{k-1} - 1}{m} \right),
\]
with equality if and only if for any codewords \( c_1, c_2 \in C^* \) with the same weight, there exist integers \( i, j \) and \( a \in \mathbb{F}_q^* \) such that \( \mu^i_q \rho^j q^m \sigma(a)(c_1) = c_2 \).
Proof. By Proposition 1, it is enough to count the number of orbits of \(\langle \mu_q, \rho^l, M \rangle\) on \(C^*\). It follows from Eq. (3) and Lemma 4 that

\[
|\langle \mu_q, \rho^l, M \rangle \backslash C^*| = \frac{1}{m'm'(q-1)} \sum_{r_1=0}^{m-1} \sum_{r_2=0}^{m-1} \sum_{a \in F_q^*} |\{ c \in C^* | \mu_q^{r_1} \rho^{r_2} \sigma_a(c) = c \}|. \tag{5}
\]

Take a typical nonzero element

\[c = (c_0(x), c_1(x), \ldots, c_{l-1}(x)) \in C^*,\]

where \(c_u(x) \in R_{m \varepsilon_t}\) for \(0 \leq u \leq l - 1\). Since \(C\) is a \([l, 1]\)-linear code over \(R_{m \varepsilon_t}\), each \(c_u(x) \in \{0, F(x)\}\) where \(F(x) \in R_{m \varepsilon_t}\). Therefore, \(\mu_q^{r_1} \rho^{r_2} \sigma_a(c) = c\) if and only if

\[\mu_q^{r_1} \rho^{r_2} \sigma_a(F(x)) = F(x).\]

By Eq. (1),

\[F(x) = \sum_{j=0}^{k-1} (f_0 + f_1 \zeta^{i_q q^j} + \cdots + f_{k-1} \zeta^{(k-1)i_q q^j}) e_{i_q q^j} \in R_{m \varepsilon_t}.\]

Note that \(e_{i_q q^j} = \frac{1}{m} \sum_{v=0}^{m-1} \zeta^{-i_q q^j v} x^v\) and \(\rho^{r_2} \sigma_a(e_{i_q q^j}) = a \zeta^{i_q q^{r_2 j}} e_{i_q q^j}\) thus

\[\mu_q^{r_1} \rho^{r_2} \sigma_a(e_{i_q q^j}) = a \zeta^{i_q q^{r_2 j}} e_{i_q q^{-r_2 j+j}},\]

where the subscript \(i_q q^{-r_2 j+j}\) is calculated modulo \(m\). Then we have

\[\mu_q^{r_1} \rho^{r_2} \sigma_a(F(x)) = \mu_q^{r_1} \rho^{r_2} \sigma_a \left( \sum_{j=0}^{k-1} (f_0 + f_1 \zeta^{i_q q^j} + \cdots + f_{k-1} \zeta^{(k-1)i_q q^j}) e_{i_q q^j} \right)\]

\[= \sum_{j=0}^{k-1} (f_0 + f_1 \zeta^{i_q q^j} + \cdots + f_{k-1} \zeta^{(k-1)i_q q^j}) \mu_q^{r_1} \rho^{r_2} \sigma_a(e_{i_q q^j})\]

\[= \sum_{j=0}^{k-1} a \zeta^{i_q q^{r_2 j}} (f_0 + f_1 \zeta^{i_q q^j} + \cdots + f_{k-1} \zeta^{(k-1)i_q q^j}) e_{i_q q^{-r_2 j+j}}\]

\[= \sum_{j=0}^{k-1} a \zeta^{i_q q^{-r_2 j+j} q^{r_2 j}} (f_0 + f_1 \zeta^{i_q q^{-r_2 j+j}} + \cdots + f_{k-1} \zeta^{(k-1)i_q q^{-r_2 j+j}}) q^{r_2 j} e_{i_q q^{-r_2 j+j}}\]

\[= \sum_{j=0}^{k-1} a \zeta^{i_q q^{1+j r_2}} (f_0 + f_1 \zeta^{i_q q^j} + \cdots + f_{k-1} \zeta^{(k-1)i_q q^j}) q^{r_2 j} e_{i_q q^j}.\]

Hence \(\mu_q^{r_1} \rho^{r_2} \sigma_a(F(x)) = F(x)\) if and only if

\[a(f_0 + f_1 \zeta^{i_q q^j} + \cdots + f_{k-1} \zeta^{(k-1)i_q q^j}) q^{r_2 j-1} = \zeta^{-i_q q^{1+j r_2}} \quad \text{for} \quad 0 \leq j \leq k - 1,\]

17
which is equivalent to

\[ a(f_0 + f_1\zeta^{i_1} + \cdots + f_{k-1}\zeta^{(k-1)i_1})q^{r-1} = \zeta^{-iuq^{r+2}}. \]

Since the minimal polynomial of \( \zeta^{i_1} \) over \( \mathbb{F}_q \) is of degree \( k \), the set

\[ \{ f_0 + f_1\zeta^{i_1} + \cdots + f_{k-1}\zeta^{(k-1)i_1} | f_v \in \mathbb{F}_q, 0 \leq v \leq k-1 \} \]

forms a subfield of \( \mathbb{F}_{q^m} \) of size \( q^k \). Therefore, the number of \( \mathbb{F}_q \) satisfying \( \mu_q^r \rho^{s_0} \sigma_0(\mathbb{F}_q) = c \) is equal to the number of \( \mathbb{F}(x) \in R_{m\in} \) satisfying \( \mu_q^r \rho^{s_0} \sigma_0(\mathbb{F}(x)) = \mathbb{F}(x) \), which is equal to the number of \( \alpha \in \mathbb{F}_{q^k}^* \) such that \( a\alpha q^{r-1} = \zeta^{-iuq^{r+2}} \). By the proof of [7, Theorem 3.1], we have the following three facts:

1. The number of \( \alpha \in \mathbb{F}_{q^k}^* \) such that \( a\alpha q^{r-1} = \zeta^{-iuq^{r+2}} \) is equal to 0 or \( q^\gcd(k,r_1) - 1 \).

2. Let \( \mathbb{F}_q \) and \( \mathbb{F}_{q^k}^* \) be generated by \( \xi \) and \( \theta \), respectively. For \( 0 \leq r_1 \leq m'-1 \), denote \( S(r_1) = \{ 0 \leq r_2 \leq m-1|\zeta^{-iuq^{r+2}} \in \langle \xi \rangle \langle \theta^{q^{r-1}} \rangle \} \), and then \( |S(r_1)| = \gcd(m, i_1|\langle \xi \rangle \langle \theta^{q^{r-1}} \rangle \}) \).

3. Suppose \( r_2 \in S(r_1) \) and denote \( R(r_1, r_2) = \{ 0 \leq r \leq q-2|\zeta^{-iuq^{r+2}} \in \xi^r \langle \theta^{q^{r-1}} \rangle \} \).

Then, \( |R(r_1, r_2)| = |\langle \xi \rangle \langle \theta^{q^{r-1}} \rangle | \).

