Finite Fields and Their Applications 18 (2012) 144–159

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

The weight distribution of some irreducible cyclic codes

Anuradha Sharma [a,*], Gurmeet K. Bakshi [b]

[a] Department of Mathematics, Indian Institute of Technology Delhi, New Delhi 110016, India
[b] Centre for Advanced Study in Mathematics, Panjab University, Chandigarh 160014, India

ARTICLE INFO

Article history:
Received 30 August 2010
Revised 12 April 2011
Accepted 6 July 2011
Available online 22 July 2011
Communicated by Jacques Wolfmann

MSC:
94B15

Keywords:
Irreducible cyclic codes
Cyclotomic cosets
Weight distribution

ABSTRACT

Let $\mathbb{F}_q$ be the finite field with q elements, p be an odd prime co-prime to q and $m \geqslant 1$ be an integer. In this paper, we explicitly determine the weight distribution of all the irreducible cyclic codes of length p^m over $\mathbb{F}_q$ from their generating polynomials in three different cases, when (i) the multiplicative order of q modulo p^m is $\phi(p^m)$, (ii) the multiplicative order of q modulo p^m is a power of p, and (iii) the multiplicative order of q modulo p^m is twice a power of p.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements and let n be a positive integer co-prime to q. A cyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$ with the property that if $(a_0, a_1, a_2, \ldots, a_{n-1}) \in \mathcal{C}$, then the cyclic shift $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is also in $\mathcal{C}$. A cyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is also called a q-ary cyclic code of length n. We can also regard $\mathcal{C}$ as an ideal in the principal ideal ring $R_n := \mathbb{F}_q[x]/\langle x^n - 1\rangle$ under the vector space isomorphism from $\mathbb{F}_q^n$ to R_n given by $(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. It is known that any ideal $\mathcal{C}$ in R_n is generated by a unique monic polynomial $g(x)$, which is a divisor of $(x^n - 1)$, called the generating polynomial of $\mathcal{C}$. A minimal ideal in R_n is called an irreducible cyclic code of length n over $\mathbb{F}_q$.

If $\mathcal{C}$ is a cyclic code of length n over $\mathbb{F}_q$ and $v \in \mathcal{C}$, then the weight of v, $wt(v)$, is defined to be the number of non-zero coordinates in v. If $A_w^{(n)}$ denotes the number of codewords in $\mathcal{C}$ of weight w, $w \geqslant 0$, then the list $A_0^{(n)}, A_1^{(n)}, \ldots, A_n^{(n)}$ is called the weight distribution of $\mathcal{C}$. The weight distribution

* Corresponding author.
E-mail addresses: anuradha@maths.iitd.ac.in (A. Sharma), gkbakshi@pu.ac.in (G.K. Bakshi).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.07.002

of irreducible cyclic codes has been an interesting object of study for a long time and is known in some cases (see [1–7,9,10,12–14]). Ding [2] determined the weight distribution of q-ary irreducible cyclic codes of length n provided $2 \leqslant \frac{q^{O_n(q)}-1}{n} \leqslant 4$, where $O_n(q)$ denotes the multiplicative order of q modulo n. He also pointed out that the weight formulas become quite messy if $\frac{q^{O_n(q)}-1}{n} \geqslant 5$ and therefore finding the weight distribution of q-ary irreducible cyclic codes is a notoriously difficult problem.

In the previous paper [12], the authors, along with Raka, have determined the weight distribution of all the irreducible cyclic codes of length 2^m over $\mathbb{F}_q$. In this paper, we determine the weight distribution of all the irreducible cyclic codes of length p^m over $\mathbb{F}_q$, where p is an odd prime co-prime to q and $m \geqslant 1$ is an integer, in three different cases, when (i) the multiplicative order of q modulo p^m is $\phi(p^m)$; (ii) the multiplicative order of q modulo p^m is a power of p; (iii) the multiplicative order of q modulo p^m is twice a power of p. In Section 2, we list all the irreducible cyclic codes of length p^m over $\mathbb{F}_q$ and show that in order to determine the weight distribution of any of these codes, it is sufficient to find the weight distribution of the q-ary irreducible cyclic code of length p^r, $1 \leqslant r \leqslant m$, which corresponds to the q-cyclotomic coset containing 1 (Theorem 1). In Section 3, we find the weight distribution of the irreducible cyclic code of length p^r, $1 \leqslant r \leqslant m$, which corresponds to the q-cyclotomic coset containing 1 in the three different cases listed above (Theorems 2–4). Finally, in Section 4, we also give some illustrative examples.

2. Irreducible cyclic codes and their weight distribution

Let $\mathbb{F}_q$ be the finite field with q elements and let n be a positive integer co-prime to q. Let α denote a primitive nth root of unity in some extension field of $\mathbb{F}_q$. For any integer s, $0 \leqslant s \leqslant n-1$, the q-cyclotomic coset of s modulo n is the set

$$C_s := \left\{s, sq, sq^2, \ldots, sq^{n_s-1}\right\},$$

where n_s is the least positive integer such that $sq^{n_s} \equiv s \pmod{n}$. Corresponding to the q-cyclotomic coset C_s, define

$$M_s^{(n)}(x) := \prod_{j \in C_s} \left(x - \alpha^j\right)$$

and

$$\mathcal{M}_s^{(n)} := \text{the ideal in } R_n \text{ generated by } \frac{x^n - 1}{M_s^{(n)}(x)}.$$

It is known that $M_s^{(n)}(x)$ is the minimal polynomial of α^s over $\mathbb{F}_q$ and $\mathcal{M}_s^{(n)}$ is an irreducible cyclic code of length n over $\mathbb{F}_q$, called the q-ary irreducible cyclic code of length n corresponding to the q-cyclotomic coset C_s. Furthermore, if $C_{s_1}, C_{s_2}, \ldots, C_{s_k}$ are all the distinct q-cyclotomic cosets modulo n, then $\mathcal{M}_{s_1}^{(n)}, \mathcal{M}_{s_2}^{(n)}, \ldots, \mathcal{M}_{s_k}^{(n)}$ are precisely all the distinct irreducible cyclic codes of length n over $\mathbb{F}_q$. For details, see [8, Chapters 7 and 8]. We have the following:

Theorem 1. *Let $\mathbb{F}_q$ be the finite field with q elements, p be an odd prime co-prime to q and $m \geqslant 1$ be an integer. Let g be a primitive root modulo p^m.*

(i) *The codes $\mathcal{M}_0^{(p^m)}$, $\mathcal{M}_{g^k p^j}^{(p^m)}$, $0 \leqslant j \leqslant m-1$, $0 \leqslant k \leqslant \frac{\phi(p^{m-j})}{O_{p^{m-j}}(q)} - 1$, are precisely all the distinct irreducible cyclic codes of length p^m over $\mathbb{F}_q$, where ϕ denotes Euler's Phi function.*

(ii) *All the non-zero codewords in $\mathcal{M}_0^{(p^m)}$ have weight p^m.*

(iii) *The code* $\mathcal{M}_{g^k p^j}^{(p^m)}$ *is equivalent to the code* $\mathcal{M}_{p^j}^{(p^m)}$ *and therefore they have the same weight distribution.*

(iv) $\mathcal{M}_{p^j}^{(p^m)}$ *is the repetition code of the irreducible cyclic code* $\mathcal{M}_1^{(p^{m-j})}$ *of length* p^{m-j} *corresponding to the* q*-cyclotomic coset containing* 1*, repeated* p^j *times. Furthermore, for any* $w \geqslant 0$*,*

$$A_w^{(p^m)} = \begin{cases} 0 & \text{if } p^j \text{ does not divide } w; \\ A_{w'}^{(p^{m-j})} & \text{if } w = p^j w',\ 0 \leqslant w' \leqslant p^{m-j}, \end{cases}$$

where $A_w^{(p^m)}$ *(resp.* $A_w^{(p^{m-j})}$*),* $w \geqslant 0$*, denote the weight distribution of* $\mathcal{M}_{p^j}^{(p^m)}$ *(resp.* $\mathcal{M}_1^{(p^{m-j})}$*).*

Proof. By [11, Lemma 1], all the distinct q-cyclotomic cosets modulo p^m are given by C_0, $C_{g^k p^j}$, $0 \leqslant j \leqslant m-1$, $0 \leqslant k \leqslant \frac{\phi(p^{m-j})}{o_{p^{m-j}}(q)} - 1$. Therefore, (i) follows. (ii) and (iii) are obvious. The proof of (iv) is similar to that of Lemma 2 of [12]. □

It thus follows from the above theorem that the weight distribution of all the q-ary irreducible cyclic codes of length p^m can be determined from the weight distribution of q-ary irreducible cyclic code $\mathcal{M}_1^{(p^r)}$ of length p^r $(1 \leqslant r \leqslant m)$, which corresponds to the q-cyclotomic coset containing 1.

