J. Algebra Comb. Discrete Appl.
6(1) • 1–11

Received: 21 August 2017
Accepted: 2 December 2018

Journal of Algebra Combinatorics Discrete Structures and Applications

Weight distribution of a class of cyclic codes of length 2^n

Research Article

Manjit Singh, **Sudhir Batra**

Abstract: Let $\mathbb{F}_q$ be a finite field with q elements and n be a positive integer. In this paper, we determine the weight distribution of a class cyclic codes of length 2^n over $\mathbb{F}_q$ whose parity check polynomials are either binomials or trinomials with 2^l zeros over $\mathbb{F}_q$, where integer $l \geq 1$. In addition, constant weight and two-weight linear codes are constructed when $q \equiv 3 \pmod 4$.

2010 MSC: 12E05, 12E20, 94B05, 11T71

Keywords: Linear codes, Reversible codes, Weight distributions, Constant weight codes

1. Introduction

A linear $[m,k]_q$ code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^m$. Let λ be a nonzero element in $\mathbb{F}_q$. A linear code C of length m over $\mathbb{F}_q$ is called a λ-constacyclic code if

$$(c_1, c_2, \ldots, c_{m-1}, c_0\lambda) \in C, \ \forall \ (c_0, c_1, c_2, \ldots, c_{m-1}) \in C.$$

A λ-constacyclic code of length m over $\mathbb{F}_q$ is called a simple-root code if $\gcd(m,q) = 1$; otherwise it is called repeated-root code. If we identify a vector $(a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_q^m$ with a polynomial $a_0x^{m-1} + a_1x^{m-2} + \cdots + a_{m-1}$ modulo $(x^m - \lambda)$ in $\mathbb{F}_q[x]$, then a simple-root λ-constacyclic code C can be interpreted as an ideal of the quotient ring $\mathcal{R} = \mathbb{F}_q[x]/\langle x^m - \lambda\rangle$. It is well known that each ideal in $\mathcal{R}$ is of the form $\langle g(x)\rangle$, where $g(x)$ is a monic divisor of $x^m - \lambda$ in $\mathbb{F}_q[x]$. The polynomial $g(x)$ is known as the generator polynomial of the code C and the corresponding factor $h(x) = (x^m - \lambda)/g(x)$ of $x^m - \lambda$ is referred to as the parity check polynomial of the code C. If $h(x)$ is a product of t monic irreducible factors over $\mathbb{F}_q$, then we say C with t zeros over $\mathbb{F}_q$. A constacyclic code is called an irreducible code over $\mathbb{F}_q$ if $t = 1$,

Manjit Singh (Corresponding Author), Sudhir Batra; Department of Mathematics, Deenbandhu Chhotu Ram University of Science and Technology, Murthal-131039, Sonepat, India (email: manjitsingh.math@gmail.com, batrasudhir@rediffmail.com).

http://dx.doi.org/10.13069/jacodesmath.505364

and a reducible code over $\mathbb{F}_q$ if $t \geq 2$. A $\lambda-$constacyclic code C is called cyclic if $\lambda = 1$ and negacyclic if $\lambda = -1$.

Let A_i be the number of codewords of a linear code C of length m over $\mathbb{F}_q$ with Hamming weight i, where $0 \leq i \leq m$. Note that $A_0 = 1$ and $A_i = 0$ for all $1 \leq i < d$, where d is the minimum Hamming distance of the code. The sequence $(1, A_1, A_2, \ldots, A_m)$ is called the weight distribution of the code C. Cyclic codes are the most important class of linear codes for a wide variety of applications. In the last few decades, the weight distribution of irreducible cyclic codes have been studied extensively (see [3, 9, 12]). However, not much is known about the weight distribution of reducible codes except in very specific cases.

Vega [11] presented a new family of two-weight reducible cyclic codes that can be constructed as the direct sum of two one-weight irreducible codes. For any $q = p^m$, where p is an odd prime, $m \geq 3$, $k \geq 1$ and $\gcd(k, m) = 1$, Feng and Luo [4] obtained weight distribution of cyclic codes C_1 of dimension $2m$ and C_2 of dimension $3m$ over $\mathbb{F}_p$ of length $n = q - 1$ with parity-check polynomial $h_2(x)h_3(x)$ and $h(x) = h_1(x)h_2(x)h_3(x)$ respectively, where $h_1(x)$, $h_2(x)$ and $h_3(x)$ are the minimal polynomials of π^{-1}, π^{-2} and $\pi^{-(p^k+1)}$ over $\mathbb{F}_p$, respectively, for a primitive element π of $\mathbb{F}_q$ with $\deg h_i(x) = m$ for $i = 1, 2, 3$. For doing this, they computed the value distribution of multi-sets of exponential sums using quadratic form over $\mathbb{F}_p$.

Yang, Xiong, Ding and Luo [14] proposed a class of cyclic codes C of length n over $\mathbb{F}_q$ with parity-check polynomial $h(x) = h_{a_1}(x)h_{a_2}(x) \cdots h_{a_t}(x)$, where $h_{a_i}(x)$ is the minimal polynomial of γ^{-a_i} over $\mathbb{F}_q$, $\deg h_{a_i}(x) = m$, $r = q^m$, γ is a generator of $\mathbb{F}_r^*$ and $n = (r-1)/\delta$, $\delta = \gcd(r-1, a_1, a_2, \ldots, a_t)$ and integer $e \geq t \geq 2$ with $e|(q-1)$. They remarked that it may be very difficult to find the weight distribution of this class of codes if the integers a_i are not chosen in the right way or the Gaussian periods have many different values. The values of the Gaussian periods are in general very hard to determine. Hence they obtained the weight distribution of this class of codes when $t = e$ and the Gaussian periods of order N are known, including the cases that $N = 1, 2, 3$, semi-primitive case and a special index 2 case.

Recently, assuming $\ell^v||(q-1)$, where ℓ is a prime and v is an integer, and $q \equiv 1 \pmod 4$ if $\ell = 2$, Zhu, Yue and Hu [15] have applied a combinatorial method to obtain not only the weight distribution of all cyclic codes of length ℓ^m with two zeros over $\mathbb{F}_q$, but also the weight distribution of a special cyclic code of length ℓ^m with three zeros over $\mathbb{F}_q$.