According to these three facts and the similar calculation as in [7, Theorem 3.1], we have that

\[
|\langle \mu_q, \rho^I, M \rangle \rangle | C^* | = \frac{1}{m'm(q-1)} \sum_{r_1=0}^{m'-1} \sum_{r_2 \in S(r_1)} \sum_{r_2 \in R(r_1, r_2)} (q^\gcd(k,r_1) - 1)
\]

\[
= \frac{1}{m'm(q-1)} \sum_{r_1=0}^{m'-1} |S(r_1)||R(r_1, r_2)| (q^\gcd(k,r_1) - 1)
\]

\[
= \frac{1}{m'm(q-1)} \sum_{r_1=0}^{m'-1} \gcd(m|\langle \xi \rangle \langle \theta^{q^{r-1}} \rangle |, i_1|\langle \xi \rangle \langle \theta^{q^{r-1}} \rangle |) (q^\gcd(k,r_1) - 1)
\]

\[
= \frac{1}{k} \sum_{r|k} \varphi \left( \frac{k}{r} \right) \gcd \left( q^r - 1, \frac{q^k - 1}{q - 1}, \frac{i_1(q^k - 1)}{m} \right).
\]

The proof is completed. \( \square \)
4.2 Proof of Theorem 1 and Corollary 1

Proof. It is easy to check that \( \mathcal{C}^* \) is equal to

\[
\bigsqcup_{\{j_1,j_2,\ldots,j_u\} \subseteq \{1,2,\ldots,U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} C_{t_{j_1}} \setminus \{0\} \oplus C_{t_{j_2}} \setminus \{0\} \oplus \cdots \oplus C_{t_{j_u}} \setminus \{0\},
\]

which is a disjoint union. For all \( j_1, j_2, \ldots, j_u \), \( C_{t_{j_v}} \) is a linear code over \( R_m \mathcal{E}_{t_{j_v}} \) of length \( l \) with \( 1 \leq v \leq u \). Let \( s_{j_1,j_2,\ldots,j_u} \) be the number of orbits of \( \langle \rho^l \rangle \) acting on

\[
C_{t_{j_1}} \setminus \{0\} \oplus C_{t_{j_2}} \setminus \{0\} \oplus \cdots \oplus C_{t_{j_u}} \setminus \{0\},
\]

which is denoted by \( \mathcal{C}^l_{j_1,j_2,\ldots,j_u} \). Thus the group \( \langle \rho^l \rangle \) can act on the set \( \mathcal{C}^l_{j_1,j_2,\ldots,j_u} \) in the same way as the group action on \( \mathcal{C} \). Then, we have

\[
\mathcal{C}^* = \bigsqcup_{\{j_1,j_2,\ldots,j_u\} \subseteq \{1,2,\ldots,U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} \mathcal{C}^l_{j_1,j_2,\ldots,j_u}
\]

and

\[
|\langle \rho^l \rangle \setminus \mathcal{C}^*| = \sum_{\{j_1,j_2,\ldots,j_u\} \subseteq \{1,2,\ldots,U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} s_{j_1,j_2,\ldots,j_u}.
\]

It is enough to compute the number of orbits of the group \( \langle \rho^l \rangle \) acting on \( \mathcal{C}^l_{j_1,j_2,\ldots,j_u} \).

According to Eq. (8), we only need to compute the value of \( |\text{Fix}(\rho^l)| \) for each divisor \( r \) of \( m \). Let \( c = c_{t_{j_1}} + c_{t_{j_1}} + \cdots + c_{t_{j_u}} \in \mathcal{C}^l_{j_1,j_2,\ldots,j_u} \), where \( c_{t_{j_v}} \in C_{t_{j_v}} \setminus \{0\} \subseteq (R_m \mathcal{E}_{t_{j_v}})^l \) for \( v = 1, 2, \ldots, u \). Suppose that for each \( v = 1, 2, \ldots, u \),

\[
c_{t_{j_v}} = (c_{t_{j_v},0}(x), c_{t_{j_v},1}(x), \ldots, c_{t_{j_v},l-1}(x)),
\]

where \( c_{t_{j_v},v'}(x) = \sum_{j=0}^{k_{t_{j_v}}-1} \sum_{u'=0}^{k_{t_{j_v}}-1} c_{v',u',t_{j_v}} \zeta^{u't_{j_v}} q^l e_{t_{j_v}} q^j \) for \( 0 \leq v' \leq l - 1 \). Then we have

\[
\rho^l(c) = \rho^l(c_{t_{j_1}}) + \rho^l(c_{t_{j_2}}) + \cdots + \rho^l(c_{t_{j_u}})
\]

\[
= \left( x^r \sum_{v=1}^{u} c_{t_{j_v},0}(x), x^r \sum_{v=1}^{u} c_{t_{j_v},1}(x), \ldots, x^r \sum_{v=1}^{u} c_{t_{j_v},l-1}(x) \right),
\]

where for each \( 0 \leq v' \leq l - 1 \),

\[
x^r \sum_{v=1}^{u} c_{t_{j_v},v'}(x) = \sum_{j=0}^{k_{t_{j_1}}-1} \zeta^{j t_{j_1}} q^l r \sum_{u'=0}^{k_{t_{j_1}}-1} c_{v',u',t_{j_1}} \zeta^{u't_{j_1}} q^j e_{t_{j_1}} q^j + \cdots
\]

\[
+ \sum_{j=0}^{k_{t_{j_v}}-1} \zeta^{j t_{j_v}} q^l r \sum_{u'=0}^{k_{t_{j_v}}-1} c_{v',u',t_{j_v}} \zeta^{u't_{j_v}} q^l q e_{t_{j_v}} q^j.
\]
Then we can conclude that \( \rho^l(c) = c \) if and only if \( \rho^l(c_{t_1}) + \rho^l(c_{t_1}) + \cdots + \rho^l(c_{t_u}) = c_{t_1} + c_{t_1} + \cdots + c_{t_u} \) if and only if \( x^r \sum_{v=1}^{u} c_{t_{jv}}(x) = \sum_{v=1}^{u} c_{t_{jv}}(x) \) for \( 1 \leq v' \leq l-1 \) if and only if \( \zeta^{i_{jv}}q^{r} = 1 \) for all \( v \) and \( j \) if and only if \( m|w^{i_{jv}q^{r}} \) for all \( v \) and \( j \) if and only if \( m|i_{jv}r \) for \( 1 \leq v \leq u \) if and only if \( \frac{m}{r}|i_{jv} \) for \( 1 \leq v \leq u \). It follows that

\[
|\text{Fix}(\rho^l)| = \begin{cases} 
\prod_{v=1}^{u}(q^{K_{jv}} - 1), & \text{if } \frac{m}{r}|i_{jv} \text{ for all } v = 1, 2, \ldots, u; \\
0, & \text{otherwise.}
\end{cases}
\]

Using Eq. (3), the number of orbits of \( \langle \rho^l \rangle \) on \( C^*_j \) is

\[
s_{j_1j_2\cdots j_u} = |\langle \rho^l \rangle \setminus C^*_j| = \frac{1}{m} \sum_{r|m} \varphi\left(\frac{m}{r}\right)|\text{Fix}(\rho^l)| = \frac{1}{m} \sum_{r|m} \varphi\left(\frac{m}{r}\right)\prod_{v=1}^{u}(q^{K_{jv}} - 1)
\]

\[
= \frac{\gcd(m, i_{t_1}, i_{t_2}, \ldots, i_{t_u})}{m} \prod_{v=1}^{u}(q^{K_{jv}} - 1).
\]