3. The weight distribution of $\mathcal{M}_1^{(p^r)}$, $1 \leqslant r \leqslant m$

Throughout this section, $\mathbb{F}_q$ denotes the finite field with q elements, p an odd prime co-prime to q and $m \geqslant 1$, an integer. Let $1 \leqslant r \leqslant m$ be fixed throughout. In this section, we determine the weight distribution of q-ary irreducible cyclic code $\mathcal{M}_1^{(p^r)}$ of length p^r corresponding to the q-cyclotomic coset containing 1, in the following three different cases:

(i) the multiplicative order of q modulo p^m is $\phi(p^m)$;
(ii) the multiplicative order of q modulo p^m is a power of p;
(iii) the multiplicative order of q modulo p^m is twice a power of p.

3.1. The multiplicative order of q modulo p^m is $\phi(p^m)$

We first fix some notations. Let $\mathbb{Z}$ denote the set of integers. For any $t, \nu \in \mathbb{Z}$, $t \geqslant 1$ and $\nu \geqslant 2$, let

$$P_t(\nu) := \left\{ (\nu_1, \nu_2, \ldots, \nu_t) \in \mathbb{Z}^t \;\middle|\; 2 \leqslant \nu_j \leqslant p \text{ for all } j,\ \sum_{j=1}^{t} \nu_j = \nu \right\}.$$

Given $(\nu_1, \nu_2, \ldots, \nu_t) \in P_t(\nu)$, set

$$L(\nu_1, \nu_2, \ldots, \nu_t) := \left\{ (\ell_1, \ell_2, \ldots, \ell_t) \in \mathbb{Z}^t \;\middle|\; \ell_j \geqslant \nu_j - 2 \text{ for all } j,\ \sum_{j=1}^{t} \ell_j \leqslant p - 2t \right\}.$$

Given $(\ell_1, \ell_2, \ldots, \ell_t) \in L(\nu_1, \nu_2, \ldots, \nu_t)$, put $A(\nu_1, \nu_2, \ldots, \nu_t; \ell_1, \ell_2, \ldots, \ell_t)$ to be equal to

$$a_{(\ell_1, \ell_2, \ldots, \ell_t)} \binom{\ell_1}{\nu_1 - 2} \binom{\ell_2}{\nu_2 - 2} \cdots \binom{\ell_t}{\nu_t - 2} (q-1)^t (q-2)^{\nu - 2t},$$

where

$$a_{(\ell_1,\ell_2,\ldots,\ell_t)} = \sum_{k_1=1}^{p-\sum_{i=1}^{t}\ell_i-2t+1} \sum_{k_2=k_1+\ell_1+2}^{p-\sum_{i=2}^{t}\ell_i-2(t-1)+1} \cdots \sum_{k_{t-1}=k_{t-2}+\ell_{t-2}+2}^{p-\sum_{i=t-1}^{t}\ell_i-3} \sum_{k_t=k_{t-1}+\ell_{t-1}+2}^{p-\ell_t-1} 1. \tag{1}$$

Definition 1. For any integer $\nu \geqslant 0$, define $N(\nu)$ to be equal to

1, if $\nu = 0$;
0, if $\nu = 1$ or $\nu \geqslant p+1$;
$\sum_{t\geqslant 1} \sum_{(\nu_1,\nu_2,\ldots,\nu_t)\in P_t(\nu)} \sum_{(\ell_1,\ell_2,\ldots,\ell_t)\in L(\nu_1,\nu_2,\ldots,\nu_t)} A(\nu_1,\nu_2,\ldots,\nu_t;\ell_1,\ell_2,\ldots,\ell_t)$, otherwise.

We are now ready to state

Theorem 2. *Let $\mathbb{F}_q$ be the finite field with q elements, p be an odd prime co-prime to q and $m \geqslant 1$ be an integer. If the multiplicative order of q modulo p^m is $\phi(p^m)$, then the weight distribution $A_w^{(p^r)}$, $w \geqslant 0$, of the q-ary irreducible cyclic code $\mathcal{M}_1^{(p^r)}$ is given by*

$$A_w^{(p^r)} = \sum N(w_1)N(w_2)\cdots N(w_{p^{r-1}}),$$

where the summation runs over all tuples $(w_1, w_2, \ldots, w_{p^{r-1}})$ of non-negative integers w_i's satisfying $\sum_{i=1}^{p^{r-1}} w_i = w$.

We need some preparation to prove this theorem.
Let e_i, $1 \leqslant i \leqslant p^r$, be the canonical basis of $\mathbb{F}_q^{p^r}$.

Lemma 1. *If the multiplicative order of q modulo p^m is $\phi(p^m)$, then the generating polynomial of $\mathcal{M}_1^{(p^r)}$ is $x^{p^{r-1}} - 1$, and the vectors*

$$e_{i+p^{r-1}} - e_i, \quad 1 \leqslant i \leqslant (p-1)p^{r-1},$$

constitute a basis of $\mathcal{M}_1^{(p^r)}$ over $\mathbb{F}_q$.

Proof. Let α be a primitive p^rth root of unity in some extension of $\mathbb{F}_q$. Then the generating polynomial $g(x)$ of $\mathcal{M}_1^{(p^r)}$ is $\frac{x^{p^r}-1}{M_\alpha(x)}$ with $M_\alpha(x) = \prod_{j\in C_1}(x-\alpha^j)$, where C_1 is the q-cyclotomic coset of 1 modulo p^r. Observe that the multiplicative order of q modulo p^m is $\phi(p^m)$ and $1 \leqslant r \leqslant m$ yields that the multiplicative order of q modulo p^r is $\phi(p^r) = (p-1)p^{r-1}$. Therefore, the q-cyclotomic coset modulo p^r containing 1 is $\{1, q, q^2, \ldots, q^{(p-1)p^{r-1}-1}\}$, which is a reduced residue system modulo p^r. As a result, the roots of $M_\alpha(x)$ are precisely all the primitive p^rth roots of unity. Also note that the roots of the polynomial $\frac{x^{p^r}-1}{x^{p^{r-1}}-1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}$ are also precisely all the primitive p^rth roots of unity, which gives $M_\alpha(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1}$ and hence $g(x) = x^{p^{r-1}} - 1$. Now, by [8, Chapter 7, Theorem 1], $\mathcal{M}_1^{(p^r)}$ is the subspace of R_{p^r} spanned by $g(x), xg(x), \ldots, x^{(p-1)p^{r-1}-1}g(x)$. But under the standard isomorphism from R_{p^r} to $\mathbb{F}_q^{p^r}$, $x^{i-1}g(x)$ corresponds to $e_{i+p^{r-1}} - e_i$ for each i, which proves the result. □

For $1 \leqslant i \leqslant p^{r-1}$, let V_i be the vector subspace of $\mathbb{F}_q^{p^r}$ spanned by

$$e_{i+jp^{r-1}} - e_{i+(j-1)p^{r-1}}, \quad 1 \leqslant j \leqslant p-1.$$

Definition 2. We say that a vector $v \in V_i$ is a nice vector if

$$v = \sum_{j=k}^{k+\ell} \alpha_j (e_{i+jp^{r-1}} - e_{i+(j-1)p^{r-1}}),$$

where $0 \neq \alpha_j \in \mathbb{F}_q$, $k \geqslant 1$, $\ell \geqslant 0$, $k+\ell \leqslant p-1$. The integer ℓ is called the length of v denoted $\ell(v)$; k is called the initial point of v, denoted by $I(v)$; and $k+\ell$ is called the end point of v, denoted by $E(v)$.

Definition 3. Let $v_1, v_2, \ldots, v_t \in V_i$. We say that $v_1, v_2, \ldots, v_t$ is a chain in V_i if each v_j, $1 \leqslant j \leqslant t$, is a nice vector and $I(v_j) \geqslant E(v_{j-1}) + 2$ for $2 \leqslant j \leqslant t$.

Remark 1.