In this paper, we present a class of cyclic codes of length 2^n with 2^l zeros over $\mathbb{F}_q$, where q is an odd prime power and $n > l \geq 1$. Further, using the explicit forms of codewords, the weight distribution of these codes is determined explicitly. We make use of Diophantine equation and its solutions to obtain the explicit form of weights of codewords and the number of codewords of the given weight of these cyclic codes. It is observed that, when $q \equiv 3 \pmod 4$, the problem of finding the weight distribution is transferred into a problem of determining the weight distribution of a two-weight negacyclic code, which turns out to be associated with counting the number of constant weight linear codes. These codes are known for applicability of various association schemes and traceability schemes, which justify their practical applications in engineering perspective (see [1, 2, 5–7]). In particular, these codes are of special interest in authentication codes [2] and traceability schemes [6].

The paper is organized as follows: The necessary notations and some auxiliary results are provided in Section 2. In Section 3, we describe a class of negacyclic and hence cyclic codes of length 2^n with 2^l zeros over $\mathbb{F}_q$. It is observed that these reducible codes are reversible when $q \equiv 3 \pmod 4$. In Section 4, constant weight linear codes and two-weight negacyclic codes are constructed and the weight distribution of cyclic codes of length 2^n with 2^l zeros over $\mathbb{F}_q$ are determined. In the end of this section, we give an example illustrating the results. In Section 5, we conclude the paper.

2. Preliminaries

The paper follows the standard notation of finite fields. The multiplicative group of $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^*$. It is well known that $\mathbb{F}_q^*$ is a cyclic group of order $q - 1$. For any integer $m \geq 2$, let $\nu_2(m)$ denote the highest power of 2 dividing m. Let q be an odd prime power, $s = \nu_2(q-1)$ and $u = \nu_2(q^2-1)$. Then $u - s = \nu_2(q+1) \geq 1$. Readily note that (i) $u - s = 1$ if and only if $q \equiv 1 \pmod 4$, and (ii) $s = 1$ if and only if $q \equiv 3 \pmod 4$.

Let α_k be a primitive 2^kth root of unity in $\mathbb{F}_q^*$. Also, let β_k be a primitive 2^kth root of unity in $\mathbb{F}_{q^2}^*$ when $s+1 \leq k \leq u$. Notice that $\beta_{s+1}^2 = \alpha_s$. Since $\beta_k \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, the minimal polynomial of β_k over $\mathbb{F}_q$ is $x^2 - (\beta_k + \beta_k^q)x + \beta_k^{q+1}$.

If $f(x)$ is an irreducible polynomial over $\mathbb{F}_q$ and $f(0) \neq 0$, then, for any integer $k \geq 2$, the following result is useful to check the irreducibility of the polynomial of the type of $f(x^k)$ over $\mathbb{F}_q$.

Lemma 2.1. *[13, Theorem 10.15] Let $f(x)$ be any irreducible polynomial over $\mathbb{F}_q$ of degree $l \geq 1$. Suppose that $f(0) \neq 0$ and $f(x)$ is of order e which is equal to the order of any root of $f(x)$. Let k be a positive integer, then the polynomial $f(x^k)$ is irreducible over $\mathbb{F}_q$ of order ke if and only if the following three conditions are satisfied:*

(i) Every prime divisor of k divides e;

(ii) $\gcd(k, \frac{q^l-1}{e}) = 1$;

(iii) If $4|k$, then $4|(q^l-1)$.

We end this section with the following lemma.

Lemma 2.2. *Let q be an odd prime power and $r \geq 1$ be an integer. Then*

(i) For any $2 \leq k \leq s$, $x^{2^r} - \alpha_k$ is a product of 2^l monic irreducible binomial factors of degree 2^{r-l} over $\mathbb{F}_q$, where $l = \min\{r, s-k\}$.

(ii) For any $s+2 \leq k \leq u$, $x^{2^{r+1}} - (\beta_k + \beta_k^q)x^{2^r} + \beta_k^{q+1}$ is a product of 2^l monic irreducible trinomial factors of degree 2^{r-l} over $\mathbb{F}_q$, where $l = \min\{r, u-k\}$.

Proof. (i) For any fixed $2 \leq k \leq s$, let $l = \min\{r, s-k\}$. Then $2^{k+l}|(q-1)$, $\alpha_{k+l} \in \mathbb{F}_q^*$ such that $\alpha_k = \alpha_{k+l}^{2^l}$. The set $S_k = \{\alpha_{k+l}^{2^k i+1} : 1 \leq i \leq 2^l\}$ contains 2^l distinct elements of order 2^{k+l} in $\mathbb{F}_q^*$. For any $\alpha \in S_k$, $x^{2^{r-l}} - \alpha$ is a factor of $x^{2^r} - \alpha_k$. Since $\gcd(2^{r-l}, \frac{q-1}{2^{k+l}}) = 1$, by Lemma 2.1, $x^{2^{r-l}} - \alpha$ is irreducible over $\mathbb{F}_q$ for every $\alpha \in S_k$.
(ii) For any fixed $s+2 \leq k \leq u$, let $l = \min\{r, u-k\}$. Then $2^{k+l}|(q^2-1)$, $\beta_{k+l} \in \mathbb{F}_{q^2}^*$ such that $\beta_k = \beta_{k+l}^{2^l}$. The set $T_k = \{\beta_{k+l}^{2^k i+1} : 1 \leq i \leq 2^l\}$ contains 2^l distinct elements of order 2^{k+l} in $\mathbb{F}_{q^2}^*$. In view of the part (i), $x^{2^{r-l}} - \eta$ is an irreducible factor of $x^{2^r} - \beta_k$ over $\mathbb{F}_{q^2}$ for every $\eta \in T_k$. For any $\eta \in T_k$, we notice that $\beta_k = \eta^{2^l}$ and $\beta_k^q = (\eta^q)^{2^l}$. Further, $x^{2^{r-l}} - \eta$ is a factor of $x^{2^r} - \beta_k$ over $\mathbb{F}_{q^2}$ if and only if $x^{2^{r-l}} - \eta^q$ is a factor of $x^{2^r} - \beta_k^q$ over $\mathbb{F}_{q^2}$. This bijection of factors of $x^{2^r} - \beta_k$ and $x^{2^r} - \beta_k^q$ over $\mathbb{F}_{q^2}$ generates a unique factor $(x^{2^{r-l}} - \eta)(x^{2^{r-l}} - \eta^q) = x^{2^{r-l+1}} - (\eta + \eta^q)x^{2^{r-l}} + \eta^{q+1} \in \mathbb{F}_q[x]$ of $(x^{2^r} - \beta_k)(x^{2^r} - \beta_k^q) = x^{2^{r+1}} - (\beta_k + \beta_k^q)x^{2^r} + \beta_k^{q+1} \in \mathbb{F}_q[x]$ for every $\eta \in T_k$. Since $\gcd(2^{r-l}, \frac{q^2-1}{2^{k+l}}) = 1$, hence by Lemma 2.1, $x^{2^{r-l+1}} - (\eta + \eta^q)x^{2^{r-l}} + \eta^{q+1}$ is irreducible over $\mathbb{F}_q$ for every $\eta \in T_k$. □

