J. Algebra Comb. Discrete Appl.
2(1) • 39-63
Received: 20 October 2014; Accepted: 6 December 2014
DOI 10.13069/jacodesmath.36866

Journal of Algebra Combinatorics Discrete Structures and Applications

Recent progress on weight distributions of cyclic codes over finite fields*

Research Article

Hai Q. Dinh[1], Chengju Li[2]§, Qin Yue[2]***

1. Departments of Mathematical Sciences, Kent State University, Warren, OH 44484, USA

2. Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, P.R. China

Abstract: Cyclic codes are an interesting type of linear codes and have wide applications in communication and storage systems due to their efficient encoding and decoding algorithms. In coding theory it is often desirable to know the weight distribution of a cyclic code to estimate the error correcting capability and error probability. In this paper, we present the recent progress on the weight distributions of cyclic codes over finite fields, which had been determined by exponential sums. The cyclic codes with few weights which are very useful are discussed and their existence conditions are listed. Furthermore, we discuss the more general case of constacyclic codes and give some equivalences to characterize their weight distributions.

2010 MSC: 94B15, 11T71, 11T24

Keywords: Linear codes, Weight distribution, Cyclic codes, Finite fields, Gauss periods, Gauss sums, Exponential sums, Quadratic forms

1. Introduction

The classes of cyclic codes play a very significant role in the theory of error-correcting codes. Cyclic codes can be efficiently encoded using shift registers, and they have rich algebraic structures for efficient error detection and correction, which explains their preferred role in engineering. Information Theory and Coding Theory have been widely considered to be born in 1948, when Claude Shannon's[1] landmark paper [75] on the mathematical theory of communication, showed that good codes exist[2]. Cyclic codes were

* *The second and third authors are supported by NNSF of China (No. 11171150)*
** *E-mail: hdinh@kent.edu*
§ *E-mail: lichengju1987@163.com*
*** *E-mail: yueqin@nuaa.edu.cn*
[1] *Claude Elwood Shannon (April 30, 1916 - February 24, 2001) was an American mathematician, electronic engineer, and cryptographer, who is refered to as "the father of information theory" [43]. Shannon is also credited*

introduced as early as 1957, nine years after that, in a series of papers by Prange [67]-[71]. Since then, cyclic codes have been the most studied of all codes. Many well known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either cyclic codes or can be constructed from cyclic codes.

In this paper, we survey some results on the weight distributions of cyclic codes over finite fields that have been recently determined by exponential sums. For a prime p, let $\mathbb{F}_q$ be a finite field of characteristic p with q elements, i.e., $q = p^s$, for some positive integer s. An $[n, k, d]$ linear code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum distance d. Hereafter, we always assume that the code length n and the field characteristic p are coprime [3]. The code $\mathcal{C}$ is called cyclic if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. By identifying the vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ with

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1),$$

any code $\mathcal{C}$ of length n over $\mathbb{F}_q$ corresponds to a subset of $\mathbb{F}_q[x]/(x^n-1)$. Then $\mathcal{C}$ is a cyclic code if and only if the corresponding subset is an ideal of $\mathbb{F}_q[x]/(x^n-1)$. Note that every ideal of $\mathbb{F}_q[x]/(x^n-1)$ is principal. Hence there is a monic polynomial $g(x)$ with least degree such that $\mathcal{C} = \langle g(x) \rangle$ and $g(x) \mid (x^n - 1)$. Then $g(x)$ is called the generator polynomial and $h(x) = (x^n - 1)/g(x)$ is called the check polynomial of the cyclic code $\mathcal{C}$. Suppose that $h(x)$ has t irreducible factors over $\mathbb{F}_q$, we call $\mathcal{C}$ the dual of the cyclic code with t zeros.

Let A_i be the number of codewords with Hamming weight i in the code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by

$$1 + A_1 x + A_2 x^2 + \cdots + A_n x^n.$$

The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the weight distribution of the code $\mathcal{C}$. In coding theory it is often desirable to know the weight distributions of the codes because they can be used to estimate the error correcting capability and the error probability of error detection and correction with respect to some decoding algorithms. This is quite useful in practice. Unfortunately, it is a very hard problem in general and remains open for most cyclic codes.

Let $r = q^m$ for a positive integer m and α a generator of $\mathbb{F}_r^*$. Let $h(x) = h_1(x)h_2(x)\cdots h_t(x)$, where $h_j(x)$ $(1 \le j \le t)$ are distinct monic irreducible polynomials over $\mathbb{F}_q$. Let $g_j = \alpha^{-s_j}$ be a root of $h_j(x)$ and

as the founder of both digital computer and digital circuit design theory, when, in 1937, as a 21-year-old master's student at MIT, he wrote a thesis establishing that electrical application of Boolean algebra could construct and resolve any logical, numerical relationship. It has been claimed that this has been the most important master's thesis of all time. Shannon contributed to the field of cryptanalysis during World War II and afterwards, including basic work on code breaking.

[2] *Shannon's theorem ensures that our hopes of getting the correct messages to the users will be fulfilled a certain percentage of the time. Based on the characteristics of the communication channel, it is possible to build the right encoders and decoders so that this percentage, although not 100%, can be made as high as we desire. However, the proof of Shannon's theorem is probabilistic and only guarantees the exixtence of such good codes. No specific codes were constructed in the proof that provides the desired accuracy for a given channel. The main goal of Coding Theory is to establish good codes that fulfill the assertions of Shannon's theorem. During the last 50 years, while many good codes have been constructed, but only from 1993, with the introduction of turbo codes [7], the rediscoveries of LDPC codes, and the study of related codes and associated iterative decoding algorithms, researchers started to see codes that approach the expectation of Shannon's theorem in practice.*

[3] *The case when the code length n is divisible by the characteristic p of the field yields the so-called repeated-root codes, which were first studied since 1967 by Berman [5], and then in the 1970s and 1980s by several authors such as Massey et al. [61], Falkner et al. [33], Roth and Seroussi [72]. However, repeated-root codes were first investigated in the most generality in the 1990s by Castagnoli et al. [16], and van Lint [77], where they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad. To distinguish the two cases, codes when the code-length is not divisible by the characteristic p of the field are called simple-root codes.*

n_j the order of g_j for $0 \le s_j \le r-2$ $(1 \le j \le t)$. Let m_j be the least positive integer such that $q^{m_j} \equiv 1 \pmod{n_j}$. In fact, we have $\deg(h_j(x)) = m_j$ for $j = 1, 2, \ldots, t$. Denote $\delta = \gcd(r-1, s_1, s_2, \ldots, s_t)$ and $n = \frac{r-1}{\delta}$. A cyclic code $\mathcal{C}$ can be defined by

$$\mathcal{C} = \{c(a_1, a_2, \ldots, a_t) : a_j \in \mathbb{F}_{q^{m_j}}\}, \tag{1}$$

where

$$c(a_1, a_2, \ldots, a_t) = (\sum_{j=1}^{t} \mathrm{Tr}_{q^{m_j}/q}(a_j), \sum_{j=1}^{t} \mathrm{Tr}_{q^{m_j}/q}(a_j g_j), \ldots, \sum_{j=1}^{t} \mathrm{Tr}_{q^{m_j}/q}(a_j g_j^{n-1})) \tag{2}$$

and $\mathrm{Tr}_{q^{m_j}/q}$ denotes the trace function from $\mathbb{F}_{q^{m_j}}$ to $\mathbb{F}_q$. It follows from Delsarte's Theorem [22] that the code $\mathcal{C}$ is an $[n, k]$ cyclic code over $\mathbb{F}_q$ with the check polynomial $h(x)$, where $k = m_1 + m_2 + \cdots + m_t$.

In the rest of this paper, we use g_i to denote the corresponding cyclic code. If we only give g_1 and g_2, we mean that the dual of cyclic code has two zeros and the product of the minimal polynomials of g_1 and g_2 over $\mathbb{F}_q$ is the check polynomial of such cyclic code. It is similar for cyclic codes whose duals have more zeros. In most cases, we also only list the cyclic codes whose weight distributions are known because they may have many nonzero weights. The reader can get the details on weight distributions in the corresponding references which are given.

For any $a_1, a_2, \ldots, a_t \in \mathbb{F}_r$, the Hamming weight of $c(a_1, a_2, \ldots, a_t)$ is equal to

$$W_H(c(a_1, a_2, \ldots, a_t)) = n - Z(r, t),$$

where

$$Z(r, t) = |\{0 \le i \le n-1 : \sum_{j=1}^{t} \mathrm{Tr}_{q^{m_j}/q}(a_j g_j^i) = 0\}|.$$

Let ϕ be the canonical additive character of $\mathbb{F}_q$. Then $\psi_j = \phi \circ \mathrm{Tr}_{q^{m_j}/q}$ is the canonical additive character of $\mathbb{F}_r$. By the orthogonal property of additive characters we have

$$\begin{aligned} Z(r, t) &= \sum_{i=0}^{n-1} \frac{1}{q} \sum_{y \in \mathbb{F}_q} \phi(y \sum_{j=1}^{t} \mathrm{Tr}_{q^{m_j}/q}(a_j g_j^i)) \\ &= \frac{1}{q} \sum_{j=1}^{t} \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_q} \psi_j(y a_j g_j^i). \end{aligned} \tag{3}$$

Hence determining the weight distribution of cyclic code is equivalent to determining the multiset

$$\{Z(r, t) : a_j \in \mathbb{F}_{q^{m_j}} \text{ for } j = 1, 2, \ldots t\}.$$

In general, it is very difficult and remains open for most cases. However, the weight distributions of cyclic codes had been determined in a few cases by using mathematical tools, such as Gauss periods, Gauss sums, quadratic forms, and the numbers of the solutions of equations over finite fields.

In view of the trace representation (2) of $\mathcal{C}$, it is natural to study the weight distributions of irreducible cyclic codes (i.e., $t = 1$) and the duals of cyclic codes with two or three zeros (i.e., $t = 2$ or 3). There are few results [53, 90] on weight distributions of cyclic codes with arbitrary zeros. Moreover, Ding and Yang [27] used Gauss periods to give an excellent survey on weight distributions of irreducible cyclic codes. In this paper, we mainly investigate the weight distributions of reducible cyclic codes which had been determined by exponential sums. The cyclic codes with few weights which are very useful are discussed and their existence conditions are listed.

The rest of this paper is organized as follows. In Section 2, we study the weight distributions of cyclic codes whose duals have two or three zeros. In Section 3, we present the results on weight distributions

of cyclic codes whose duals have arbitrary zeros. In Section 4, we investigate the cyclic codes with Niho exponents. In Section 5, the cyclic codes with few weights are discussed and their existence conditions are listed. Section 6 discusses the more general case of constacyclic codes, we present some methods to study the equivalence classes of constacyclic codes. All constacyclic codes that are in the same equivalence class of cyclic codes share the same weight distributions and all results from previous sections hold for such constacyclic codes.

It is impractical to mention all recent work on weight distributions of cyclic codes in this paper. We focus on the weight distributions determined by exponential sums and some results may be omitted. An apparent omission is the weight distributions determined by combinatorial methods. However, we hope that this paper will show that weight distributions of cyclic codes which are determined by exponential sums in general.

2. Weights of the duals of cyclic codes with two or three zeros

We begin with the weight distributions of cyclic codes whose duals have two or three zeros because Ding and Yang had given an elegant survey on irreducible cyclic codes. For details we refer the readers to [27] and the references therein. Below we consider the cyclic codes whose duals have two zeros. The weight distributions of such codes are settled for a few special cases and is quite complex in general [17].

Let g_1, g_2, and g_3 be three zeros of $h_1(x), h_2(x)$, and $h_3(x)$, respectively, and $\mathcal{C}$ the cyclic code as (1) with the check polynomial $h(x) = h_1(x)h_2(x)h_3(x)$. Now we assume that $m_1 = m_2 = m_3 = m$ if we do not give a special statement and α is a primitive element of $\mathbb{F}_{q^m}$. The weights of $\mathcal{C}$ were first studied in [14, 18, 81] by using exponential sums and combinatorial methods. Yuan et al. [91] used exponential sums to present the weight distributions of cyclic codes from perfect nonlinear functions. We refer the reader to [15] for a survey of highly nonlinear functions. Feng and Luo [34] presented a unified way to determine the weight distributions of cylic codes defined by perfect nonlinear functions.

