AAECC (2019) 30:93–106
https://doi.org/10.1007/s00200-018-0361-3

ORIGINAL PAPER

Several classes of binary linear codes and their weight enumerators

Fei Li[1] · Yang Yan[2] · Qiuyan Wang[3] · Tongjiang Yan[4]

Received: 30 July 2017 / Revised: 19 May 2018 / Accepted: 25 May 2018 /
Published online: 29 May 2018

Abstract In the past decades, linear codes with a few weights have been extensively studied for their applications in space communication, data storage and cryptography etc. We construct several classes of binary linear codes and determine their weight distributions. Most of these codes can be used in secret sharing schemes.

Keywords Binary linear code · Weight distribution · Secret sharing

Mathematics Subject Classification 94B05 · 94A62 · 11T71

This research is supported by National Natural Science Foundation of China (61602342).

✉ Fei Li
cczxlf@163.com

✉ Qiuyan Wang
wangyan198801@163.com

Yang Yan
yanyang9021@iie.ac.cn

Tongjiang Yan
yantoji@163.com

1 Faculty of School of Statistics and Applied Mathematics, Anhui University of Finance and Economics, Bengbu 233030, Anhui, China

2 Faculty of National Engineering Laboratory for Information Security Technologies, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, China

3 Faculty of School of Computer Science and Software Engineering, Tianjin Polytechnic University, Tianjin 300387, China

4 Faculty of College of Science, China University of Petroleum, Qingdao 266580, China

1 Introduction

Throughout this paper, let $q = 2^m$ for a positive integer m. Let $\mathbb{F}_q$ denote the finite field with q elements and g be a generator of $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$.

Let $\mathbb{F}_2^n$ denote the vector space of all n-tuples over the binary field $\mathbb{F}_2$. A binary code C of length n is a subset of $\mathbb{F}_2^n$. Usually, the vectors in C are called codewords of C. For any codewords $\mathbf{x}$ and $\mathbf{y}$ in C, the Hamming distance $d(\mathbf{x}, \mathbf{y})$ is defined as the number of coordinates in which $\mathbf{x}$ and $\mathbf{y}$ differ. The minimum distance of a code C is the smallest distance between distinct codewords. An $[n, k, d]$ binary linear code C is defined as a k-dimensional subspace of $\mathbb{F}_2^n$ with minimum (Hamming) distance d.

For a codeword $\mathbf{c} \in C$, the (Hamming) weight $wt(\mathbf{c})$ is the number of nonzero coordinates in $\mathbf{c}$. We use A_i to denote the number of codewords of weight i in C. Then $(1, A_1, \ldots, A_n)$ is called the weight distribution of C, and the weight enumerator is defined as the polynomial $1 + A_1 x + A_2 x^2 + \cdots + A_n x^n$. If the number of nonzero A_i $(1 \leq i \leq n)$ equals t, then C is called a t-weight code. The reader is referred to [23] for the general theory of linear codes.

The weight distribution is an important research topic in coding theory, as it contains crucial information for computing the probability of error correction and detection. A great deal of researchers are devoted to constructing and determining specific linear codes [6,15,17,26,29,30,33]. The weight distribution of Reed–Solomon codes was determined by Blake [1] and Kith [24]. A survey of the Hamming weights of irreducible cyclic codes was given by Ding and Yang in [16]. The weight distributions of reducible cyclic codes can be found in [13,19–21,25,35].

Recently, in [9,14], Ding proposed a generic construction of linear codes as follows.

Let $D = \{d_1, d_2, \ldots, d_n\} \subseteq \mathbb{F}_q^*$ and Tr denote the absolute trace function from $\mathbb{F}_q$ onto its prime subfield $\mathbb{F}_p$. A linear code C_D of length n can be constructed by

$$C_D = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) : x \in \mathbb{F}_q\}.$$

Here and hereafter D is called the defining set of C_D. This method has been widely used in the literature to acquire linear codes with a few weights [8,10–12,18,31,32,34,37–39].

Choosing the defining set D is an important and interesting problem. Several kinds of defining sets were discussed in [9]. For example, D can optionally be the preimage of quadratic forms over $\mathbb{F}_q$ for odd characteristic p [33,34]. Using the theory of quadratic forms, the authors of [33,34] determined the weight distributions.

Motivated by the work in [9] and [10], for a subset D of $\mathbb{F}_q^*$, we can construct a class of linear codes $\overline{C}_D$ by the image (multiset) of D under a function f over $\mathbb{F}_q$. Namely, we define $\overline{C}_D$ as

$$\overline{C}_D = \left\{(\mathrm{Tr}\,(xf(d)))_{d \in D} : x \in \mathbb{F}_q\right\}. \tag{1}$$

In the paper, we choose $f(x) = x^{2^h+1}$, where $h < m$ is a positive factor of m. Note that f is a quadratic form over $\mathbb{F}_q$.