3. Negacyclic and cyclic codes

For any $1 \leq k \leq s$ and integer $r \geq 0$, we define a negacyclic $[2^{k+r-1}, 2^r]_q$ code and a cyclic $[2^{k+r}, 2^r]_q$ code over $\mathbb{F}_q$ by $N_r^{(k)} = \langle N_r^{(k)}(x) \rangle$ and $C_r^{(k)} = \langle C_r^{(k)}(x) \rangle$, respectively, with the generator polynomials

$$N_r^{(k)}(x) = \frac{x^{2^{r+k-1}} + 1}{x^{2^r} - \alpha_k} \text{ and } C_r^{(k)}(x) = \frac{x^{2^{r+k}} - 1}{x^{2^r} - \alpha_k}.$$

Note that $N_r^{(1)}$ is the whole space $\mathbb{F}_q^{2^r}$. By Lemma 2.2, for each $2 \le k \le s$, $N_r^{(k)}$ and $C_r^{(k)}$ are the codes with 2^l zeros over $\mathbb{F}_q$, where $l = \min\{r, s-k\}$.

Lemma 3.1. *For any $1 \le k \le s$ and integer $r \ge 0$,*

$$N_r^{(k)} = \{(\mathbf{b}, \mathbf{b}\alpha_k, \ldots, \mathbf{b}\alpha_k^{2^{k-1}-1}) : \mathbf{b} \in \mathbb{F}_q^{2^r}\}$$

and

$$C_r^{(k)} = \{(\mathbf{b}, \mathbf{b}\alpha_k, \ldots, \mathbf{b}\alpha_k^{2^{k-1}-1}, -\mathbf{b}, -\mathbf{b}\alpha_k, \ldots, -\mathbf{b}\alpha_k^{2^{k-1}-1}) : \mathbf{b} \in \mathbb{F}_q^{2^r}\}.$$

Proof. For $1 \le k \le s$, observe that $\alpha_k^{2^{k-1}} = -1$. It follows that

$$x^{2^{k-1}} + 1 = (x - \alpha_k) \sum_{i=0}^{2^{k-1}-1} \alpha_k^i x^{2^{k-1}-i-1}$$

and for any $r \ge 0$,

$$x^{2^{r+k-1}} + 1 = (x^{2^r} - \alpha_k) \sum_{i=0}^{2^{k-1}-1} \alpha_k^i x^{2^r(2^{k-1}-i-1)} = (x^{2^r} - \alpha_k) N_r^{(k)}(x).$$

Therefore the generator polynomial of $N_r^{(k)}$ is

$$N_r^{(k)}(x) = \sum_{i=0}^{2^{k-1}-1} \alpha_k^i x^{2^r(2^{k-1}-i-1)}.$$

Let $\mathbf{b} = (b_0, b_1, \ldots, b_{2^r-1}) \in \mathbb{F}_q^{2^r}$ be a message word and the corresponding message polynomial be $\mathbf{b}(x) = \sum_{j=0}^{2^r-1} b_j x^{2^r-j-1} \in \mathbb{F}_q[x]$. Then the code polynomial of $N_r^{(k)}$ is given by:

$$\mathbf{b}(x)\left(\frac{x^{2^{r+k-1}}+1}{x^{2^r}-\alpha_k}\right) = \sum_{i=0}^{2^{k-1}-1}\sum_{j=0}^{2^r-1} b_j \alpha_k^i x^{2^{r+k-1}-2^r i-j-1}.$$

The polynomial on the right hand side can be expressed as a vector of the form $(\mathbf{b}, \mathbf{b}\alpha_k, \ldots, \mathbf{b}\alpha_k^{2^{k-1}-1})$ by substituting $i = 0, 1, \ldots, 2^{k-1}-1$. Hence, we have

$$N_r^{(k)} = \{(\mathbf{b}, \mathbf{b}\alpha_k, \ldots, \mathbf{b}\alpha_k^{2^{k-1}-1})\}.$$

Since the generator polynomial of $C_r^{(k)}$ is

$$C_r^{(k)}(x) = N_r^{(k)}(x)\left(x^{2^{r+k-1}} - 1\right),$$

so we obtain $C_r^{(k)} = \{(c, -c) : c = (\mathbf{b}, \mathbf{b}\alpha_k, \ldots, \mathbf{b}\alpha_k^{2^{k-1}-1}) \in N_r^{(k)}\}$. □

Lemma 3.1 is valid for every odd q. Consider the case $q \equiv 3 \pmod 4$, i.e., $s = 1$, then we obtain the following trivial codes:

$$N_r^{(1)} = \mathbb{F}_q^{2^r} \text{ and } C_r^{(1)} = \{(c, -c) : c \in \mathbb{F}_q^{2^r}\}.$$

In the rest of this section, we assume $q \equiv 3 \pmod 4$. In order to define a class of cyclic codes with parity check polynomial of the type $x^{2^{r+1}} - (\beta_k + \beta_k^q)x^{2^r} + \beta_k^{q+1}$ with 2^l zeros, where $l = \min\{r, u-k\}$, we need a bit more notations of [10].