Theorem 2.1. *The weight distributions of the following cyclic codes defined by perfect nonlinear functions are known:*

1. $g_1 = \alpha^{-1}, g_2 = \alpha^{-(p^l+1)}$, *where* $q = p$, $l \geq 0$ *is an integer, and* $m/\gcd(m, l)$ *is odd [35, 91];*
2. $g_1 = \alpha^{-1}, g_2 = \alpha^{-\frac{3^l+1}{2}}$, *where* $q = 3$, l *is odd, and* $\gcd(m, l) = 1$ *[35].*

Remark 2.2. *Let the assumptions and the notations be as above theorem. Then* $f(x) = x^{p^l+1}$ *is called Dembowski-Ostrom function [23] and* $f(x) = x^{\frac{3^l+1}{2}}$ *is called Coulter-Matthews function [21].*

2.1. Quadratic forms and weight distributions

Quadratic form is an effective tool to determine the weight distributions of cyclic codes. Below we recall some results on quadratic forms. We refer the readers to [54] for more details on quadratic forms. Let H be an $m \times m$ symmetric matrix over $\mathbb{F}_p$. By identifying $\mathbb{F}_{p^m}$ with $\mathbb{F}_p^m$, a function $Q(x)$ from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ is called a quadratic form over $\mathbb{F}_p$ if

$$Q(x) = XHX^{\perp}, \text{ where } X = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_p^m.$$

Suppose that $r = \text{rank}(H)$. Then there exists $M \in \text{GL}_m(\mathbb{F}_p)$ such that $H' = MHM^{\perp}$ is a diagonal matrix and $H' = \text{diag}(a_1, \ldots, a_r, 0, \ldots, 0)$, where $a_i \in \mathbb{F}_p$ for $1 \leq i \leq r$. Let $\Delta = a_1 \cdots a_r$ ($\Delta = 1$ if $r = 0$). Then we have the following proposition.

Proposition 2.3. *[35, 54] Suppose that p is an odd prime. Let $(\frac{\Delta}{p})$ denote the Legendre symbol and $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ be a complex p-th root of unity. Then we have*

$$\sum_{X\in\mathbb{F}_p^m} \zeta_p^{XHX^\perp} = \begin{cases} (\frac{\Delta}{p})p^{m-\frac{r}{2}}, & \text{if } p\equiv 1 \pmod 4; \\ (\frac{\Delta}{p})(\sqrt{-1})^r p^{m-\frac{r}{2}}, & \text{if } p\equiv 3 \pmod 4. \end{cases}$$

By employing the above proposition, Feng and Luo [35, 55] presented the weight distributions of several classes of cyclic codes. Since then a series of jobs were motivated by their original idea.

Theorem 2.4. *Let l be a positive integer. Then the weight distributions of cyclic codes over $\mathbb{F}_p$ (p odd prime) had been determined by using quadratic forms in the following cases:*

1. $g_1 = \alpha^{-2}, g_2 = \alpha^{-(p^l+1)}$, *where* $m \geq 3$ *and* $\gcd(m,l) = 1$ *[35];*
2. $g_1 = \alpha^{-2}, g_2 = \alpha^{-(p^l+1)}$, *and* $g_3 = \alpha^{-1}$, *where* $m \geq 3$ *and* $\gcd(m,l) = 1$ *[35];*
3. $g_1 = \alpha^{-2}, g_2 = \alpha^{-(p^l+1)}$, *where* $m \geq 2$ *and* $1 \leq l \leq m-1$ *[55];*
4. $g_1 = \alpha^{-2}, g_2 = \alpha^{-(p^l+1)}$, *and* $g_3 = \alpha^{-1}$, *where* $m \geq 2$ *and* $1 \leq l \leq m-1$ *[55];*
5. $g_1 = \alpha^{-1}, g_2 = \alpha^{-\frac{p^l+1}{2}}$, *where* $l/\gcd(m,l)$ *is odd [58];*
6. $g_1 = \alpha^{-1}, g_1 = \alpha^{-(p^l+1)}$, *and* $g_3 = \alpha^{-(p^{3l}+1)}$, *where* $m/\gcd(m,l)$ *is odd [92];*
7. $g_1 = -\alpha^{-1}, g_2 = \alpha^{-\frac{p^l+1}{2}}$, *where* $m/\gcd(m,l) \geq 3$ *is odd [96];*
8. $g_1 = \alpha^{-1}, g_2 = \alpha^{-\frac{p^{2l}+1}{2}}$, *and* $g_3 = \alpha^{-\frac{p^{4l}+1}{2}}$, *where* $m \geq 5$ *is odd and* $\gcd(m,l) = 1$ *[98];*
9. $g_1 = \alpha^{-(p^l+1)}, g_2 = \alpha^{-(p^{3l}+1)}$, *where* $m/\gcd(m,l)$ *is even [95];*
10. $g_1 = \alpha^{-1}, g_1 = \alpha^{-(p^l+1)}$, *and* $g_3 = \alpha^{-(p^{3l}+1)}$, *where* $m/\gcd(m,l)$ *is even [95];*
11. $g_1 = \alpha^{-2}, g_2 = \alpha^{-(p^{2l}+1)}$, *and* $g_3 = \alpha^{-(p^{4l}+1)}$, *where* $m/\gcd(m,l)$ *is odd [94];*
12. $g_1 = \alpha^{-1}, g_2 = -\alpha^{-1}$, *and* $g_3 = \alpha^{-\frac{p^l+1}{2}}$, *where* $m \geq 3$ *is odd and* $\gcd(m,l)=1$ *[57];*
13. $g_1 = \alpha^{-2}, g_2 = \alpha^{-4}$, *and* $g_3 = \alpha^{-10}$, *where* $p = 3$ *[56].*

There is a parallel result on the exponential sums over quadratic forms for even p. Luo et al. [59] investigated these exponential sums and gave the weight distributions of cyclic codes associated with generalized Kasami sequences.

Theorem 2.5. *[59] For even m, let l be an integer with $1 \leq l \leq m-1$ and $l \neq \frac{m}{2}$. Then the weight distributions of binary cyclic codes $\mathcal{C}$ are known in the following cases:*

1. $g_1 = \alpha^{-(2^{\frac{m}{2}}+1)}$ *and* $g_2 = \alpha^{-(2^l+1)}$;
2. $g_1 = \alpha^{-(2^{\frac{m}{2}}+1)}, g_2 = \alpha^{-(2^l+1)}$, *and* $g_3 = \alpha^{-1}$.

Remark 2.6. *In the above theorem, $m_1 = \frac{m}{2}, m_2 = m$ and $m_3 = m$.*

For the binary cyclic codes whose duals have two zeros, the calculations of their weight distributions is more important because it is equivalent to determine the value distribution of the cross-correlation function between two m-sequences and the Walsh transforms of monomials over finite fields. In fact, they represent the same mathematical problem (i.e., the calculation of exponential sum) in most cases. For more results of their relationships, cross-correlation function between two m-sequences, and the Walsh transforms of monomials, we refer the readers to [13, 36, 38, 40, 41, 44, 51, 65, 93] and references therein.

2.2. Gauss periods and weight distributions

There is another useful tool which is called Gauss periods to determine the weight distributions of cyclic codes. Now we recall the definition of Gauss period.

Let $r-1=nN$ and α be a fixed primitive element of $\mathbb{F}_r$, where $r=q^m=p^{sm}$. We define $C_i^{(N,r)}=\alpha^i\langle\alpha^N\rangle$ for $i=0,1,\ldots,N-1$, where $\langle\alpha^N\rangle$ denotes the subgroup of $\mathbb{F}_r^*$ generated by α^N. The Gauss periods of order N are given by

$$\eta_i^{(N,r)}=\sum_{x\in C_i^{(N,r)}}\psi(x),$$

where ψ is the canonical additive character of $\mathbb{F}_r$ and $\eta_i^{(N,r)}=\eta_{i \pmod N}^{(N,r)}$ if $i\geq N$. In general, the explicit evaluation of Gauss periods is a very difficult problem. However, they can be computed in a few cases: $N=2,3,4$, semi-primitive case, and index 2 case [27, 64]. By using these known Gauss periods, the weight distributions of some classes of cyclic codes were determined.

For future use, here we also introduce Gauss sums which are closely related to Gauss periods. Let

$$\lambda:\mathbb{F}_r^*\to\mathbb{C}^*$$

be a multiplicative character of $\mathbb{F}_r^*$. Now we define the Gauss sum over $\mathbb{F}_r$ by

$$G(\lambda)=\sum_{x\in\mathbb{F}_r^*}\lambda(x)\psi(x).$$

It is easy to see that $G(\lambda_0)=-1$, where λ_0 is the trivial multiplicative character, i.e., $\lambda_0(x)=1$ for all $x\in\mathbb{F}_r^*$. Gauss sums can be viewed as the Fourier coefficients in the Fourier expansion of the restriction of ψ to $\mathbb{F}_r^*$ in terms of the multiplicative characters of $\mathbb{F}_r$, i.e.,

$$\psi(x)=\frac{1}{r-1}\sum_{\lambda\in\widehat{\mathbb{F}}_r^*}G(\overline{\lambda})\lambda(x),\ \text{for } x\in\mathbb{F}_r^*. \tag{4}$$

By (4), we can obtain

$$\eta_i^{(N,r)}=\frac{1}{N}\sum_{j=0}^{N-1}\zeta_N^{-ij}G(\lambda^j)=\frac{1}{N}(-1+\sum_{j=1}^{N-1}\zeta_N^{-ij}G(\lambda^j)),$$

where λ is a primitive multiplicative character of order N over $\mathbb{F}_r^*$. Generally, the explicit determination of Gauss sums is a difficult problem. However, they can be explicitly evaluated in the following cases [6, 89]: quadratic Gauss sums, semi-primitive Gauss sums, and index 2 Gauss sums.

Ding [24] used Gauss periods to determine the weight distributions of irreducible cyclic codes. Moreover, a survey on the weight distributions of irreducible cyclic codes determined by Gauss periods was given by Ding and Yang [27]. Below we consider the weight distributions of reducible cyclic codes.

Let $m_1=m_2=m$, $r=q^m$, and α a generator of $\mathbb{F}_r^*$. Let h be a positive factor of $q-1$ and $e>1$ an integer such that $e\mid\gcd(q-1,hm)$. Define

$$g=\alpha^{\frac{q-1}{h}},n=\frac{h(r-1)}{q-1},\beta=\alpha^{\frac{r-1}{e}},N=\gcd(\frac{r-1}{q-1},\frac{e(q-1)}{h}).$$

We easily see that the order of g is n and $(\beta g)^n=1$. It had been proved that the minimal polynomials of g^{-1} and $(\beta g)^{-1}$ over $\mathbb{F}_q$ are distinct except when $q=3,h=1,e=m=2$ [87]. Hence their product is a factor of x^n-1.

Let $g_1=g^{-1}$ and $g_2=(\beta g)^{-1}$. In general, we have $m_1=m_2=m$. Thus the corresponding cyclic code $\mathcal{C}$ is an $[n,2m]$ code. If $\mathbb{F}_r^*=\langle g_1\rangle=\langle g_2\rangle$, then the weight distribution of the code $\mathcal{C}$ which is

called the dual of primitive cyclic code with two zeros had been studied in [9, 13, 14, 18, 62, 63, 74]. In this subsection, we only consider cyclic codes whose weight distributions are determined by Gauss periods, so we do not describe the results on primitive cyclic codes here. In fact, to determine the weight distributions of cyclic codes, more mathematical tools are employed, such as Gauss sums, Jacobi sums, and elliptic curves.

Theorem 2.7. *Let $g_1 = g^{-1}$ and $g_2 = (\beta g)^{-1}$. Then the weight distribution of cyclic code $\mathcal{C}$ were determined by Gauss periods in the following cases:*

1. *$e > 1$ and $N = 1$ [60];*
2. *$e = 2$ and $N = 2$ [60];*
3. *$e = 2$ and $N = 3$ [26];*
4. *$e = 2$ and $p^j + 1 \equiv 0 \pmod N$ for some positive integer j [26];*
5. *$e = 3$ and $N = 2$ [82];*
6. *$e = 2$, $N \equiv 3 \pmod 4$ is a prime, $\frac{N-1}{2} \mid sm$, and p is of index 2 modulo N which means $[\mathbb{Z}_N^* : \langle p \rangle] = 2$ and $-1 \notin \langle p \rangle$, where $\langle p \rangle$ is a subgroup generated by p in $\mathbb{Z}_N^*$ [37];*
7. *$e = 4$ and $N = 2$ [86];*
8. *$e = 3$ and $N = 3$ [87];*
9. *$e = 2$ and $p^j + 1 \equiv 0 \pmod N$ for some positive integer j [88].*

In [79], Vega presented an extended version for the class of cyclic codes studied by Ma et al. [60] and gave their weight distributions. Moreover, a general description for such reducible cyclic codes which generalizes the code $\mathcal{C}$ with $e = 2$ was given by Vega and Morales [80]. The weight distributions of these general cyclic codes were determined explicitly and the main tool is also Gauss periods.