Therefore, the number of orbits of \( \langle \rho^l \rangle \) on \( C^* = C \setminus \{0\} \) is equal to

\[
\sum_{\{j_1, j_2, \ldots, j_u\} \subseteq \{1, 2, \ldots, U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} \frac{\gcd(m, i_{t_1}, i_{t_2}, \ldots, i_{t_u})}{m} \prod_{v=1}^{u}(q^{K_{jv}} - 1).
\]

Let \( U = 2 \), then we have

\[
|\langle \rho^l \rangle \setminus C^*| = |\langle \rho^l \rangle \setminus C^*_{t_1, t_2}| + s_{t_1} + s_{t_2}.
\]

By Lemma 5 we immediately get

\[
|\langle \rho^l \rangle \setminus C^*_{t_1, t_2}| = \frac{\gcd(m, i_{t_1}, i_{t_2})(q^{K_{t_1}} - 1)(q^{K_{t_2}} - 1)}{m},
\]

\[
s_{t_1} = \frac{\gcd(m, i_{t_1})(q^{K_{t_1}} - 1)}{m}, s_{t_2} = \frac{\gcd(m, i_{t_2})(q^{K_{t_2}} - 1)}{m},
\]

which gives the desired result.

\[\square\]

### 4.3 Proof of Theorem 2 and Corollary 2

**Proof.** It is easy to check that \( C^* \) is equal to

\[
\bigcup_{\{j_1, j_2, \ldots, j_u\} \subseteq \{1, 2, \ldots, U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} C_{t_1} \setminus \{0\} \oplus C_{t_2} \setminus \{0\} \oplus \cdots \oplus C_{t_u} \setminus \{0\},
\]

20
which is a disjoint union. For all \( j_1, j_2, \ldots, j_u \), \( C_{t_{j_u}} \) is a linear code over \( R_m \varepsilon_{t_{j_u}} \) of length \( l \) with \( 1 \leq v \leq u \). Let \( s_{j_1 j_2 \cdots j_u} \) be the number of orbits of \( \langle \rho^l, M \rangle \) acting on 
\[
C_{t_{j_1}} \setminus \{0\} \oplus C_{t_{j_2}} \setminus \{0\} \oplus \cdots \oplus C_{t_{j_u}} \setminus \{0\},
\]
which is denoted by \( C^\sharp_{j_1 j_2 \cdots j_u} \). Thus the group \( \langle \rho^l, M \rangle \) can act on the set \( C^\sharp_{j_1 j_2 \cdots j_u} \) in the same way as the group action on \( C \). Then, we have
\[
C^* = \bigsqcup_{\{j_1, j_2, \ldots, j_u\} \subseteq \{1, 2, \ldots, U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} C^\sharp_{j_1 j_2 \cdots j_u}
\]
and
\[
|\langle (\rho^l, M) \rangle \setminus C^*| = \sum_{\{j_1, j_2, \ldots, j_u\} \subseteq \{1, 2, \ldots, U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} s_{j_1 j_2 \cdots j_u}.
\]
It is enough to compute the number of orbits of the group \( \langle \rho^l, M \rangle \) acting on \( C^\sharp_{j_1 j_2 \cdots j_u} \).

According to Eq. (4), the number of orbits of \( \langle \rho^l, M \rangle \) on \( C^\sharp_{j_1 j_2 \cdots j_u} \) is equal to
\[
|\langle (\rho^l, M) \rangle \setminus C^\sharp_{j_1 j_2 \cdots j_u}| = \frac{1}{q - 1} \sum_{r \mid (q - 1)} \varphi \left( \frac{q - 1}{r} \right) |\text{Fix}(\sigma^r_\xi)|
\]
with \( \text{Fix}(\sigma^r_\xi) = \{ (\rho^l)(c) \in (\rho^l) \setminus C^\sharp_{j_1 j_2 \cdots j_u} | (\rho^l)(c) = (\rho^l)(\xi^r c) \} \). Therefore, it is enough to calculate the value of \( |\text{Fix}(\sigma^r_\xi)| \). Note that \( (\rho^l)(c) = (\rho^l)(\xi^r c) \) is equivalent to requiring that there exists an integer \( z \) such that \( \rho^z(c) = \xi^r c \).

Let \( c = c_{t_{j_1}} + c_{t_{j_2}} + \cdots + c_{t_{j_u}} \in C^\sharp_{j_1 j_2 \cdots j_u} \), where \( c_{t_{j_v}} \in C_{t_{j_v}} \setminus \{0\} \subseteq (R_m \varepsilon_{t_{j_v}})^l \) for \( v = 1, 2, \ldots, u \). Then \( \rho^z(c) = \xi^r c \) if and only if
\[
\rho^z(c_{t_{j_v}}) = \xi^r c_{t_{j_v}} \quad \text{for} \quad v = 1, 2, \ldots, u. \tag{6}
\]

From the proof of Lemma 6, we have that the equalities (6) hold if and only if
\[
\frac{q - 1}{r} \mid \frac{m}{\gcd(m, i_{t_{j_v}})} \quad \text{for} \quad v = 1, 2, \ldots, u.
\]
It follows from the proof of Theorem 1 that if \( \frac{q - 1}{r} \) is a divisor \( \frac{m}{\gcd(m, i_{t_{j_v}})} \) for \( v = 1, 2, \ldots, u \), then
\[
|\text{Fix}(\sigma^r_\xi)| = \frac{\gcd(m, i_{t_{j_1}}, i_{t_{j_2}}, \ldots, i_{t_{j_u}})}{m} \prod_{v=1}^{u} (q^{K_{t_{j_v}}} - 1);
\]

21
otherwise, \(|\text{Fix}(\sigma^r_\xi)| = 0\). Therefore,
\[
\begin{align*}
    s_{j_1,j_2,...,j_u} &= |(\rho^j \times M) \setminus C^0_{j_1,j_2,...,j_u}| \\
    &= \frac{1}{q-1} \sum_{r|(q-1)} \varphi\left(\frac{q-1}{r}\right) |\text{Fix}(\sigma^r_\xi)| \\
    &= \frac{\gcd(m, i_{t_{j_1}}, i_{t_{j_2}}, ..., i_{t_{j_u}}) \prod_{\nu=1}^u (q^{K_{t_{j\nu}}} - 1)}{m(q-1)} \\
    &= \frac{\sum_{r|(q-1), r \parallel \frac{m}{\gcd(m, i_{t_{j_1}}, i_{t_{j_2}}, ..., i_{t_{j_u}})}} \varphi\left(\frac{q-1}{r}\right)}{m(q-1)} \\
    &= \frac{\gcd(m, i_{t_{j_1}}, i_{t_{j_2}}, ..., i_{t_{j_u}}) \prod_{\nu=1}^u (q^{K_{t_{j\nu}}} - 1)}{m(q-1)} \\
    &= \gcd\left(q-1, \frac{m}{\gcd(m, i_{t_{j_1}})}, ..., \frac{m}{\gcd(m, i_{t_{j_u}})}\right) \\
\end{align*}
\]
Therefore, the number of orbits of \(\langle \rho^j, M \rangle\) on \(C^* = C \setminus \{0\}\) is equal to
\[
\sum_{\{j_1,j_2,...,j_u\} \subseteq \{1,2,...,U\}, 1 \leq j_1 < j_2 < ... < j_u \leq U} \frac{\gcd(m, i_{t_{j_1}}, i_{t_{j_2}}, ..., i_{t_{j_u}}) \prod_{\nu=1}^u (q^{K_{t_{j\nu}}} - 1)}{m(q-1)} \\
\cdot \gcd\left(q-1, \frac{m}{\gcd(m, i_{t_{j_1}})}, ..., \frac{m}{\gcd(m, i_{t_{j_u}})}\right).
\]