For any $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, let $\mathbb{T}(x) = x + x^q$ and $\mathbb{N}(x) = x^{q+1}$. It follows that the minimal polynomial of β_2 over $\mathbb{F}_q$ is x^2+1, and the minimal polynomial of β_k over $\mathbb{F}_q$ is $x^2 - \mathbb{T}(\beta_k)x + \mathbb{N}(\beta_k)$ for every $3 \le k \le u$. For every $1 \le i \le 2^{k-2}$ and $3 \le k \le u$, there are exactly 2^{k-2} elements of the form $\mathbb{T}(\beta_k^{2i-1})$ and $\mathbb{N}(\beta_k^{2i-1}) = \beta_k^{q+1} = \pm 1$. In order to avoid cumbersome notations, for a fixed k, we denote $\xi = \mathbb{T}(\beta_k)$, $\epsilon = \beta_k^{q+1}$. Note that $\xi = 0$ if $k = 2$; $\epsilon = 1$ for $2 \le k \le u-1$ and $\epsilon = -1$ for $k = u$. Further, for any integer $i \ge 0$ and $3 \le k \le u$, we define the followings:

(i) $\delta_i = \dfrac{\beta_k^i - \beta_k^{qi}}{\beta_k - \beta_k^q}$ with $\delta_0 = 0$, $\delta_1 = 1$ and $\delta_{2^{k-1}-i} = \epsilon^i \delta_i$ for every $0 \le i \le 2^{k-1}-1$. In view of [10, Lemma 3.1], $\delta_i = \xi\delta_{i-1} - \epsilon\delta_{i-2}$ for $2 \le i \le 2^{k-1}-1$, with $\delta_0 = 0$ and $\delta_1 = 1$.

(ii) $\gamma_i(a,b) = \delta_{i+1}a + \delta_i b$, where $a, b \in \mathbb{F}_q$.

Lemma 3.2. *Let $3 \le k \le u$ be a fixed integer and $a, b \in \mathbb{F}_q$. Then, the sequence $(\gamma_i(a,b))_{i\ge 0}$ satisfies the recursive relation*

$$\gamma_i(a,b) = \xi\gamma_{i-1}(a,b) - \epsilon\gamma_{i-2}(a,b), \textit{ for } i \ge 2$$

with $\gamma_0(a,b) = a$, $\gamma_1(a,b) = \xi a + \epsilon b$. For any given $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$, the sequence $\gamma_i = \gamma_i(a,b)$ contains 2^k terms satisfying $\gamma_{2^{k-1}+i} = -\gamma_i$ for every $0 \le i \le 2^{k-1}-1$.

Proof. By our definition $\gamma_i(a,b) = \delta_{i+1}a + \delta_i b$, where $0 \le i \le 2^{k-1}-1$ and $a, b \in \mathbb{F}_q$, it is immediate. □

For any fixed $3 \le k \le u$, observe that $x^2 - \xi x + \epsilon$ is a divisor of $x^{2^{k-1}}+1$, but not a divisor of $x^{2^{k-1}}-1$. Let $\mathsf{N}_k(x) = \dfrac{x^{2^{k-1}}+1}{x^2 - \xi x + \epsilon}$. (If $k = 2$, then $\xi = 0$, $\epsilon = 1$ and hence $\mathsf{N}_k(x) = 1$.) Further, for any integer $r \ge 0$, $x^{2^{r+1}} - \xi x^{2^r} + \epsilon$ is a divisor of $x^{2^{r+k-1}}+1$. Let $\mathsf{N}_{r,k}(x) = \dfrac{x^{2^{r+k-1}}+1}{x^{2^{r+1}} - \xi x^{2^r} + \epsilon}$ and $\mathsf{C}_{r,k}(x) = \mathsf{N}_{r,k}(x)(x^{2^{r+k-1}}-1)$. Then $\mathsf{N}_{r,k}(x) = \mathsf{N}_k(x^{2^r})$. For any integer $r \ge 0$, we define a negacyclic $[2^{r+k-1}, 2^{r+1}]_q$ code and a cyclic $[2^{r+k}, 2^{r+1}]_q$ code over $\mathbb{F}_q$ by $\mathsf{N}_{r,k} = \langle \mathsf{N}_{r,k}(x)\rangle$, $\mathsf{C}_{r,k} = \langle \mathsf{C}_{r,k}(x)\rangle$ with $\mathsf{N}_k = \mathsf{N}_{0,k}$, a 2-dimensional negacyclic code of length 2^{k-1} over $\mathbb{F}_q$. For $3 \le k \le u$, by Lemma 2.2, $\mathsf{N}_{r,k}$ and $\mathsf{C}_{r,k}$ are the codes with 2^l zeros over $\mathbb{F}_q$.

Remark 3.3. *Let $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m \in \mathbb{F}_q[x]$ be a polynomial of degree m. The reciprocal polynomial of $f(x)$ is the polynomial $f^*(x) = x^m f(x^{-1}) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$. Further, $f(x)$ is said to be reversible provided $f^*(x) = f(x)$. A reversible code is a code such that reversing the order of the components of a codeword gives always a codeword. Massey [8] showed that reversible cyclic codes are those which have self-reciprocal generator polynomials. For any integer $r \ge 0$, the polynomial $x^{2^{r+1}} - \xi x^{2^r} + 1$ is reversible. By Lemma 2.2, $x^{2^{r+1}} - \xi x^{2^r} + 1$ is reducible over $\mathbb{F}_q$ and hence $\mathsf{C}_{r,k}$ is a reducible and reversible cyclic code. Cyclic codes can be decoded by sequential circuits, and hence the invariance of these codes under the reversing transformation is of special interest [8].*

Theorem 3.4. *For any fixed k in $3 \le k \le u$, the negacyclic $[2^{k-1}, 2]_q$-code is given by $\mathsf{N}_k = \{(\gamma_0(a,b), \gamma_1(a,b), \ldots, \gamma_{2^{k-1}-1}(a,b) : a, b \in \mathbb{F}_q\}$. Further, for any integer $r \ge 0$, the negacyclic $[2^{r+k-1}, 2^{r+1}]_q$ code $\mathsf{N}_{r,k}$ is*

$$\mathsf{N}_{r,k} = \underbrace{\mathsf{N}_k \times \mathsf{N}_k \times \cdots \times \mathsf{N}_k}_{2^r \, copies}.$$

Proof. For any fixed $3 \leq k \leq u$, observe that

$$\begin{aligned} \mathsf{N}_k(x) &= \frac{x^{2^{k-1}}+1}{(x-\beta_k)(x-\beta_k^q)} = \sum_{i=1}^{2^{k-1}-1} \left(\frac{\beta_k^i - \beta_k^{iq}}{\beta_k - \beta_k^q} \right) x^{2^{k-1}-i-1} \\ &= \sum_{i=1}^{2^{k-1}-1} \delta_i x^{2^{k-1}-i-1}. \end{aligned}$$

The code polynomial of N_k is

$$\begin{aligned} (ax+b)\mathsf{N}_k(x) &= \sum_{i=1}^{2^{k-1}-1} \delta_i (ax+b) x^{2^{k-1}-i-1} \\ &= \sum_{i=0}^{2^{k-1}-1} \left(a\delta_{i+1} + b\delta_i\right) x^{2^{k-1}-i-1}. \end{aligned}$$

In view of Lemma 3.2, we obtain the desired form of N_k.