Theorem 2.8. *[80] Suppose that q is odd and sm is even. Let d, a_1, a_2, and δ be four integers such that $2d \mid sm, a_1 - a_2 = \pm\frac{r-1}{2}$, and $\delta = \gcd(\frac{r-1}{q-1}, a_1)$. Let λ_1, λ_2 be two divisors of $q-1$ such that $\gcd(q-1, \frac{a_i}{\delta}) = \frac{q-1}{\lambda_i}$ for $i = 1, 2$. Fix $\delta' = \gcd(2, \frac{\Delta}{\delta})$ and $\lambda = \max\{\lambda_1, \lambda_2\}$. Let $g_1 = \alpha^{-a_1}$ and $g_2 = \alpha_{-a_2}$. If $\delta\delta' \mid (p^d + 1)$ and $2\delta < \frac{r-1}{p_1^d}$, then*

1. *the corresponding cyclic code $\mathcal{C}$ is an $[n, 2m]$ code with $n = \lambda\frac{\Delta}{\delta}$ and its weight distribution can be computed explicitly;*
2. *$\mathcal{C}$ is a projective linear code which means the minimum weight of its dual code is at least three if and only if $\delta' = 1$ and $\lambda = 2$.*

In this subsection, we have investigated the weight distributions of cyclic codes in the case $m_1 = m_2 = m$. Now we concentrate on the case $m_1 \neq m_2$. In [46, 47], the authors used Gauss periods to express the weight distributions of such cyclic codes. Moreover, a more general result on cyclic codes whose duals have two zeros was given in [48]. Based on the expression via Gauss periods, the weight distributions of several classes of cyclic codes were explicitly presented.

Let α be a fixed primitive element of $\mathbb{F}_r$ and $\mathbb{F}_{q^{m_i}}^* = \langle \alpha_i \rangle$, where $\alpha_i = \alpha^{\frac{r-1}{q^{m_i}-1}}$ for $i = 1, 2$. Denote $q^{m_i} - 1 = n_i N_i$, $g_i = \alpha_i^{-N_i}$, $d = \gcd(n_1, n_2)$, and $n = \frac{n_1 n_2}{d}$.

Theorem 2.9. *[48] If $\gcd(n_1, n_2) = d$, $n_1 N_1 = q^{m_1} - 1$, $n_2 N_2 = q^{m_2} - 1$, $M_1 = \frac{q^{m_1}-1}{q-1}, M_2 = \frac{q^{m_2}-1}{q-1}, d_1 = \gcd(M_1, N_1), d_2 = \gcd(M_2, N_2), d_3 = \gcd(\frac{M_1 d N_2}{d_4}, dN_1)$, and $d_4 = \gcd(M_2, dN_2)$, then the weight distribution of the cyclic code $\mathcal{C}$ with $g_1 = \alpha_1^{-N_1}$ and $g_2 = \alpha_2^{-N_2}$ is given by Table 1.*

Table 1. Weight distribution of cyclic code $\mathcal{C}$ with $g_1 = \alpha_1^{-N_1}$ and $g_2 = \alpha_2^{-N_2}$.

Weight	Frequency
0	1
$\frac{(q-1)n_1n_2}{dq} - \frac{(q-1)d_1n_2}{qdN_1}\eta_j^{(d_1,q^{m_1})}$	$\frac{q^{m_1}-1}{d_1}(0 \le j \le d_1-1)$
$\frac{(q-1)n_1n_2}{dq} - \frac{(q-1)d_2n_1}{qdN_2}\eta_j^{(d_2,q^{m_2})}$	$\frac{q^{m_2}-1}{d_2}(0 \le j \le d_2-1)$
$\frac{(q-1)n_1n_2}{dq} - \frac{(q-1)d_3d_4}{qd^2N_1N_2}\sum_{t=0}^{d-1}\sum_{i=0}^{\frac{dN_2}{d_4}-1}\eta_{N_2t+M_2i+j}^{(dN_2,q^{m_2})}\eta_{N_1t+M_1i+k}^{(d_3,q^{m_1})}$	$\frac{(q^{m_1}-1)(q^{m_2}-1)}{dd_3N_2}\begin{pmatrix} 0 \le j \le dN_2-1 \\ 0 \le k \le d_3-1 \end{pmatrix}$

Table 2. Weight distribution of $\mathcal{C}$ from two distinct finite fields.

Weight	Frequency
0	1
$q^{m_1-1}(q^{m_2}-1)$	$q^{m_1}-1$
$q^{m_2-1}(q^{m_1}-1)$	$q^{m_2}-1$
$\frac{(q^{m_1}-1)(q^{m_2}-1)}{q} - \frac{\delta}{q}\sum_{v=0}^{\delta-1}\eta_{v+k}^{(\delta,q^{m_1})}\eta_{v+j}^{(\delta,q^{m_2})}$	$\frac{(q^{m_1}-1)(q^{m_2}-1)}{\delta^2}(0 \le k,j \le \delta-1)$

As an application of Theorem 2.9, the weight distribution of cyclic code from two distinct finite fields (i.e., $N_1 = N_2 = 1$) was presented.

Theorem 2.10. *[48] Let m_1, m_2 be two positive divisors of m with $\gcd(m_1, m_2) = 1$, $n_1 = q^{m_1} - 1$, and $n_2 = q^{m_2} - 1$. If $\gcd(q-1, m_1 - m_2) = \delta$, then $\mathcal{C}$ is a $[\frac{(q^{m_1}-1)(q^{m_2}-1)}{q-1}, m_1 + m_2]$ cyclic code and its weight distribution is given by Table 2.*

If $\gcd(m_1, m_2) = 1$, then the weight distributions of the cyclic codes $\mathcal{C}$ can be explicitly determined when the Gauss periods of order δ are known.

Corollary 2.11. *[48] Let $r = q^m$, m_1, m_2 be two divisors of m with $\gcd(m_1, m_2) = 1$.*

1. *If $\gcd(q-1, m_1 - m_2) = 1$, then the corresponding cyclic code $\mathcal{C}$ is a $[\frac{(q^{m_1}-1)(q^{m_2}-1)}{q-1}, m_1 + m_2]$ three-weight cyclic code and its weight distribution can be explicitly determined.*
2. *If $\gcd(q-1, m_1 - m_2) = 2$, then the corresponding cyclic code $\mathcal{C}$ is a $[\frac{(q^{m_1}-1)(q^{m_2}-1)}{q-1}, m_1 + m_2]$ four-weight cyclic code and its weight distribution can be explicitly determined.*

In particular, if $(q-1) \mid m_1$ or $(q-1) \mid m_2$, then we have $\delta = 1$ by $\gcd(m_1, m_2) = 1$. Thus $\mathcal{C}$ is a three-weight cyclic code. Moreover, if $q = 2$, then the corresponding code $\mathcal{C}$ is a three-weight binary cyclic code which is more interesting in communication and storage systems.

If $N_1 = N_2 = 2$, then we have the following theorem.

Theorem 2.12. *[48] Let $r = q^m$ with q odd, m_1, m_2 be two divisors of m with $\gcd(m_1, m_2) = 1$ and $(q-1) \mid m_1$ or $(q-1) \mid m_2$, $n_1 = \frac{q^{m_1}-1}{2}$, and $n_2 = \frac{q^{m_2}-1}{2}$. Then the corresponding code $\mathcal{C}$ is a $[\frac{(q^{m_1}-1)(q^{m_2}-1)}{2(q-1)}, m_1 + m_2]$ cyclic code with five nonzero weights and its weight distribution can be explicitly determined.*

More classes of cyclic codes can be presented by Theorem 2.9 and it is unnecessary to state them here. We refer the readers to [46–48] for more results.

In fact, the weight distributions of most cyclic codes whose duals have few zeros are open. Moreover, zeta functions were also employed to determine the weight distributions of the duals of cyclic codes with

two zeros [9]. It is a good research problem to present the weight distributions of cyclic codes by using zeta functions, quadratic forms, Gauss periods, or other mathematical tools.

3. Weight distributions of cyclic codes with arbitrary zeros

In this section, we survey the weight distributions of cyclic codes with arbitrary zeros. It is in general very difficult to compute $Z(r,t)$ if the dual of cyclic code has more zeros. Hence there are few results on such cyclic codes.

3.1. Hermitian forms graphs and weight distributions

Let G be a finite Abelian group and D a subset of G. The Cayley graph $\mathrm{Cay}(G,D)$ on G with connection set D is the directed graph with vertex set G and edge set $\{(g,h): g,h\in G, gh^{-1}\in D\}$.

Let $A=(a_{gh})$ with entries in $\{0,1\}$ be a square matrix such that $a_{gh}=1$ if $gh^{-1}\in D$ and $a_{gh}=0$ otherwise. We call A the adjacency matrix of $\mathrm{Cay}(G,D)$. It is known that each character χ of G corresponds to an eigenvector of A with eigenvalue $\chi(D)=\sum_{d\in D}\chi(d)$. Furthermore, the spectrum of $\mathrm{Cay}(G,D)$ is the multiset $\{\chi(D):\chi\in\widehat{G}\}$, where $\widehat{G}$ is the character group of G.

In this subsection, we always suppose that $m=2l$ for some integer l and $s=1$, i.e., $q=p$. A matrix H over $\mathbb{F}_{p^2}$ is called Hermitian if $H=H^*$, where H^* is the conjugate transpose of H. Let $\mathcal{H}$ denote the Abelian group formed by all $l\times l$ Hermitian matrices over $\mathbb{F}_{p^2}$ under the matrix addition. The Hermitian forms graph is the Cayley graph $\mathrm{Cay}(\mathcal{H},\mathcal{D})$, where $\mathcal{D}=\{H\in\mathcal{H}:\mathrm{rank}(H)=1\}$. Let $W=\mathbb{F}_{p^2}^l$. Then the Hermitian forms graph on W is the Cayley graph $\mathrm{Cay}(\mathcal{H},\mathcal{D})$. The eigenvalues of the Hermitian forms graph were first computed by Stanton [76] and a more accessible formula was given in [10] by using the Gaussian binomial coefficients. For details and more information on the spectrum of Hermitian forms graph, we refer the readers to [10].

Li et al. [53] proposed an elegant method to study this problem by building a connection between the corresponding exponential sums and the spectra of Hermitian forms graphs.

For odd l, we denote $t=\frac{l-1}{2}$. Suppose that α is a primitive element of $\mathbb{F}_r$. Let $g_j=\alpha^{-(p^{2i-1}+1)}$ for $j=1,3,\ldots,t$ and $g_{t+1}=\alpha^{-(p^l+1)}$. Then we have $m_1=m_2=\cdots=m_t=m$ and $m_{t+1}=\frac{m}{2}$ and .

Theorem 3.1. *[53] The corresponding code $\mathcal{C}$ is a $[r-1,\frac{m^2}{4}]$ cyclic code and its weight distribution can be exactly determined.*

Very recently, Zhou et al. [99] generalized this class of p-ary cyclic codes proposed in [53] and the weight distributions of the generalized cyclic codes were settled for both even l and odd l along with the idea of Li, Hu, Feng, and Ge.

Theorem 3.2. *[99] Let $t=\lfloor\frac{m}{2}\rfloor$. Then the weight distributions of the following cyclic codes over $\mathbb{F}_q$ (q is a prime power here) are known:*

1. $g_j=\alpha^{-(p^{2j-1}+1)}$ $(j=1,2,\ldots,t)$, $g_{t+1}=\alpha^{-(p^l+1)}$ *for odd m;*
2. $g_j=\alpha^{-(p^{2j-1}+1)}$ $(j=1,2,\ldots,t)$, $g_{t+1}=\alpha^{-(p^l+1)}$, *and* $g_{t+2}=\alpha^{-1}$ *for odd m;*
3. $g_j=\alpha^{-(p^{2j-1}+1)}$ $(j=1,2,\ldots,t)$ *for even m;*
4. $g_j=\alpha^{-(p^{2j-1}+1)}$ $(j=1,2,\ldots,t)$, $g_{t+1}=\alpha^{-1}$ *for even m.*

3.2. Yang-Xiong-Ding-Luo cyclic codes

By Yang-Xiong-Ding-Luo cyclic codes we mean a class of cyclic codes with arbitrary number of zeros proposed in [90]. Now we describe this class of cyclic codes.

Main Assumptions: Let $r = q^m = p^{sm}$ be a prime power for two integers s, m and let $e \geq t \geq 2$. Assume that

1. $a \not\equiv 0 \pmod{r-1}$ and $e \mid (r-1)$;
2. $a_j \equiv a + \frac{r-1}{e}\Delta_j \pmod{r-1}$, $1 \leq j \leq t$, where $\Delta_u \neq \Delta_v$ for any $u \neq v$ and $\gcd(\Delta_2 - \Delta_1, \ldots, \Delta_t - \Delta_1, e) = 1$;
3. $g_j = \alpha^{-a_j}$ for $1 \leq j \leq t$, their minimal polynomials over $\mathbb{F}_q$ are pairwise distinct, and $m_1 = m_2 = \cdots = m_t = m$.

Denote

$$\delta = \gcd(r-1, a_1, a_2, \ldots, a_t), n = \frac{r-1}{\delta},$$

and

$$N = \gcd(\frac{r-1}{q-1}, ae).$$

We easily see that

$$e\delta \mid N(q-1).$$

It follows from Delsarte's Theorem [22] that the corresponding code $\mathcal{C}$ is an $[n, tm]$ cyclic code over $\mathbb{F}_q$.