Table 1 The weight distribution of the codes of Theorem 1

Weight w	Multiplicity A
0	1
2^{m-2}	$2^m - 1 - 2^{m-h}$
$2^{m-2} - 2^{\frac{m+h-4}{2}}$	$2^{m-h-1} + (-1)^a 2^{\frac{m-h-2}{2}}$
$2^{m-2} + 2^{\frac{m+h-4}{2}}$	$2^{m-h-1} - (-1)^a 2^{\frac{m-h-2}{2}}$

Table 2 The weight distribution of the codes of Corollary 1

Weight w	Multiplicity A
0	1
2^{m-1}	1
2^{m-2}	$2^{m+1} - 2 - 2^{m-h+1}$
$2^{m-2} - 2^{\frac{m+h-4}{2}}$	2^{m-h}
$2^{m-2} + 2^{\frac{m+h-4}{2}}$	2^{m-h}

Generally speaking, the theory and results of quadratic forms on a finite field with an odd characteristic cannot be easily extended to those of quadratic forms on a finite field with characteristic 2. We shall employ exponential sums to investigate the weight distributions of the following two classes of binary linear codes $\overline{C}_D$ with

$$D = D_a = \{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = a\},\ a \in \mathbb{F}_2, \tag{2}$$

$$D = \mathbb{F}_q^*. \tag{3}$$

Naturally, a generalization of the code $\overline{C}_D$ is defined as

$$\overline{C}'_D = \left\{ \left(\mathrm{Tr}\left(x d^{2^h+1} + u \right) \right)_{d \in D} : u \in \mathbb{F}_2,\ x \in \mathbb{F}_q \right\}. \tag{4}$$

The weight distributions of linear codes $\overline{C}_{D_a}$ and $\overline{C}'_{D_a}$ are then settled and the main results are listed as follows.

Theorem 1 *Let m/h be odd. Then, the code $\overline{C}_{D_a}$ of* (2) *is a $[2^{m-1} - 1 + a, m]$ binary linear code with the weight distribution in Table 1.*

Corollary 1 *Let m/h be odd. Then, the code $\overline{C}'_{D_1}$ defined in* (4) *is a $[2^{m-1}, m+1]$ binary linear code with the weight distribution in Table 2.*

Corollary 2 *Let m/h be odd. Then, the code $\overline{C}'_{D_0}$ defined in* (4) *is a $[2^{m-1} - 1, m+1]$ binary linear code with the weight distribution in Table 3.*

The above theorem presents the parameters of $\overline{C}_{D_a}$ $(a = 0, 1)$ for the case in which $m/h \equiv 1 \pmod 2$. Next, we assume m/h is even and $m = 2e$ for a positive integer $e > 1$. In this case, the parameters of $\overline{C}_{D_a}$ $(a = 0, 1)$ are given in the two theorems below.

Table 3 The weight distribution of the codes of Corollary 2

Weight w	Multiplicity A
0	1
$2^{m-1}-1$	1
2^{m-2}	2^m-1-2^{m-h}
$2^{m-2}-1$	2^m-1-2^{m-h}
$2^{m-2}-2^{\frac{m+h-4}{2}}$	$2^{m-h-1}+2^{\frac{m-h-2}{2}}$
$2^{m-2}+2^{\frac{m+h-4}{2}}-1$	$2^{m-h-1}+2^{\frac{m-h-2}{2}}$
$2^{m-2}+2^{\frac{m+h-4}{2}}$	$2^{m-h-1}-2^{\frac{m-h-2}{2}}$
$2^{m-2}-2^{\frac{m+h-4}{2}}-1$	$2^{m-h-1}-2^{\frac{m-h-2}{2}}$

Table 4 The weight distribution of the codes of Theorem 2

Weight w	Multiplicity A
0	1
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e+h-1}$	$\frac{2^{m-2h-1}-1-(-1)^{\frac{e}{h}}2^{e-h-1}}{2^h+1}$
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e+h-2}$	$(2^h-1)2^{m-2h}$
2^{m-2}	$2^{m-1}-(-1)^{\frac{e}{h}}(2^h-1)(2^{m-2h-1}+2^{e-h-1})$
$2^{m-2}-(-1)^{\frac{e}{h}}2^{e-1}$	$\frac{2^{m-1}(2^h+2^{-2h}-1)-2^h+(-1)^{\frac{e}{h}}2^{e-1}(2^h+2^e-2^{e-2h})}{2^h+1}$

Theorem 2 *Let m/h be even and $m/h > 2$. Then, the code $\overline{C}_{D_0}$ of (2) is a $[2^{m-1}-1, m]$ binary linear code with the weight distribution in Table 4.*

Corollary 3 *Let m/h be even. Then, the code $\overline{C}'_{D_0}$ defined in (4) is a $[2^{m-1}-1, m+1]$ binary linear code with the weight distribution in Table 5.*

Theorem 3 *Let m/h be even and $m/h > 2$. Then, the code $\overline{C}_{D_1}$ of (2) is a $[2^{m-1}, m]$ binary linear code with the weight distribution in Table 6.*

Corollary 4 *Let m/h be even. Then, the code $\overline{C}'_{D_1}$ defined in (4) is a $[2^{m-1}, m+1]$ binary linear code with the weight distribution in Table 7.*

Let $D = \mathbb{F}_q^*$. If m/h is odd, then $\gcd\left(2^h+1, 2^m-1\right) = 1$ (Lemma 2.1, [5]). So $f(x) = x^{2^h+1}$ is a permutation polynomial over $\mathbb{F}_q^*$. It is well known that $|\{x \in \mathbb{F}_q^* : \mathrm{Tr}(\alpha x) = 0\}| = 2^{m-1}-1$ for every $\alpha \in \mathbb{F}_q^*$. Therefore, we have that $\overline{C}_D$ of (3) is a constant-weight linear code with parameters $[2^m-1, m, 2^m-2^{m-1}]$. It is optimal by the Griesmer bound (Chapter 2, [23]) in this case. If $m/h > 2$ is even, the code $\overline{C}_D$ is a two-weight binary linear code, and the weight distribution of $\overline{C}_D$ is given in Theorem 4 below.