Now, for any integer $r \geq 0$, we have

$$\mathsf{N}_{r,k}(x) = \mathsf{N}_k(x^{2^r}) = \sum_{i=1}^{2^{k-1}-1} \delta_i x^{2^r(2^{k-1}-i-1)}.$$

Let $\mathbf{a}(x) = \sum_{j=0}^{2^{r+1}-1} a_j x^{2^{r+1}-j-1}$ be the polynomial representation of the vector $\mathbf{a} = (a_0, a_1, \dots, a_{2^{r+1}-1}) \in \mathbb{F}_q^{2^{r+1}}$. If we denote $b_j = a_{j+2^r}$ for $0 \leq j \leq 2^r - 1$, then $\mathbf{a} = (a_0, a_1, \dots, a_{2^r-1}, b_0, b_1, \dots, b_{2^r-1})$ and

$$\mathbf{a}(x) = \sum_{j=0}^{2^r-1} (a_j x^{2^r} + b_j) x^{2^r-j-1}.$$

The code polynomial of $\mathsf{N}_{r,k}$ is

$$\begin{aligned} \mathbf{a}(x)\mathsf{N}_{r,k}(x) &= \sum_{j=0}^{2^r-1} \sum_{i=1}^{2^{k-1}-1} \delta_i (a_j x^{2^r} + b_j) x^{2^r(2^{k-1}-i)-j-1} \\ &= \sum_{j=0}^{2^r-1} \left(\sum_{i=0}^{2^{k-1}-2} a_j \delta_{i+1} x^{2^r(2^{k-1}-i)-j-1} + \sum_{i=1}^{2^{k-1}-1} b_j \delta_i x^{2^r(2^{k-1}-i)-j-1} \right) \\ &= \sum_{j=0}^{2^r-1} \sum_{i=0}^{2^{k-1}-1} \left(a_j \delta_{i+1} + b_j \delta_i\right) x^{2^{r+k-1}-2^r i-j-1}. \end{aligned}$$

Let $\gamma_{i,j} = \gamma_i(a_j, b_j) = a_j\delta_{i+1} + b_j\delta_i$, where $0 \leq i \leq 2^{k-1} - 1$ and $0 \leq j \leq 2^r - 1$. Note that any codeword in N_k is of the form $(c_0, c_1, \dots, c_{2^{k-1}-1})$ with $c_i = \gamma_i(a, b)$ for $0 \leq i \leq 2^{k-1} - 1$. Similarly, let us denote $c_{2^{k-1}j+i} = \gamma_{i,j} = \gamma_i(a_j, b_j)$ for $0 \leq j \leq 2^r - 1$. Then any codeword of $\mathsf{N}_{r,k}$ can be expressed as $(c_0, c_1, \dots, c_{2^{r+k-1}-1})$ in which for every $0 \leq i \leq 2^{k-1} - 1$, there exists $0 \leq l \leq 2^{k-1} - 1$ such that $c_{2^{k-1}j+i} = c_l$. Let $\mathcal{E}_j = \{(c_{2^{k-1}j+0}, c_{2^{k-1}j+1}, \dots, c_{2^{k-1}j+2^{k-1}-1})\}$. Then $\mathcal{E}_j$ is a block subcode of $\mathsf{N}_{r,k}$ such that $\mathcal{E}_j = \mathsf{N}_k$. Since $\mathsf{N}_{r,k} = \{(\bar{c}_0, \bar{c}_1, \dots, \bar{c}_{2^r-1}) : \bar{c}_j \in \mathcal{E}_j\}$, we have

$$\mathsf{N}_{r,k} = \{(\bar{c}_0, \bar{c}_1, \dots, \bar{c}_{2^r-1}) : \bar{c}_j \in \mathsf{N}_k \text{ for } 0 \leq j \leq 2^r - 1\}.$$

This completes the proof. □

4. Weight distributions

In this section, we determine the weight distribution of codes defined in the last section. The following theorem gives the weight distribution of $C_r^{(k)}$ for $2 \le k \le s$.

Theorem 4.1. *Let $q \equiv 1 \pmod 4$ and $2 \le k \le s$. Then, for any integer $r \ge 0$, the weight distribution of $C_r^{(k)}$ is given by:*

$$A_{2^k j} = \binom{2^r}{j}(q-1)^j \ \ ;where\ \ 0 \le j \le 2^r.$$

Proof. Let $\mathbf{b} = (b_0, b_1, \ldots, b_{2^r-1})$ be a message word. Further, let j denote the number of nonzero symbols in $\mathbf{b}$. Since each nonzero symbol has $q-1$ choices and there are exactly $\binom{2^r}{j}$ message word with j nonzero symbols, the number of message word having j nonzero symbols is $\binom{2^r}{j}(q-1)^j$, where $0 \le j \le 2^r$.

By Lemma 3.1, any codeword of $C_r^{(k)}$ is of the type $(c, -c)$, where $c \in N_r^{(k)}$ such that

$$c = (\mathbf{b}, \mathbf{b}\alpha_k, \ldots, \mathbf{b}\alpha_k^{2^{k-1}-1}) \text{ with } \mathbf{b} = (b_0, b_1, \ldots, b_{2^r-1}).$$

Using the form of codeword c, the weight of c is $2^{k-1}j$ and the number of codewords of weight $2^{k-1}j$ are also $\binom{2^r}{j}(q-1)^j$. It follows that, the weight of any codeword of $C_r^{(k)}$ is $2^k j$ and the number of codewords of weight $2^k j$ is same as the number of codewords of weight $2^{k-1}j$. Therefore $A_{2^k j} = \binom{2^r}{j}(q-1)^j$. □

Remark 4.2. *For any integer $r \ge 0$, $C_r^{(1)} = \{(c, -c) : c = (b_0, b_1, \ldots, b_{2^r-1})\}$, the weight distribution of $C_1^{(1)}$ is $A_{2j} = \binom{2^r}{j}(q-1)^j$.*

In rest of the section, we determine the weight distribution of cyclic codes $\mathsf{C}_{r,k}$ for $3 \le k \le u$ and integer $r \ge 0$. At first, we determine the weight distribution of $\mathsf{N}_{r,k}$. In view of Theorem 3.4, the weight distribution of $\mathsf{N}_{r,k}$ can be derived from the weight distribution of N_k. Fundamentally, we need to compute the weight distribution of N_k. In this connection, some additional conventions are explained here.

