Des. Codes Cryptogr. (2016) 81:1–9
DOI 10.1007/s10623-015-0125-z

Two classes of cyclic codes and their weight enumerator

Haode Yan[1] · **Chunlei Liu**[1]

Received: 12 April 2015 / Revised: 16 July 2015 / Accepted: 24 July 2015 / Published online: 8 August 2015

Abstract Let p be an odd prime, and m, k and d be positive integers such that $2 \leq k \leq \frac{m+1}{2}$ and $\gcd(m, d) = 1.\pi$ is a primitive element of the finite field $\mathbb{F}_{p^m}$. The weight enumerator of cyclic codes over $\mathbb{F}_p$ whose duals have $2k$ zeros $\pi^{-(p^{jd}+1)/2}$ and $-\pi^{-(p^{jd}+1)/2}$($j = 0, 1, \ldots, k-1$) is determined in the present paper. The weight enumerator of cyclic codes over $\mathbb{F}_p$ whose duals have $2k-1$ zeros $\pi^{-(p^{(k-1)d}+1)/2}$, $\pi^{-(p^{jd}+1)/2}$ and $-\pi^{-(p^{jd}+1)/2}$($j = 0, 1, \ldots, k-2$) is also determined when $2 \nmid \frac{m}{gcd(m,k-1)}$ holds.

Keywords Cyclic code · Weight enumerator · Finite field

Mathematics Subject Classification 94B15 · 11T71

1 Introduction

Recall that an $[n, l, d]$ linear code $\mathcal{C}$ over the finite field $\mathbb{F}_p$ is a linear subspace of $\mathbb{F}_p^n$ with dimension l and minimum Hamming distance d, where p is a prime. Let A_i denote by the number of codewords in $\mathcal{C}$ with Hamming weight i in a code $\mathcal{C}$ of length n, the weight enumerator of $\mathcal{C}$ is defined by

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

The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the weight distribution of the code $\mathcal{C}$, which is a very important parameter of the code. For instance, the error correcting capability of a code

Communicated by T. Helleseth.

✉ Haode Yan
hdyan@sjtu.edu.cn

Chunlei Liu
clliu@sjtu.edu.cn

1 Department of Mathematics, Shanghai Jiaotong University, Shanghai 200240, China

is closely related to its weight distribution. In addition, the weight distribution of a code also allows the computation of the error probability of error detection and correction. Thus, it is important to study the weight distribution of a linear code, both in theory and applications.

An $[n, k]$ linear code $\mathcal{C}$ is called cyclic over $\mathbb{F}_p$ if for any $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, also $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. It is well-known that a linear code $\mathcal{C}$ in $\mathbb{F}_p^n$ is cyclic if and only if $\mathcal{C}$ is an ideal of the polynomial residue class ring $\mathbb{F}_p[x]/(x^n - 1)$. Since $\mathbb{F}_p[x]/(x^n - 1)$ is a principal ideal ring, every cyclic code corresponds to a principal ideal $(g(x))$ of the multiples of a polynomial $g(x)$ which is the monic polynomial of lowest degree in the ideal. This polynomial $g(x)$ is called the generator polynomial, and $h(x) = (x^n - 1)/g(x)$ is called the parity-check polynomial of the code $\mathcal{C}$. We also recall that a cyclic code is called irreducible if its parity-check polynomial is irreducible over $\mathbb{F}_p$, otherwise, it is called reducible. A cyclic code over $\mathbb{F}_p$ is said to have t zeros if all the zeros of the generator polynomial of the code form t conjugate classes, or equivalently, the generator polynomial has t irreducible factors over $\mathbb{F}_p$.

Cyclic codes have wide applications in both storage and communication systems. Moreover, cyclic codes are applied in association schemes [3] and secret schemes [4]. Therefore, determining the weight enumerator of a cyclic code is an important research object in coding theory. But the weight distribution is known for only a few special classes. For example, the weight distribution of some irreducible cyclic codes has been studied in [1,2,5,6,20]. For cyclic codes with two zeros, the weight distribution is known in special cases [7,8,10,12,18, 22,24,26]. Studies for other cyclic codes refer to [9,11,13,14,17,23,27,28,30,31].