(i) If $v_1, v_2, \ldots, v_t$ is a chain in V_i, then $wt(\sum_{j=1}^t v_j) = \sum_{j=1}^t wt(v_j)$.
(ii) Any $v \in V_i$ can be written as $v = \sum_{j=1}^t v_j$, where $v_1, v_2, \ldots, v_t$ is a chain in V_i.

Lemma 2.

(i) *If $0 \neq v \in V_i$, then $2 \leqslant wt(v) \leqslant p$.*
(ii) *If $v \in V_i$ is a nice vector of length ℓ, then $2 \leqslant wt(v) \leqslant \ell + 2$.*
(iii) *If ℓ, k, ν are integers satisfying $0 \leqslant \ell \leqslant p-1$, $1 \leqslant k \leqslant p-\ell-1$ and $2 \leqslant \nu \leqslant \ell+2$, then the number of nice vectors in V_i of length ℓ, weight ν and initial point k is $\binom{\ell}{\nu-2}(q-1)(q-2)^{\nu-2}$. (Note that this number is independent of the choice of the initial point and i.)*

Proof. (i) Let $v \in V_i$. Then

$$\begin{aligned} v &= \sum_{j=1}^{p-1} \alpha_j (e_{i+jp^{r-1}} - e_{i+(j-1)p^{r-1}}) \\ &= -\alpha_1 e_i + \alpha_{p-1} e_{i+(p-1)p^{r-1}} + \sum_{j=1}^{p-2} (\alpha_j - \alpha_{j+1}) e_{i+jp^{r-1}}, \end{aligned} \tag{2}$$

$\alpha_j \in \mathbb{F}_q$. If $v \neq 0$, then at least one $\alpha_j \neq 0$, which gives $wt(v) \geqslant 2$. Also it is clear from (2) that $wt(v) \leqslant p$. This proves (i).

(ii) is similar to (i).

(iii) If $v \in V_i$ is a nice vector of length ℓ, weight ν and $I(v) = k$, then

$$\begin{aligned} v &= \sum_{j=k}^{k+\ell} \alpha_j (e_{i+jp^{r-1}} - e_{i+(j-1)p^{r-1}}) \\ &= -\alpha_k e_{i+(k-1)p^{r-1}} + \alpha_{k+\ell} e_{i+(k+\ell)p^{r-1}} + \sum_{j=k}^{k+\ell-1} (\alpha_j - \alpha_{j+1}) e_{i+jp^{r-1}}, \end{aligned}$$

where $0 \neq \alpha_j \in \mathbb{F}_q$, $k \leqslant j \leqslant k+\ell$. Now observe that the weight of v is ν if and only if out of a total of ℓ differences $\alpha_j - \alpha_{j+1}$ $(k \leqslant j \leqslant k+\ell-1)$, exactly $(\nu-2)$ are non-zero, which happens if and only if there exist $i_1, i_2, \ldots, i_{\nu-2}$, $k \leqslant i_1 < i_2 < \cdots < i_{\nu-2} \leqslant k+\ell-1$ such that $\alpha_k = \alpha_{k+1} = \cdots = \alpha_{i_1}, \alpha_{i_1} \neq \alpha_{i_1+1}, \alpha_{i_1+1} = \alpha_{i_1+2} = \cdots = \alpha_{i_2}, \alpha_{i_2} \neq \alpha_{i_2+1}, \ldots, \alpha_{i_{\nu-2}} \neq \alpha_{i_{\nu-2}+1}, \alpha_{i_{\nu-2}+1} = \cdots = \alpha_{k+\ell}$. It can be seen that the total number of choices of such a nice vector v is $\binom{\ell}{\nu-2}(q-1)(q-2)^{\nu-2}$. $\square$

Lemma 3. *Let $1 \leqslant i \leqslant p^{r-1}$. Given an integer ν satisfying $2 \leqslant \nu \leqslant p$, there are precisely $N(\nu)$ elements in V_i having weight ν.*

Proof. Let $A(\nu)$ denote the set of all codewords in V_i having weight ν. For any $t \geqslant 1$, $(\nu_1, \nu_2, \ldots, \nu_t) \in P_t(\nu)$, and $(\ell_1, \ell_2, \ldots, \ell_t) \in L(\nu_1, \nu_2, \ldots, \nu_t)$, let

$$V_i(\nu_1, \nu_2, \ldots, \nu_t; \ell_1, \ell_2, \ldots, \ell_t) := \left\{ \sum_{j=1}^{t} v_j \;\middle|\; \begin{array}{l} v_1, v_2, \ldots, v_t \text{ is a chain in } V_i \\ wt(v_j) = \nu_j,\ \ell(v_j) = \ell_j,\ 1 \leqslant j \leqslant t \end{array} \right\}.$$

We assert that

$$A(\nu) = \bigcup_{t \geqslant 1} \bigcup_{(\nu_1, \nu_2, \ldots, \nu_t) \in P_t(\nu)} \bigcup_{(\ell_1, \ell_2, \ldots, \ell_t) \in L(\nu_1, \nu_2, \ldots, \nu_t)} V_i(\nu_1, \nu_2, \ldots, \nu_t; \ell_1, \ell_2, \ldots, \ell_t), \tag{3}$$

and moreover, this union is disjoint. It follows from Remark 1(i), that the right-hand side of (3) is contained in the left-hand side. Now, let $v \in A(\nu)$. By Remark 1, $v = \sum_{j=1}^{t} v_j$, where $v_1, v_2, \ldots, v_t$ is a chain in V_i and $\nu = wt(v) = \sum_{j=1}^{t} wt(v_j)$. Let $\nu_j = wt(v_j)$ and $\ell_j = \ell(v_j)$. By Lemma 2, $2 \leqslant \nu_j \leqslant p$, $\ell_j \geqslant \nu_j - 2$ for all j. Also $\sum_{j=1}^{t} \ell_j = \sum_{j=1}^{t} (E(v_j) - I(v_j)) = \sum_{j=2}^{t} (E(v_{j-1}) - I(v_j)) + E(v_t) - I(v_1) \leqslant p - 2t$, as $I(v_1) \geqslant 1$, $E(v_t) \leqslant p-1$ and $I(v_j) - E(v_{j-1}) \geqslant 2$. This gives $(\ell_1, \ell_2, \ldots, \ell_t) \in L(\nu_1, \nu_2, \ldots, \nu_t)$ and $v \in V_i(\nu_1, \nu_2, \ldots, \nu_t; \ell_1, \ell_2, \ldots, \ell_t)$, which proves the assertion (3). It is clear that the union in the right-hand side of (3) is disjoint.

We next assert that $|V_i(\nu_1, \nu_2, \ldots, \nu_t; \ell_1, \ell_2, \ldots, \ell_t)|$ equals

$$a_{(\ell_1, \ell_2, \ldots, \ell_t)} \binom{\ell_1}{\nu_1 - 2} \binom{\ell_2}{\nu_2 - 2} \cdots \binom{\ell_t}{\nu_t - 2} (q-1)^t (q-2)^{\nu - 2t}, \tag{4}$$

where $a_{(l_1, l_2, \ldots, l_t)}$ is as given in Eq. (1). In order to find $|V_i(\nu_1, \nu_2, \ldots, \nu_t; \ell_1, \ell_2, \ldots, \ell_t)|$, we need to find the number of chains $v_1, v_2, \ldots, v_t$ in V_i such that $wt(v_j) = \nu_j$ and $\ell(v_j) = \ell_j$ for all j. Let $k_j = I(v_j)$. Then, $k_1 \geqslant 1$, $k_t + \ell_t \leqslant p-1$ and $k_{j-1} + \ell_{j-1} + 2 \leqslant k_j$ for $2 \leqslant j \leqslant t$. This gives

$$1 \leqslant k_1 \leqslant p - \sum_{i=1}^{t} \ell_i - 2t + 1,$$

$$k_1 + \ell_1 + 2 \leqslant k_2 \leqslant p - \sum_{i=2}^{t} \ell_i - 2(t-1) + 1,$$

$$\cdots$$

$$k_{t-2} + \ell_{t-2} + 2 \leqslant k_{t-1} \leqslant p - \sum_{i=t-1}^{t} \ell_i - 3,$$

$$k_{t-1} + \ell_{t-1} + 2 \leqslant k_t \leqslant p - \ell_t - 1.$$

Therefore the total number of choices for the initial points $k_1, k_2, \ldots, k_t$ is