Let $\Theta : \mathbb{F}_q^2 \to \mathsf{N}_k$ be a mapping, defined as

$$\Theta((a,b)) = (c_0, c_1, \ldots, c_{2^{k-1}-1}),$$

where $c_i = \gamma_i(a,b)$ for any $a, b \in \mathbb{F}_q$. Then Θ is an $\mathbb{F}_q$-isomorphism. Further, for any fixed $0 \le i \le 2^{k-1}-1$, let $\mathbb{K}_i = \{(a,b) \in \mathbb{F}_q^2 : c_i = 0\}$. Observe that $\mathbb{K}_i$ is an 1-dimensional subspace of $\mathbb{F}_q^2$ with $\mathbb{K}_0 = \{(0,b) : b \in \mathbb{F}_q\} = \mathbb{F}_q$ and $\mathbb{K}_{2^{k-1}-1} = \{(a,0) : a \in \mathbb{F}_q\} = \mathbb{F}_q$. Denote $\mathbb{N}_i = \Theta(\mathbb{K}_i)$, a copy of $\mathbb{K}_i$ in N_k. Obviously, $\mathbb{N}_i$ is also an 1-dimensional subspace of N_k.

A code C with the same Hamming distance between every pair of its codewords is called an equidistant code. If all the codewords of a code C carry the same weight, then C is called constant weight code. A code C with both of these properties is known as equidistant constant weight code. A linear constant weight code is always an equidistant code. The following result presents a class of constant weight codes, which are applied in many areas [2, 5, 6].

Lemma 4.3. *For each $0 \le i \le 2^{k-1}-1$ and $3 \le k \le u$, $\mathbb{N}_i$ is a constant weight linear code such that $\mathbb{N}_0 = \{(0, \delta_1 a, \delta_2 a, \ldots, \delta_{2^{k-1}-1}a) : a \in \mathbb{F}_q\}$, $\mathbb{N}_{2^{k-1}-1} = \{(\delta_1 a, \delta_2 a, \ldots, \delta_{2^{k-1}-1}a, 0) : a \in \mathbb{F}_q\}$ and for any $1 \le i \le 2^{k-1}-2$,*

$$\mathbb{N}_i = \{(a, \delta_1(\lambda_1 - \lambda_i)a, \ldots, \delta_j(\lambda_j - \lambda_i)a, \ldots, -\epsilon\lambda_i a) : a \in \mathbb{F}_q\}$$

with $\mathbb{N}_i \cap \mathbb{N}_j = \{(0, 0, \ldots, 0)\}$ *for* $1 \leq i \neq j \leq 2^{k-1} - 1$*, where* $\lambda_i = \delta_{i+1}/\delta_i$ *for* $1 \leq i \leq 2^{k-1} - 2$*.*

Proof. For any $(a, b) \in \mathbb{K}_i$, there exists a unique $(c_0, c_1, \ldots, c_{2^{k-1}-1}) \in \mathbb{N}_i$ such that $c_i = \gamma_i(a, b) = \delta_{i+1}a + \delta_i b = 0$. If $c_0 = 0$, then $a = 0$ and $c_j = \delta_j b$ for $1 \leq j \leq 2^{k-1} - 1$. It follows that $\mathbb{N}_0 = \{(0, \delta_1 b, \ldots, \delta_{2^{k-1}-1}b) : b \in \mathbb{F}_q\}$. Also if $c_{2^{k-1}-1} = 0$, then $b = 0$ and $c_j = \delta_{j+1}a$ for $0 \leq j \leq 2^{k-1} - 2$ and hence $\mathbb{N}_{2^{k-1}-1} = \{(\delta_1 a, \delta_2 a, \ldots, \delta_{2^{k-1}-1}a, 0) : a \in \mathbb{F}_q\}$. Further, let $1 \leq i \leq 2^{k-1} - 2$ and $(a, b) \in \mathbb{K}_i$ i.e., $c_i = \gamma_i(a, b) = 0$. Then $b = -\lambda_i a$, where $\lambda_i = \delta_{i+1}/\delta_i$ for $1 \leq i \leq 2^{k-1} - 2$. It follows that

$$\mathbb{N}_i = \{(a, \delta_1(\lambda_1 - \lambda_i)a, \ldots, \delta_j(\lambda_j - \lambda_i)a, \ldots, -\epsilon\lambda_i a) : a \in \mathbb{F}_q\}.$$

Next we shall show that $\mathbb{N}_i$ is constant weight code. This assertion obviously holds for $i = 0$ and $i = 2^{k-1} - 1$. Further, let $1 \leq i \leq 2^{k-1} - 2$. For this, we must show that c_i is the only zero in $(c_0, c_1, \ldots, c_{2^{k-1}-1})$. Assume $c_i = c_j = 0$ for $j \neq i$. Then $\lambda_i = \lambda_j$ for $i \neq j$. This implies $\beta_k \in \mathbb{F}_q$ for $3 \leq k \leq u$, which is a contradiction as $2^k \nmid (q - 1)$ for $k \geq 2$ when $q \equiv 3 \pmod 4$. So $c_j \neq 0$ for any $j \neq i$. Therefore the weight of any nonzero codeword of $\mathbb{N}_i$ is $2^{k-1} - 1$ for every $0 \leq i \leq 2^{k-1} - 1$ and $\mathbb{N}_i \cap \mathbb{N}_j = \{(0, 0, \ldots, 0)\}$ for every $1 \leq i \neq j \leq 2^{k-1} - 1$. This proves the result. □

We now move to determine the weight distribution of N_k for $3 \leq k \leq u$.