It was proved that Condition (3) can be met by the following simple criterion.

Criterion: [90] Suppose that for any proper factor ℓ of m (i.e. $\ell \mid m$ and $\ell < m$) we have

$$\frac{r-1}{q^\ell - 1} \nmid N.$$

Then Condition (3) in the Main Assumptions holds. In particular, if $N \leq \sqrt{r}$, then Condition (3) in the Main Assumptions is met.

If $t = 2$, let $a_1 = \frac{q-1}{h}$ and $a_2 = \frac{q-1}{h} + \frac{r-1}{e}$ for positive integers e, h such that $e \mid h$ and $h \mid (q-1)$, the code $\mathcal{C}$ had been studied in [26, 37, 60, 82, 86–88]. Hence this class of cyclic codes with arbitrary zeros can be viewed as the generalization of cyclic codes whose duals have two zeros. The proper choices of these a_i's is key to compute the weight distribution of the code $\mathcal{C}$. It may be very difficult to find the weight distribution if the integers a_i are not chosen in the right way.

If $t = e \geq 2$, the set $\{\Delta_j : 1 \leq j \leq e\}$ is a complete residue system modulo e, so we may take $\Delta_1 = 0, \Delta_2 = 1, \ldots, \Delta_e = e - 1$.

Theorem 3.3. *[90] Under the Main Assumptions, when $N = 1$ and $t = e \geq 2$, the corresponding code $\mathcal{C}$ is a t-weight cyclic code over $\mathbb{F}_q$ and its weight distribution can be explicitly presented.*

The Gauss periods are known for $N = 2, 3, 4$, semi-primitive case, and index 2 case. Hence the weight distributions of more cyclic codes can be determined.

Theorem 3.4. *[90] Suppose that the Gaussian periods $\eta_j^{(N,r)}$ of order N have μ distinct values $\{\eta_1, \eta_2, \ldots, \eta_\mu\}$, and for each $i (1 \leq i \leq \mu)$, there are exactly τ_i distinct js such that $\eta_j^{(N,r)} = \eta_i$. (Note that $\tau_1 + \tau_2 + \cdots + \tau_\mu = N$.) Then, the corresponding code $\mathcal{C}$ is an $[n, em]$ cyclic code over $\mathbb{F}_q$ with at most $\binom{\mu+e}{e} - 1$ nonzero weights and its weight distribution can be explicitly presented when Gauss periods are known.*

3.3. Cyclic codes from $\mathbb{F}_l$ conjugates

Let $\mathbb{F}_q$ be a finite field with $q = l^t$ and γ a primitive element of $\mathbb{F}_q$, where l is a prime power and t is a positive integer. Let g be an element in the algebraic closure of $\mathbb{F}_q$ and $m_g(x)$ its minimal polynomial over $\mathbb{F}_q$. Suppose that $\deg(m_g(x)) = m$ and $\mathbb{F}_{q^m} = \mathbb{F}_q(g)$. Then $g = \alpha^{-N}$ and $N \mid (q^m - 1)$, where α is a primitive element of $\mathbb{F}_{q^m}$.

Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_q$ with check polynomial

$$h(x) = m_g(x)m_{g^l}(x)\cdots m_{g^{l^{t-1}}}(x),$$

where $m_{g^{l^u}}(x)$ is the minimal polynomial of g^{l^u} over $\mathbb{F}_q$ for $u = 0, 1, \ldots, t-1$. It follows from Delsarte's Theorem [22] that the code $\mathcal{C}$ is an $[n, tm]$ cyclic code over $\mathbb{F}_q$, where $n = \frac{q^m-1}{N}$. It is well known that $g(x) = (x^n - 1)/h(x) \in \mathbb{F}_q[x]$ and every codeword of $\mathcal{C}$ is $c(x) = a(x)g(x)$, where $a(x) \in \mathbb{F}_q[x]$ and $\deg(a(x)) \leq tm - 1$. Note that the roots of $h(x)$ are all the conjugates of g with respect to $\mathbb{F}_l$. Then $h(x) \in \mathbb{F}_l[x]$ is the minimal polynomial of g over $\mathbb{F}_l$ and $g(x) \in \mathbb{F}_l[x]$. For $a(x) \in \mathbb{F}_q[x]$, $\deg(a(x)) \leq tm-1$, by $\mathbb{F}_q = \mathbb{F}_l \oplus \gamma\mathbb{F}_l \oplus \cdots \oplus \gamma^{t-1}\mathbb{F}_l$ we have

$$a(x) = s_0(x) + \gamma s_1(x) + \cdots + \gamma^{t-1}s_{t-1}(x),$$

where $s_u(x) \in \mathbb{F}_l[x]$ and $\deg(s_u(x)) \leq tm - 1$ for $u = 0, 1, \ldots, t-1$. Then we get

$$c(x) = a(x)g(x) = s_0(x)g(x) + \gamma s_1(x)g(x) + \cdots + \gamma^{t-1}s_{t-1}(x)g(x).$$

It is easy to see that each $s_u(x)g(x)$ is a codeword of the irreducible cyclic code over $\mathbb{F}_l$ whose check polynomial is $h(x)$ for $u = 0, 1, \ldots, t-1$. Let $\mathrm{T} := \mathrm{Tr}_{q^m/l}$ denote the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_l$. Then by the trace representation of the irreducible cyclic code, the cyclic code $\mathcal{C}$ can be expressed by

$$\mathcal{C} = \{\mathbf{c}(a_0, a_1, \ldots, a_{t-1}) : a_0, a_1, \ldots, a_{t-1} \in \mathbb{F}_{q^m}\},$$

where

$$\mathbf{c}(a_0, a_1, \ldots, a_{t-1}) = (\sum_{u=0}^{t-1}\gamma^u\mathrm{T}(a_u), \sum_{u=0}^{t-1}\gamma^u\mathrm{T}(a_u\alpha^N), \ldots, \sum_{u=0}^{t-1}\gamma^u\mathrm{T}(a_u(\alpha^N)^{n-1})). \tag{5}$$

When $\gcd(\frac{q^m-1}{l-1}, N) = 1$, the zeros of the check polynomial of the cyclic code $\mathcal{C}$ are α^{-Nl^u} for $u = 0, 1, \ldots, t-1$. In [90], Yang et al. also dealt with such problem and the zeros of the check polynomials of Yang-Xiong-Ding-Luo cyclic codes are $\alpha^{-(a+\frac{q^m-1}{t}u)}$ for $u = 0, 1, \ldots, t-1$, where $t \mid (q^m - 1)$ and $a \not\equiv 0 \pmod{q^m - 1}$. Hence this class of cyclic codes with arbitrary number of zeros are different from Yang-Xiong-Ding-Luo cyclic codes.

Theorem 3.5. *[49] Let the notations be as above. If* $\gcd(\frac{q^m-1}{l-1}, N) = 1$*, then the corresponding code* $\mathcal{C}$ *is a* t*-weight cyclic code and its weight distribution can be explicitly determined.*

4. Weight distributions of cyclic codes with Niho exponents

In this section, we always assume that $q = p$, i.e., $s = 1$. Now we consider the weight distributions of cyclic codes over $\mathbb{F}_p$ with Niho exponents which are due to [65].

A positive integer d is of Niho exponent if $d \equiv p^i \pmod{p^l - 1}$, where $m = 2l$ for some integer l. Without loss of generality, we can assume that $d \equiv 1 \pmod{p^l-1}$. For two Niho exponents $d = s(p^l-1)+1$ and $d' = s'(p^l - 1) + 1$, we call them equivalent if $d' \equiv p^i d \pmod{p^m - 1}$ for some integer i. Moreover, $d \equiv p^l d \pmod{p^m - 1}$ if and only if $s + s' \equiv 1 \pmod{p^l + 1}$. Hence, s can be restricted in the range $1 \leq s \leq p^{l-1} + 1$.

Let $g_1 = \alpha^{-d_1}$ and $g_2 = \alpha^{-d_2}$ for two Niho exponents d_1, d_2. Suppose that g_1 and g_2 are not conjugates over $\mathbb{F}_p$. To determine the weight distribution of the corresponding cyclic code $\mathcal{C}$, by (3) we have to deal with the exponential sums

$$T(a,b) = \sum_{x\in\mathbb{F}_r} \psi_1(a_1 x^{d_1})\psi_2(a_2 x^{d_2}) = \zeta_p^{\mathrm{Tr}_{p^{m_1}/p}(a_1 x^{d_1})+\mathrm{Tr}_{p^{m_2}/p}(a_2 x^{d_2})}$$

for $a_1, a_2 \in \mathbb{F}_r$. If one of d_1, d_2 is equal to 1 and $p = 2$, this class of cyclic codes with few nonzero weights were studied [18]. Li, Feng, and Ge [52] gave some sufficient conditions for these codes to have few nonzero weights for both $p = 2$ and odd p.

Some preliminaries are necessary for determining the exponential sums $T(a,b)$. Let $\mathbb{F}_{p^m}$ be a finite field with $m = 2l$ and $r = p^m$. Denote $S = \{x \in \mathbb{F}_r : x\bar{x} = 1\}$, where $\bar{x} = x^{p^l}$. Then S is a cyclic group of order $p^l + 1$ and $S = \langle\eta\rangle$ with $\eta = \alpha^{p^l-1}$.

Lemma 4.1. *[52, 65] For two Niho exponents $d_1 = s_1(p^l-1)+1$ and $d_2 = s_2(p^l-1)+1$, we have*

$$T(a,b) = (N(a,b-1))p^l,$$

where $N(a,b)$ is the number of $z \in S$ satisfying

$$az^{s_1} + \bar{a}z^{1-s_1} + bz^{s_2} + \bar{b}z^{1-s_2} = 0.$$

From the properties of trace function, we easily obtain the following moment identities which is very important to determine the value distribution of $T(a,b)$.

Lemma 4.2. *1.* $\sum_{a,b\in\mathbb{F}_r} T(a,b) = p^{2m}$.

2. $\sum_{a,b\in\mathbb{F}_r} T(a,b)^2 = p^{2m}N_2(d_1,d_2)$, *where $N_2(d_1,d_2)$ is the number of solutions of the equations*

$$\begin{cases} x^{d_1} + y^{d_1} = 0 \\ x^{d_2} + y^{d_2} = 0 \end{cases}, \quad x, y \in \mathbb{F}_r.$$

3. $\sum_{a,b\in\mathbb{F}_r} T(a,b)^3 = p^{2m}N_3(d_1,d_2)$, *where $N_3(d_1,d_2)$ is the number of solutions of the equations*

$$\begin{cases} x^{d_1} + y^{d_1} + z^{d_1} = 0 \\ x^{d_2} + y^{d_2} + z^{d_2} = 0 \end{cases}, \quad x, y, z \in \mathbb{F}_r.$$

From the above two lemmas we see that determining the weight distributions of cyclic codes with Niho exponents is equivalent to count the number of solutions of the equation and the system of equations over finite fields. Hence, if cyclic codes with Niho exponents have many nonzero weights, it is very difficult to determine their weight distributions. Recently, Li, Feng, and Ge [52] presented the weight distributions of three classes of cyclic codes with Niho exponents.

Theorem 4.3. *[52] Let $\mathcal{C}$ be a cyclic code defined by $g_1 = \alpha^{-d_1}$ and $g_2 = \alpha^{-d_2}$ for two Niho exponents d_1, d_2. Then the weight distribution of the p-ary cyclic code $\mathcal{C}$ with the following Niho exponents are known:*

1. *$p = 2$, $d_1 = 2^l + 1$, and $d_2 = s_2(2^l-1)+1$, where $s_2 \not\equiv \frac{1}{2} \pmod{2^l+1}$;*
2. *$p = 2$, $l \geq 2$, $d_1 = s_1(2^l-1)+1$, and $d_2 = s_2(2^l-1)+1$, where $s_1 = 2^{k-1}t - \frac{t-1}{2}$ and $s_2 = 2^{k-1}t + \frac{t+1}{2}$ for integers k ($1 \leq k \leq l$) and t (t is odd and $1 \leq t \leq 2^l+1$) satisfying $2^{k-1}t, 2^{k+1}t \not\equiv 0 \pmod{2^l+1}$ and $m \equiv -1 \pmod{k}$ or $\gcd(k, 2m) = 1$;*
3. *p is odd, $d_1 = s_1(p^l-1)+1$, and $d_2 = s_2(p^l-1)+1$, where $s_1 = \frac{t+2}{4}$ and $s_2 == \frac{3t+2}{4}$ for integer t satisfying $t \equiv 2 \pmod 4$ and $t \not\equiv 0 \pmod{p^l+1}$.*

5. Cyclic codes with few weights

Cyclic codes with few weights are of much interest in coding theory due to their applications in cryptography and combinatorics. In this section, we begin with some definitions.

A linear code is called to be projective if the minimum weight of its dual code is at least three. Moreover, a linear code is a N-weight code if the number of non-zero weights of this code is N.