Let \(U = 2\), we have
\[
\langle \rho^j, M \rangle \setminus C^* = s'_{t_1,t_2} + s'_{t_1} + s'_{t_2}.
\]
By Lemma 6, we see that
\[
\begin{align*}
    s'_{t_1,t_2} &= \frac{\gcd(m, i_{t_1}, i_{t_2})(q^{K_{t_1}} - 1)(q^{K_{t_2}} - 1)}{m(q-1)} \cdot \gcd\left(q-1, \frac{m}{\gcd(m, i_{t_1})}, \frac{m}{\gcd(m, i_{t_2})}\right), \\
    s'_{t_1} &= \frac{\gcd(m, i_{t_1})(q^{K_{t_1}} - 1)}{m(q-1)} \cdot \gcd\left(q-1, \frac{m}{\gcd(m, i_{t_1})}\right), \\
    s'_{t_2} &= \frac{\gcd(m, i_{t_2})(q^{K_{t_2}} - 1)}{m(q-1)} \cdot \gcd\left(q-1, \frac{m}{\gcd(m, i_{t_2})}\right),
\end{align*}
\]
giving the desired result.

### 4.4 Proof of Theorem 3 and Corollary 3

It is easy to check that \(C^*\) is equal to
\[
\bigcup_{\{j_1,j_2,...,j_u\} \subseteq \{1,2,...,U\}, 1 \leq j_1 < j_2 < ... < j_u \leq U} C_{t_{j_1}} \setminus \{0\} \oplus C_{t_{j_2}} \setminus \{0\} \oplus \cdots \oplus C_{t_{j_u}} \setminus \{0\},
\]

\[
\]
which is a disjoint union. For all \( j_1, j_2, \ldots, j_u \), \( C_{t_{j_v}} \) is a linear code over \( R_{m^e t_{j_v}} \) of dimension 1 and length \( l \) with \( 1 \leq v \leq u \). Let \( s_{j_1 j_2 \ldots j_u} \) be the number of orbits of \( \langle \mu_q, \rho^l, M \rangle \) acting on

\[
C_{t_{j_1}} \setminus \{0\} \oplus C_{t_{j_2}} \setminus \{0\} \oplus \cdots \oplus C_{t_{j_u}} \setminus \{0\},
\]

which is denoted by \( C^\sharp_{j_1 j_2 \ldots j_u} \). Thus the group \( \langle \mu_q, \rho^l, M \rangle \) can act on the set \( C^\sharp_{j_1 j_2 \ldots j_u} \) in the same way as the group action on \( C \). Then, we have

\[
C^* = \bigsqcup_{\{j_1, j_2, \ldots, j_u\} \subseteq \{1, 2, \ldots, U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} C^\sharp_{j_1 j_2 \ldots j_u}
\]

and

\[
|\langle \mu_q, \rho^l, M \rangle \setminus C^*| = \sum_{\{j_1, j_2, \ldots, j_u\} \subseteq \{1, 2, \ldots, U\}, 1 \leq j_1 < j_2 < \cdots < j_u \leq U} s_{j_1 j_2 \ldots j_u}.
\]

It is enough to compute the number of orbits of the group \( \langle \mu_q, \rho^l, M \rangle \) acting on \( C^\sharp_{j_1 j_2 \ldots j_u} \). According to Eq. (5), the number of orbits of \( \langle \mu_q, \rho^l, M \rangle \) on \( C^\sharp_{j_1 j_2 \ldots j_u} \) is equal to

\[
|\langle \mu_q, \rho^l, M \rangle \setminus C^\sharp_{j_1 j_2 \ldots j_u}| = \frac{1}{m^e m(q - 1)} \sum_{r_1=0}^{m'-1} \sum_{r_2=0}^{m-1} \sum_{a \in F_q^*} |\{c \in C^\sharp_{j_1 j_2 \ldots j_u} | \mu_q^{r_1} \rho^{r_2} \sigma_a(c) = c\}|.
\]

Let \( c = c_{t_{j_1}} + c_{t_{j_2}} + \cdots + c_{t_{j_u}} \in C^\sharp_{j_1 j_2 \ldots j_u} \), where \( c_{t_{j_v}} \in C_{t_{j_v}} \setminus \{0\} \subseteq (R_{m^e t_{j_v}})^l \) for \( v = 1, 2, \ldots, u \). Then \( \mu_q^{r_1} \rho^{r_2} \sigma_a(c_{t_{j_v}}) = c_{t_{j_v}} \) if and only if

\[
\mu_q^{r_1} \rho^{r_2} \sigma_a(c_{t_{j_v}}) = c_{t_{j_v}} \quad \text{for} \quad v = 1, 2, \ldots, u.
\]

(7)

Since \( C_{t_{j_v}} \) is a \([l, 1]\)-linear code over \( R_{m^e t_{j_v}} \) with generator matrix

\[
[a_{j_v,0}(x), a_{j_v,1}(x), \ldots, a_{j_v,l-1}(x)],
\]

where \( a_{j_v,v'} \in \{0, f_{j_v}(x)\} \) for \( 0 \leq v' \leq l - 1 \), each component of \( c_{t_{j_v}} \) is \( 0 \) or \( F_v(x) \), where \( F_v(x) = \sum_{v'=0}^{k_{j_v}-1} f_{v,v'} \zeta^{j_{t_{j_v}}} \in R_{m^e t_{j_v}} \). Hence, the Eq. (7) is equivalent to

\[
\mu_q^{r_1} \rho^{r_2} \sigma_a(F_v(x)) = F_v(x) \quad \text{for} \quad v = 1, 2, \ldots, u,
\]

which is equivalent to

\[
a(f_{v,0} + f_{v,1} \zeta^{j_{t_{j_v}}} + \cdots + f_{v,k_{j_v}-1} \zeta^{(k_{j_v}-1)j_{t_{j_v}}}) \psi^{r_1-1} = \zeta^{k_{j_v} - q r_2} \quad \text{for} \quad v = 1, 2, \ldots, u,
\]