Throughout this paper, let m, k and d be positive integers such that $2 \le k \le \frac{m+1}{2}$ and $\gcd(m, d) = 1$. Let p be an odd prime and π be a primitive element of the finite field $\mathbb{F}_{p^m}$. For $j = 0, 1, \ldots, k-1$, let $h_j(x)$ and $h_{-j}(x)$ be the minimal polynomials of $\pi^{-(p^{jd}+1)/2}$ and $-\pi^{-(p^{jd}+1)/2}$ over $\mathbb{F}_p$, respectively. It is easy to check that $h_{j_1}(x)$ and $h_{j_2}(x)$ are polynomials of degree m and are pairwise distinct, for $j_1, j_2 \in \{\pm 0, \pm 1, \ldots, \pm(k-1)\}$. The cyclic codes over $\mathbb{F}_p$ with parity-check polynomial $h_0(x)h_1(x)$ have been extensively studied in [4,16,21,25]. Zhou and Ding [29] proved that the cyclic codes over $\mathbb{F}_p$ with parity-check polynomial $h_{-0}(x)h_1(x)$ have three nonzero weights, and determined their weight distributions. In [15], it was proved that the cyclic codes over $\mathbb{F}_p$ with parity-check polynomial $h_0(x)h_{-0}(x)h_1(x)$ have six nonzero weights and their weight distributions were determined as well.

General cases are more interesting. Let $\mathcal{C}_{m,d,2k}$ and $\mathcal{C}_{m,d,2k-1}$ be the cyclic codes with parity-check polynomial $\prod_{j=0}^{k-1} h_j(x)h_{-j}(x)$ and $h_{k-1}(x)\prod_{j=0}^{k-2} h_j(x)h_{-j}(x)$, respectively. In this paper, the weight enumerator of the cyclic code $\mathcal{C}_{m,d,2k}$ is determined as following.

Theorem 1.1 *Let m, d and k be positive integers such that $2 \le k \le \frac{m+1}{2}$ and $(m, d) = 1$. Then $\mathcal{C}_{m,d,2k}$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, 2km, \frac{1}{2}(p-1)(p^{m-1} - p^{[\frac{m}{2}]-2+k})]$. Furthermore, the weight enumerator of $\mathcal{C}_{m,d,2k}$ is $(\alpha_k(z^{\frac{1}{2}}))^2$, where $\alpha_k(z)$ is determined in Theorem 2.1 (details in Sect. 2).*

If $2 \nmid \frac{m}{gcd(m,k-1)}$, the weight enumerator of the cyclic code $\mathcal{C}_{m,d,2k-1}$ is also determined as following.

Theorem 1.2 *Let m and d be positive integers such that $2 \nmid \frac{m}{gcd(m,k-1)}$ and $(m, d) = 1$, where k is a positive integer satisfying $3 \le k \le \frac{m+1}{2}$. Then $\mathcal{C}_{m,d,2k-1}$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, (2k-1)m, \frac{1}{2}(p-1)(p^{m-1} - p^{[\frac{m}{2}]-3+k})]$. Furthermore, the weight enumerator of $\mathcal{C}_{m,d,2k-1}$ is*

$$\left(\alpha_{k-1}\left(z^{\frac{1}{2}}\right)\right)^2 + \frac{1}{p^m-1}\left(\alpha_k\left(z^{\frac{1}{2}}\right) - \alpha_{k-1}\left(z^{\frac{1}{2}}\right)\right)^2,$$

where $\alpha_k(z)$ is determined in Theorem 2.1 (details in Sect. 2).

Remark $\mathcal{C}_{m,d,2k-1}$ in the case of $k = 2$ has been studied in [15], and the minimum distance has different expression between cases of $k = 2$ and $3 \leq k \leq \frac{m+1}{2}$, therefore, only the case of $3 \leq k \leq \frac{m+1}{2}$ is presented here.

2 Preliminaries

In this section, we will introduce a result by Kai-Uwe Schmidt [19]. We need the Gaussian binomial coefficients, which are defined by

$$\binom{n}{s}_q = \prod_{t=0}^{s-1}(q^n - q^t)/(q^s - q^t).$$

For $j = 0, 1, \ldots, k-1$, let $H_j(x)$ be the minimal polynomials of $\pi^{-(p^{jd}+1)}$ over $\mathbb{F}_p$, respectively. Let $\widetilde{\mathcal{C}}_{m,d,k}$ be the cyclic code over $\mathbb{F}_p$ with parity-check polynomial $\prod_{j=0}^{k-1} H_j(x)$. Then it can be expressed as

$$\widetilde{\mathcal{C}}_{m,d,k} = \left\{\mathbf{c}_{(u_0,u_1,\ldots,u_{k-1})} : (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_{p^m}^k\right\},$$

where

$$\mathbf{c}_{(u_0,u_1,\ldots,u_{k-1})} = \left(Tr\left(\sum_{j=0}^{k-1} u_j \pi^{(p^{jd}+1)t}\right)\right)_{t=0}^{p^m-2},$$

and $Tr(\cdot)$ is the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. $\widetilde{\mathcal{C}}_{m,d,k}$ has length $p^m - 1$ and dimension km. Moreover, the weight enumerator of $\widetilde{\mathcal{C}}_{m,d,k}$, denoted by $\alpha_k(z)$, is determined. We have the following result.