Theorem 4.4. *The negacyclic code* N_k *is a two-weight code for* $3 \leq k \leq u$*. Further, if* $\ell_0^{(k)}$ *and* $\ell_1^{(k)}$ *are non-zero weights of* N_k *and if* $A^{(0)}_{\ell_i^{(k)}}$ *is the number of words of weight* $\ell_i^{(k)}$ *in* N_k*, then*

$$\ell_0^{(k)} = 2^{k-1},\ \ell_1^{(k)} = \ell_0^{(k)} - 1,$$
$$A^{(0)}_{\ell_0^{(k)}} = (q - 2^{k-1} + 1)(q - 1) \text{ and } A^{(0)}_{\ell_1^{(k)}} = 2^{k-1}(q - 1).$$

Proof. Let $c = (c_0, c_1, \ldots, c_{2^{k-1}-1}) \in \mathsf{N}_k$ be a codeword with $c_i = \gamma_i(a, b)$, where $a, b \in \mathbb{F}_q$. For a moment, if $c_i = 0$ and $c_j = 0$ for some $i \neq j$, then $a = b = 0$. In this case c becomes a zero codeword. Thus no two symbols of a nonzero codeword c can be simultaneously zero. Therefore the possible weight of nonzero c is $\ell_i^{(k)} = 2^{k-1} - i$ for $i = 0, 1$. For any fixed $0 \leq i \leq 2^{k-1} - 1$, by Lemma 4.3, $\mathbb{N}_i$ has $q - 1$ nonzero codewords of weight $2^{k-1} - 1$ and one codeword of weight zero. Let $\mathbb{N} = \bigcup_{i=0}^{2^{k-1}-1} \mathbb{N}_i$ and $\mathbb{M} = \{c \in \mathsf{N}_k : c \notin \mathbb{N}\}$. Then $\mathsf{N}_k = \mathbb{M} \cup \mathbb{N}$ and $\mathbb{M} \cap \mathbb{N} = \emptyset$. Observe that $\mathbb{N}$ has $(q - 1)2^{k-1}$ codewords of weight $2^{k-1} - 1$. Therefore, $\mathbb{M}$ has $(q^2 - 1) - (q - 1)2^{k-1} = (q - 1)(q - 2^{k-1} + 1)$ nonzero codewords of weight 2^{k-1}. □

Remark 4.5. *Take* $q + 1 = 2^{k-1}$ *for some* $3 \leq k \leq u$*, then by Lemma 4.3,* $\mathbb{M} = \emptyset$ *and* $\mathbb{N} = \mathsf{N_k}$*. Equivalently,* $\mathsf{N_k}$ *is a linear constant weight code with constant weight* $2^{k-1} - 1$*. For example,* $\mathsf{N_6}$ *is a constant weight code of length* 32 *with the constant weight* 31 *over* $\mathbb{F}_{31}$*. Further, if* $q + 1 \neq 2^{k-1}$*, but* $q + 1 = 2^k$ *for some* $2 \leq k \leq u - 1$*, then* $\mathsf{N_k}$ *is a linear* 2*-weight code of the same frequency* $2^{k-1}(q - 1)$*, i.e.,* $A^{(0)}_{\ell_i^{(k)}} = 2^{k-1}(q - 1)$ *for* $i = 0, 1$ *(see Example 4.8).*

The following result determines the weight distribution of $\mathsf{N}_{r,k}$ recursively using the weight distribution of N_k.

Theorem 4.6. *For any* $r \geq 0$ *and* $3 \leq k \leq u$*, the weight distribution of negacyclic codes* $\mathsf{N}_{r,k}$ *over* $\mathbb{F}_q$ *is*

$$A_{\ell^{(k)}} = \sum_{(x,y)} \binom{2^r}{x}\binom{2^r - x}{y} \left((q - 2^{k-1} + 1)(q - 1)\right)^x \left(2^{k-1}(q - 1)\right)^y,$$

where (x, y) *varies over all possible solutions of the Diophantine equation* $2^{k-1}x + (2^{k-1} - 1)y = \ell^{(k)}$ *such that* $0 \leq x \leq 2^r, 0 \leq y \leq 2^r - x$*.*

Proof. In view of Theorem 3.4,

$$\mathsf{N}_{r,k} = \underbrace{\mathsf{N}_k \times \mathsf{N}_k \times \cdots \times \mathsf{N}_k}_{2^r \quad \text{copies}}.$$

If $\mathbf{c} \in \mathsf{N}_{r,k}$ is any codeword, then there are 2^r vectors $\bar{c}_1, \bar{c}_2, \ldots, \bar{c}_{2^r}$ (not necessarily distinct) in N_k such that $\mathbf{c} = (\bar{c}_1, \bar{c}_2, \ldots, \bar{c}_{2^r})$. By Theorem 4.4, the possible weights of codewords $\bar{c}_j \in \mathsf{N}_k$, where $1 \leq j \leq 2^r$, are $\ell_i^{(k)} = 2^{k-1} - i$ for $i = 0, 1, 2^{k-1}$. Let x_i, for $i = 0, 1, 2^{k-1}$, be the number of $\bar{c}_j$'s in a codeword $\mathbf{c}$ of weight $\ell_i^{(k)}$. Clearly $x_1 + x_2 + x_{2^{k-1}} = 2^r$. Further, if $\ell^{(k)}$ denotes the weight of $\mathbf{c}$, then $\ell^{(k)} = \ell_0^{(k)} x_0 + \ell_1^{(k)} x_1$.

For the given 2^r copies of N_k, we first can choose the x_0 copies of weight 2^{k-1} in $\binom{2^r}{x_0}$ ways. From $2^r - x_0$ copies of N_k, we can select the x_1 copies of them, having weight $2^{k-1} - 1$, in $\binom{2^r - x_0}{x_1}$ ways. Now we can select the $x_{2^{k-1}}$ copies from the remaining $2^r - x_0 - x_1$ copies, having weight zero, in $\binom{2^r - x_0 - x_1}{x_{2^{k-1}}}$ ways. This can be done in only one way because $2^r - x_0 - x_1 = x_{2^{k-1}}$. By Theorem 4.4, $A_{2^{k-1}} = (q-1)(q - 2^{k-1} + 1)$ and $A_{2^{k-1}-1} = (q-1)2^{k-1}$. Therefore

$$A_{2^{k-1}x_0} = \binom{2^r}{x_0}\big((q - 2^{k-1} + 1)(q-1)\big)^{x_0} \text{ and } A_{(2^{k-1}-1)x_1} = \binom{2^r - x_0}{x_1}\big(2^{k-1}(q-1)\big)^{x_1}.$$