Table 5 The weight distribution of the codes of Corollary 3

Weight w	Multiplicity A
0	1
$2^{m-1}-1$	1
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e+h-1}$	$\frac{2^{m-2h-1}-1-(-1)^{\frac{e}{h}}2^{e-h-1}}{2^h+1}$
$2^{m-2}-(-1)^{\frac{e}{h}}2^{e+h-1}-1$	$\frac{2^{m-2h-1}-1-(-1)^{\frac{e}{h}}2^{e-h-1}}{2^h+1}$
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e+h-2}$	$(2^h-1)2^{m-2h}$
$2^{m-2}-(-1)^{\frac{e}{h}}2^{e+h-2}-1$	$(2^h-1)2^{m-2h}$
2^{m-2}	$2^{m-1}-(-1)^{\frac{e}{h}}(2^h-1)(2^{m-2h-1}+2^{e-h-1})$
$2^{m-2}-1$	$2^{m-1}-(-1)^{\frac{e}{h}}(2^h-1)(2^{m-2h-1}+2^{e-h-1})$
$2^{m-2}-(-1)^{\frac{e}{h}}2^{e-1}$	$\frac{2^{m-1}(2^h+2^{-2h}-1)-2^h+(-1)^{\frac{e}{h}}2^{e-1}(2^h+2^e-2^{e-2h})}{2^h+1}$
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e-1}-1$	$\frac{2^{m-1}(2^h+2^{-2h}-1)-2^h+(-1)^{\frac{e}{h}}2^{e-1}(2^h+2^e-2^{e-2h})}{2^h+1}$

Table 6 The weight distribution of the codes of Theorem 3

Weight w	Multiplicity A
0	1
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e+h-1}$	$\frac{2^{m-2h-1}+(-1)^{\frac{e}{h}}2^{e-h-1}}{2^h+1}$
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e+h-2}$	$(2^h-1)2^{m-2h}$
2^{m-2}	$2^{m-1}-1+(-1)^{\frac{e}{h}}2^{e-h-1}(2^h-1)-(2^h-1)2^{m-2h-1}$
$2^{m-2}-(-1)^{\frac{e}{h}}2^{e-1}$	$\frac{(2^e-(-1)^{\frac{e}{h}})2^{e+h-1}}{2^h+1}$

Theorem 4 *Let $m/h > 2$ be even and $D = \mathbb{F}_q^*$. Then the code $\overline{C}_D$ of* (3) *is a $[2^m-1, m]$ binary linear code with the weight distribution in Table 8.*

If m/h is even, we know $\gcd(2^h+1, 2^m-1) = 2^h+1$, i.e., $2^h+1 \mid 2^m-1$. Hence $f(x) = x^{2^h+1}$ is a (2^h+1)-to-1 function over $\mathbb{F}_q^*$ in the case that $m/h \equiv 0 \pmod 2$. This implies that a binary code can be punctured from the code $\overline{C}_D$ in Theorem 4.

Let $\overline{D} = \{x^{2^h+1} : x \in \mathbb{F}_q^*\}$ and

$$\overline{C}_{\overline{D}} = \left\{(\mathrm{Tr}(xd))_{d\in\overline{D}} : x \in \mathbb{F}_q\right\}. \tag{5}$$

Then the parameters of $\overline{C}_{\overline{D}}$ can easily be derived from those of the code $\overline{C}_D$ in Theorem 4, and are given in the following corollary.

Corollary 5 *Let $m/h > 2$ be even. Then the code $\overline{C}_{\overline{D}}$ is a $[(2^m-1)/(2^h+1), m]$ binary linear code with the weight distribution in Table 9.*

Table 7 The weight distribution of the codes of Corollary 4

Weight w	Multiplicity A
0	1
2^{m-1}	1
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e+h-1}$	$\frac{2^{m-2h-1}+(-1)^{\frac{e}{h}}2^{e-h-1}}{2^h+1}$
$2^{m-2}-(-1)^{\frac{e}{h}}2^{e+h-1}$	$\frac{2^{m-2h-1}+(-1)^{\frac{e}{h}}2^{e-h-1}}{2^h+1}$
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e+h-2}$	$(2^h-1)2^{m-2h}$
$2^{m-2}-(-1)^{\frac{e}{h}}2^{e+h-2}$	$(2^h-1)2^{m-2h}$
2^{m-2}	$2^m-2+(-1)^{\frac{e}{h}}2^{e-h}(2^h-1)-(2^h-1)2^{m-2h}$
$2^{m-2}-(-1)^{\frac{e}{h}}2^{e-1}$	$\frac{(2^e-(-1)^{\frac{e}{h}})2^{e+h-1}}{2^h+1}$
$2^{m-2}+(-1)^{\frac{e}{h}}2^{e-1}$	$\frac{(2^e-(-1)^{\frac{e}{h}})2^{e+h-1}}{2^h+1}$

Table 8 The weight distribution of the codes of Theorem 4

Weight w	Multiplicity A
0	1
$2^{m-1}-(-1)^{\frac{e}{h}}2^{e-1}$	$\frac{(2^m-1)2^h}{2^h+1}$
$2^{m-1}+(-1)^{\frac{e}{h}}2^{e+h-1}$	$\frac{2^m-1}{2^h+1}$

Table 9 The weight distribution of the codes of Corollary 5

Weight w	Multiplicity A
0	1
$\frac{2^{m-1}-(-1)^{\frac{e}{h}}2^{e-1}}{2^h+1}$	$\frac{(2^m-1)2^h}{2^h+1}$
$\frac{2^{m-1}+(-1)^{\frac{e}{h}}2^{e+h-1}}{2^h+1}$	$\frac{2^m-1}{2^h+1}$

Example 1 Let $(m,h)=(5,1)$. A Magma program shows that $\overline{C}_{D_0}$ has parameters $[15,5,6]$ and weight enumerator $1+10x^6+15x^8+6x^{10}$, while $\overline{C}_{D_1}$ has parameters $[16,5,6]$ and weight enumerator $1+6x^6+15x^8+10x^{10}$, which both agree with Theorem 1. Here $\overline{C}_{D_0}$ is almost optimal since the optimal one has parameters $[15,5,7]$.