23
by the proof of Lemma 7. For $1 \leq v \leq u$, the minimal polynomial of $\zeta^{t_jv}$ over $\mathbb{F}_q$ is of degree $k_{t_jv}$, and so the set

$$\{f_{v,0} + f_{v,1}\zeta^{t_jv} + \cdots + f_{v,k_{t_jv}-1}\zeta^{(k_{t_jv}-1)t_jv} \mid f_{v,v'} \in \mathbb{F}_q, 0 \leq v' \leq k_{t_jv} - 1\}$$

forms a subfield $\mathbb{F}_{q^{k_{t_jv}}}$ of $\mathbb{F}_{q^m}$. Then the number of $c \in C^2_{t_1t_2\cdots t_u}$ satisfying $\mu_1^{r_1} \rho_2^{r_2} \sigma_a(c) = c$ is equal to the number of $u$-tuples $(\alpha_{t_{j_1}}, \alpha_{t_{j_2}}, \ldots, \alpha_{t_{j_u}})$ with $\alpha_{t_{j_v}} \in \mathbb{F}_{q^{k_{t_{j_v}}}}$ such that $a\alpha_{t_{j_v}}^{q^{r_1} - 1} = \zeta^{-it_{j_v}q^{r_1}r_2}$ for all $1 \leq v \leq u$, which is easily checked to be 0 or $\prod_{v=1}^u (q^{\gcd(k_{t_{j_v}}, r_1)} - 1)$. By the proof of [7, Lemma 3.1], we have the following two facts:

1. For $1 \leq v \leq u$, let $\mathbb{F}_{q^{k_{t_{j_v}}}}$ be generated by $\theta_{t_{j_v}}$. Let $\mathbb{F}_q$ be generated by $\zeta$. For $0 \leq r_1 \leq m' - 1$, denote $S(r_1)$ by

   $$\{0 \leq r_2 \leq m - 1 \mid \exists 0 \leq r_3 \leq q - 2 \text{ s.t. } \zeta^{-it_{j_v}q^{r_1}r_2} \in \langle \theta_{t_{j_v}}^{q^{r_1} - 1} \rangle \text{ for all } 1 \leq v \leq u\}.$$

   Then,

   $$|S(r_1)| \leq \gcd \left( m, \frac{it_{j_1}I}_{\gcd(I, I_{t_{j_1}})} \frac{it_{j_u}I_{t_{j_u}}}{\gcd(I_{t_{j_u}}, I_{t_{j_{u-1}}})}, \frac{(i_{t_{j_2}} - i_{t_{j_1}})I_{t_{j_1}} I_{t_{j_2}}}{\gcd(I_{t_{j_1}}, I_{t_{j_1}})} \cdots, \frac{(i_{t_{j_u}} - i_{t_{j_{u-1}}})I_{t_{j_{u-1}}} I_{t_{j_u}}}{\gcd(I_{t_{j_{u-1}}}, I_{t_{j_u}})} \right),$$

   where $I = q - 1$ and $I_{t_{j_v}} = \frac{q^{k_{t_{j_v}} - 1}}{q^{\gcd(k_{t_{j_v}}, r_1)} - 1}$ for $v = 1, 2, \ldots, u$.

2. Suppose $r_2 \in S(r_1)$ and denote $R(r_1, r_2)$ by

   $$\{0 \leq r_3 \leq q - 2 \mid \zeta^{-it_{j_v}q^{r_1}r_2} \in \langle \theta_{t_{j_v}}^{q^{r_1} - 1} \rangle \text{ for all } 1 \leq v \leq u\}.$$

   Then, $|R(r_1, r_2)| = \gcd(I, I_{t_{j_1}}, \ldots, t_{j_u})$.

According to these two facts and the similar calculation as in [7, Lemma 3.1], we have
Therefore, the number of orbits of $\langle \mu_q, \rho^l, M \rangle \backslash C^*_{j_1, j_2, \ldots, j_u}$ is obtained.

Let $U = 2$, we have

$$|\langle \mu_q, \rho^l, M \rangle \backslash C^*| = s_{t_1} + s_{t_2} + s_{t_1, t_2}.$$

According to the proofs of Lemma 7 and [7, Theorem 3.3], we have

$$s_{t_v} = \frac{1}{k_{t_v}} \sum_{r|k_{t_v}} \varphi\left(\frac{k_{t_v}}{r}\right) \gcd\left(q^r - 1, \frac{q^{k_{t_v}} - 1}{q - 1}, \frac{i_{t_v}(q^{k_{t_v}} - 1)}{m}\right) \quad \text{for} \quad v = 1, 2,$$

$$s_{t_1, t_2} = \frac{1}{m'} \sum_{r=0}^{m'-1} \gcd\left((q^{\gcd(k_{t_1}, r)} - 1) \gcd\left(q^{\gcd(k_{t_1}, r)} - 1, \frac{q^{k_{t_1}} - 1}{q - 1}, \frac{i_{t_1}(q^{k_{t_1}} - 1)}{m}\right),\frac{i_{t_1}(q^{k_{t_1}} - 1)}{m}\right),$$

which gives the desired result.

5 Remarks and examples

Remark 1. The reference [25, Theorem 5] says that if $C$ is a $[n = lm, K]$ strongly quasi-cyclic code of co-index $m$ over $\mathbb{F}_q$, then $s(C) \leq \frac{K - 1}{m}$. If $\gcd(m, i_t) = 1$, then Lemma 5 generalizes and improves [25, Theorem 5] by removing the constrain “strongly” and characterizing a necessary and sufficient condition for the codes meeting bounds.
We include three examples to show that the upper bounds given in Lemma 5 and Theorem 1 are tight.

**Example 1.** Take $m = 9$, $l = 2$ and $q = 2$ in Lemma 5. All the distinct 2-cyclotomic cosets modulo 9 are given by

$$
\Gamma_0 = \{0\}, \Gamma_1 = \{1, 2, 4, 5, 7, 8\}, \Gamma_2 = \{3, 6\}.
$$

Consider the linear code $C$ over $R_m\varepsilon_2$, where the primitive idempotent $\varepsilon_2$ corresponds to $\Gamma_2$. Suppose $\zeta$ is a primitive $m$-th root of unity. Actually, let $h(x) = \prod_{r \in \Gamma_2} (x - \zeta^r) = x^2 + x + 1$, then $g(x) = (x^m - 1)/h(x)$ is a generator polynomial of $R_m\varepsilon_2$. Let $[1, g(x)]$ be the generator matrix of $C$ over $R_m\varepsilon_2$. Then $K = 1 \cdot |\Gamma_2| = 2$. By Lemma 5 we have

$$
s(C) \leq \frac{\gcd(m, iT)(q^K - 1)}{m} = \frac{\gcd(9, 3)(2^2 - 1)}{9} = 1.
$$

Hence, the number of nonzero weights of $C$ must be equal to 1. Moreover, Lemma 5 also tells us that all the nonzero codewords of $C$ are in the same $\langle \rho^l \rangle$-orbit.