Theorem 2.1 [19] *We have, $\alpha_k(z) = 1 + \sum_{i,\tau} a_{i,\tau} z^{w_{i,\tau}}$, where $m - 2k + 2 \leq i \leq m$, $\tau = 1$ or -1 and*

$$w_{i,\tau} = \begin{cases} p^{m-1}(p-1) & for \quad odd\ i, \\ \left(p^{m-1} - \tau\eta(-1)^{i/2} p^{m-i/2-1}\right)(p-1) & for \quad even\ i. \end{cases}$$

η is the quadratic character of $\mathbb{F}_p$. If m is odd,

$$a_{2u-1,\tau} = \frac{1}{2}\binom{\frac{m-1}{2}}{u-1}_{p^2} \sum_{j=0}^{k+u-\frac{m+3}{2}} (-1)^j p^{j(j-1)} \binom{u}{j}_{p^2} \left(p^{\left(k+u-j-\frac{m+1}{2}\right)m} - 1\right),$$

$$a_{2u,\tau} = \frac{1}{2}\left(p^{2u} + \tau\eta(-1)^u p^u\right)\binom{\frac{m-1}{2}}{u}_{p^2} \sum_{j=0}^{k+u-\frac{m+3}{2}} (-1)^j p^{j(j-1)} \binom{u}{j}_{p^2} \left(p^{(k+u-j-\frac{m+1}{2})m} - 1\right).$$

If m is even,

$$a_{2u-1,\tau}=\frac{1}{2}(p^{2u}-1)\binom{\frac{m}{2}}{u}_{p^2}\sum_{j=0}^{k+u-\frac{m+4}{2}}(-1)^j p^{j(j-1)}\binom{u-1}{j}_{p^2}p^{mk+2j-(m+1)(\frac{m+2}{2}+j-u)},$$

$$a_{2u,\tau}=\frac{1}{2}\binom{\frac{m}{2}}{u}_{p^2}\sum_{j=0}^{k+u-\frac{m+2}{2}}(-1)^j p^{j(j-1)}\binom{u}{j}_{p^2}\left(p^{mk+2j-(m+1)(\frac{m}{2}+j-u)}-1\right)$$
$$+\frac{\tau}{2}\eta(-1)^u p^u\binom{\frac{m}{2}}{u}_{p^2}\sum_{j=0}^{k+u-\frac{m+2}{2}}(-1)^j p^{j(j-1)}\binom{u}{j}_{p^2}\left(p^{m(k-1)-(m-1)(\frac{m}{2}+j-u)}-1\right).$$

3 The weight enumerator of $\mathcal{C}_{m,d,2k}$

Theorem 1.1 can be proved as following. Obviously, $\mathcal{C}_{m,d,2k}$ has length p^m-1 and dimension $2km$. Also, it can be expressed as

$$\mathcal{C}_{m,d,2k}=\left\{\mathbf{c}_{(a_0,a_1,\ldots,a_{k-1},b_0,b_1,\ldots,b_{k-1})}:a_0,\ldots,a_{k-1},b_0,\ldots,b_{k-1}\in\mathbb{F}_{p^m}\right\},$$

where

$$\mathbf{c}_{(a_0,a_1,\ldots,a_{k-1},b_0,b_1,\ldots,b_{k-1})}=\left(Tr\left(\sum_{j=0}^{k-1}\left(a_j\left(\pi^{(p^{jd}+1)/2}\right)^t+b_j\left(-\pi^{(p^{jd}+1)/2}\right)^t\right)\right)\right)_{t=0}^{p^m-2}.$$

Let λ be a fixed nonsquare element in $\mathbb{F}_{p^m}$.