Example 2 If $(m,h)=(6,1)$, a Magma program shows that $\overline{C}_{D_0}$ has parameters $[31,6,8]$ and weight enumerator $1+3x^8+16x^{12}+26x^{16}+18x^{20}$. If $(m,h)=(8,2)$, a Magma program shows that $\overline{C}_{D_0}$ has parameters $[127,8,56]$ and weight enumerator $1+108x^{56}+98x^{64}+48x^{80}+x^{96}$. Therefore, our experimental results here agree with Theorem 2. Note that the code $\overline{C}_{D_0}$ with parameters $[31,6,8]$ is far from being optimal, since an optimal $[31,6]$ code has minimum distance 15. And the code $\overline{C}_{D_1}$

with parameters [127, 8, 56] is close to an optimal code, since an optimal [127, 8] code has minimum distance 63.

Example 3 If $(m, h) = (6, 1)$, a Magma program shows that $\overline{C}_{D_1}$ has parameters [32, 6, 8] and weight enumerator $1+2x^8+16x^{12}+21x^{16}+24x^{20}$. If $(m, h) = (8, 2)$, a Magma program shows that $\overline{C}_{D_1}$ has parameters [128, 8, 56] and weight enumerator $1 + 96x^{56} + 109x^{64} + 48x^{80} + 2x^{96}$. Therefore, our experimental results here agree with Theorem 3.

Example 4 If $(m, h) = (8, 1)$, a Magma program shows that $\overline{C}_D$ has parameters [255, 8, 120] and weight enumerator $1 + 170x^{120} + 85x^{144}$. If $(m, h) = (8, 2)$, a Magma program shows that $\overline{C}_D$ has parameters [255, 8, 120] and weight enumerator $1 + 204x^{120} + 51x^{160}$. Therefore, our experimental results here agree with Theorem 4. Here the code $\overline{C}_{\overline{D}}$ in Corollary 5 in the two specific cases has parameters [85, 8, 40] and [51, 8, 24], respectively, both of which are optimal due to the Griesmer bound.

2 Preliminaries

In this section, we present some results on exponential sums, which will be needed in calculating the weight distributions of the codes of (2).

An additive character of $\mathbb{F}_q$ is a group homomorphism χ from $(\mathbb{F}_q, +)$ into the multiplicative group of complex numbers of absolute value 1, i.e., $\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in \mathbb{F}_q$. Each additive character over $\mathbb{F}_q$ can be given by

$$\chi_b(c) = (-1)^{\mathrm{Tr}(bc)} \text{ for all } c \in \mathbb{F}_q,$$

for some $b \in \mathbb{F}_q$. The additive character χ_0 is called *trivial*, whereas other characters χ_b with $b \in \mathbb{F}_q^*$ are called *nontrivial*. Among the additive characters of $\mathbb{F}_q$, we have the *canonical additive character* χ_1 defined by $\chi_1(c) = (-1)^{\mathrm{Tr}(c)}$ for all $c \in \mathbb{F}_q$. See [27] for more information about characters over finite fields.

Define the exponential sum

$$S_h(a, b) = \sum_{x \in \mathbb{F}_q} \chi_1\left(ax^{2^h+1} + bx\right),$$

where $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, and h is a proper positive divisor of m. In general, to evaluate an exponential sum over a finite field is challenging. So far it has been determined only in certain special cases [2–5,20,22]. The following lemmas present the values of $S_h(a, b)$.

Lemma 1 (Theorem 4.1, [5]) *If m/h is odd, then $\sum_{x \in \mathbb{F}_q} \chi_1\left(ax^{2^h+1}\right) = 0$ for each $a \in \mathbb{F}_q^*$.*

Lemma 2 (Theorem 4.2, [5]) *Let $b \in \mathbb{F}_q^*$ and suppose m/h is odd. Then, $S_h(a, b) = S_h(1, bc^{-1})$, where $c \in \mathbb{F}_q^*$ is the unique element satisfying $c^{2^h+1} = a$. Further, we have*

$$S_h(1,b)=\begin{cases}0, & \text{if } \mathrm{Tr}_h(b)\neq 1,\\ \pm 2^{\frac{m+h}{2}}, & \text{if } \mathrm{Tr}_h(b)=1,\end{cases}$$

where and hereafter Tr_h *is the trace function from* $\mathbb{F}_q$ *to* $\mathbb{F}_{2^h}$.

Lemma 3 (Theorem 5.2, [5]) *Let* m/h *be even and* $m=2e$ *for some integer* e. *Then,*

$$S_h(a,0)=\begin{cases}(-1)^{\frac{e}{h}}2^e, & \text{if } a\neq g^{t(2^h+1)} \text{ for any integer } t,\\ -(-1)^{\frac{e}{h}}2^{e+h}, & \text{if } a=g^{t(2^h+1)} \text{ for some integer } t,\end{cases}$$

where g is a generator of $\mathbb{F}_q^*$.