**Example 2.** Take $m = 15$, $l = 3$ and $q = 2$ in Lemma 5. All the distinct 2-cyclotomic cosets modulo 15 are given by

$$
\Gamma_0 = \{0\}, \Gamma_1 = \{1, 2, 4, 8\}, \Gamma_2 = \{3, 6, 9, 12\}, \Gamma_3 = \{7, 11, 13, 14\}, \Gamma_4 = \{5, 10\}.
$$

Consider the linear code $C$ over $R_m\varepsilon_0$, where the primitive idempotent $\varepsilon_0$ corresponds to $\Gamma_0$. Actually, let $h(x) = x - 1$, then $g(x) = (x^m - 1)/h(x)$ is a generator polynomial of $R_m\varepsilon_0$. Let

$$
\begin{pmatrix}
1 & 0 & g(x) \\
0 & 1 & 0
\end{pmatrix}
$$

be the generator matrix of $C$ over $R_m\varepsilon_0$. Then $K = 2 \cdot |\Gamma_0| = 2$. By Lemma 5 we have

$$
s(C) \leq \frac{\gcd(m, iT)(q^K - 1)}{m} = \frac{\gcd(15, 0)(2^2 - 1)}{15} = 3.
$$

Using the Magma software programming [4], we see that the weight distribution of the quasi-cyclic code $C$ is $1 + x^{15} + x^{30} + x^{45}$, showing that the exact value of $s(C) = 3$.

**Example 3.** Take $m = 9$, $l = 2$ and $q = 2$ in Theorem 1. All the distinct 2-cyclotomic cosets modulo 9 are as shown in Example 1. Consider the quasi-cyclic code $C = C_0 \oplus C_2$, where $C_0$ is a linear code over $R_m\varepsilon_0$ and $C_2$ is a linear code over $R_m\varepsilon_2$, where the primitive idempotent $\varepsilon_0$ and $\varepsilon_2$ corresponds to $\Gamma_0$ and $\Gamma_2$, respectively.
respectively. Actually, let \( h_1(x) = x + 1 \) and \( h_2(x) = x^2 + x + 1 \), then \( g_1(x) = (x^m - 1)/h_1(x) \) and \( g_2(x) = (x^m - 1)/h_2(x) \) are the generator polynomial of \( R_{m\varepsilon_0} \) and \( R_{m\varepsilon_2} \), respectively. Let \([1, g_i(x)]\) be the generator matrix of \( C_i \) over \( R_{m\varepsilon_i} \) with \( i = 0, 2 \). Then \( K_1 = 1 \cdot |\Gamma_0| = 1 \) and \( K_2 = 1 \cdot |\Gamma_2| = 2 \). By Theorem 1, we have

\[
s(C) \leq \frac{\gcd(9, 0, 3)(2 - 1)(2^2 - 1)}{9} + \frac{\gcd(9, 0)(2 - 1)}{9} + \frac{\gcd(9, 3)(2^2 - 1)}{9} = 3.
\]

Using the Magma software programming [4], we see that the weight distribution of the quasi-cyclic code \( C \) is \( 1 + 3x^6 + 3x^{12} + x^{18} \), showing that the exact value of \( s(C) = 3 \). Moreover, Lemma 5 also tells us that any two nonzero codewords of \( C \) with the same weight are in the same \( (\rho^i) \)-orbit.

**Remark 2.** The reference [25, Theorem 3] says that if \( C \) is a \([n = lm, K]\) strongly quasi-cyclic code of co-index \( m \) over \( \mathbb{F}_q \), then

\[
s(C) \leq \frac{l(q^K - 1)}{\text{lcm}(q - 1, n)} = \frac{\gcd(lm, q - 1)(q^K - 1)}{m(q - 1)}.
\]

If \( \gcd(m, i) = 1 \), then Lemma 6 says that

\[
s(C) \leq \frac{\gcd(m, q - 1)(q^K - 1)}{m(q - 1)} \leq \frac{\gcd(lm, q - 1)(q^K - 1)}{m(q - 1)}.
\]

Therefore, Lemma 6 generalizes and improves [25, Theorem 3] by removing the constrain “strongly” and characterizing a necessary and sufficient condition for the codes meeting bounds.

Next, we also include three examples to show that the upper bounds given in Lemma 6 and Theorem 2 are tight.

**Example 4.** Take \( m = 91 \), \( l = 2 \) and \( q = 9 \) in Lemma 6. \( \Gamma_2 = \{8, 72, 11\} \) is the 9-cyclotomic coset modulo 91 containing 8. Consider the linear code \( C \) over \( R_{m\varepsilon_2} \), where the primitive idempotent \( \varepsilon_2 \) corresponds to \( \Gamma_2 \). Suppose \( g(x) \) is a generator polynomial of \( R_{m\varepsilon_2} \). Let \([1, g(x)]\) be the generator matrix of \( C \) over \( R_{m\varepsilon_2} \). Then \( K = 1 \cdot |\Gamma_2| = 3 \). By Lemma 6 we have

\[
s(C) \leq \frac{\gcd(m, (q - 1)i)(q^K - 1)}{m(q - 1)} = \frac{\gcd(31, (9 - 1)8)(9^3 - 1)}{91(9 - 1)} = 1.
\]

Hence, the number of nonzero weights of \( C \) must be equal to 1. Moreover, Lemma 5 also tells us that all the nonzero codewords of \( C \) are in the same \( (\rho^i, M) \)-orbit.
Example 5. Take $m = 39$, $l = 2$ and $q = 5$ in Lemma \([3]\). $\Gamma_1 = \{1, 5, 8, 25\}$ is the 5-cyclotomic coset modulo 39 containing 1. Consider the linear code $C$ over $R_{m\varepsilon_1}$, where the primitive idempotent $\varepsilon_1$ corresponds to $\Gamma_1$. Suppose $g(x)$ is a generator polynomial of $R_{m\varepsilon_1}$. Let $[1, g(x)]$ be the generator matrix of $C$ over $R_{m\varepsilon_2}$. Then $K = 1 \cdot |\Gamma_1| = 4$. By Lemma \([3]\) we have

$$s(C) \leq \frac{\gcd(m, (q-1)i)|q^K-1|}{m(q-1)} = \frac{\gcd(39, (5-1)1)(5^4-1)}{39(5-1)} = 4.$$  

Using the Magma software programming \([4]\), we see that the weight distribution of the quasi-cyclic code $C$ is $1+156x^{59}+156x^{62}+156x^{63}+156x^{66}$, showing that the exact value of $s(C) = 4$. Moreover, Lemma \([3]\) also tells us that any two nonzero codewords of $C$ with the same weight are in the same $\langle \rho', M \rangle$-orbit.

Example 6. Take $m = 26$, $l = 2$ and $q = 3$ in Theorem \([2]\). All the distinct 3-cyclotomic cosets modulo 26 are given by

$$\Gamma_0 = \{0\}, \Gamma_1 = \{1, 3, 9\}, \Gamma_2 = \{2, 4, 6\}, \Gamma_3 = \{4, 10, 12\}, \Gamma_4 = \{5, 15, 19\},$$

$$\Gamma_5 = \{13\}, \Gamma_6 = \{7, 11, 21\}, \Gamma_7 = \{8, 20, 24\}, \Gamma_8 = \{14, 16, 22\}, \Gamma_9 = \{17, 23, 25\}.$$  

