

Linear codes from a generic construction

Can Xiang¹

Received: 12 July 2015 / Accepted: 10 September 2015 / Published online: 30 September 2015
© Springer Science+Business Media New York 2015

Abstract A generic construction of linear codes over finite fields has recently received a lot of attention, and many one-weight, two-weight and three-weight codes with good error correcting capability have been produced with this generic approach. The first objective of this paper is to establish relationships among some classes of linear codes obtained with this approach, so that the parameters of some classes of linear codes can be derived from those of other classes with known parameters. In this way, linear codes with new parameters will be derived. The second is to present a class of three-weight binary codes and consider their applications in secret sharing.

Keywords Cyclic codes · Linear codes · Weight distribution · Weight enumerator

Mathematics Subject Classifications (2010) 94B05 · 94B15 · 94B60

1 Introduction

Throughout this paper, let p be a prime and let $q = p^m$ for some positive integer m . An $[n, \kappa, \omega]$ linear code \mathcal{C} over $\text{GF}(p)$ is a κ -dimensional subspace of $\text{GF}(p)^n$ with minimum (Hamming) distance ω . Let A_i denote the number of codewords with Hamming weight i in a code \mathcal{C} of length n . The *weight enumerator* of \mathcal{C} is defined by $1 + A_1z + A_2z^2 + \cdots + A_nz^n$. A code \mathcal{C} is said to be a t -weight code if the number of nonzero A_i in the sequence (A_1, A_2, \dots, A_n) is equal to t . The sequence $(1, A_1, A_2, \dots, A_n)$ is called the

✉ Can Xiang
cxiangcxiang@hotmail.com

¹ College of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

weight distribution of \mathcal{C} . An $[n, \kappa, \omega]$ code \mathcal{C} is called *optimal* if its parameters $[n, \kappa, \omega]$ meet a bound on linear codes, and *almost optimal* if $[n, \kappa, \omega + 1]$ or $[n, \kappa + 1, \omega]$ meets a bound on linear codes.

A generic construction of linear codes over finite fields has attracted a lot of attention in the past eight years (see, for example, [8–11, 13, 14, 17]). Many classes of one-weight, two-weight and three-weight codes were obtained with this approach. The first goal of this paper is to establish a few relations among some classes of linear codes obtained with this approach, so that the parameters of some classes of linear codes can be derived from those of other classes with known parameters. In this way, linear codes with new parameters will be derived. The second is to present a class of three-weight binary codes and consider their applications in secret sharing.

2 Group characters in $\text{GF}(q)$

An *additive character* of $\text{GF}(q)$ is a nonzero function χ from $\text{GF}(q)$ to the set of nonzero complex numbers such that $\chi(x + y) = \chi(x)\chi(y)$ for any pair $(x, y) \in \text{GF}(q)^2$. For each $b \in \text{GF}(q)$, the function

$$\chi_b(c) = \epsilon_p^{\text{Tr}(bc)} \quad \text{for all } c \in \text{GF}(q) \quad (1)$$

defines an additive character of $\text{GF}(q)$, where and whereafter $\epsilon_p = e^{2\pi\sqrt{-1}/p}$ is a primitive complex p th root of unity. When $b = 0$, $\chi_0(c) = 1$ for all $c \in \text{GF}(q)$, and is called the *trivial additive character* of $\text{GF}(q)$. The character χ_1 in (1) is called the *canonical additive character* of $\text{GF}(q)$. It is known that every additive character of $\text{GF}(q)$ can be written as $\chi_b(x) = \chi_1(bx)$ [16, Theorem 5.7].

3 A generic construction of linear codes

Let $D = \{d_1, d_2, \dots, d_n\} \subseteq \text{GF}(q)$, where again $q = p^m$. Let Tr denote the trace function from $\text{GF}(q)$ onto $\text{GF}(p)$ throughout this paper. We define a linear code of length n over $\text{GF}(p)$ by

$$\mathcal{C}_D = \{(\text{Tr}(xd_1), \text{Tr}(xd_2), \dots, \text{Tr}(xd_n)) : x \in \text{GF}(q)\}, \quad (2)$$

and call D the *defining set* of this code \mathcal{C}_D . By definition, the dimension of the code \mathcal{C}_D is at most m .