Lemma 4 (Theorem 5.3, [5]) *Let* $b\in\mathbb{F}_q^*$ *and suppose* m/h *is even such that* $m=2e$ *for some integer* e. *Let* $f(x)=a^{2^h}x^{2^{2h}}+ax\in\mathbb{F}_q[x]$. *There are two cases.*

1. *If* $a\neq g^{t(2^h+1)}$ *for any integer* t, *then* f *is a permutation polynomial of* $\mathbb{F}_q$. *Let* x_0 *be the unique element satisfying* $f(x)=b^{2^h}$. *Then,*

$$S_h(a,b)=(-1)^{\frac{e}{h}}2^e\chi_1\left(ax_0^{2^h+1}\right).$$

2. *If* $a=g^{t(2^h+1)}$, *then* $S_h(a,b)=0$ *unless the equation* $f(x)=b^{2^h}$ *is solvable. If the equation is solvable, with solution* x_0 *say, then,*

$$S_h(a,b)=\begin{cases}-(-1)^{\frac{e}{h}}2^{e+h}\chi_1\left(ax_0^{2^h+1}\right), & \text{if } \mathrm{Tr}_h(a)=0,\\ (-1)^{\frac{e}{h}}2^e\chi_1\left(ax_0^{2^h+1}\right), & \text{if } \mathrm{Tr}_h(a)\neq 0.\end{cases}$$

Lemma 5 (Theorem 3.1, [5]) *Let* g *be a primitive element of* $\mathbb{F}_q$. *For any* $a\in\mathbb{F}_q^*$, *consider the equation* $a^{2^h}x^{2^{2h}}+ax=0$ *over* $\mathbb{F}_q$.

1. *If* m/h *is odd, then there are* 2^h *solutions to this equation for any choice of* $a\in\mathbb{F}_q^*$.
2. *If* m/h *is even, then there are two possible cases. If* $a=g^{t(2^h+1)}$ *for some* t, *then there are* 2^{2h} *solutions to this equation. If* $a\neq g^{t(2^h+1)}$ *for any* t, *then there exists one solution only,* $x=0$.

3 Proofs

We follow the notation from Sect. 2 above. In this section, we determine the length of the code $\overline{C}_{D_a}$ $(a=0,1)$ of (2) and provide a formula for the weight of a codeword $\mathbf{c}_b$ $(b\in\mathbb{F}_q^*)$ in $\overline{C}_{D_a}$ $(a=0,1)$. We also provide the proofs of the presented theorems. As for the corollaries, it is not difficult to prove them via their corresponding theorems, thus we omit the details.

By the definition of D_a $(a = 0, 1)$, we know

$$|D_a| = \begin{cases} 2^{m-1} - 1, & \text{if } a = 0, \\ 2^{m-1}, & \text{if } a = 1. \end{cases}$$

We define $N(a, b) = \{x \in \mathbb{F}_q : \mathrm{Tr}(x) = a \text{ and } \mathrm{Tr}(bx^{2^h+1}) = 0\}$, and denote by $wt(\mathbf{c}_b)$ the Hamming weight of the codeword $\mathbf{c}_b$ with $b \in \mathbb{F}_q^*$ of the code $\overline{C}_{D_a}$ $(a = 0, 1)$. It can be easily checked that

$$wt(\mathbf{c}_b) = 2^{m-1} - |N(a, b)|. \tag{6}$$

In terms of exponential sums, for $b \in \mathbb{F}_q^*$, we have

$$\begin{aligned} |N(a,b)| &= 2^{-2} \sum_{x\in\mathbb{F}_q} \left(\sum_{y\in\mathbb{F}_2} (-1)^{y\mathrm{Tr}(x)-ya} \right) \left(\sum_{z\in\mathbb{F}_2} (-1)^{z\mathrm{Tr}\left(bx^{2^h+1}\right)} \right) \\ &= 2^{-2} \sum_{x\in\mathbb{F}_q} \left(1 + (-1)^{\mathrm{Tr}(x)-a} \right) \left(1 + (-1)^{\mathrm{Tr}\left(bx^{2^h+1}\right)} \right) \\ &= 2^{m-2} + 2^{-2} \sum_{x\in\mathbb{F}_q} (-1)^{\mathrm{Tr}\left(bx^{2^h+1}\right)} + 2^{-2} \sum_{x\in\mathbb{F}_q} (-1)^{\mathrm{Tr}\left(x+bx^{2^h+1}\right)-a} \\ &= 2^{m-2} + 2^{-2} \left(S_h(b, 0) + (-1)^a S_h(b, 1) \right). \end{aligned} \tag{6'}$$

Based on the above discussion, the weight distribution of $\overline{C}_{D_a}$ can be determined by using the value distribution of $S_h(b, c)$ with $b \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_2$. By the lemmas presented in Sect. 2, we are ready to compute the weight distributions of the codes $\overline{C}_{D_a}$ $(a = 0, 1)$.