The weight of the codeword $\mathbf{c}_{(a_0,a_1,\ldots,a_{k-1},b_0,b_1,\ldots,b_{k-1})}=(c_0,c_1,\ldots,c_{p^m-2})$ in $\mathcal{C}_{m,d,2k}$ is given by

$$\begin{aligned}
&W(\mathbf{c}_{(a_0,a_1,\ldots,a_{k-1},b_0,b_1,\ldots,b_{k-1})})\\
&=\#\{0\le t\le p^m-2:c_t\ne 0\}\\
&=\#\left\{0\le t\le p^m-2,t\ even:Tr\left(\sum_{j=0}^{k-1}(a_j+b_j)(\pi^t)^{(p^{jd}+1)/2}\right)\ne 0\right\}\\
&\quad+\#\left\{0\le t\le p^m-2,t\ odd:Tr\left(\sum_{j=0}^{k-1}(a_j-b_j)(\pi^t)^{(p^{jd}+1)/2}\right)\ne 0\right\}\\
&=\frac{1}{2}\left(\#\left\{0\le t\le p^m-2:Tr\left(\sum_{j=0}^{k-1}(a_j+b_j)(\pi^t)^{p^{jd}+1}\right)\ne 0\right\}\right.\\
&\quad\left.+\#\left\{0\le t\le p^m-2:Tr\left(\sum_{j=0}^{k-1}(a_j-b_j)\lambda^{(p^{jd}+1)/2}(\pi^t)^{p^{jd}+1}\right)\ne 0\right\}\right)\\
&=\frac{1}{2}\left(W\left(\mathbf{c}_{(a_0+b_0,a_1+b_1,\ldots,a_{k-1}+b_{k-1})}\right)\right.\\
&\quad\left.+W\left(\mathbf{c}_{\left((a_0-b_0)\lambda,(a_1-b_1)\lambda^{(p^d+1)/2},\ldots,(a_{k-1}-b_{k-1})\lambda^{(p^{(k-1)d}+1)/2}\right)}\right)\right),
\end{aligned}$$

where $\mathbf{c}_{(a_0+b_0,a_1+b_1,\ldots,a_{k-1}+b_{k-1})}$ and $\mathbf{c}_{((a_0-b_0)\lambda,(a_1-b_1)\lambda^{(p^d+1)/2},\ldots,(a_{k-1}-b_{k-1})\lambda^{(p^{(k-1)d}+1)/2})}$ are codewords in $\widetilde{\mathcal{C}}_{m,d,k}$. Notice that the map $\mathcal{C}_{m,d,2k}\to\widetilde{\mathcal{C}}_{m,d,k}\times\widetilde{\mathcal{C}}_{m,d,k}$,

$$(a_0,\ldots,b_{k-1})\mapsto\left((a_0+b_0,\ldots,a_{k-1}+b_{k-1}),\left((a_0-b_0)\lambda,\ldots,(a_{k-1}-b_{k-1})\lambda^{(p^{(k-1)d}+1)/2}\right)\right)$$

is bijective, we conclude that the weight enumerator of the code $\mathcal{C}_{m,d,2k}$ is

$$\sum_{a\in\mathcal{C}}\sum_{b\in\mathcal{C}}z^{(W(a)+W(b))/2},$$

where $\mathcal{C}=\widetilde{\mathcal{C}}_{m,d,k}$. This is easily seen to be equal to

$$\left(\sum_{c\in\mathcal{C}}z^{W(c)/2}\right)^2,$$

which is $(\alpha_k\left(z^{\frac{1}{2}}\right))^2$. Theorem 1.1 is proved.

4 The weight enumerator of $\mathcal{C}_{m,d,2k-1}$ for odd $\frac{m}{gcd(m,k-1)}$

Let $\mathcal{C}_{m,d,2k-1}$ be the cyclic code defined in Sect. 1. We shall prove Theorem 1.2 in this section, assuming $2\nmid\frac{m}{gcd(m,k-1)}$. There is a partition of cyclic code $\widetilde{\mathcal{C}}_{m,d,k}$

$$\widetilde{\mathcal{C}}_{m,d,k}=\bigcup_{v\in\mathbb{F}_{p^m}}\mathcal{C}_{k-1,v}.$$

For each $v\in\mathbb{F}_{p^m}$, $\mathcal{C}_{k-1,v}$ is a set of codewords and it can be expressed as

$$\mathcal{C}_{k-1,v}=\{\mathbf{c}_{(u_0,u_1,\ldots,u_{k-2},v)}:u_0,u_1,\ldots,u_{k-2}\in\mathbb{F}_{p^m}\},$$

where

$$\mathbf{c}_{(u_0,u_1,\ldots,u_{k-2},v)}=\left(Tr\left(\left(\sum_{j=0}^{k-2}u_j\pi^{(p^{jd}+1)t}\right)+v\pi^{(p^{(k-1)d}+1)t}\right)\right)_{t=0}^{p^m-2}.$$

We denote $\alpha_{k-1,v}(z)$ by the weight enumerator of $\mathcal{C}_{k-1,v}$. Notice $\mathcal{C}_{k-1,0}=\widetilde{\mathcal{C}}_{m,d,k-1}$, hence $\alpha_{k-1,0}(z)=\alpha_{k-1}(z)$. If $v\neq 0$, we have the following lemma.