$$\sum_{k_1=1}^{p-\sum_{i=1}^{t}\ell_i-2t+1} \sum_{k_2=k_1+\ell_1+2}^{p-\sum_{i=2}^{t}\ell_i-2(t-1)+1} \cdots \sum_{k_{t-1}=k_{t-2}+\ell_{t-2}+2}^{p-\sum_{i=t-1}^{t}\ell_i-3} \sum_{k_t=k_{t-1}+\ell_{t-1}+2}^{p-\ell_t-1} 1,$$

which is equal to $a_{(\ell_1,\ell_2,\ldots,\ell_t)}$. By Lemma 2(iii), the number of nice vectors v_j of length ℓ_j, weight ν_j and having a fixed initial point k_j, is given by $\binom{\ell_j}{\nu_j-2}(q-1)(q-2)^{\nu_j-2}$ for each j, $1 \leqslant j \leqslant t$. Consequently, the total number of vectors in $V_i(\nu_1, \nu_2, \ldots, \nu_t; \ell_1, \ell_2, \ldots, \ell_t)$ is given by

$$a_{(\ell_1,\ell_2,\ldots,\ell_t)} \binom{\ell_1}{\nu_1-2}\binom{\ell_2}{\nu_2-2}\cdots\binom{\ell_t}{\nu_t-2}(q-1)^t(q-2)^{\nu-2t},$$

which proves the assertion (4). The lemma now immediately follows from (3) and (4). □

We are now ready to prove Theorem 2.

Proof of Theorem 2. Let $w \geqslant 0$ and let $\mathcal{A}(w)$ denote the codewords in $\mathcal{M}_1^{(p^r)}$ having weight w. For any tuple $(w_1, w_2, \ldots, w_{p^{r-1}})$ of non-negative integers w_i's satisfying $\sum_{i=1}^{p^{r-1}} w_i = w$, define

$$\mathcal{S}_{(w_1,w_2,\ldots,w_{p^{r-1}})} = \left\{ \sum_{i=1}^{p^{r-1}} c_i \;\middle|\; c_i \in V_i,\ wt(c_i) = w_i,\ 1 \leqslant i \leqslant p^{r-1} \right\}.$$

It follows from Lemma 1 and the definition of V_i's that $\mathcal{A}(w) = \bigcup \mathcal{S}_{(w_1,w_2,\ldots,w_{p^{r-1}})}$, where the union runs over all tuples $(w_1, w_2, \ldots, w_{p^{r-1}})$ of integers w_i's satisfying $w_i \geqslant 0$ and $\sum_{i=1}^{p^{r-1}} w_i = w$, and also it is clear that the union is disjoint. Therefore,

$$A_w^{(p^r)} = \left| \bigcup \mathcal{S}_{(w_1,w_2,\ldots,w_{p^{r-1}})} \right| = \sum |\mathcal{S}_{(w_1,w_2,\ldots,w_{p^{r-1}})}|.$$

But $|\mathcal{S}_{(w_1,w_2,\ldots,w_{p^{r-1}})}| = N_1(w_1)N_2(w_2)\cdots N_{p^{r-1}}(w_{p^{r-1}})$, where $N_i(w_i)$ is the number of codewords in V_i having weight w_i. However, by Lemma 3, $N_i(w_i)$ equals $N(w_i)$ for any i, which completes the proof. □

3.2. The multiplicative order of q modulo p^m is a power of p

Theorem 3. *Let $\mathbb{F}_q$ be the finite field with q elements, p be an odd prime co-prime to q and $m \geqslant 1$ be an integer. Suppose that the multiplicative order of q modulo p^m is p^d for some integer d (note that $0 \leqslant d < m$). Then, if*

(i) *$r \leqslant m-d$, the only possible non-zero weight in $\mathcal{M}_1^{(p^r)}$ is p^r, which is attained by all its $q-1$ non-zero codewords.*
(ii) *$r > m-d$, the weight distribution $A_w^{(p^r)}$, $w \geqslant 0$, of $\mathcal{M}_1^{(p^r)}$ is given by*

$$A_w^{(p^r)} = \begin{cases} 0 & \text{if } p^{m-d} \text{ does not divide } w; \\ \binom{p^{r-(m-d)}}{w'}(q-1)^{w'} & \text{if } w = p^{m-d}w',\ 0 \leqslant w' \leqslant p^{r-(m-d)}. \end{cases}$$

In order to prove Theorem 3, we first prove the following:

Lemma 4. *Let p, q, m, d be as defined in Theorem 3. Then $O_{p^r}(q)$, the multiplicative order of q modulo p^r, is given by*

$$O_{p^r}(q) = \begin{cases} 1 & \text{if } r \leqslant m-d; \\ p^{r-(m-d)} & \text{if } r > m-d. \end{cases}$$

Proof. First we assert that

$$O_{p^{m-d}}(q) = 1. \tag{5}$$

To prove this, let $O_{p^{m-d}}(q) = t$. Working, as in [11, Lemma 1], we get $O_{p^m}(q) = tp^d$. As it is given that $O_{p^m}(q) = p^d$, we get $t = 1$, which proves (5).

If $r \leqslant m-d$, then by (5), we have $O_{p^r}(q) = 1$. For the case $r > m-d$, working again as in [11, Lemma 1], we obtain that $O_{p^r}(q) = p^{r-(m-d)}$. This proves the lemma. □

Lemma 5. *Let p, q, m, d be as in Theorem 3. If $r > m-d$, then there exists a primitive p^{m-d}th root of unity $\beta \in \mathbb{F}_q$, such that the vectors*

$$\sum_{j=0}^{p^{m-d}-1} \beta^{j+1} e_{i+jp^{r-(m-d)}}, \quad 1 \leqslant i \leqslant p^{r-(m-d)},$$

constitute a basis of $\mathcal{M}_1^{(p^r)}$ over $\mathbb{F}_q$.

Proof. By Lemma 4, the q-cyclotomic coset modulo p^r containing 1 is $\{1, q, q^2, \ldots, q^{p^{r-(m-d)}-1}\}$. Therefore $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{p^{r-(m-d)}-1}}$ are precisely all the roots of the minimal polynomial of α over $\mathbb{F}_q$. We also observe that $x^{p^{r-(m-d)}} - \alpha^{p^{r-(m-d)}} \in \mathbb{F}_q[x]$ and $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{p^{r-(m-d)}-1}}$ are precisely all its roots. Therefore, $x^{p^{r-(m-d)}} - \alpha^{p^{r-(m-d)}}$ is the minimal polynomial of α over $\mathbb{F}_q$ and hence the generating polynomial $g(x)$ of $\mathcal{M}_1^{(p^r)}$ is $\frac{x^{p^r}-1}{x^{p^{r-(m-d)}}-\alpha^{p^{r-(m-d)}}} = \beta + \beta^2 x^{p^{r-(m-d)}} + \beta^3 x^{2p^{r-(m-d)}} + \cdots + \beta^{p^{m-d}-1} x^{(p^{m-d}-2)p^{r-(m-d)}} + x^{(p^{m-d}-1)p^{r-(m-d)}}$, where $\beta = \alpha^{-p^{r-(m-d)}}$. Now, as a vector subspace of R_{p^r}, $\mathcal{M}_1^{(p^r)}$ is spanned by $g(x), xg(x), \ldots, x^{p^{r-(m-d)}-1} g(x)$. Since, under the standard isomorphism from R_{p^r} to $\mathbb{F}_q{}^{p^r}$, $x^{i-1}g(x)$ corresponds to $\sum_{j=0}^{p^{m-d}-1} \beta^{j+1} e_{i+jp^{r-(m-d)}}$ for $1 \leqslant i \leqslant p^{r-(m-d)}$, the result follows. □

Proof of Theorem 3. (i) Let α be a primitive p^rth root of unity in some extension of $\mathbb{F}_q$. If $r \leqslant m-d$, by Lemma 4, the multiplicative order of q modulo p^r is 1. Therefore $\alpha^{q-1} = 1$, i.e., $\alpha \in \mathbb{F}_q$ and the minimal polynomial of α over $\mathbb{F}_q$ is $x - \alpha$. Hence $\mathcal{M}_1^{(p^r)}$ is a 1-dimensional subspace of $\mathbb{F}_q^{p^r}$ generated by $\frac{x^{p^r}-1}{x-\alpha} = \alpha^{p^r-1} + \alpha^{p^r-2}x + \alpha^{p^r-3}x^2 + \cdots + \alpha x^{p^r-2} + x^{p^r-1}$ and therefore every codeword of $\mathcal{M}_1^{(p^r)}$ is a scalar multiple of $\alpha^{p^r-1} + \alpha^{p^r-2}x + \alpha^{p^r-3}x^2 + \cdots + \alpha x^{p^r-2} + x^{p^r-1}$. This implies that the only possible non-zero weight in $\mathcal{M}_1^{(p^r)}$ is p^r, which is attained by all its $(q-1)$ non-zero codewords.