Proof of Theorem 1 We present only the proof for $\overline{C}_{D_0}$, since the proof for the case in which $a = 1$ is similar. By Lemma 1, we have $S_h(b, 0) = 0$ for $b \in \mathbb{F}_q^*$. It follows from Lemma 2 that

$$S_h(b, 1) = S_h\left(1, c^{-1}\right) = \begin{cases} 0, & \text{if } \mathrm{Tr}_h\left(c^{-1}\right) \neq 1, \\ \pm 2^{\frac{m+h}{2}}, & \text{if } \mathrm{Tr}_h\left(c^{-1}\right) = 1, \end{cases} \tag{7}$$

where $b \in \mathbb{F}_q^*$ and $c^{2^h+1} = b$. We get

$$|N(0, b)| \in \left\{ 2^{m-2}, 2^{m-2} - 2^{\frac{m+h-4}{2}}, 2^{m-2} + 2^{\frac{m+h-4}{2}} \right\}.$$

Hence, the weight $wt(\mathbf{c}_b)$ of the codeword $\mathbf{c}_b$ $(b \in \mathbb{F}_q^*)$ in $\overline{C}_{D_0}$ satisfies

$$wt(\mathbf{c}_b) \in \left\{ 2^{m-2}, 2^{m-2} \pm 2^{\frac{m+h-4}{2}} \right\}.$$

Suppose $w_1 = 2^{m-2} - 2^{\frac{m+h-4}{2}}$, $w_2 = 2^{m-2}$, $w_3 = 2^{m-2} + 2^{\frac{m+h-4}{2}}$. Note that if m/h is odd, then $\gcd\left(2^h + 1, 2^m - 1\right) = 1$. This means that when b ranges over $\mathbb{F}_q^*$, the

element c with $c^{2^h+1} = b$ takes on each element of $\mathbb{F}_q^*$ exactly once. Hence, we obtain

$$\begin{aligned}&\left|\left\{c \in \mathbb{F}_q^* : \mathrm{Tr}_h\left(c^{-1}\right) \neq 1, c^{2^h+1} = b \text{ and } b \in \mathbb{F}_q^*\right\}\right| \\ &= 2^m - 1 - \left|\left\{c \in F_q^* : \mathrm{Tr}_h\left(c^{-1}\right) = 1, c^{2^h+1} = b \text{ and } b \in \mathbb{F}_q^*\right\}\right| \\ &= 2^m - 2^{m-h} - 1,\end{aligned}$$

i.e., $A_{w_2} = 2^m - 2^{m-h} - 1$. (Please see the definition of A_i in the second paragraph of page 2.) The first two Pless Power Moments (Page 260, [23]) yield the following two equations:

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} = 2^m - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} = n2^{m-1}. \end{cases} \tag{8}$$

Here $n = 2^{m-1} - 1$. Solving the system of equations (8), we get Theorem 1. And we complete the proof. □

Next, we assume $m/h \equiv 0 \pmod 2$, $m = 2e$, and g is a generator of $\mathbb{F}_q^*$. In order to give a proof of Theorem 2, we need the following auxiliary lemma. This lemma can be found in equation (10) in [10].

Lemma 6 *Let* $T_0 = \left\{x \in \mathbb{F}_q : \mathrm{Tr}\left(x^{2^h+1}\right) = 0\right\}$ *and* $T_1 = \mathbb{F}_q \backslash T_0$. *If* m/h *is even with* $m = 2e$, *then* $|T_0| = 2^{m-1} - (-1)^{\frac{e}{h}} 2^{e+h-1}$ *and* $|T_1| = 2^{m-1} + (-1)^{\frac{e}{h}} 2^{e+h-1}$.

Proof of Theorem 2 For $b \in \mathbb{F}_q^*$, if $b \neq g^{t(2^h+1)}$ for any integer t, then by Lemma 3, we have $S_h(b, 0) = (-1)^{\frac{e}{h}} 2^e$, and by Lemma 4, we get

$$S_h(b, 1) = (-1)^{\frac{e}{h}} 2^e \chi_1\left(b x_0^{2^h+1}\right),$$

where x_0 satisfies $b^{2^h} x_0^{2^{2h}} + b x_0 = 1$.

If $b = g^{t(2^h+1)}$ for some integer t, then by Lemma 3, we obtain

$$S_h(b, 0) = -(-1)^{\frac{e}{h}} 2^{e+h}.$$

Assume $c = g^t$, then $b = c^{2^h+1}$ and it follows from Lemma 2 that $S_h(b, 1) = S_h\left(1, c^{-1}\right)$. For the above $c \in \mathbb{F}_q^*$, let $f_c(x) = x^{2^{2h}} + x - \left(c^{-1}\right)^{2^h}$. If $f_c(x)$ has no root in $\mathbb{F}_q^*$, by Lemma 4, we obtain $S_h(b, 1) = S_h(1, c^{-1}) = 0$. Note that $\mathrm{Tr}_h(1) = 0$, since m/h is even. If $f_c(x)$ has a root x_0 in $\mathbb{F}_q^*$, by Lemma 4, we get

$$S_h(b, 1) = S_h(1, c^{-1}) = -(-1)^{\frac{e}{h}} 2^{e+h} \chi_1\left(x_0^{2^h+1}\right).$$

By Equations (6) and (6′), we know that for $b \in \mathbb{F}_q^*$, $wt(\mathbf{c}_b)$ belongs to the set

$$\left\{2^{m-2} + (-1)^{\frac{e}{h}} 2^{e+h-1}, 2^{e-2}(2^e + (-1)^{\frac{e}{h}} 2^h), 2^{m-2}, 2^{m-2} - (-1)^{\frac{e}{h}} 2^{e-1}\right\}.$$

Define $w_1 = 2^{m-2} + (-1)^{\frac{e}{h}} 2^{e+h-1}$, $w_2 = 2^{e-2}(2^e + (-1)^{\frac{e}{h}} 2^h)$, $w_3 = 2^{m-2}$, $w_4 = 2^{m-2} - (-1)^{\frac{e}{h}} 2^{e-1}$.