Lemma 4.1 *For any $v\in\mathbb{F}^*_{p^m}$, we have $\alpha_{k-1,v}(z)=\alpha_{k-1,1}(z)$.*

Proof Let ζ_p be a primitive pth root of unity. In terms of exponential sums, the weight of the codeword $\mathbf{c}_{(u_0,u_1,\ldots,u_{k-2},v)}=(c_0,c_1,\ldots,c_{p^m-2})$ in $\mathcal{C}_{k-1,v}$ is given by

$$\begin{aligned}W(\mathbf{c}_{(u_0,u_1,\ldots,u_{k-2},v)})&=\#\{0\le t\le p^m-2:c_t\neq 0\}\\&=p^m-1-\frac{1}{p}\sum_{t=0}^{p^m-2}\sum_{y\in\mathbb{F}_p}\zeta_p^{yc_t}\\&=p^m-1-\frac{1}{p}\sum_{t=0}^{p^m-2}\sum_{y\in\mathbb{F}_p}\zeta_p^{yTr\left(\left(\sum_{j=0}^{k-2}u_j\pi^{(p^{jd}+1)t}\right)+v\pi^{\left(p^{(k-1)d}+1\right)t}\right)}\\&=p^m-1-\frac{1}{p}\sum_{y\in\mathbb{F}_p}\sum_{x\in\mathbb{F}^*_{p^m}}\zeta_p^{yTr\left(\left(\sum_{j=0}^{k-2}u_jx^{p^{jd}+1}\right)+vx^{p^{(k-1)d}+1}\right)}\end{aligned}$$

Since $\frac{m}{gcd(m,k-1)}$ is odd, $\gcd(p^{(k-1)d}+1, p^m-1)=2$. Let γ be an element in $\mathbb{F}_{p^m}^*$, when γ traverses $\mathbb{F}_{p^m}^*$, $\gamma^{p^{(k-1)d}+1}$ traverses all square elements in $\mathbb{F}_{p^m}^*$. We conclude that there exist $\gamma \in \mathbb{F}_{p^m}^*$ and $\mu \in \mathbb{F}_p^*$ such that $v=\mu\gamma^{p^{(k-1)d}+1}$. Then we have

$$\begin{aligned}
&W(\mathbf{c}_{(u_0,u_1,\ldots,u_{k-2},v)})\\
&= p^m - 1 - \frac{1}{p}\sum_{y\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_{p^m}^*}\zeta_p^{yTr\left(\left(\sum_{j=0}^{k-2}u_j x^{p^{jd}+1}\right)+\mu(\gamma x)^{p^{(k-1)d}+1}\right)}\\
&= p^m - 1 - \frac{1}{p}\sum_{y\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_{p^m}^*}\zeta_p^{\mu yTr\left(\left(\sum_{j=0}^{k-2}\mu^{-1}u_j\gamma^{-(p^{jd}+1)}(\gamma x)^{p^{jd}+1}\right)+(\gamma x)^{p^{(k-1)d}+1}\right)}\\
&= p^m - 1 - \frac{1}{p}\sum_{y\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_{p^m}^*}\zeta_p^{yTr\left(\left(\sum_{j=0}^{k-2}\mu^{-1}u_j\gamma^{-(p^{jd}+1)}x^{p^{jd}+1}\right)+x^{p^{(k-1)d}+1}\right)}\\
&= W\left(\mathbf{c}_{(\mu^{-1}u_0\gamma^{-2},\mu^{-1}u_1\gamma^{-(p^d+1)},\ldots,\mu^{-1}u_{k-2}\gamma^{-(p^{(k-2)d}+1)},1)}\right).
\end{aligned}$$

Notice that the map $\mathcal{C}_{k-1,v}\to\mathcal{C}_{k-1,1}$,

$$\mathbf{c}_{(u_0,u_1,\ldots,u_{k-2},v)} \mapsto \mathbf{c}_{\left(\mu^{-1}u_0\gamma^{-2},\mu^{-1}u_1\gamma^{-(p^d+1)},\ldots,\mu^{-1}u_{k-2}\gamma^{-(p^{(k-2)d}+1)},1\right)}$$

is bijective, so we assert that the weight distributions of $\mathcal{C}_{k-1,v}$ and $\mathcal{C}_{k-1,1}$ are the same, which implies $\alpha_{k-1,v}(z)=\alpha_{k-1,1}(z)$ for any $v\in\mathbb{F}_{p^m}^*$. Lemma 4.1 now is proved. □

From the above lemma, one immediately deduces the following.