(ii) If $r > m-d$, by Lemma 5, any codeword $c \in \mathcal{M}_1^{(p^r)}$ can be written as $c = \sum_{i=1}^{p^{r-(m-d)}} \sum_{j=0}^{p^{m-d}-1} \alpha_i \beta^{j+1} e_{i+jp^{r-(m-d)}}$, $\alpha_i \in \mathbb{F}_q$. Clearly, $wt(c)$ is $p^{m-d}w'$, where w' is the number of non-zero α_i's. Thus $A_w^{(p^r)} = 0$ if p^{m-d} does not divide w. Moreover a codeword in $\mathcal{M}_1^{(p^r)}$ has weight $w = p^{m-d}w'$ if and only if it is a linear combination of any w' basis vectors over $\mathbb{F}_q$ out of a total $p^{r-(m-d)}$ basis vectors of $\mathcal{M}_1^{(p^r)}$. This implies that there are $\binom{p^{r-(m-d)}}{w'}(q-1)^{w'}$ codewords in $\mathcal{M}_1^{(p^r)}$ having weight $p^{m-d}w'$, which proves the theorem. □

3.3. The multiplicative order of q modulo p^m is twice a power of p

We now determine the weight distribution of $\mathcal{M}_1^{(p^r)}$, when $O_{p^m}(q) = 2p^d$ for some $d \geqslant 0$. As $O_{p^m}(q)$ is a divisor of $\phi(p^m)$, we have $d \leqslant m-1$. Let $u = min(r, m-d)$. For any integer $\nu \geqslant 0$, define

$$n(\nu) := \begin{cases} 1 & \text{if } \nu = 0; \\ (q-1)p^u & \text{if } \nu = p^u - 1; \\ (q-1)(q-p^u+1) & \text{if } \nu = p^u; \\ 0 & \text{otherwise.} \end{cases}$$

In this case, we have the following:

Theorem 4. *The weight distribution $A_w^{(p^r)}$, $w \geqslant 0$, of $\mathcal{M}_1^{(p^r)}$ is given by*

$$A_w^{(p^r)} = \sum n(w_1)n(w_2)\cdots n(w_{p^{r-u}}),$$

where the summation runs over all tuples $(w_1, w_2, \ldots, w_{p^{r-u}})$ of non-negative integers w_i's satisfying $w_1 + w_2 + \cdots + w_{p^{r-u}} = w$.

Lemma 6. *Let p, q, m, d be as above. Then*

$$O_{p^r}(q) = \begin{cases} 2 & \text{if } r \leqslant m-d; \\ 2p^{r-(m-d)} & \text{if } r > m-d. \end{cases}$$

Proof. Proof is similar to that of Lemma 4. □

Lemma 7. *Let p, q, m, d, u be as above. There exist non-zero $b_0, b_1, \ldots, b_{p^u-2} \in \mathbb{F}_q$ such that the following vectors*

$$\Re_i := \sum_{j=0}^{p^u-2} b_j e_{i+jp^{r-u}}, \quad 1 \leqslant i \leqslant 2p^{r-u},$$

constitute a basis of $\mathcal{M}_1^{(p^r)}$ over $\mathbb{F}_q$.

Proof. By Lemma 6, the q-cyclotomic coset modulo p^r containing 1 is $\{1, q, q^2, \ldots, q^{2p^{r-u}-1}\}$. Therefore, if α is a primitive p^rth root of unity in some extension of $\mathbb{F}_q$, then $\alpha, \alpha^q, \ldots, \alpha^{q^{2p^{r-u}-1}}$ are precisely all the zeros of the minimal polynomial of α over $\mathbb{F}_q$. We observe that

(i) $x^{p^{r-u}} - \alpha^{p^{r-u}} \in \mathbb{F}_{q^2}[x]$ and $\alpha, \alpha^{q^2}, \ldots, \alpha^{q^{2p^{r-u}-2}}$ are precisely all its zeros; and
(ii) $x^{p^{r-u}} - \alpha^{p^{r-u}q} \in \mathbb{F}_{q^2}[x]$ and $\alpha^q, \alpha^{q^3}, \ldots, \alpha^{q^{2p^{r-u}-1}}$ are precisely all its zeros.

As a consequence,

$$\left(x^{p^{r-u}} - \alpha^{p^{r-u}}\right)\left(x^{p^{r-u}} - \alpha^{p^{r-u}q}\right) = x^{2p^{r-u}} - \left(\alpha^{p^{r-u}} + \alpha^{p^{r-u}q}\right)x^{p^{r-u}} + 1$$

is the minimal polynomial of α over $\mathbb{F}_q$. Thus the generating polynomial $g(x)$ of the minimal ideal $\mathcal{M}_1^{(p^r)}$ is $\frac{x^{p^r}-1}{x^{2p^{r-u}} - (\alpha^{p^{r-u}} + \alpha^{p^{r-u}q})x^{p^{r-u}} + 1}$. By division algorithm, we have

$$g(x) = \frac{x^{p^r} - 1}{x^{2p^{r-u}} - (\alpha^{p^{r-u}} + \alpha^{p^{r-u}q})x^{p^{r-u}} + 1}$$
$$= b_0 + b_1 x^{p^{r-u}} + b_2 x^{2p^{r-u}} + \cdots + b_{p^u-2} x^{(p^u-2)p^{r-u}},$$

where

$$b_0 = -1, \qquad b_1 = -\left(\alpha^{p^{r-u}} + \alpha^{p^{r-u}q}\right),$$
$$b_i - \left(\alpha^{p^{r-u}} + \alpha^{p^{r-u}q}\right) b_{i-1} + b_{i-2} = 0 \quad \text{for } 2 \leqslant i \leqslant p^u - 2,$$

and

$$b_{p^u-3} = \alpha^{p^{r-u}} + \alpha^{p^{r-u}q}, \qquad b_{p^u-2} = 1.$$

On solving the above recurrence relation, we get that

$$b_i = \frac{-(\alpha^{p^{r-u}})^{(i+1)} + (\alpha^{p^{r-u}})^{q(i+1)}}{\alpha^{p^{r-u}} - \alpha^{p^{r-u}q}}. \tag{6}$$

We claim that all the b_i's are non-zero. Note that $b_i = 0$ if and only if $(\alpha^{p^{r-u}})^{(q-1)(i+1)} = 1$, which holds if and only if $(q-1)(i+1) \equiv 0 \pmod{p^u}$, as $\alpha^{p^{r-u}}$ is a primitive p^uth root of unity. By Lemma 6, $q-1$ is not divisible by p. Therefore, we get $(i+1) \equiv 0 \pmod{p^u}$. But this is not possible, because $1 \leqslant i+1 \leqslant p^u - 1 < p^u$. This proves the claim.

Now, $\mathcal{M}_1^{(p^r)}$ is spanned by $g(x), xg(x), \ldots, x^{2p^{r-u}-1}g(x)$ and under the standard isomorphism from R_{p^r} to $\mathbb{F}_q^{p^r}$, $x^{i-1}g(x)$ corresponds to $\Re_i$ for $1 \leqslant i \leqslant 2p^{r-u}$, the result follows. □

For $1 \leqslant i \leqslant p^{r-u}$, let

$$U_i := \text{the subspace of } \mathbb{F}_q^{p^r} \text{ generated by } \Re_i \text{ and } \Re_{i+p^{r-u}}.$$

Lemma 8. *For any $\nu \geqslant 0$, the number of codewords in U_i of weight ν is $n(\nu)$.*

Proof. It is enough to show that the only possible non-zero weights in U_i are $p^u - 1$ and p^u, and that there are precisely $(q-1)p^u$ and $(q-1)(q-p^u+1)$ codewords in U_i having weight $p^u - 1$ and p^u respectively. Let $c \in U_i$ be a non-zero codeword. Then there exist $\alpha_1, \alpha_2 \in \mathbb{F}_q$, not both zero, such that

$$c = \alpha_1 \Re_i + \alpha_2 \Re_{i+p^{r-u}}$$
$$= \alpha_1 b_0 e_i + \alpha_2 b_{p^u-2} e_{i+(p^u-1)p^{r-u}} + \sum_{j=1}^{p^u-2} (\alpha_1 b_j + \alpha_2 b_{j-1}) e_{i+jp^{r-u}}.$$

Case I. One of the α_1 or α_2 is zero.