The next step is to determine the number A_{w_i} of codewords with weight w_i. If $f_c(x) = 0$ (for some $c \in \mathbb{F}_q$) is solvable in $\mathbb{F}_q$, by Lemma 5, there are 2^{2h} solutions of this equation over $\mathbb{F}_q$. Since $\gcd(2^h, 2^m - 1) = 1$, it can be easily checked that $\left\{x_0 \in \mathbb{F}_q : x_0^{2^{2h}} + x_0 = (c^{-1})^{2^h}, c \in \mathbb{F}_q\right\} = \mathbb{F}_q$. Hence we get

$$\left|\left\{c \in \mathbb{F}_q^* : x^{2^{2h}} + x = (c^{-1})^{2^h} \text{ is solvable in } \mathbb{F}_q\right\}\right| = 2^{m-2h} - 1,$$

and $\left|\left\{c \in \mathbb{F}_q^* : x^{2^{2h}} + x = (c^{-1})^{2^h} \text{ has no root in } \mathbb{F}_q\right\}\right| = 2^m - 2^{m-2h}$.

Since x^{2^h+1} is a $(2^h + 1)$-to-1 function on $\mathbb{F}_q$, there are $\frac{2^m - 2^{m-2h}}{2^h+1}$ elements b ($b = c^{2^h+1} \in \mathbb{F}_q^*$) such that $S_h(b, 1) = 0$, i.e., $A_{w_2} = \frac{2^m - 2^{m-2h}}{2^h+1}$. It follows from Lemmas 4 and 6 that

$$\left|\left\{c \in \mathbb{F}_q^* : S_h(1, c^{-1}) = (-1)^{\frac{e}{h}} 2^{e+h}\right\}\right| = \frac{2^{m-1} + (-1)^{\frac{e}{h}} 2^{e+h-1}}{2^{2h}}.$$

Then we have

$$\left|\left\{b \in \mathbb{F}_q^* : b = c^{2^h+1} \text{ and } S_h(b, 1) = (-1)^{\frac{e}{h}} 2^{e+h}\right\}\right| = \frac{2^{m-1} + (-1)^{\frac{e}{h}} 2^{e+h-1}}{2^{2h}(2^h + 1)}.$$

Therefore, $A_{w_1} = \frac{2^{m-2h-1} - 1 - (-1)^{\frac{e}{h}} 2^{e-h-1}}{2^h+1}$. By the Pless Power Moments (Page 260, [23]), we obtain the following two equations:

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} + A_{w_4} = 2^m - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} + w_4 A_{w_4} = 2^{m-1}(2^{m-1} - 1). \end{cases} \tag{9}$$

The solutions to the set of equations in (9) yield the weight distribution presented in Table 4. The proof of Theorem 2 is completed. □

We omit a proof for Theorem 3, since it is similar to that of Theorem 2. By the proof of Theorem 2, it is also straightforward to prove Theorem 4. So the proof for Theorem 4 is left to the reader.

4 Concluding remarks

In this paper, we presented several classes of binary linear codes with a few weights. A number of linear codes with at most five weights were discussed in [7,8,11,12,38,39].

Further, some interesting binary linear codes constructed by a similar method were presented in [10,28,30]. The binary codes presented in our paper were rather different than the above due to the following three reasons:

1. Most differently, the binary codes in our paper were defined by $C_D = \{(\mathrm{Tr}(xf(d)))_{d\in D} : x \in \mathbb{F}_q\}$, where $f(d) = d^{2^h+1}$, whereas $f(d) = d$ was used in [10,28,30].
2. We selected the defining sets using a different approach, thereby causing the codes in our paper to have different lengths.
3. The binary linear codes in our paper were constructed with new parameters and have at most nine weights, whereas the binary codes in [10,28,30] have two or three weights.

It should be remarked that the parameters of the binary linear codes $\overline{C}_{D_0}$ in Theorem 1 are the same as those in Theorem 1 in [10]. By Magma, we found the code $\overline{C}_{D_0}$ to be equivalent to that in Theorem 1 of [10] for $(m, h) = (3, 1)$. But for $(m, h) = (5, 1)$ and $(7, 1)$, they are not equivalent. It is open whether the two classes of codes are equivalent or not. The reader is invited to attack this problem.

A polynomial of the form

$$f(x) = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{ij}x^{2^i+2^j}, a_{ij} \in \mathbb{F}_q$$

is called a quadratic form over $\mathbb{F}_{2^m}$. It should be interesting to settle the parameters and weight distribution of $\overline{C}_D$ if we replace x^{2^h+1} with more general quadratic forms.

Denote the minimum and maximum nonzero weights of a linear code C over $\mathbb{F}_p$ by $w_{\min}$ and $w_{\max}$, respectively. By the results in [36], if the code C satisfies the inequality

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p},$$

then C can be employed to construct secret sharing schemes with interesting properties.

Let $m > h + 2$. Then, for the codes in Theorem 1, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{m-2} - 2^{\frac{m+h-4}{2}}}{2^{m-2} + 2^{\frac{m+h-4}{2}}} > \frac{1}{2}.$$

If $(m, h) \neq (4, 1)$ or $(6, 1)$, then for the codes in Theorems 2 and 3, it can be easily checked that

$$\frac{w_{\min}}{w_{\max}} > \frac{1}{2}.$$

This conclusion is also true for Theorem 4 and Corollary 5.

Hence, the binary linear codes presented in Theorems 1–4 and Corollary 5 are suitable for constructing secret sharing schemes in many cases.