A cyclic code of length n over $\mathbb{F}_q$ is irreducible if its check polynomial is irreducible (its polynomial representation is a minimal ideal). It is said to be non-degenerate if its check polynomial is a primitive divisor of $x^n - 1$ over $\mathbb{F}_q$ (that is, the order of this polynomial is n).

5.1. One-weight cyclic codes

Let $\mathbb{F}_r$ be a finite field with $r = q^m$ elements. When the length of a cyclic code $\mathcal{C}$ is $r - 1$ and the check polynomial is the minimal polynomial over $\mathbb{F}_q$ of a primitive root of $\mathbb{F}_r$ (in fact, $\mathcal{C}$ is an irreducible cyclic code), then the code $\mathcal{C}$ is called a simplex code or a subfield code. It is easily proved that $\mathcal{C}$ is a 1-weight code with $(q-1)q^{m-1}$ as its unique non-zero weight.

In [84], Wolfmann first gave some descriptions of one-weight cyclic codes via Pless identities [66]. Furthermore, Vega and Wolfmann [81] presented a better and more simple characterization of one-weight irreducible cyclic codes.

Theorem 5.1. *[81] Let $\mathcal{C}$ be an $[n, k]$ irreducible cyclic code over $\mathbb{F}_q$ with $n = \lambda\frac{r-1}{q-1}$, where λ divides $q-1$. Let ρ be the order of the check polynomial of $\mathcal{C}$, that is, the common order of its roots. The following assertions are equivalent:*

1. *$\mathcal{C}$ is a one-weight cyclic code;*
2. *$\mathcal{C}$ contains a codeword of weight λq^{m-1};*
3. $\frac{\rho}{\gcd(\rho, q-1)} = \frac{q^m-1}{q-1}$.

5.2. Two-weight cyclic codes

Two-weight linear codes are closely related to strongly regular graphs, partial difference sets, and finite projective spaces. There is a survey [12] to investigate their relationships.

For two-weight irreducible cyclic codes, Schmidt and White [73] in 2002 gave a classification by Gauss sums. They presented some necessary and sufficient numerical conditions on the parameters of an irreducible cyclic code to have at most two nonzero weights. It is conjectured that an irreducible cyclic code is a two-weight code if and only if it is a semi-primitive code or one of the eleven sporadic examples. Moreover, they gave a partial proof of this conjecture via generalized Riemann hypothesis.

Let $q = p$ be a prime, and let u, m be positive integers such that u divides $\frac{p^m-1}{p-1}$. Let $\mathcal{C}$ be an irreducible cyclic code over $\mathbb{F}_p$ defined by $g_1 = \alpha^{-u}$. For a positive integer x, let $S_p(x)$ denote the sum of the p-digits of x, that is, if

$$x = l_0 + l_1 p + \cdots + l_v p^v,$$

where $0 \le l_i \le p - 1$ and $l_v \neq 0$, then

$$S_p(x) = l_0 + l_1 + \cdots + l_v.$$

Denote $f =: \mathrm{ord}_u(p)$ (i.e., the least positive integer such that $p^f \equiv 1 \pmod{u}$) and

$$\theta = \theta(u, p) =: \frac{1}{p-1} \min\{S_p(\frac{j(p^f-1)}{u}) : 1 \le j < u\}.$$

Table 3. Eleven sporadic examples with $u \leq 100000$

u	p	s	f	θ	κ	ϵ
11	3	1	5	2	5	+1
19	5	1	9	4	9	+1
35	3	1	12	5	17	+1
37	7	1	9	4	9	+1
43	11	1	7	3	21	+1
67	17	1	33	16	33	+1
107	3	1	53	25	53	+1
133	5	1	18	8	33	-1
163	41	1	81	40	81	+1
323	3	1	144	70	161	+1
499	5	1	249	123	249	+1

Then we have the following theorem.

Theorem 5.2. *[73] Let the notations be as above. If $m = fl$ for some integer l, then $\mathcal{C}$ is a two-weight code if and only if there exists a positive integer κ satisfying*

$$\kappa \mid (u-1),$$

$$\kappa p^{l\theta} \equiv \epsilon \pmod{u},$$

$$\kappa(u-\kappa) = (u-1)p^{l(f-2\theta)},$$

where $\epsilon = \pm 1$. Moreover, the two nonzero weights are

$$w_1 = (p-1)p^{l\theta-1}(p^{l(f-\theta)} - \epsilon\kappa)/u,$$

$$w_2 = w_1 + \epsilon(p-1)p^{l\theta-1}.$$

Conjecture 5.3. *[73] An irreducible cyclic code is a two-weight code if and only if it is a semi-primitive code or one of the eleven sporadic examples in Table 3.*

In [85], Wolfmann gave a characterization of projective two-weight linear codes. Furthermore, a family of projective 2-weight irreducible cyclic codes were presented.

Theorem 5.4. *[85] Let $\mathcal{C}$ be a non-degenerate irreducible cyclic code of length n over $\mathbb{F}_q$ with $\gcd(n,q) = 1$. Let $\mathbb{F}_{q^m}$ be the splitting field of $x^n - 1$ over $\mathbb{F}_q$ and let $nN = q^m - 1$. If :*

1. $\gcd(n, q-1) = 1$,
2. *$m = 2fl$ such that $(q-1)(q^f+1) \equiv 0 \pmod{N}$,*
3. *$N \neq q-1$ and $d \neq (q-1)(q^{fl}+1)$,*

then C is a projective two-weight code.

Similarly, a conjecture on projective two-weight non-degenerate irreducible cyclic codes was proposed in [85].

Conjecture 5.5. *[85] Any projective two-weight non-degenerate irreducible cyclic code is a code satisfying conditions (1)-(3) of Theorem 5.4 except for eleven special cases deduced from Table 3.*

Wolfmann [84] also characterized projective two-weight cyclic codes and proved that if a linear code $\mathcal{C}$ is a two-weight projective cyclic code of dimension m over $\mathbb{F}_q$, then either:

(1) $\mathcal{C}$ is irreducible, or

(2) if $q \neq 2$, $\mathcal{C}$ is the direct sum of two one-weight irreducible cyclic codes of length $n = \lambda\frac{q^m-1}{q-1}$, where λ divides $q-1$ and $\lambda \neq 1$ and direct sum means direct sum as vector spaces.

It is clear that the code $\mathcal{C}$ is reducible in case (2) of Wolfmann's characterization [84]. Two-weight reducible cyclic codes had also been presented in [39] and [81]. Motivated by these results, in 2008, Vega [78] presented a family of two-weight reducible cyclic codes which were constructed as the direct sum of two one-weight cyclic codes and obtained their weight distributions. Moreover, this new family gives a unified explanation for all these two-weight cyclic codes that were presented in [39] and [81]. To get Vega's result, Gauss sum introduced in Section 2 is a necessary tool.

Theorem 5.6. *[78] Let p, q, and m be defined as before. Denote $\Delta = \frac{q^m-1}{q-1}$. Let a_1, a_2 and v be integers such that $a_1 q^i \not\equiv a_2 \pmod{q^m-1}$, for all $i \geq 0$, $v = \gcd(a_1 - a_2, q-1)$, and $a_2 \in \mathbb{Z}_\Delta^*$. For some integer ℓ satisfying $\ell \mid \gcd(a_1, a_2, q-1)$, we set $\lambda = \frac{(q-1)\ell}{\gcd(a_1,a_2,q-1)}$, $n = \lambda\Delta$, $\mu = \frac{q-1}{\Delta}$, and $\xi = \frac{q-1}{v}$. Let $h_1(x), h_2(x) \in \mathbb{F}_q[x]$ be the minimal polynomials of α^{-a_1} and α^{-a_2}, respectively. Suppose that at least one of the following two conditions holds:*

1. *$p = 2, k = 2, v = 1$, and a_1 is a unit in the ring $\mathbb{Z}_\Delta$, or*
2. *for some integer j , with $1 \leq p^j < q^m$, we have*

$$(1 + \widetilde{a_2}(a_1 - a_2))p^j \equiv 1 \pmod{\Delta v},$$

where $\widetilde{a_2}$ is the inverse of a_2 in $\mathbb{Z}_\Delta$. Then the following four assertions are true:

(a) $h_1(x)$ and $h_2(x)$ are the check polynomials for two different one-weight cyclic codes of length n and dimension m.

(b) $\mu \mid v$ and $\lambda > \frac{v}{\mu}$.

(c) If $\mathcal{C}$ is the cyclic code with check polynomial $h_1(x)h_2(x)$, then $\mathcal{C}$ is an $[n, 2m]$ two-weight cyclic code with weight enumerator polynomial

$$A(x) = 1 + \frac{\mu}{v}n(q-1)z^{(\lambda-\frac{v}{\mu})q^{m-1}} + (q^{2m} - 1 - \frac{\mu}{v}n(q-1)z^{\lambda q^{m-1}}.$$

(d) $\mathcal{C}$ is a projective code if and only if $\mu = v$.

5.3. Three-weight cyclic codes

Cyclic codes with three nonzero weights have been applied in association schemes [11] and secret sharing schemes [97]. Hence constructing three-weight cyclic codes is a good research problem. Recently, perfect nonlinear (or planar) and almost perfect nonlinear functions are employed to find three weight cyclic codes.

In [91], Yuan, Ding, and Carlet used planar functions to get two classes of three-weight cyclic codes. Feng and Luo [34] presented a unified way to investigate the weight distributions of cyclic codes from planar functions.

Theorem 5.7. *Let $m \geq 3$ be odd and let q be an odd prime. Then the corresponding cyclic code C is a three-weight $[q^m - 1, 2m]$ cyclic code in the following cases:*

Table 4. Weight distribution of cyclic code from planar functions.

Weight	Frequency
0	1
$(q-1)q^{m-1}-q^{\frac{m-1}{2}}$	$\frac{(q-1)(q^m-1)(q^{m-1}+q^{\frac{m-1}{2}})}{2}$
$(q-1)q^{m-1}$	$(q^m-1)(q^{m-1}+1)$
$(q-1)q^{m-1}+q^{\frac{m-1}{2}}$	$\frac{(q-1)(q^m-1)(q^{m-1}-q^{\frac{m-1}{2}})}{2}$

Table 5. Weight distribution of cyclic code in [34].

Weight	Frequency
0	1
$(q-1)q^{m-1}-\frac{q-1}{2}q^{\frac{m-1}{2}}$	$(q^m-1)(q^{m-1}+q^{\frac{m-1}{2}})$
$(q-1)q^{m-1}$	$(q^m-1)(q^m-2q^{m-1}+1)$
$(q-1)q^{m-1}+\frac{q-1}{2}q^{\frac{m-1}{2}}$	$(q^m-1)(q^{m-1}-q^{\frac{m-1}{2}})$

1. $g_1=\alpha^{-1}$ *and* $g_2=\alpha^{-(q^l+1)}$ *[91];*
2. $g_1=\alpha^{-1}$ *and* $g_2=\alpha^{-\frac{q^l+1}{2}}$, *where* $q=3, \gcd(m,l)=1$, *and* h *is odd [34, 91].*

Moreover, its weight distribution is presented in Table 4.

Luo and Feng [58] extended the second construction in Theorem 5.7.

Theorem 5.8. *[58] Let* $m\geq 3$ *be odd and let* q *be an odd prime. Then the code* $\mathcal{C}$ *over* $\mathbb{F}_q$ *defined by* $g_1=\alpha^{-1}$ *and* $g_2=\alpha^{-v}$ *is a three-weight* $[q^m-1,2m]$ *cyclic code with the weight distribution in Table 5 if* $v=\frac{q^l+1}{2}$, *where* l *is a positive integer satisfying* $\gcd(2m,l)=1$.

We remark that Table 4 and Table 5 are same when $p=3$. Additionally, Ding, Gao, and Zhou [25, 96] presented several classes of three-weight cyclic codes over $\mathbb{F}_3$ from almost perfect nonlinear functions.

Theorem 5.9. *Let* $q=3$ *and* $\mathcal{C}$ *be the ternary cyclic code defined by* $g_1=\alpha^{-1}$ *and* $g_2=\alpha^{-v}$. *Then* $\mathcal{C}$ *is a* $[q^m-1,2m]$ *three-weight cyclic code with weight distribution depicted in Table 4 or 5 in the following cases:*

1. m *is odd and* $v=\frac{3^{m+1}-1}{4}$ *[25];*
2. m *is odd and* $v=3^{\frac{m+1}{2}}-1$ *[97];*
3. $m\equiv 3 \pmod 4$ *and* $v=\frac{3^{\frac{m+1}{2}}-1}{2}$ *[97];*
4. $m\equiv 1 \pmod 4$ *and* $v=\frac{3^{\frac{m+1}{2}}-1}{2}+\frac{3^m-1}{2}$ *[97];*
5. $m\equiv 3 \pmod 4$ *and* $v=\frac{3^{m+1}-1}{8}$ *[97];*
6. $m\equiv 1 \pmod 4$ *and* $v=\frac{3^{m+1}-1}{8}+\frac{3^m-1}{2}$ *[97];*
7. $m\equiv 3 \pmod 4$ *and* $v=(3^{\frac{m+1}{4}}-1)(3^{\frac{m+1}{2}}+1)$ *[97];*
8. $m\equiv 7 \pmod 8$ *and* $v=(3^{\frac{m+1}{8}}-1)(3^{\frac{m+1}{4}}+1)(3^{\frac{m+1}{2}}+1)$ *[25].*

Table 6. Weight distribution of three classes of cyclic code in [25].