Consider the quasi-cyclic code $C = C_1 \oplus C_5$, where $C_1$ is a linear code over $R_{m\varepsilon_1}$ and $C_5$ is a linear code over $R_{m\varepsilon_5}$, where the primitive idempotent $\varepsilon_1$ and $\varepsilon_5$ corresponds to $\Gamma_1$ and $\Gamma_5$, respectively. Let $g_1(x)$ and $g_2(x)$ be the generator polynomial of $R_{m\varepsilon_1}$ and $R_{m\varepsilon_5}$, respectively. Let $[1, g_1(x)]$ be the generator matrix of $C_1$ over $R_{m\varepsilon_1}$, and $[0, g_2(x)]$ be the generator matrix of $C_5$ over $R_{m\varepsilon_5}$. Then $K_1 = 1 \cdot |\Gamma_1| = 3$ and $K_2 = 1 \cdot |\Gamma_5| = 1$. By Theorem \([2]\) we have

$$s(C) \leq \frac{\gcd(26, 1, 13)(3^3-1)(3-1)}{26(3-1)} \cdot \gcd\left(3-1, \frac{26}{\gcd(26, 1)}; \frac{26}{\gcd(26, 13)}\right)$$

$$+ \frac{\gcd(26, 1)(3^3-1)}{26(3-1)} \cdot \gcd\left(3-1, \frac{26}{\gcd(26, 1)}\right)$$

$$+ \frac{\gcd(26, 13)(3-1)}{26(3-1)} \cdot \gcd\left(3-1, \frac{26}{\gcd(26, 13)}\right)$$

$$= 4.$$  

Using the Magma software programming \([4]\), we see that the weight distribution of the quasi-cyclic code $C$ is $1 + 2x^{26} + 26x^{32} + 26x^{36} + 26x^{38}$, showing that the exact value of $s(C) = 4$. Moreover, Lemma \([5]\) also tells us that any two nonzero codewords of $C$ with the same weight are in the same $\langle \rho', M \rangle$-orbit.
Remark 3. Let $C$ be a one-generator quasi-cyclic code over $\mathbb{F}_q$. In Theorem 3, we consider that $\langle \mu_q, \rho^l, M \rangle$ is a subgroup of $\text{Aut}(C)$ which is larger than the automorphism groups $\langle \rho^l \rangle$ and $\langle \rho^l, M \rangle$. Therefore, the upper bound in Theorem 3 is tighter than that in Theorems 1 and 2 if $C$ is a one-generator quasi-cyclic code.

Next, we also include three examples to show that the upper bounds given in Lemma 7 and Theorem 3 are tight, and also are compared with that in Lemma 6 and Theorem 2.

Example 7. Take $m = 11$, $l = 2$ and $q = 4$ in Lemma 7. All the distinct 4-cyclotomic cosets modulo 11 are given by

$\Gamma_0 = \{0\}, \Gamma_1 = \{1, 3, 4, 5, 9\}, \Gamma_2 = \{2, 6, 7, 8, 10\}.$

Consider the linear code $C$ over $R_m\varepsilon_1$, where the primitive idempotent $\varepsilon_1$ corresponds to $\Gamma_1$. Suppose $g(x)$ is a generator polynomial of $R_m\varepsilon_1$. Let $[0, g(x)]$ be the generator matrix of $C$ over $R_m\varepsilon_1$. Then $K_1 = 1 \cdot |\Gamma_1| = 5$. By Lemma 6 we have

$$s(C) \leq \frac{\gcd(m, (q-1)i)(q^K - 1)}{m(q-1)} = \frac{\gcd(11, (4-1)1)(4^5 - 1)}{11(4-1)} = 31.$$ 

Using Lemma 7, we have

$$s(C) \leq \frac{1}{5} \sum_{r \mid 5} \varphi\left(\frac{5}{r}\right) \gcd\left(4^r - 1, \frac{4^5 - 1}{4 - 1}, \frac{1 \cdot (4^5 - 1)}{11}\right)$$

$$= \frac{1}{5} (\varphi(5) + 31\varphi(1)) = \frac{1}{5} (4 + 31) = 7.$$ 

Using the Magma software programming [4], we see that the weight distribution of the quasi-cyclic code $C$ is $1 + 165x^6 + 165x^7 + 165x^8 + 330x^9 + 165x^{10} + 33x^{11}$, showing that the exact value of $s(C) = 6$.

Example 8. Take $m = 9$, $l = 2$ and $q = 2$ in Theorem 3. All the distinct 2-cyclotomic cosets modulo 9 are as shown in Example 1. Consider the quasi-cyclic code $C = C_0 \oplus C_1$, where $C_0$ is a linear code over $R_m\varepsilon_0$ and $C_1$ is a linear code over $R_m\varepsilon_1$, where the primitive idempotent $\varepsilon_0$ and $\varepsilon_1$ corresponds to $\Gamma_0$ and $\Gamma_1$, respectively. Let $g_1(x)$ and $g_2(x)$ be the generator polynomial of $R_m\varepsilon_0$ and $R_m\varepsilon_1$, respectively. Let $[0, g_1(x)]$ be the generator matrix of $C_0$ over $R_m\varepsilon_0$, and $[g_2(x), 0]$ be the generator matrix of $C_1$ over $R_m\varepsilon_1$. Then $K_1 = 1 \cdot |\Gamma_0| = 1$ and $K_2 = 1 \cdot |\Gamma_1| = 6$. 

29
By Theorem 2, we have
\[
s(C) \leq \frac{\gcd(9, 0, 1)(2 - 1)(2^6 - 1)}{9(2 - 1)} \cdot \gcd\left(2 - 1, \frac{9}{\gcd(9, 0)}, \frac{9}{\gcd(9, 1)}\right) \\
+ \frac{\gcd(9, 0)(2 - 1)}{9(2 - 1)} \cdot \gcd\left(2 - 1, \frac{9}{\gcd(9, 0)}\right) \\
+ \frac{\gcd(9, 1)(2^6 - 1)}{9(2 - 1)} \cdot \gcd\left(2 - 1, \frac{9}{\gcd(9, 1)}\right) \\
= 7 + 1 + 7 = 15.
\]

Using Theorem 3 and Corollary 3, we have
\[
s(C) \leq \frac{1}{6} \sum_{r \mid 6} \varphi\left(\frac{6}{r}\right) \gcd\left(2^r - 1, \frac{2^6 - 1}{2 - 1}, \frac{1}{9} \cdot (2^6 - 1)\right) \\
+ \frac{1}{6} \sum_{r = 0}^{5} \gcd\left(\gcd(2^\gcd(6, r) - 1, 2^\gcd(6, r) - 1, \frac{2^6 - 1}{9}), \frac{2^6 - 1}{9}\right) \\
= 1 + 3 + 3 = 7.
\]

Using the Magma software programming [4], we see that the weight distribution of the quasi-cyclic code \(C\) is 1 + 9\(x^2\) + 27\(x^4\) + 27\(x^6\) + \(x^9\) + 9\(x^{11}\) + 27\(x^{13}\) + 27\(x^{15}\), showing that the exact value of \(s(C) = 7\). Moreover, Theorem 3 also tells us that any two nonzero codewords of \(C\) with the same weight are in the same \(\langle \mu_q, \rho', M \rangle\)-orbit.