References

1. Blake, I.F., Kith, K.: On the complete weight enumerator of Reed–Solomon codes. SIAM J. Disc. Math. **4**(2), 164–171 (1991)
2. Carlitz, L.: Exolicite evaluation of certain exponential sums. Math. Scand. **44**, 5–16 (1979)
3. Carlitz, L.: Evaluation of some exponential sums over a finite field. Math. Nachr. **96**, 319–339 (1980)
4. Coulter, R.S.: Explicit evaluation of some Weil sums. Acta Arith. **83**, 241–251 (1998)
5. Coulter, R.S.: On the evaluation of a class of Weil sums in characteristic 2. N. Z. J. Math. **28**, 171–184 (1999)
6. Choi, S.T., Kim, J.Y., No, J.S., Chung, H.: Weight distribution of some cyclic codes. In: Proceedings of the International Symposium on Information Theory, pp. 2911–2913 (2012)
7. Courteau, B., Wolfmann, J.: On triple-sum-sets and two or three weights codes. Discrete Math. **50**, 179–191 (1984)
8. Ding, C.: A class of three-weight and four-weight codes. In: Xing, C., et al. (eds.) Proceedings of the Second International Workshop on Coding Theory and Cryptography, Lecture Notes in Computer Science. Springer, vol. 5557, pp. 34–42(2009)
9. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015)
10. Ding, K., Ding, C.: Bianry linear codes with three weights. IEEE Commun. Lett. **18**(11), 1879–1882 (2014)
11. Ding, K., Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans. Inf. Theory **61**(11), 5835–5842 (2015)
12. Ding, C., Gao, Y., Zhou, Z.: Five families of three-weight ternary cyclic codes and their duals. IEEE Trans. Inf. Theory **59**(12), 7940–7946 (2013)
13. 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)
14. Ding, C., Luo, J., Niederreiter, H.: Two-weight codes punctured from irreducible cyclic codes. In: Li, Y., et al. (eds.) Proceedings of the First Worshop on Coding and Cryptography, pp. 119–124. World Scientific, Singapore (2008)
15. Ding, C., Li, C., Li, N., Zhou, Z.: Three-weight cyclic codes and their weight distributions. Disctrete Math. **339**(2), 415–427 (2016)
16. Ding, C., Yang, J.: Hamming weights in irreducible cyclic codes. Discrete Math. **313**(4), 434–446 (2013)
17. Ding, C., Niederreiter, H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory **53**(6), 2274–2277 (2007)
18. Du, X., Wan, Y.: Linear codes from quadratic forms. Appl. Algebra Eng. Commun. Comput. **28**(6), 535–547 (2017)
19. 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)
20. Feng, K., Luo, J.: Weight distribution of some reducible cyclic codes. Finite Fields Appl. **14**(2), 390–409 (2008)
21. Feng, T., Leung, K., Xiang, Q.: Binary cyclic codes with two primitive nonzeros. Sci. China Math. **56**(7), 1403–1412 (2012)
22. Hou, X.: Explicit evaluation of certain exponential sums of binary quadratic functions. Finite Fields Appl. **13**, 843–868 (2007)
23. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
24. Kith, K.: Complete weight enumeration of Reed-Solomon codes, Masters thesis, Department of Electrical and Computing Engineering, University of Waterloo, Waterloo, Ontario, Canada (1989)
25. Luo, J., Feng, K.: On the weight distribution of two classes of cyclic codes. IEEE Trans. Inf. Theory **54**(12), 5332–5344 (2008)
26. Li, C., Yue, Q., Li, F.: Hamming weights of the duals of cyclic codes with two zeros. IEEE Trans. Inf. Theory **60**(7), 3895–3902 (2014)
27. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, New York (1997)
28. Qi, Y., Tang, C., Huang, D.: Binary linear codes with few weights. IEEE Commun. Lett. **20**(2), 208–211 (2016)
29. Tang, C., Xiang, C., Feng, K.: Linear codes with few weights from inhomogeneous quadratic functions. Des. Codes Cryptogr. **83**(3), 691–714 (2017)

30. Wang, Q., Ding, K., Xue, R.: Binary linear codes with two weights. IEEE Commun. Lett. **19**(7), 1097–1100 (2015)
31. Wang, Q., Ding, K., Lin, D., Xue, R.: A kind of three-weight linear codes. Cryptogr. Commun. **9**(3), 315–322 (2017)
32. Yang, S., Kong, X., Tang, C.: A construction of linear codes and their complete weight enumerators. Finite Fields Their Appl. **48**, 196–226 (2017)
33. Yang, S., Yao, Z.-A., Zhao, C.-A.: A class of three-weight linear codes and their complete weight enumerators. Cryptogr. Commun. **9**, 133–149 (2017)
34. Yang, S., Yao, Z.-A.: Complete weight enumerators of a family of three-weight linear codes. Des. Codes Cryptogr. **82**(3), 663–674 (2017)
35. 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)
36. Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**(1), 206–212 (2006)
37. Zhang, D., Fan, C., Peng, D., Tang, X.: Complete weight enumerators of some linear codes from quadratic forms. Cryptogr. Commun. **9**, 151–163 (2017)
38. Zhou, Z., Ding, C.: A class of three-weight cyclic codes. Finite Fields Their Appl. **25**, 79–93 (2014)
39. Zhou, Z., Li, N., Fan, C., Helleseth, T.: Linear codes with two or three weights from quadratic bent functions. Des. Codes Cryptogr. **81**(2), 283–295 (2016)