Weight	Frequency
0	1
$(q-1)(q^{m-1}-q^{\frac{m-1}{2}})$	$\frac{1}{2}(q^m-1)(q^{m-1}+q^{\frac{m-1}{2}})$
$(q-1)q^{m-1}$	$(q^m-1)(q^m-q^{m-1}+1)$
$(q-1)(q^{m-1}+q^{\frac{m-1}{2}})$	$\frac{1}{2}(q^m-1)(q^{m-1}-q^{\frac{m-1}{2}})$

Table 7. Case: $v \equiv 1+\frac{q-1}{2} \pmod{q-1}$.

Weight	Frequency
0	1
$(q-1)q^{m-1}-\frac{q-1}{2}q^{\frac{m+d-2}{2}}$	$(q^m-1)(q^{m-d}+q^{\frac{m-d}{2}})$
$(q-1)q^{m-1}$	$(q^m-1)(q^m-2q^{m-d}+1)$
$(q-1)q^{m-1}+\frac{q-1}{2}q^{\frac{m+d-2}{2}}$	$(q^m-1)(q^{m-d}-q^{\frac{m-d}{2}})$

Remark 5.10. *For $q=3$, x^v is an almost perfect nonlinear function over $\mathbb{F}_{q^m}$ for the following v:*

1. $v=3^{\frac{m+1}{2}}-1$;
2. $v=\frac{3^{\frac{m+1}{2}}-1}{2}$ *if* $m\equiv 3 \pmod 4$;
3. $v=\frac{3^{\frac{m+1}{2}}-1}{2}+\frac{3^m-1}{2}$ *if* $m\equiv 1 \pmod 4$;
4. $v=\frac{3^{m+1}-1}{8}$ *if* $m\equiv 3 \pmod 4$;
5. $v=\frac{3^{m+1}-1}{8}+\frac{3^m-1}{2}$ *if* $m\equiv 1 \pmod 4$.

There are another three classes of three-weight cyclic codes whose weight distributions are given in Table 6 and are different from the one in Table 4 or 5.

Theorem 5.11. *[25] Let $q=3$ and $\mathcal{C}$ be the ternary cyclic code defined by $g_1=\alpha^{-1}$ and $g_2=\alpha^{-v}$. Then $\mathcal{C}$ is a $[q^m-1,2m]$ three-weight cyclic code with weight distribution depicted in Table 6 if*

1. $v=\frac{3^{m+1}-1}{3^h+1}+\frac{3^m-1}{2}$, *where* $\frac{m+1}{h}$ *is even; or*
2. $v=(3^{\frac{m+1}{8}}-1)(3^{\frac{m+1}{4}}+1)(3^{\frac{m+1}{2}}+1)+\frac{3^m-1}{2}$, *where* $m\equiv 7 \pmod 8$; *or*
3. $v=(3^{\frac{m+1}{4}}-1)(3^{\frac{m+1}{2}}+1)+\frac{3^m-1}{2}$, *where* $m\equiv 3 \pmod 4$.

In 2014, Li et al. [50] gave a more general description of three-weight cyclic codes defined by $g_1=\alpha^{-1}$ and $g_2=\alpha^{-v}$.

Theorem 5.12. *[50] Let $m\geq 3$ be odd. Let q be any odd prime. If v is an integer satisfying $(q^l+1)v\equiv 2 \pmod{q^m-1}$ for some positive integer v with $\gcd(m,l)=d$, then $\mathcal{C}$ is a $[q^m-1,2m]$ cyclic code with the weight distribution in Table 7 if $v\equiv 1+\frac{q-1}{2} \pmod{q-1}$ and Table 8 when $v\equiv 1 \pmod{q-1}$.*

There are more classes of three-weight cyclic codes presented in the literature. Three-weight cyclic codes were also constructed from Niho exponents [52] and two distinct finite fields [48]. It is unnecessary to list all the results on three-weight cyclic codes and we have to omit some results here. In [35, 96], the cyclic codes were proved to be three-weight by using quadratic forms.

Table 8. **Case:** $v \equiv 1 \pmod{q-1}$.

Weight	Frequency
0	1
$(q-1)(q^{m-1}-q^{\frac{m+d-2}{2}})$	$\frac{1}{2}(q^m-1)(q^{m-d}+q^{\frac{m-d}{2}})$
$(q-1)q^{m-1}$	$(q^m-1)(q^m-q^{m-d}+1)$
$(q-1)(q^{m-1}+q^{\frac{m+d-2}{2}})$	$\frac{1}{2}(q^m-1)(q^{m-d}-q^{\frac{m-d}{2}})$

Theorem 5.13. *Let q be a prime and $\mathcal{C}$ a cyclic code over $\mathbb{F}_q$ defined by $g_1 = \alpha^{-v_1}$ and $g_2 = \alpha^{-v_2}$. Then $\mathcal{C}$ is a $[q^m-1, 2m]$ three-weight cyclic codes in the following cases:*

1. *$v_1 = 2$ and $v_2 = p^l + 1$, where $m \geq 3$ is odd and $\gcd(m,l) = 1$ [35];*
2. *$v_1 = \frac{q^m+1}{2}$ and $v_2 = \frac{q^l+1}{2}$, where $\gcd(m,l) = 1$ [96].*

6. Generalization to constacyclic codes

The concept of cyclic codes was extended naturally to negacyclic codes,[4] and then to constacyclic codes. Given a nonzero element λ of $\mathbb{F}_q$, a linear code C of length n over $\mathbb{F}_q$ is called λ-*constacyclic* if $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$ for every $(c_0, c_1, \cdots, c_{n-1}) \in C$. Just like cyclic codes, λ-constacyclic codes of length n over $\mathbb{F}_q$ are classified as the ideals $\langle g(X)\rangle$ of the quotient ring $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle$, where the generator polynomial $g(X)$ is the unique monic polynimial of minimum degree in the code, which is a divisor of $X^n - \lambda$. When $\lambda = 1$, λ-constacyclic codes are just cyclic codes and when $\lambda = -1$, λ-constacyclic codes are negacyclic codes. In general, the dual of a λ-constacyclic code of length n is a λ^{-1}-constacyclic code of length n.

There are cases when one code can be mapped onto another by means of a map which preserves the Hamming distances. Two codes C_1, C_2 are considered to be of the same quality if there exists a mapping $\varphi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ with $\varphi(C_1) = C_2$ which preserves the Hamming distance, i.e. $d_H\big(\varphi(\mathbf{a}), \varphi(\mathbf{a}')\big) = d_H(\mathbf{a}, \mathbf{a}')$, for any $\mathbf{a}, \mathbf{a}' \in \mathbb{F}_q^n$. Mappings with the latter property are called isometries, and such codes are naturally called equivalent. There are various ways in which such an equivalence relation can be defined. For example, if C_1, C_2 are linear codes, then we can naturally assume furthermore that the isometry φ is a linear map (e.g., [8]).

Since each λ-constacyclic code is an ideal of $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle$, it is natural to assume that isometries between constacyclic codes preserve the algebraic structures and Hamming distances. It turns out that if we can classify all the equivalence classes of constacyclic codes, we then only have to study the representative of those equivalence classes. In particular, if we can determine all constacyclic codes that are equivalent to cyclic codes, then all our results about Hamming weight and weight distributions of cyclic codes in previous sections hold true for those constacyclic codes. We devote this section to consider two type of equivalences, and for each type, we give the necessary and sufficient conditions for λ- and μ-constacyclic codes to be equivalent.

[4] *As mentioned before, cyclic codes were introduced in 1957. Just about 11 years after that, negacyclic codes over finite fields $\mathbb{F}_p$ were initiated by Berlekamp in 1968 [3, 4], where he showed that these codes are more useful for correcting errors measured relative to the Lee metric. Berlekamp also designed a decoding algorithm that can correct errors with Lee weight at most $\frac{p-1}{2}$. A couple of years after that, in 1971, Kelsch and Green [45] were sucessful to provide non-binary negacyclic codes exceeding Berlekamp's $\frac{p-1}{2}$ bound. They constructed 2-error-correcting negacyclic codes of length $\frac{3^m-1}{2}$ with redundancy $2m$ over $\mathbb{F}_3$, and all negacyclic codes of length $\frac{p^m-1}{2}$ with redundancy mt over $\mathbb{F}_p$.*

First of all, some special results have been obtained in the literature.

Lemma 6.1. *[42, Lemma 3.1] or [1, Corollary 2.1] Let n be a positive integer, and $\lambda \in \mathbb{F}_q^*$. If $\mu^n\lambda = 1$ for some $\mu \in \mathbb{F}_q^*$, then*

$$\mathbb{F}_q[X]/\langle X^n - \lambda\rangle \longrightarrow \mathbb{F}_q[X]/\langle X^n - 1\rangle, \quad X \mapsto \mu X$$

is an $\mathbb{F}_q$-algebra isomorphism which is Hamming distance preserving.

In particular, in case n is odd, for $\lambda = -1$, it is obvious that $\mu = -1$ satisfies the hypothesis of the above lemma. That means that negacyclic codes of odd length are scalar equivalent to cyclic codes of the same length, which is a well known result that was proven to be true for the more general case when the alphabet is a finite commutative ring.

Noting this fact, Dinh [29] established a one-to-one correspondence between negacyclic and cyclic codes, carrying results on negacyclic codes to cyclic codes accordingly.

Proposition 6.2. *[29, Proposition 6.1] Let p be an odd prime and q a power of p. Then the map $\xi : \frac{\mathbb{F}_q[X]}{\langle X^{p^s}+1\rangle} \mapsto \frac{\mathbb{F}_q[X]}{\langle X^{p^s}-1\rangle}$, given by $f(X) \mapsto f(-X)$, is an $\mathbb{F}_q$-algebra isomorphism. In particular, for $A \subseteq \frac{\mathbb{F}_q[X]}{\langle X^{p^s}+1\rangle}$, $B \subseteq \frac{\mathbb{F}_q[X]}{\langle X^{p^s}-1\rangle}$ such that $\xi(A) = B$, then A is an ideal of $\frac{\mathbb{F}_q[X]}{\langle X^{p^s}+1\rangle}$ if and only if B is an ideal of $\frac{\mathbb{F}_q[X]}{\langle X^{p^s}-1\rangle}$. Equivalently, A is a negacyclic code of length p^s over $\mathbb{F}_q$ if and only if B is a cyclic code of length p^s over $\mathbb{F}_q$.*

Later on, Dinh in [30] showed that all constacyclic codes of length p^s over $\mathbb{F}_q$ are scalar equivalent to negacyclic codes.

Proposition 6.3. *[30, Proposition 3.1] Let p be an odd prime and q a power of p. Let $\lambda \in \mathbb{F}_q^*$. Then there exists a unique element λ_0 in $\mathbb{F}_q^*$ such that $\lambda_0^{p^s} = -\lambda^{-1}$. Let Φ be the map $\Phi : \frac{\mathbb{F}_q[X]}{\langle X^{p^s}+1\rangle} \mapsto \frac{\mathbb{F}_q[X]}{\langle X^{p^s}-\lambda\rangle}$, given by $\Phi(f(X)) = f(\lambda_0 X)$. Then Φ is an $\mathbb{F}_q$-algebra isomorphism, and it is Hamming distance preserving.*

For the more general alphabets of finite rings, [83] showed that cyclic and negacyclic codes over $\mathbb{Z}_4$ have the same structure for odd code lengths. Dinh and López-Permouth in [28] generalized that to obtain that this fact holds true for cyclic and negacyclic codes of odd lengths over any finite chain ring. Batoul *et al.* in [2, Proposition 3.4] extended this result to a more general setting.

Generalizing the ideas above, Chen *et al.* in [19] introduced a concept called "isometry" for the nonzero elements of $\mathbb{F}_q$ to classify constacyclic codes over $\mathbb{F}_q$ such that the constacyclic codes belonging to the same isometry class have the same distance structures and the same algebraic structures.