Lemma 4.2 *We have,*

$$\alpha_{k-1,v}(z)=\begin{cases}\alpha_{k-1}(z), & v=0,\\ \frac{1}{p^m-1}(\alpha_k(z)-\alpha_{k-1}(z)), & v\in\mathbb{F}_{p^m}^*.\end{cases}$$

Now we prove Theorem 1.2. Obviously, $\mathcal{C}_{m,d,2k-1}$ has length p^m-1 and dimension $(2k-1)m$. Moreover, it can be expressed as

$$\mathcal{C}_{m,d,2k-1}=\left\{\mathbf{c}_{(a_0,\ldots,a_{k-1},b_0,\ldots,b_{k-2})}: a_0,a_1,\ldots,a_{k-1},b_0,b_1,\ldots,b_{k-2}\in\mathbb{F}_{p^m}\right\},$$

where

$$\mathbf{c}_{(a_0,\ldots,a_{k-1},b_0,\ldots,b_{k-2})}=\left(Tr\left(\sum_{j=0}^{k-1}a_j\pi^{t(p^{jd}+1)/2}+\sum_{j=0}^{k-2}b_j\left(-\pi^{(p^{jd}+1)/2}\right)^t\right)\right)_{t=0}^{p^m-2}.$$

The weight of the codeword $\mathbf{c}_{(a_0,\ldots,a_{k-1},b_0,\ldots,b_{k-2})} = (c_0, c_1, \ldots, c_{p^m-2})$ in $\mathcal{C}_{m,d,2k-1}$ is given by

$$
\begin{aligned}
& W(\mathbf{c}_{(a_0,\ldots,a_{k-1},b_0,\ldots,b_{k-2})}) \\
&= \#\{0 \le t \le p^m-2 : c_t \ne 0\} \\
&= \#\left\{0 \le t \le p^m-2, t\ even : Tr\left(a_{k-1}(\pi^t)^{(p^{(k-1)d}+1)/2} + \sum_{j=0}^{k-2}(a_j+b_j)(\pi^t)^{(p^{jd}+1)/2}\right) \ne 0\right\} \\
&\quad + \#\left\{0 \le t \le p^m-2, t\ odd : Tr\left(a_{k-1}(\pi^t)^{(p^{(k-1)d}+1)/2} + \sum_{j=0}^{k-2}(a_j-b_j)(\pi^t)^{(p^{jd}+1)/2}\right) \ne 0\right\} \\
&= \frac{1}{2}\left(\#\left\{t : Tr\left(a_{k-1}(\pi^t)^{p^{(k-1)d}+1} + \sum_{j=0}^{k-2}(a_j+b_j)(\pi^t)^{p^{jd}+1}\right) \ne 0\right\}\right. \\
&\quad \left. + \#\left\{t : Tr\left(\lambda^{(p^{(k-1)d+1})/2}a_{k-1}(\pi^t)^{p^{(k-1)d}+1} + \sum_{j=0}^{k-2}(a_j-b_j)\lambda^{(p^{jd}+1)/2}(\pi^t)^{p^{jd}+1}\right) \ne 0\right\}\right) \\
&= \frac{1}{2}\left(W\left(\mathbf{c}_{(a_0+b_0,\ldots,a_{k-2}+b_{k-2},a_{k-1})}\right)\right. \\
&\quad \left. + W\left(\mathbf{c}_{((a_0-b_0)\lambda,\ldots,(a_{k-2}-b_{k-2})\lambda^{(p^{(k-2)d}+1)/2},a_{k-1}\lambda^{(p^{(k-1)d+1})/2})}\right)\right).
\end{aligned}
$$