If $\alpha_1 = 0$, then $wt(c) = wt(\Re_{i+p^{r-u}}) = p^u - 1$. Similarly, if $\alpha_2 = 0$, then $wt(c) = wt(\Re_i) = p^u - 1$. Note that there are a total of $2(q-1)$ such codewords in U_i.

Case II. Both α_1 and α_2 are non-zero.

We assert that among the possible non-zero entries $\alpha_1 b_0$, $\alpha_1 b_j + \alpha_2 b_{j-1}$ $(1 \leqslant j \leqslant p^u - 2)$, $\alpha_2 b_{p^u-2}$ of c, at most one of the entries can be zero.

Clearly, $\alpha_1 b_0$ and $\alpha_2 b_{p^u-2}$ can't be zero. If $\alpha_1 b_j + \alpha_2 b_{j-1} = 0$ and $\alpha_1 b_k + \alpha_2 b_{k-1} = 0$ for some j, k, $1 \leqslant j < k \leqslant p^u - 2$, then $\alpha_1(b_j b_{k-1} - b_k b_{j-1}) = 0$. But, using (6), we have $b_j b_{k-1} - b_k b_{j-1} = -b_{k-j-1}$, which gives $-\alpha_1 b_{k-j-1} = 0$. This gives a contradiction, since both α_1 and b_{k-j-1} are non-zero. This proves our assertion.

As a consequence of the assertion, the weight of c is either p^u or $p^u - 1$. However $wt(c) = p^u - 1$ if and only if $\alpha_2 = -\alpha_1 b_j b_{j-1}^{-1}$ for some j, $1 \leqslant j \leqslant p^u - 2$. Since $-\alpha_1 b_1 b_0^{-1}, -\alpha_1 b_2 b_1^{-1}, \ldots, -\alpha_1 b_{p^u-2} b_{p^u-3}^{-1}$ are all distinct, we get that, for each choice of α_1, there are $p^u - 2$ choices of α_2. Hence there are $(q-1)(p^u-2)$ codewords c having weight $p^u - 1$ with α_1 and α_2 both non-zero. The remaining $(q-1)^2 - (q-1)(p^u-2)$ codewords have weight p^u.

Combining the two cases, the result follows. □

Proof of Theorem 4. Let $w \geqslant 0$. For any tuple $(w_1, w_2, \ldots, w_{p^{r-u}})$ of non-negative integers w_i's satisfying $\sum_{i=1}^{p^{r-u}} w_i = w$, define

$$\mathcal{S}_{(w_1, w_2, \ldots, w_{p^{r-u}})} = \left\{ \sum_{i=1}^{p^{r-u}} c_i \;\middle|\; c_i \in U_i,\ wt(c_i) = w_i,\ 1 \leqslant i \leqslant p^{r-u} \right\}.$$

It follows from Lemma 7 and the definition of U_i's that $\bigcup \mathcal{S}_{(w_1, w_2, \ldots, w_{p^{r-1}})}$ is precisely the set of all the elements in $\mathcal{M}_1^{(p^r)}$ having weight w, where the union runs over all tuples $(w_1, w_2, \ldots, w_{p^{r-u}})$ of non-negative integers w_i's satisfying $\sum_{i=1}^{p^{r-u}} w_i = w$. It is easily seen that the union is disjoint. Therefore,

$$A_w^{(p^r)} = \left| \bigcup \mathcal{S}_{(w_1, w_2, \ldots, w_{p^{r-1}})} \right| = \sum |\mathcal{S}_{(w_1, w_2, \ldots, w_{p^{r-1}})}|.$$

But $|\mathcal{S}_{(w_1, w_2, \ldots, w_{p^{r-1}})}| = N_1(w_1) N_2(w_2) \cdots N_{p^{r-1}}(w_{p^{r-1}})$, where $N_i(w_i)$ is the number of codewords in U_i having weight w_i. However, by Lemma 8, $N_i(w_i)$ equals $n(w_i)$ for all i, which completes the proof. □

4. Some examples

In this section, we determine the weight distribution of the ternary irreducible cyclic codes $\mathcal{M}_1^{(25)}$ and $\mathcal{M}_1^{(49)}$, 7-ary irreducible cyclic code $\mathcal{M}_1^{(3^r)}$ $(r \geqslant 1)$, binary irreducible cyclic code $\mathcal{M}_1^{(9)}$ and the quaternary code $\mathcal{M}_1^{(25)}$.

4.1. Example 1

Let $p = 5$, $r = 2$ and $q = 3$. As the multiplicative order of 3 modulo 25 is $\phi(25)$, we apply Theorem 2 to compute the weight distribution $A_0^{(25)}, A_1^{(25)}, \ldots, A_{25}^{(25)}$ of the ternary code $\mathcal{M}_1^{(25)}$. For this purpose, we first compute the numbers $N(\nu)$, $\nu \geqslant 0$. By Definition 1, $N(0) = 1$ and $N(\nu) = 0$ if $\nu = 1$ or $\nu \geqslant 6$. We now compute $N(2)$, $N(3)$, $N(4)$ and $N(5)$. In this case, by (1), we have

$$a_{(\ell_1)} = 4 - \ell_1 \quad \text{and} \quad a_{(\ell_1, \ell_2)} = \frac{(2 - \ell_1 - \ell_2)(3 - \ell_1 - \ell_2)}{2}.$$

Therefore,

$$N(2) = \sum_{\ell_1=0}^{3} A(2;\ell_1) = \sum_{\ell_1=0}^{3} a_{(\ell_1)} \binom{\ell_1}{0} (q-1) = 20,$$

$$N(3) = \sum_{\ell_1=1}^{3} A(3;\ell_1) = \sum_{\ell_1=1}^{3} a_{(\ell_1)} \binom{\ell_1}{1} (q-1) = 20,$$

$$\begin{aligned} N(4) &= \sum_{\ell_1=2}^{3} A(4;\ell_1) + \sum_{\ell_1\geqslant 0,\,\ell_2\geqslant 0}^{\ell_1+\ell_2\leqslant 1} A(2,2;\ell_1,\ell_2) \\ &= \sum_{\ell_1=1}^{3} a_{(\ell_1)} \binom{\ell_1}{2} (q-1) + \sum_{\ell_1\geqslant 0,\,\ell_2\geqslant 0}^{\ell_1+\ell_2\leqslant 1} a_{(\ell_1,\ell_2)} \binom{\ell_1}{0}\binom{\ell_2}{0} (q-1)^2 = 30, \end{aligned}$$

$$\begin{aligned} N(5) &= \sum_{\ell_1=3} A(5;\ell_1) + \sum_{\ell_1\geqslant 0,\,\ell_2\geqslant 1}^{\ell_1+\ell_2\leqslant 1} A(2,3;\ell_1,\ell_2) + \sum_{\ell_1\geqslant 1,\,\ell_2\geqslant 0}^{\ell_1+\ell_2\leqslant 1} A(3,2;\ell_1,\ell_2) \\ &= a_{(3)}(q-1) + a_{(0,1)}(q-1)^2 + a_{(1,0)}(q-1)^2 = 10. \end{aligned}$$