Definition 6.4. *[19, Definition 3.1] Let $\lambda, \mu \in \mathbb{F}_q^*$. We say that an $\mathbb{F}_q$-algebra isomorphism*

$$\varphi : \quad \mathbb{F}_q[X]/\langle X^n - \mu\rangle \longrightarrow \mathbb{F}_q[X]/\langle X^n - \lambda\rangle$$

is an isometry *if it preserves the Hamming distances on the algebras, i.e.*

$$d_H\big(\varphi(\mathbf{a}), \varphi(\mathbf{a}')\big) = d_H(\mathbf{a}, \mathbf{a}'), \qquad \forall\ \mathbf{a}, \mathbf{a}' \in \mathbb{F}_q[X]/\langle X^n - \mu\rangle.$$

And, if there is an isometry between $\mathbb{F}_q[X]/\langle X^n-\lambda\rangle$ and $\mathbb{F}_q[X]/\langle X^n-\mu\rangle$, then we say that λ is n-isometric to μ in $\mathbb{F}_q$, written $\lambda \cong_n \mu$.

Clearly, the n-isometry "$\cong_n$" is an equivalence relation on $\mathbb{F}_q^*$, hence $\mathbb{F}_q^*$ is partitioned into n-isometry classes. If $\lambda \cong_n \mu$, then the λ-constacyclic codes of length n are in one to one correspondence with the μ-constacyclic codes of length n such that the corresponding constacyclic codes have the same dimension and the same distance distribution, specifically, have the same minimum distance; at that case for convenience, the λ-constacyclic codes of length n are said to be *isometric* to the μ-constacyclic codes of length n. So, it is enough to study the n-isometry classes of constacyclic codes.

We have the following result.

Theorem 6.5. *[19, Theorem 3.2] For any $\lambda, \mu \in \mathbb{F}_q^*$, the following three statements are equivalent to each other:*

(i) $\lambda \cong_n \mu$.

(ii) $\langle \lambda, \xi^n \rangle = \langle \mu, \xi^n \rangle$, *where* $\langle \lambda, \xi^n \rangle$ *denotes the subgroup of* $\mathbb{F}_q^*$ *generated by* λ *and* ξ^n.

(iii) *There is a positive integer* $k < n$ *with* $\gcd(k, n) = 1$ *and an element* $a \in \mathbb{F}_q^*$ *such that* $a^n \lambda = \mu^k$ *and the following map*

$$\varphi_a : \quad \mathbb{F}_q[X]/\langle X^n - \mu^k \rangle \longrightarrow \mathbb{F}_q[X]/\langle X^n - \lambda \rangle, \tag{6}$$

which maps any element $f(X) + \langle X^n - \mu^k \rangle$ *of* $F_q[X]/\langle X^n - \mu^k \rangle$ *to the element* $f(aX) + \langle X^n - \lambda \rangle$ *of* $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$, *is an isometry.*

In particular, the number of n*-isometry classes of* $\mathbb{F}_q^*$ *is equal to the number of positive divisors of* $\gcd(n, q-1)$.

Taking $\mu = 1$, we see that $\lambda \cong_n 1$ implies that there is an isometry $\varphi_a : \mathbb{F}_q[X]/\langle X^n - 1 \rangle \to \mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ such that $\varphi(X) = aX$. Thus for the constacyclic codes n-isometric to cyclic codes, the following consequence is closely related to [42, Lemma 3.1] or [1, Corollary 2.1].

Corollary 6.6. *[19, Corollary 3.4] Let* n *be a positive integer, and* $\lambda \in \mathbb{F}_q^*$. *The* λ*-constacyclic codes of length* n *are isometric to the cyclic codes of length* n *if and only if* $a^n \lambda = 1$ *for an element* $a \in \mathbb{F}_q^*$; *further, in that case the map*

$$\varphi_a : \quad \mathbb{F}_q[X]/\langle X^n - 1 \rangle \longrightarrow \mathbb{F}_q[X]/\langle X^n - \lambda \rangle, \tag{7}$$

which maps $f(X)$ *to* $f(aX)$, *is an isometry, and*

$$X^n - \lambda = \lambda \cdot M_{r_1}(aX)^{p^s} M_{r_2}(aX)^{p^s} \cdots M_{r_\rho}(aX)^{p^s} \tag{8}$$

is an irreducible factorization of $X^n - \lambda$ *in* $\mathbb{F}_q[X]$, *where* $n = n' p^s$ *with* $s \geq 0$ *and* $p \nmid n'$, $M_{r_i}(X)$ *is the irreducible factor of* $X^{n'} - 1$ *over* $\mathbb{F}_q$ *corresponding to the* q*-cyclotomic coset containing* r_i. *In particular, any* λ*-constacyclic code* C *has a generator polynomial as follows:*

$$\prod_{i=1}^{\rho} M_{\eta^{r_i}}(aX)^{e_i}, \qquad 0 \leq e_i \leq p^s, \text{ for any } \ i = 1, \cdots, \rho. \tag{9}$$

As an immediate application of Corollary 6.6, the next result can be regarded as a generalization of Proposition 6.3.

Corollary 6.7. *(cf. [19, Corollary 3.5]) If* n *is a positive integer coprime to* $q-1$, *then there is only one* n*-isometry class in* $\mathbb{F}_q^*$; *in particular, for any* $\lambda \in \mathbb{F}_q^*$ *the* λ*-constacyclic codes of length* n *are isometric to the cyclic codes of length* n, *i.e.* $a^n \lambda = 1$ *for an* $a \in \mathbb{F}_q^*$ *and all the (7), (8) and (9) hold.*

Although $\lambda \cong_n \mu$ means there exists an isometry ϕ between the rings $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ and $\mathbb{F}_q[X]/\langle X^n - \mu \rangle$, it is not easy to connect the generator polynomial of the λ-constacyclic code C with the generator polynomial of $\phi(C)$, and as a result, it is not easy to describe the relationship between the duals $C^\perp$ and $\phi(C)^\perp$.

To overcome this problem, Chen, Dinh and Liu in [20] considered a more specified relationship than the isometry " $\cong_n$ ", that enabled us to obtain a much more explicit description of the generator polynomials of all constacyclic codes. This detailed description also allows us to establish the generator polynomials of the dual codes. A new equivalence relationship " $\sim_n$ " is introduced on the nonzero elements of $\mathbb{F}_q$ to classify constacyclic codes of length n over $\mathbb{F}_q$. Some necessary and sufficient conditions for any two nonzero elements of $\mathbb{F}_q$ to be equivalent to each other are established. It is shown that, if $\lambda \sim_n \mu$ then there exists a very explicit $\mathbb{F}_q$-algebra isomorphism φ between $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ and $\mathbb{F}_q[X]/\langle X^n - \mu \rangle$. Furthermore, the generator polynomial of the λ-constacyclic code C and the generator polynomial of the μ-constacyclic code $\varphi(C)$ are connected in a very simple way.

Definition 6.8. *[20, Definition 3.1] Let n be a positive integer. For any elements λ, μ of $\mathbb{F}_q^*$ we say that λ and μ are* n-equivalent *in $\mathbb{F}_q^*$ and denote by $\lambda \sim_n \mu$ if the polynomial $\lambda X^n - \mu$ has a root in $\mathbb{F}_q$. In this case, we say λ-constacyclic codes are n-equivalent to μ-constacyclic codes.*

It is routine to check that $\sim_n$ is an equivalence relationship on $\mathbb{F}_q^*$. The next result shows that λ and μ are n-equivalent if and only if they are belonging to the same coset of $\langle \xi^n \rangle$ in $\langle \xi \rangle$. In other words, the cosets of $\langle \xi^n \rangle$ in $\langle \xi \rangle$ give all the n-equivalence classes, thus each n-equivalence class contains the same number of elements.

Theorem 6.9. *[20, Theorem 3.2] For any $\lambda, \mu \in \mathbb{F}_q^*$, the following four statements are equivalent:*

(i) *There exists an $a \in \mathbb{F}_q^*$ such that*

$$\psi : \ \mathbb{F}_q[X]/\langle X^n - \mu \rangle \ \to \ \mathbb{F}_q[X]/\langle X^n - \lambda \rangle$$

$$f(X) \mapsto f(aX),$$

is an $\mathbb{F}_q$-algebra isomorphism.

(ii) *λ and μ are n-equivalent in $\mathbb{F}_q^*$.*

(iii) $\lambda^{-1}\mu \in \langle \xi^n \rangle$.

(iv) $(\lambda^{-1}\mu)^d = 1$, *where* $d = \frac{q-1}{\gcd(n,q-1)}$.

In particular, the number of the n-equivalence classes in $\mathbb{F}_q^*$ is $\gcd(n, q-1)$.

Comparing with the equivalence relation " $\cong_n$ " mentioned previously, one can easily find that $\lambda \sim_n \mu$ implies $\lambda \cong_n \mu$. However, the converse of this statement is not true in general. In fact, Theorem 6.5 implies that if $\lambda \cong_n \mu$ then there exists a positive integer k coprime to n such that $\lambda \sim_n \mu^k$. Therefore, every isometry class is equal to some unions of n-equivalence classes. We give the following illustrative example.

Example 6.10. *Take $q = 2^4$ and $n = 6$ in Theorem 6.9. Clearly,* $\gcd(6, 2^4 - 1) = 3$ *and*

$$\mathbb{F}_{2^4}^* = \langle \xi \rangle \bigcup \xi\langle \xi \rangle \bigcup \xi^2\langle \xi \rangle.$$

This implies that ξ and ξ^2 are not 6-equivalent. However, it is readily seen that there are just two 6-isometry classes and $\xi \cong_n \xi^2$.

7. Concluding remarks

In this paper, we investigated the weight distributions of cyclic codes determined by exponential sums. It is clear that Gauss periods, Gauss sums, and quadratic forms are important tools. The weight distributions of cyclic codes have been studied for many years and are known in some cases. However, it remains open for most cyclic codes. Thus there are many challenging problems to be solved.

Acknowledgment: The authors are very grateful to the reviewers and the editor for their valuable comments and suggestions that improved the quality of this paper.

References

[1] N. Aydin, I. Siap, D. K. Ray-Chaudhuri, *The structure of 1-generator quasi-twisted codes and new linear codes*, Designs Codes Cryptogr. 24, 313-326, 2001.

[2] A. Batoul, K. Guenda, T. A. Gulliver, *On self-dual cyclic codes over finite chain rings*, Designs Codes Cryptogr. 70, 347-358, 2014.

[3] E. R. Berlekamp, *Negacyclic Codes for the Lee Metric, Proceedings of the Conference on Combinatorial Mathematics and Its Applications*, Chapel Hill, N.C., University of North Carolina Press, 298-316, 1968.

[4] E. R. Berlekamp, *Algebraic Coding Theory*, revised 1984 edition, Aegean Park Press, 1984.

[5] S. D. Berman, *Semisimple cyclic and Abelian codes. II*, Kibernetika (Kiev) 3 (1967), 21-30 (Russian). English translation: Cybernetics 3, 17-23,1967.

[6] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley-Interscience Publication, 1998.

[7] C. Berrou, A. Glavieux, and P. Thitimajshima, *Near Shannon limit error-correcting coding and decoding: Turbo-codes*, 1993.

[8] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. A. Kohnert, A. Wassermann, *Error Correcting Linear Codes: Classification by Isometry and Applications*, Springer, Berlin, 2006.

[9] N. Boston and G. McGuire, *The weight distribution of cyclic codes with two zeros and zeta functions*, J. Symbolic Comput., 45(7), 723-733, 2010.

[10] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, Berlin, Germany: Springer-Verlag, 18, 1989, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)].

[11] A. R. Calderbank and J. M. Goethals, *Three-weight codes and association schemes*, Philips J. Res., 39, 143-152, 1984.

[12] R. Calderbank and W. M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc., 18, 97-122, 1986.

[13] A. Canteaut, P. Charpin, and H. Dobbertin, *Weight divisibility of cyclic codes, highly nonlinear functions on* $\mathbb{F}_{2^m}$ *and crosscorrelation of maximum-length sequences*, SIAM J. Discrete Math., 13(1), 105-138, 2000.

[14] C. Carlet, P. Charpin, and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. 15(2), 125-156, 1998.

[15] C. Carlet and C. Ding, *Highly nonlinear mappings*, J. Complexity, 20(2), 205-244, 2004.

[16] G. Castagnoli, J. L. Massey, P. A. Schoeller and N. von Seemann, *On repeated-root cyclic codes*, IEEE Trans. Inform. Theory 37, 337-342, 1991.

[17] P. Charpin, *Open problems on cyclic codes, in Handbook of Coding Theory, Part 1: Algebraic Coding*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, ch. 11, 1998.

[18] P. Charpin, *Cyclic codes with few weights and Niho exponents*, J. Combin. Theory Ser. A, 108, 247-259, 2004.

[19] B. Chen, Y. Fan, L. Lin, H. Liu, *Constacyclic codes over finite fields*, Finite Fields Appl. 18, 1217-1231, 2012.

[20] B. Chen, H. Q. Dinh, H. Liu, *Repeated-root constacyclic codes of length* ℓp^s *and their duals*, Discrete Appl. Math. 177, 60-70, 2014.

[21] R. S. Coulter and R. W. Matthews, *Planar functions and planes of Lenz- Barlotti class II*, Des., Codes, Cryptogr., 10, 167-184, 1997.