$\mathbf{c}_{(a_0+b_0,\ldots,a_{k-2}+b_{k-2},a_{k-1})}$ and $\mathbf{c}_{((a_0-b_0)\lambda,\ldots,(a_{k-2}-b_{k-2})\lambda^{(p^{(k-2)d}+1)/2},a_{k-1}\lambda^{(p^{(k-1)d+1})/2})}$ are codewords in $\mathcal{C}_{k-1,a_{k-1}}$ and $\mathcal{C}_{k-1,a_{k-1}\lambda^{(p^{(k-1)d+1})/2}}$, respectively. By an argument similar to the proof of Theorem 1.1, the weight enumerator of $\mathcal{C}_{m,d,2k-1}$ is given by

$$
\sum_{a_{k-1}\in\mathbb{F}_{p^m}} \alpha_{k-1,a_{k-1}}\left(z^{\frac{1}{2}}\right)\alpha_{k-1,a_{k-1}\lambda^{(p^{(k-1)d+1})/2}}\left(z^{\frac{1}{2}}\right).
$$

By Lemma 4.2, Theorem 1.2 now follows.

5 Concluding remarks

In this paper, the weight enumerator of cyclic code $\mathcal{C}_{m,d,2k}$ is completely determined when $(m,d)=1$. The weight enumerator of cyclic code $\mathcal{C}_{m,d,2k-1}$ is also determined under the condition $(m,d)=1$ and $2 \nmid \frac{m}{gcd(m,k-1)}$. Moreover, when $(m,d)=e$, the weight enumerator of $\mathcal{C}_{m,d,2k}$ and $\mathcal{C}_{m,d,2k-1}$ are also determined as following. Since the proof is similar to that of Theorems 1.1 or 1.2, we omit the details.

Theorem 5.1 *Let m and d be positive integers such that $(m,d)=e$. Let k be a positive integer satisfying $2 \le k \le \frac{m+e}{2e}$. Then $\mathcal{C}_{m,d,2k}$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m-1, \frac{2km}{e}, \frac{1}{2}(p^e-1)(p^{m-e}-p^{e([\frac{m}{2e}]-2+k)})]$. Furthermore, the weight enumerator of $\mathcal{C}_{m,d,2k}$ is $(\beta_k(z^{\frac{1}{2}}))^2$, where $\beta_k(z)$ is the weight enumerator of $\widetilde{\mathcal{C}}_{m,d,k}$, which can be deduced from [19].*

Theorem 5.2 *Let m and d be positive integers such that $(m,d)=e$ and $2 \nmid \frac{\frac{m}{e}}{gcd(\frac{m}{e},k-1)}$, where k is a positive integer satisfying $2 \le k \le \frac{m+e}{2e}$. Then $\mathcal{C}_{m,d,3}$ is a cyclic code over $\mathbb{F}_{p^e}$ with parameters $[p^m-1, \frac{3m}{e}, \frac{1}{2}(p^e-1)p^{m-e}]$ and $\mathcal{C}_{m,d,2k-1}$ is a cyclic code over $\mathbb{F}_{p^e}$*

with parameters $[p^m - 1, \frac{(2k-1)m}{e}, \frac{1}{2}(p^e - 1)(p^{m-e} - p^{e([\frac{m}{2e}]-3+k)})]$ *when* $3 \leq k \leq \frac{m+e}{2e}$. *Furthermore, the weight enumerator of* $\mathcal{C}_{m,d,2k-1}$ *is*

$$\left(\beta_{k-1}\left(z^{\frac{1}{2}}\right)\right)^2 + \frac{1}{p^m - 1}\left(\beta_k\left(z^{\frac{1}{2}}\right) - \beta_{k-1}\left(z^{\frac{1}{2}}\right)\right)^2,$$

where $\beta_k(z)$ *is the weight enumerator of* $\widetilde{\mathcal{C}}_{m,d,k}$, *which can be deduced from* [19].

Acknowledgments The authors are grateful to the referees for their careful reading of the original version of this paper, their detailed comments and suggestions, which have much improved the quality of this paper.