Now Theorem 1 gives the weight distribution of the ternary irreducible cyclic code $\mathcal{M}_1^{(25)}$:

$$A_0^{(25)} = N(0) = 1,$$

$$A_1^{(25)} = 0,$$

$$A_2^{(25)} = \frac{5!}{4!} N(2) = 100,$$

$$A_3^{(25)} = \frac{5!}{4!} N(3) = 100,$$

$$A_4^{(25)} = \frac{5!}{4!} N(4) + \frac{5!}{2!3!} N(2)^2 = 4150,$$

$$A_5^{(25)} = \frac{5!}{4!} N(5) + \frac{5!}{3!} N(2)N(3) = 8050,$$

$$A_6^{(25)} = \frac{5!}{3!} N(2)N(4) + \frac{5!}{2!3!} N(3)^2 + \frac{5!}{2!3!} N(2)^3 = 96\,000,$$

$$A_7^{(25)} = \frac{5!}{3!} N(2)N(5) + \frac{5!}{3!} N(3)N(4) + \frac{5!}{2!2!} N(2)^2 N(3) = 256\,000,$$

$$\begin{aligned} A_8^{(25)} &= \frac{5!}{3!} N(3)N(5) + \frac{5!}{2!3!} N(4)^2 + \frac{5!}{2!2!} N(2)^2 N(4) + \frac{5!}{2!2!} N(2)N(3)^2 + \frac{5!}{4!} N(2)^4 \\ &= 1\,413\,000, \end{aligned}$$

$$\begin{aligned} A_9^{(25)} &= \frac{5!}{3!} N(4)N(5) + \frac{5!}{2!2!} N(2)^2 N(5) + \frac{5!}{2!} N(2)N(3)N(4) + \frac{5!}{2!3!} N(3)^3 \\ &\quad + \frac{5!}{3!} N(2)^3 N(3) = 4\,126\,000, \end{aligned}$$

$$A_{10}^{(25)} = \frac{5!}{2!3!}N(5)^2 + \frac{5!}{2!}N(2)N(3)N(5) + \frac{5!}{2!2!}N(2)N(4)^2 + \frac{5!}{2!2!}N(3)^2N(4) + \frac{5!}{3!}N(2)^3N(4) + \frac{5!}{2!2!}N(2)^2N(3)^2 + \frac{5!}{5!}N(2)^5 = 13\,941\,000,$$

$$A_{11}^{(25)} = \frac{5!}{2!}N(2)N(4)N(5) + \frac{5!}{2!2!}N(3)^2N(5) + \frac{5!}{3!}N(2)^3N(5) + \frac{5!}{2!2!}N(3)N(4)^2 + \frac{5!}{2!}N(2)^2N(3)N(4) + \frac{5!}{3!}N(2)N(3)^3 + \frac{5!}{4!}N(2)^4N(3) = 36\,220\,000,$$

$$A_{12}^{(25)} = \frac{5!}{2!2!}N(2)N(5)^2 + \frac{5!}{2!}N(3)N(4)N(5) + \frac{5!}{2!}N(2)^2N(3)N(5) + \frac{5!}{2!3!}N(4)^3 + \frac{5!}{2!2!}N(2)^2N(4)^2 + \frac{5!}{2!}N(2)N(3)^2N(4) + \frac{5!}{4!}N(2)^4N(4) + \frac{5!}{4!}N(3)^4 + \frac{5!}{2!3!}N(2)^3N(3)^2 = 87\,490\,000,$$

$$A_{13}^{(25)} = \frac{5!}{2!2!}N(3)N(5)^2 + \frac{5!}{2!2!}N(4)^2N(5) + \frac{5!}{2!}N(2)^2N(4)N(5) + \frac{5!}{2!}N(2)N(3)^2N(5) + \frac{5!}{4!}N(2)^4N(5) + \frac{5!}{2!}N(2)N(3)N(4)^2 + \frac{5!}{3!}N(3)^3N(4) + \frac{5!}{3!}N(2)^3N(3)N(4) + \frac{5!}{2!3!}N(2)^2N(3)^3 = 174\,730\,000,$$

$$A_{14}^{(25)} = \frac{5!}{2!2!}N(4)N(5)^2 + \frac{5!}{2!2!}N(2)^2N(5)^2 + 5!N(2)N(3)N(4)N(5) + \frac{5!}{3!}N(3)^3N(5) + \frac{5!}{3!}N(2)^3N(3)N(5) + \frac{5!}{3!}N(2)N(4)^3 + \frac{5!}{2!2!}N(3)^2N(4)^2 + \frac{5!}{2!3!}N(2)^3N(4)^2 + \frac{5!}{2!2!}N(2)^2N(3)^2N(4) + \frac{5!}{4!}N(2)N(3)^4 = 302\,890\,000,$$

$$A_{15}^{(25)} = \frac{5!}{2!3!}N(5)^3 + \frac{5!}{2!}N(2)N(3)N(5)^2 + \frac{5!}{2!}N(2)N(4)^2N(5) + \frac{5!}{2!}N(3)^2N(4)N(5) + \frac{5!}{3!}N(2)^3N(4)N(5) + \frac{5!}{2!2!}N(2)^2N(3)^2N(5) + \frac{5!}{3!}N(3)N(4)^3 + \frac{5!}{2!2!}N(2)^2N(3)N(4)^2 + \frac{5!}{3!}N(2)N(3)^3N(4) + N(3)^5 = 442\,410\,000,$$

$$A_{16}^{(25)} = \frac{5!}{2!}N(2)N(4)N(5)^2 + \frac{5!}{2!2!}N(3)^2N(5)^2 + \frac{5!}{3!2!}N(2)^3N(5)^2 + \frac{5!}{2!}N(3)N(4)^2N(5) + \frac{5!}{2!}N(2)^2N(3)N(4)N(5) + \frac{5!}{3!}N(2)N(3)^3N(5) + \frac{5!}{4!}N(4)^4 + \frac{5!}{2!3!}N(2)^2N(4)^3 + \frac{5!}{2!2!}N(2)N(3)^2N(4)^2 + \frac{5!}{4!}N(3)^4N(4) = 551\,650\,000,$$

$$A_{17}^{(25)} = \frac{5!}{3!}N(2)N(5)^3 + \frac{5!}{2!}N(3)N(4)N(5)^2 + \frac{5!}{2!2!}N(2)^2N(3)N(5)^2 + \frac{5!}{3!}N(4)^3N(5) + \frac{5!}{2!2!}N(2)^2N(4)^2N(5) + \frac{5!}{2!}N(2)N(3)^2N(4)N(5) + \frac{5!}{4!}N(3)^4N(5) + \frac{5!}{3!}N(4)^3N(2)N(3) + \frac{5!}{2!3!}N(3)^3N(4)^2 = 581\,400\,000,$$

$$A_{18}^{(25)} = \frac{5!}{3!}N(3)N(5)^3 + \frac{5!}{2!2!}N(4)^2N(5)^2 + \frac{5!}{2!2!}N(2)^2N(4)N(5)^2 + \frac{5!}{2!2!}N(2)N(3)^2N(5)^2 + \frac{5!}{2!}N(2)N(3)N(4)^2N(5) + \frac{5!}{3!}N(3)^3N(4)N(5) + \frac{5!}{4!}N(2)N(4)^4 + \frac{5!}{2!3!}N(3)^2N(4)^3 = 516\,100\,000,$$

$$A_{19}^{(25)} = \frac{5!}{3!}N(4)N(5)^3 + \frac{5!}{2!3!}N(2)^2N(5)^3 + \frac{5!}{2!}N(2)N(3)N(4)N(5)^2 + \frac{5!}{2!3!}N(3)^3N(5)^2 + \frac{5!}{3!}N(2)N(4)^3N(5) + \frac{5!}{2!2!}N(3)^2N(4)^2N(5) + \frac{5!}{4!}N(3)N(4)^4 = 381\,600\,000,$$

$$A_{20}^{(25)} = \frac{5!}{4!}N(5)^4 + \frac{5!}{3!}N(2)N(3)N(5)^3 + \frac{5!}{2!2!}N(2)N(4)^2N(5)^2 + \frac{5!}{2!2!}N(3)^2N(4)N(5)^2 + \frac{5!}{3!}N(3)N(4)^3N(5) + N(4)^5 = 230\,350\,000,$$

$$A_{21}^{(25)} = \frac{5!}{3!}N(2)N(4)N(5)^3 + \frac{5!}{2!3!}N(3)^2N(5)^3 + \frac{5!}{2!2!}N(3)N(4)^2N(5)^2 + \frac{5!}{4!}N(4)^4N(5) = 110\,500\,000,$$

$$A_{22}^{(25)} = \frac{5!}{4!}N(2)N(5)^4 + \frac{5!}{3!}N(3)N(4)N(5)^3 + \frac{5!}{2!3!}N(4)^3N(5)^2 = 40\,000\,000,$$

$$A_{23}^{(25)} = \frac{5!}{4!}N(3)N(5)^4 + \frac{5!}{2!3!}N(4)^2N(5)^3 = 10\,000\,000,$$

$$A_{24}^{(25)} = \frac{5!}{4!}N(4)N(5)^4 = 1\,500\,000,$$

$$A_{25}^{(25)} = N(5)^5 = 100\,000.$$

4.2. Example 2

Let $p = 3$, r be a positive integer and $q = 7$. As the multiplicative order of 7 modulo 3^m is 3^{m-1}, which is a power of 3, we apply Theorem 3 to compute the weight distribution of 7-ary irreducible cyclic code $\mathcal{M}_1^{(3^r)}$. Note that $d = m - 1$ in this case. By Theorem 3, we see that the only possible non-zero weight in $\mathcal{M}_1^{(3)}$ is 3, which is attained by all its 6 non-zero codewords. If $r \geqslant 2$, the weight distribution of $\mathcal{M}_1^{(3^r)}$ is given by

$$A_i^{(3^r)} = \begin{cases} 0 & \text{if 3 does not divide } i, \\ \binom{3^{r-1}}{j}(q-1)^j & \text{if } i = 3j,\ 0 \leqslant j \leqslant 3^{r-1}. \end{cases}$$

4.3. Example 3

Let $p = 7$, $r = 2$ and $q = 3$. The multiplicative order of 3 modulo 49 is $\phi(49)$. Working as in Example 1, we obtain the weight distribution of the ternary code $\mathcal{M}_1^{(49)}$, which is given by Table 1.