[22] P. Delsarte, *On subfield subcodes of modified Reed-Solomon codes*, IEEE Trans. Inform. Theory, 21(5), 575-576, 1975.

[23] P. Dembowski and T. G. Ostrom, *Planes of order n with collineation groups of order* n^2 , Math. Z., 193, 239-258, 1968.

[24] C. Ding, *The weight distribution of some irreducible cyclic codes*, IEEE Trans. Inf. Theory, 55(3),

955-960, 2009.
[25] C. Ding, Y. Gao, and Z. Zhou, *Five families of three-weight ternary cyclic codes and their duals*, IEEE Trans. Inform. Theory, 59(12), 7940-7946, Dec. 2013.
[26] C. Ding, Y. Liu, C. Ma, and L. Zeng, *The weight distributions of the duals of cyclic codes with two zeros*, IEEE Trans. Inform. Theory, 57(12), 8000-8006, 2011.
[27] C. Ding and J. Yang, *Hamming weights in irreducible cyclic codes*, Discrete Math., 313(4), 434-446, Feb. 2013.
[28] H. Q. Dinh, S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory, 50, 1728-1744, 2004.
[29] H. Q. Dinh, *On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions*, Finite Fields Appl. 14 , 22-40, 2008.
[30] H. Q. Dinh, *Constacylic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, Journal of Algebra, 324, 940-950, 2010.
[31] H. Q. Dinh, *Repeated-root constacyclic codes of length $2p^s$*, Finite Fields Appl. 18, 133-143, 2012.
[32] H. Q. Dinh, *Structure of repeated-root constacyclic codes of length $3p^s$ and their duals*, Discrete Math. 313, 983-991, 2013.
[33] G. Falkner, B. Kowol, W. Heise, E. Zehendner, *On the existence of cyclic optimal codes*, Atti Sem. Mat. Fis. Univ. Modena 28, 326-341, 1979.
[34] K. Feng and J. Luo, *Value distributions of exponential sums from perfect nonlinear functions and their applications*, IEEE Trans. Inform. Theory, 53(9), 3035-3041, Sep. 2007.
[35] K. Feng and J. Luo, *Weight distribution of some reducible cyclic codes*, Finite Fields Appl., 14, 390-409, 2008.
[36] T. Feng, *On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights*, Des. Codes Cryptogr., 62, 253-258, 2012.
[37] T. Feng and K. Momihara, *Evaluation of the weight distribution of a class of cyclic codes based on index 2 Gauss sums*, IEEE Trans. Inform. Theory, 59(9), 5980-5984, Sep. 2013.
[38] T. Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Math., 16(3), 209-232, 1976.
[39] T. Helleseth, *Some two-weight codes with composite parity-check polynomials*, IEEE Trans. Inform. Theory, 22, 631-632, 1976.
[40] T. Helleseth, *A note on the cross-correlation function between two binary maximal length linear sequences*, Discrete Math., 23(3), 301-307, 1978.
[41] T. Helleseth, J. Lahtonen, and P. Rosendahl, *On Niho type cross-correlation functions of m-sequences*, Finite Fields Appl., 13, 305-317, 2007.
[42] G. Hughes, *Constacyclic codes, cocycles and a $u+v \mid u-v$ construction*, IEEE Trans. Inform. Theory 46, 674-680, 2000.
[43] I. James, *Claude Elwood Shannon, 30 April 1916 - 24 February 2001*, Biographical Memoirs of Fellows of the Royal Society, 55, 257-265, 2009.
[44] T. Kasami, *The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes*, Inf. Control, 18(4), 369-394, 1971.
[45] R. G. Kelsch, D. H. Green, *Nonbinary negacyclic code which exceeds Berlekamp's $(p-1)/2$ bound*, Elec. Letters 7, 664-665, 1971.
[46] C. Li and Q. Yue, *Weight distribution of two classes of cyclic codes with respect to two distinct order elements*, IEEE Trans. Inform. Theory, 60(1), 296-303, Jan. 2014.
[47] C. Li, Q. Yue, and F. Li, *Weight distributions of cyclic codes with respect to pairwise coprime order elements*, Finite Fields Appl., 28, 94-114, 2014.
[48] C. Li, Q. Yue, and F. Li, *Hamming weights of the duals of cyclic codes with two zeros*, IEEE Trans. Inform. Theory, 60(7), 3895-3902, Jul. 2014.
[49] C. Li and Q. Yue, *Weight distributions of a class of cyclic codes from $\mathbb{F}_l$-conjugates*, submitted.
[50] C. Li, N. Li, T. Helleseth, and C. Ding, *The weight distributions of several classes of cyclic codes from APN monomials*, IEEE Trans. on Inform. Theory, 60(8), 4710-4721, Aug. 2014.
[51] N. Li, T. Helleseth, A. Kholosha, and X. Tang, *On the Walsh transform of a class of functions from Niho exponents*, IEEE Trans. Inform. Theory, 59(7), 4662-4667, Jul. 2013.
[52] S. Li, T. Feng, and G. Ge, *On the weight distribution of cyclic codes with Niho exponents*, IEEE Trans. Inform. Theory, 60(7), 3903-3912, Jul. 2014.
[53] S. Li, S. Hu, T. Feng, and G. Ge, *The weight distribution of a class of cyclic codes related to Hermitian*

forms graphs, IEEE Trans. on Inform. Theory, 59(5), 3064-3067, May 2013.
[54] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley Publishing Inc., 1983.
[55] J. Luo and K. Feng, *On the weight distribution of two classes of cyclic codes*, IEEE Trans. Inform. Theory, 54(12), 5332-5344, Dec. 2008.
[56] X. Liu and Y. Luo, *The weight distributions of some cyclic codes with three or four nonzeros over* $\mathbb{F}_3$, Des. Codes Cryptogr., 73(3), 747-768, 2013.
[57] Y. Liu, H. Yan, and C. Liu, *A class of six-weight cyclic codes and their weight distribution*, Des. Codes Cryptogr., Doi: 10.1007/s10623-014-9984-y, 2014.
[58] J. Luo and K. Feng, *Cyclic codes and sequences from generalized Coulter-Matthews function*, IEEE Trans. Inform. Theory, 54(12), 5345-5353, Dec. 2008.
[59] J. Luo, Y. Tang, and H. Wang, *Cyclic codes and sequences: the generalized Kasami case*, IEEE Trans. Inform. Theory, 56(5), 2130-2142, May 2010.
[60] C. Ma, L. Zeng, Y. Liu, D. Feng, and C. Ding, *The weight enumerator of a class of cyclic codes*, IEEE Trans. Inform. Theory, 57(1), 397-402, Jan. 2011.
[61] J. L. Massey, D. J. Costello, and J. Justesen, *Polynomial weights and code constructions*, IEEE Trans. Information Theory 19, 101-110, 1973.
[62] G. McGuire, *On three weights in cyclic codes with two zeros*, Finite Fields Appl., 10, 97-104, 2004.
[63] M. Moisio and K. Ranto, *Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros*, Finite Fields Appl. 13, 922-935, 2007.
[64] G. Myerson, *Period polynomials and Gauss sums for finite fields*, Acta Arith., 39, 251-264, 1981.
[65] Y. Niho, *Multivalued cross-correlation functions between two maximal linear recursive sequence*, Ph.D. dissertation, Univ. Southern Calif., Los Angeles, 1970.
[66] V. Pless, *Power moment identities on weight distributions in error-correcting codes*, Inf. Contr., 6, 147-152, 1962.
[67] E. Prange, *Cyclic error-correcting codes in two symbols*, TN-57-103, September 1957.
[68] E. Prange, *Some cyclic error-correcting codes with simple decoding algorithms*, TN-58-156, April 1958.
[69] E. Prange, *The use of coset equivalence in the analysis and decoding of group codes*, TN-59-164, 1959.
[70] E. Prange, *An algorithm for factoring* $x^n - 1$ *over a finite field*, TN-59-175, October 1959.
[71] E. Prange, *The use of information sets in decoding cyclic codes*, IEEE Trans. Inform. Theory 8, 85-89, 1962.
[72] R. M. Roth and G. Seroussi, *On cyclic MDS codes of length* q *over* $\mathbb{F}(q)$, IEEE Trans. Inform. Theory 32, 284-285, 1986.
[73] B. Schmidt and C. White, *All two-weight irreducible cyclic codes*, Finite Fields Appl., 8, 1-17, 2002.
[74] R. Schoof, *Families of curves and weight distribution of codes*, Bull. Amer. Math. Soc., 32(2), 171-183, 1995.
[75] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. 27 , 379-423, 623-656, 1948. Reprinted in: A mathematical theory of communication, (Eds. C.E. Shannon and W. Weaver), Univ. of Illinois Press, Urbana, IL, 1963.
[76] D. Stanton, *Three addition theorems for some q-Krawtchouk polynomials*, Geom. Dedicata, 10(1-4), 403-425, 1981.
[77] J. H. van Lint, *Repeated-root cyclic codes*, IEEE Trans. Inform. Theory 37, 343-345, 1991.
[78] G. Vega, *Two-weight classes cyclic codes constructed as the direct sum of two one-weight cyclic codes*, Finite Fields Appl., 14, 785-797, 2008.
[79] G. Vega, *The weight distribution of an extended class of reducible cyclic codes*, IEEE Trans. Inform. Theory, 58(7), 4862-4869, Jul. 2012.
[80] G. Vega and L. B. Morales, *A general description for the weight distribution of some reducible cyclic codes*, IEEE Trans. Inform. Theory, 59(9), 5994-6001, Sep. 2013.
[81] G. Vega and J. Wolfmann, *New classes of 2-weight cyclic codes*, Des. Codes Cryptogr., 42, 327-344, 2007.
[82] B. Wang, C. Tang, Y. Qi, Y. Yang, and M. Xu, *The weight distributions of cyclic codes and elliptic curves*, IEEE Trans. Inform. Theory, 58(12), 7253-7259, Dec. 2012.
[83] J. Wolfmann, *Negacyclic and cyclic codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45, 2527-2532, 1999.
[84] J. Wolfmann, *Are 2-weight projective cyclic codes irreducible?*, IEEE Trans. Inform. Theory, 51(2), 733-737, Feb. 2005.

[85] J. Wolfmann, *Projective two-weight irreducible cyclic and constacyclic codes*, Finite Fields Appl., 14, 351-360, 2008.
[86] M. Xiong, *The weight distributions of a class of cyclic codes*, Finite Fields Appl., 18, 933-945, 2012.
[87] M. Xiong, *The weight distributions of a class of cyclic codes II*, Des. Codes Cryptogr., 72(3), 511-528, 2012.
[88] M. Xiong, *The weight distributions of a class of cyclic codes III*, Finite Fields Appl., 21, 84-96, 2013.
[89] J. Yang, L. Xia, *Complete solving of explicit evaluation of Gauss sums in the index 2 case*, Sci. China Math., 53(9), 2525-2542, 2010.
[90] J. Yang, M. Xiong, C. Ding, and J. Luo, *Weight distribution of a class of cyclic codes with arbitrary number of zeros*, IEEE Trans. Inform. Theory, 59(9), 5985-5993, Sep. 2013.
[91] J. Yuan, C. Carlet, and C. Ding, *The weight distribution of a class of linear codes from perfect nonlinear functions*, IEEE Trans. Inform. Theory, 52(2), 712-717, Feb. 2006.
[92] X. Zeng, L. Hu, W. Jiang, Q. Yue, and X. Cao, *The weight distribution of a class of p-ary cyclic codes*, Finite Fields Appl., 16, 56-73, 2010.
[93] T. Zhang, S. Li, T. Feng, and G. Ge, *Some new results on the cross correlation of m-sequences*, IEEE Trans. Inform. Theory, 60(5), 3062-3068, May 2014.
[94] D. Zheng, X. Wang, X. Zeng, and L. Hu, *The weight distribution of a family of p-ary cyclic codes*, Des. Codes Cryptogr., Doi: 10.1007/s10623-013-9908-2, 2013.
[95] D. Zheng, X. Wang, X. Zeng, and L. Hu, *The weight distributions of two classes of p-ary cyclic codes*, Finite Fields Appl., 29, 202-224, 2014.
[96] Z. Zhou and C. Ding, *A class of three-weight cyclic codes*, Finite Fields Appli., 25, 79-93, Jan. 2014.
[97] Z. Zhou and C. Ding, *Seven classes of three-weight cyclic codes*, IEEE Trans. Commun., 61(10), 4120-4126, Oct. 2013.
[98] Z. Zhou, C. Ding, J. Luo, and A. Zhang, *A family of five-weight cyclic codes and their weight enumerators*, IEEE Trans. Inform. Theory, 59(10), 6674-6682, Oct. 2013.
[99] Z. Zhou, A. Zhang, C. Ding, and M. Xiong, *The weight enumerator of three families of cyclic codes*, IEEE Trans. Inform. Theory, 59(9), 6002-6009, Sep. 2013.