**Example 9.** Take \(m = 15\), \(l = 2\) and \(q = 2\) in Theorem 3. All the distinct 2-cyclotomic cosets modulo 15 are as shown in Example 2. Consider the quasi-cyclic code \(C = C_2 \oplus C_4\), where \(C_2\) is a linear code over \(R_{m\varepsilon_2}\) and \(C_4\) is a linear code over \(R_{m\varepsilon_4}\), where the primitive idempotent \(\varepsilon_2\) and \(\varepsilon_4\) corresponds to \(\Gamma_2\) and \(\Gamma_4\), respectively. Let \(g_1(x)\) and \(g_2(x)\) be the generator polynomial of \(R_{m\varepsilon_2}\) and \(R_{m\varepsilon_4}\), respectively. Let \([0, g_1(x)]\) be the generator matrix of \(C_2\) over \(R_{m\varepsilon_2}\), and \([g_2(x), 0]\) be the generator matrix of \(C_4\) over \(R_{m\varepsilon_4}\). Then \(K_2 = 1 \cdot |\Gamma_2| = 4\) and \(K_4 = 1 \cdot |\Gamma_4| = 2\).

By Theorem 2 we have
\[
s(C) \leq \frac{\gcd(15, 5, 3)(2^2 - 1)(2^4 - 1)}{15(2 - 1)} \cdot \gcd\left(2 - 1, \frac{15}{\gcd(15, 5)}, \frac{15}{\gcd(15, 3)}\right) \\
+ \frac{\gcd(15, 5)(2^2 - 1)}{15(2 - 1)} \cdot \gcd\left(2 - 1, \frac{15}{\gcd(15, 5)}\right) \\
+ \frac{\gcd(15, 3)(2^4 - 1)}{15(2 - 1)} \cdot \gcd\left(2 - 1, \frac{15}{\gcd(15, 3)}\right) \\
= 3 + 1 + 3 = 7.
\]
Using Theorem 3 and Corollary 3, we have
\[
s(C) \leq \frac{1}{2} \sum_{r|2} \varphi\left(\frac{2}{r}\right) \gcd\left(2^r - 1, \frac{2^2 - 1}{2 - 1}, \frac{5 \cdot (2^2 - 1)}{15}\right) + \\
\frac{1}{4} \sum_{r|4} \varphi\left(\frac{4}{r}\right) \gcd\left(2^r - 1, \frac{2^4 - 1}{2 - 1}, \frac{3 \cdot (2^4 - 1)}{15}\right) + \\
\frac{1}{4} \sum_{r=0}^{3} \gcd\left((2^{\gcd(2,r)} - 1) \gcd\left(2^{\gcd(4,r)} - 1, \frac{2^{\gcd(4,r)} - 1}{2^{\gcd(2,r)} - 1}, 3, 6\right)\right) = 1 + 2 + 2 = 5.
\]

Using the Magma software programming, we see that the weight distribution of the quasi-cyclic code \(C\) is \(1 + 10x^6 + 3x^{10} + 5x^{12} + 30x^{16} + 15x^{22}\), showing that the exact value of \(s(C) = 5\). Moreover, Theorem 3 also tells us that any two nonzero codewords of \(C\) with the same weight are in the same \(\langle \mu_q, \rho^l, M \rangle\)-orbit.

6 Conclusion

In this paper, we establish an explicit upper bound on the number of nonzero weights of any quasi-cyclic code with simple-root by counting the number of orbits of \(\langle \rho^l, M \rangle\) on the code \((\langle \mu_q, \rho^l, M \rangle\) on one-generator quasi-cyclic code); at the same time, we show that a quasi-cyclic code achieves the bound if and only if any two codewords with the same weight are in the same \(\langle \rho^l, M \rangle\)-orbit \((\langle \mu_q, \rho^l, M \rangle\)-orbit). Many examples (see Section 5) are included to show that our bound is tight. Our main result and its corollaries generalize and improve some of the results in [25].

A possible direction for future work is to find tight upper bounds for the number of nonzero weights of quasi-cyclic codes with repeated-root.

References

[1] T. Alderson, A note on full weight spectrum codes, Trans. Comb., vol. 8, no. 3, pp. 15-22, 2019.
[2] T. Alderson and A. Neri, Maximum weight spectrum codes, Adv. Math. Commun., vol. 13, no. 1, pp. 101-119, 2019.
[3] E. Assmus and E. Mattson, New 5-designs, J. Combinatorial Theory, vol. 6, no. 2, pp. 122-151, 1969.

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput., vol. 24, no. 3-4, pp. 235-265, 1997.

[5] P. Charpin, Open problems on cyclic codes, in Handbook of Coding Theory, V. S. Pless and C. W. Huffman, Eds. New York: Elsevier, pp. 963-1063, 1998.

[6] B. Chen, H. Liu and G. Zhang, Some minimal cyclic codes over finite fields, Discrete Math., vol. 331, pp. 142-150, 2014.

[7] B. Chen, Y. Fu and H, Liu, Improved upper bounds on the number of non-zero weights of cyclic codes, arXiv: 2305.14687.

[8] B. Chen and G. Zhang, A tight upper bound on the number of non-zero weights of a cyclic code, IEEE Trans. Inform. Theory, vol. 69, no. 2, pp. 995-1004, 2023.

[9] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Information and Control, vol. 23, no. 5, pp. 407-438, 1973.

[10] C. Ding, The weight distribution of some irreducible cyclic codes, IEEE Trans. Inform. Theory, vol. 55, no. 3, pp. 955-960, 2009.

[11] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[12] R. Hill, An extension theorem for linear codes, Des., Codes Cryptogr., vol. 17, nos. 1-3, pp. 151-157, 1999.

[13] R. Hill and P. Lizak, Extensions of linear codes, in Proc. IEEE Int. Symp. Inf. Theory, Sep. 1995, p. 345.

[14] A. Kerber, Applied Finite Group Actions, Springer-Verlag, 1999.

[15] K. Lally and P. Fitzpatrick, Algebraic structure of quasi-cyclic codes, Discr. Appl. Math., vol. 111, pp. 157-175, 2001.

[16] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 2003.

[17] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes I: Finite fields, IEEE Trans. Inform. Theory, vol. 47, no. 7, pp. 2751-2760, 2001.

[18] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes II: Chain Rings, Des. Codes Cryptogr., vol. 30, pp. 113-130, 2003.

[19] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes III: Generator Theory, IEEE Trans. Inform. Theory, vol. 51, no. 7, pp. 2692-2700, 2005.
[20] S. Ling, H. Niederreiter and P. Solé, On the algebraic structure of quasi-cyclic codes IV: Repeated Roots, Des. Codes Cryptogr., vol. 38, pp. 337-361, 2006.

[21] F. J. Macwilliams, A theorem on the distribution of weights in a systematic code, Bell Syst. Tech. J., vol. 42, no. 1, pp. 79-94, Jan. 1963.

[22] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North Holland, 1983.

[23] J. J. Rotman, Advanced Modern Algebra, Prentice Hall, 2003.

[24] M. Shi, X. Li, A. Neri and P. Solé, How many weights can a cyclic code have?, IEEE Trans. Inform. Theory, vol. 66, no. 3, pp. 1449-1459, 2020.

[25] M. Shi, A. Neri and P. Solé, How many weights can a quasi-cyclic code have?, IEEE Trans. Inform. Theory, vol. 66, no. 11, pp. 6855-6862, 2020.

[26] M. Shi, H. Zhu, P. Solé and G. D. Cohen, How many weights can a linear code have?, Des. Codes Cryptogr., vol. 87, no. 1, pp. 87-95, 2019.