4.4. Example 4

Let $p = 3$, $r = 2$ and $q = 2$. Here the multiplicative order of 2 modulo 3^m is $2 \cdot 3^{m-1}$. Therefore in order to compute the weight distribution of the binary irreducible cyclic code $\mathcal{M}_1^{(9)}$, we apply

Table 1
Weight distribution of $\mathcal{M}_1^{(49)}$.

i	$A_i^{(49)}$	i	$A_i^{(49)}$
0	1	25	969 910 063 683 593 760
1	0	26	1 790 654 838 803 056 800
2	294	27	3 050 493 737 697 029 120
3	490	28	4 793 122 232 822 019 600
4	38 514	29	6 941 199 803 483 517 600
5	124 950	30	9 254 706 084 292 721 024
6	3 067 498	31	11 344 812 587 392 058 880
7	13 953 534	32	12 763 686 491 853 906 336
8	171 229 716	33	13 151 206 405 405 332 320
9	908 996 648	34	12 377 857 222 547 767 776
10	7 200 970 812	35	10 609 256 118 069 155 232
11	38 882 658 360	36	8 251 031 985 292 980 352
12	232 647 415 364	37	5 797 561 455 260 475 264
13	1 163 267 772 576	38	3 661 514 559 604 696 704
14	5 704 586 281 212	39	2 065 636 048 964 212 480
15	25 130 378 918 120	40	1 033 039 033 643 991 360
16	104 131 710 308 136	41	453 660 994 824 554 496
17	395 598 403 779 768	42	172 850 452 904 003 392
18	1 393 909 113 195 312	43	56 252 464 760 236 416
19	4 522 134 086 000 496	44	15 312 974 670 266 112
20	13 545 368 019 542 520	45	3 386 935 883 520 000
21	37 393 735 711 741 080	46	583 349 898 055 680
22	95 230 303 830 994 752	47	73 157 815 084 032
23	223 690 731 469 716 672	48	5 917 176 220 032
24	484 865 793 817 864 368	49	230 539 333 248

Theorem 4. Note that $u = 1$ in this case. By Theorem 4, the weight distribution $A_w^{(9)}$, $0 \leqslant w \leqslant 9$, of the binary code $\mathcal{M}_1^{(9)}$ is given by

$$A_w^{(9)} = \sum n(w_1)n(w_2)n(w_3),$$

where the summation runs over all tuples (w_1, w_2, w_3) of integers w_i's satisfying $w_1 + w_2 + w_3 = w$, $w_i \geqslant 0$ for each i, and

$$n(w_i) = \begin{cases} 1 & \text{if } w_i = 0, \\ 3 & \text{if } w_i = 2, \\ 0 & \text{otherwise.} \end{cases}$$

After a little calculation, we see that $A_0^{(9)} = 1$, $A_2^{(9)} = \frac{3!}{2!}n(2) = 9$, $A_4^{(9)} = \frac{3!}{2!}n(2)^2 = 27$, $A_6^{(9)} = n(2)^3 = 27$ and $A_1^{(9)} = A_3^{(9)} = A_5^{(9)} = A_7^{(9)} = A_8^{(9)} = A_9^{(9)} = 0$. (Note that as the multiplicative order of 2 modulo 3^m is $\phi(3^m)$, we can also compute the weight distribution of $\mathcal{M}_1^{(9)}$ using Theorem 2.)

4.5. Example 5

Let $p = 5$, $r = 2$ and $q = 4$. The multiplicative order of 4 modulo 5^m is $2 \cdot 5^{m-1}$. To compute the weight distribution of the quaternary irreducible cyclic code $\mathcal{M}_1^{(25)}$, we apply Theorem 4. Note that $u = 1$ in this case. By Theorem 4, the weight distribution $A_w^{(25)}$, $0 \leqslant w \leqslant 25$, of the quaternary code $\mathcal{M}_1^{(25)}$ is given by

$$A_w^{(25)} = \sum n(w_1)n(w_2)n(w_3)n(w_4)n(w_5),$$

where the summation runs over all tuples $(w_1, w_2, w_3, w_4, w_5)$ of integers w_i's satisfying $w_1 + w_2 + w_3 + w_4 + w_5 = w$, $w_i \geqslant 0$ for each i, and

$$n(w_i) = \begin{cases} 1 & \text{if } w_i = 0, \\ 15 & \text{if } w_i = 4, \\ 0 & \text{otherwise.} \end{cases}$$

This gives $A_0^{(25)} = 1$, $A_4^{(25)} = \frac{5!}{4!}n(4) = 75$, $A_8^{(25)} = \frac{5!}{2!3!}n(4)^2 = 2250$, $A_{12}^{(25)} = \frac{5!}{2!3!}n(4)^3 = 33\,750$, $A_{16}^{(25)} = \frac{5!}{4!}n(4)^4 = 253\,125$, $A_{20}^{(25)} = n(4)^5 = 759\,375$, and the remaining $A_w^{(25)}$'s are equal to zero.

Acknowledgments

The authors are grateful to the anonymous referees for their comments and suggestions which helped to write the paper in the present form.

References

[1] L.D. Baumert, R.J. McEliece, Weights of irreducible cyclic codes, Inform. Control 20 (1972) 158–175.
[2] C. Ding, The weight distributions of some irreducible cyclic codes, IEEE Trans. Inform. Theory 55 (3) (2009) 955–960.
[3] C. Ding, T. Helleseth, H. Niederreiter, C. Xing, The minimum distance of the duals of binary irreducible cyclic codes, IEEE Trans. Inform. Theory 48 (10) (2002) 2679–2689.
[4] R.W. Fitzgerald, J.L. Yucas, Sums of Gauss sums and weights of irreducible codes, Finite Fields Appl. 11 (1) (2005) 89–110.
[5] T. Helleseth, T. Kløve, J. Mykkeltveit, The weight distribution of irreducible cyclic codes with block length $\frac{n_1(q^\ell-1)}{N}$, Discrete Math. 18 (2) (1977) 179–211.
[6] T. Kløve, The weight distribution for a class of irreducible cyclic codes, Discrete Math. 20 (1) (1977/1978) 87–90.
[7] F.J. MacWilliams, J. Seery, The weight distributions of some minimal cyclic codes, IEEE Trans. Inform. Theory 27 (6) (1981) 796–806.
[8] F.J. MacWilliams, N.J.A. Sloane, Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[9] M.J. Moisio, K.O. Väänänen, Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes, IEEE Trans. Inform. Theory 45 (4) (1999) 1244–1249.
[10] R. Segal, R.L. Ward, Weight distributions of some irreducible cyclic codes, Math. Comp. 46 (173) (1986) 341–354.
[11] A. Sharma, G.K. Bakshi, V.C. Dumir, M. Raka, Cyclotomic numbers and primitive idempotents in the ring $\mathrm{GF}(q)[x]/(x^{p^n} - 1)$, Finite Fields Appl. 10 (4) (2004) 653–673.
[12] A. Sharma, G.K. Bakshi, M. Raka, The weight distributions of irreducible cyclic codes of length 2^m, Finite Fields Appl. 13 (4) (2007) 1086–1095.
[13] M. van der Vlugt, Hasse–Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes, J. Number Theory 55 (2) (1995) 145–159.
[14] J.P. Zanotti, Weight behavior of irreducible cyclic BWD-codes, Finite Fields Appl. 2 (2) (1996) 192–203.