Since the Diophantine equation $\ell^{(k)} = \ell_0^{(k)} x + \ell_1^{(k)} y$ admits finite solutions and (x, y) varies over the set of all possible solutions, the number of codewords of weight $\ell^{(k)} = 2^{k-1}x + (2^{k-1} - 1)y$ is given by

$$A_{\ell^{(k)}} = \sum_{\substack{(x,y) \\ 0 \leq x \leq 2^r \\ 0 \leq y \leq 2^r - x}} A_{2^{k-1}x} A_{(2^{k-1}-1)y}.$$

This completes the proof. □

Theorem 4.7. *Let $q \equiv 3 \pmod 4$ and $3 \leq k \leq u$. Then, the weight distribution of cyclic code $\mathsf{C}_{r,k}$ is given by*

$$A_\ell = \sum_{\substack{(x,y) \\ \ell = 2^k x + (2^k - 2)y \\ 0 \leq x \leq 2^r, 0 \leq y \leq 2^r - x}} \binom{2^r}{x}\binom{2^r - x}{y}\big(2^{k-1}(q-1)\big)^{x+y}\left(\frac{q - 2^{k-1} + 1}{2^{k-1}}\right)^x.$$

Proof. If $\mathbf{c}$ is any codeword of $\mathsf{C}_{r,k}$, there exists a codeword $c_0 \in \mathsf{N}_{r,k}$ such that $\mathbf{c} = (c_0, -c_0)$. Observe that, for any $3 \leq k \leq u$ and $q \equiv 3 \pmod 4$, $2^{k+1} | (q+1)$. Now applying Theorem 4.6, we obtain the weight distribution of cyclic code $\mathsf{C}_{r,k}$ in the desired form. □

Note that the main result in [9] is a special case of Theorem 4.1 and Theorem 4.7.

Example 4.8. *Let $q = 7$ and $k = 3$. By Theorem 4.4, the weight distribution of a negacyclic $[4, 2, 3]_7$ code N_3 is $A_0 = 1$, $A_3 = A_4 = 24$. Further, by Theorem 4.7, the weight distribution of a reducible cyclic $[16, 4, 6]_7$ code is given by*

$$A_\ell = \sum_{\substack{(x,y) \\ 0 \leq x \leq 2, 0 \leq y \leq 2 - x}} \binom{2}{x}\binom{2 - x}{y} 24^{x+y} \textit{ with } 8x + 6y = \ell.$$

Table 4.8 characterizes the type of possible weights $\ell = 8x + 6y$ of a reducible cyclic $[16, 4, 6]_7$ code with the number of codewords A_ℓ of a given weight ℓ.

Table 4.8

ℓ	0	6	8	12	14	*16*
(x, y)	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(0, 2)$	$(1, 1)$	$(2, 0)$
A_ℓ	1	48	48	576	1152	576

5. Concluding remarks

The main contributions of this paper are the followings:

- The construction of a class of linear codes of length 2^n with 2^l zeros over $\mathbb{F}_q$ and their weight distribution. These codes are reversible when $l \geq 1$ and $q \equiv 3 \pmod 4$.
- The explicit form of the weight distribution in which the weights of codewords and the number of codewords of a given weight of these codes can be computed easily using a linear Diophantine equation and its solutions (see Example 4.8).
- The construction of constant weight linear codes and two-weight negacyclic codes of length 2^n, where 2^n divides $q + 1$ and integer $n \geq 2$. A class of linear codes with few weights are of special interest in authentication codes [2] and traceability schemes [6].

Many authors have worked on the problem of determining the weight distribution of reducible cyclic codes using mathematical tools, such as Gaussian periods and exponential sums. The values of the Gaussian periods, exponential sums are in general very hard to compute. It would be interesting to use the combinatorics approach of this paper for obtaining the weight distribution of cyclic codes of length m over $\mathbb{F}_q$ whose parity check polynomials are binomials or trinomials over $\mathbb{F}_q$ for the case $m \in \{2^n d, d^n\}$ for some odd integer d such that $d|(q - 1)$ or $d|(q + 1)$.

Acknowledgment: The authors wish to thank the anonymous referees for their valuable comments that really helped us to improve the quality of this paper.

References

[1] E. R. Berlekamp, Algebraic Coding Theory, Revised Edition, World Scientific Publishing Co. Pte. Ltd., 2015.

[2] C. Ding, D. R. Kohel, S. Ling, Secret–sharing with a class of ternary codes, Theor. Comput. Sci. 246(1–2) (2000) 285–298.

[3] H. Q. Dinh, C. Li, Q. Yue, Recent progress on weight distributions of cyclic codes over finite fields, J. Algebra Comb. Discrete Struct. Appl. 2(1) (2015) 39–63.

[4] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes, Finite Fields Appl. 14(2) (2008) 390–409.

[5] W. C. Huffman, V. Pless, Fundamentals of Error–Correcting Codes, Cambridge University Press, Cambridge, 2003.

[6] A. Kathuria, S. K. Arora, S. Batra, On traceability property of equidistant codes, Discrete Math. 340(4) (2017) 713–721.

[7] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, Cambridge, 1986.

[8] J. L. Massey, Reversible codes, Inform. Control 7(3) (1964) 369–380.

[9] 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.

[10] M. Singh, S. Batra, Some special cyclic codes of length 2^n, J. Algebra Appl. 16(1) (2017) 17 pages.

[11] G. Vega, The weight distribution of an extended class of reducible cyclic codes, IEEE Trans. Inform. Theory, 58(7) (2012) 4862–4869.

[12] M. Van Der Vlugt, Hasse–Davenport curves, Gauss sums and weight distributions of irreducible cyclic codes, J. Number Theory 55(2) (1995) 145–159.

[13] Z. Wan, Lectures on Finite Fields and Galois Rings, World Scientific Publishing, Singapore, 2003.

[14] J. Yang, M. Xiong, C. Ding, J. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, IEEE Trans. Inform. Theory 59(9) (2013) 5985–5993.

[15] X. Zhu, Q. Yue, L. Hu, Weight distributions of cyclic codes of length l^m, Finite Fields Appl. 31 (2015) 241–257.