References

1. Baumert L.D., McEliece R.J.: Weights of irreducible cyclic codes. Inf. Control. **20**(2), 158–175 (1972).
2. Baumert L.D., Mykkeltveit J.: Weight distribution of some irreducible cyclic codes. DSN Program Rep. **16**, 128–131 (1973)
3. Calderbank A.R., Goethals J.M.: Three-weight codes and association schemes. Philips J. Res. **39**, 143–152 (1984).
4. Carlet C., Ding C., Yuan J.: Linear codes from highly nonlinear functions and their secret sharing schemes. IEEE Trans. Inf. Theory **51**(6), 2089–2102 (2005).
5. Ding C.: The weight distribution of some irreducible cyclic codes. IEEE Trans. Inf. Theory **55**(3), 955–960 (2009).
6. Ding C., Yang J.: Hamming weights in irreducible cyclic codes. Discret. Math. **313**(4), 434–446 (2013).
7. Ding C., Liu Y., Ma C., Zeng L.: The weight distributions of the duals of cyclic codes with two zeros. IEEE Trans. Inf. Theory **57**(12), 8000–8006 (2011).
8. Feng T.: 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).
9. Feng K., Luo J.: Weight distribution of some reducible cyclic codes. Finite Fields Appl. **14**(2), 390–409 (2008).
10. Feng T., Momihara K.: Evaluation of the weight distribution of a class of cyclic codes based on index 2 Gauss sums. IEEE Trans. Inf. Theory **59**(9), 5980–5984 (2013).
11. Feng T., Leung K., Xiang Q.: Binary cyclic codes with two primitive nonzeros. Sci. China Math. **56**(7), 1403–1412 (2012).
12. Li C., Yue Q.: Weight distributions of two classes of cyclic codes with respect to two distinct order elements. IEEE Trans. Inf. Theory **60**(1), 296–303 (2014).
13. Li C., Li N., Helleseth T., Ding C.: The weight distributions of several classes of cyclic codes from APN monomials. IEEE Trans. Inf. Theory **60**(8), 4710–4721 (2014).
14. Liu Y., Yan H.: A class of five-weight cyclic codes and their weight distribution. Des. Codes Cryptogr. (2015). doi:10.1007/s10623-015-0056-8.
15. Liu Y., Yan H., Liu C.: A class of six-weight cyclic codes and their weight distribution. Des. Codes Cryptogr. (2014). doi:10.1007/s10623-014-9984-y.
16. Luo J., Feng K.: Cyclic codes and sequences form generalized Coulter-Matthews function. IEEE Trans. Inf. Theory **54**(12), 5345–5353 (2008).
17. Luo J., Feng K.: On the weight distribution of two classes of cyclic codes. IEEE Trans. Inf. Theory **54**(12), 5332–5344 (2008).
18. Ma C., Zeng L., Liu Y., Feng D., Ding C.: The weight enumerator of a class of cyclic codes. IEEE Trans. Inf. Theory **57**(1), 397–402 (2011).
19. Schmidt K.: Symmetric bilinear forms over finite fields with applications to coding theory, arXiv:1410.7184 (2014).
20. Sharma A., Bakshi G.: The weight distribution of some irreducible cyclic codes. Finite Fields Appl. **18**(1), 144–159 (2012).
21. Trachtenberg H.M.: On the crosscorrelation functions of maximal linear recurring sequences. Ph.D. Dissertation, University of Southern California, Los Angels (1970).
22. Vega G.: The weight distribution of an extended class of reducible cyclic codes. IEEE Trans. Inf. Theory **58**(7), 4862–4869 (2012).
23. Wang B., Tang C., Qi Y., Yang Y., Xu M.: The weight distributions of cyclic codes and elliptic curves. IEEE Trans. Inf. Theory **58**(12), 7253–7259 (2012).

24. Xiong M.: The weight distributions of a class of cyclic codes. Finite Fields Appl. **18**(5), 933–945 (2012).
25. Yang J., Xiong M., Ding C., Luo J.: Weight distribution of a class of cyclic codes with arbitrary number of zeros. IEEE Trans. Inf. Theory **59**(9), 5985–5993 (2013).
26. Yuan J., Carlet C., Ding C.: The weight distribution of a class of linear codes from perfect nonlinear functions. IEEE Trans. Inf. Theory **52**(2), 712–717 (2006).
27. Zeng X., Hu L., Jiang W., Yue Q., Cao X.: The weight distribution of a class of p-ary cyclic codes. Finite Fields Appl. **16**(1), 56–73 (2010).
28. Zheng D., Wang X., Zeng X., Hu L.: The weight distribution of a family of p-ary cyclic codes. Des. Codes Cryptogr. **75**(2), 263–275 (2015).
29. Zhou Z., Ding C.: A class of three-weight cyclic codes. Finite Fields Appl. **25**, 79–93 (2014).
30. Zhou Z., Ding C., Luo J., Zhang A.: A family of five-weight cyclic codes and their weight enumerators. IEEE Trans. Inf. Theory **59**(10), 6674–6682 (2013).
31. Zhu X., Yue Q., Hu L.: Weight distributions of cyclic codes of length l^m. Finite Fields Appl. **31**, 241–257 (2015).