The code \mathcal{C}_D depends on the specific ordering of the elements in the defining set D . However, up to column permutations, the codes obtained from different orderings are *equivalent* with respect to coordinate permutations. Hence, in this paper, we do not specify the specific ordering of the elements in D when we consider the code \mathcal{C}_D .

This construction is generic in the sense that many classes of known codes could be produced by properly selecting the defining set $D \subseteq \text{GF}(q)$. This construction technique was employed in [8–11, 13, 14, 17] for obtaining linear codes with a few weights.

This construction is generic and can produce a lot of linear codes. The parameters of the code \mathcal{C}_D depend on the selection of the defining set D . Linear codes with both poor and good error-correcting capability can be obtained with this approach.

Many classes of linear codes with a few weights and good parameters have been already obtained with this approach. In this paper, we will present a few relations among some

subclasses of linear codes obtained with this approach. In this way, we are able to derive the parameters of some other linear codes.

It is convenient to define for each $x \in \text{GF}(q)$,

$$\mathbf{c}_x = (\text{Tr}(xd_1), \text{Tr}(xd_2), \dots, \text{Tr}(xd_n)). \tag{3}$$

The Hamming weight $\text{wt}(\mathbf{c}_x)$ of \mathbf{c}_x is $n - N_x(0)$, where

$$N_x(0) = |\{1 \leq i \leq n : \text{Tr}(xd_i) = 0\}|$$

for each $x \in \text{GF}(q)$.

It is easily seen that for any $D = \{d_1, d_2, \dots, d_n\} \subseteq \text{GF}(q)$ we have

$$pN_x(0) = \sum_{i=1}^n \sum_{y \in \text{GF}(p)} e^{2\pi\sqrt{-1}y\text{Tr}(xd_i)/p} = \sum_{i=1}^n \sum_{y \in \text{GF}(p)} \chi_1(yxd_i) = n + \sum_{y \in \text{GF}(p)^*} \chi_1(yxD),$$

where χ_1 is the canonical additive character of $\text{GF}(q)$, aD denotes the set $\{ad : d \in D\}$, and $\chi_1(S) := \sum_{x \in S} \chi_1(x)$ for any subset S of $\text{GF}(q)$. Hence,

$$\text{wt}(\mathbf{c}_x) = n - N_x(0) = \frac{(p - 1)n - \sum_{y \in \text{GF}(p)^*} \chi_1(yxD)}{p}. \tag{4}$$

4 Shortening and expanding a linear code obtained from this construction

Let $D \subset \text{GF}(q)^*$ and $\hat{D} = ED$, where E is a subset of $\text{GF}(p)^*$ and

$$ED = \{ed : e \in E \text{ and } d \in D\}.$$

Let $n = |D|$, $\hat{n} = |\hat{D}|$, and $\ell = |E|$.

Our goal of this section is to establish a relation between the parameters of the two codes \mathcal{C}_D and $\mathcal{C}_{\hat{D}}$ under the condition that $|ED| = |E||D|$. Specifically, we have the following general result.

Theorem 1 *Let symbols and notation be the same as above. Assume that $\hat{n} = n\ell$. Then \mathcal{C}_D is an $[n, k]$ linear code with weight enumerator*

$$1 + A_1z + A_2z^2 + \dots + A_nz^n$$

if and only if $\mathcal{C}_{\hat{D}}$ is an $[n\ell, k]$ linear code with weight enumerator

$$1 + A_1z^\ell + A_2z^{2\ell} + \dots + A_nz^{n\ell}.$$

Proof Note that $\text{Tr}(zx) = z\text{Tr}(x)$ for all $z \in \text{GF}(p)$ and $x \in \text{GF}(q)$. We have that $\text{Tr}(zx) = 0$ if and only if $\text{Tr}(x) = 0$ for all $z \in \text{GF}(p)^*$ and $x \in \text{GF}(q)$.

Let $E = \{e_1, e_2, \dots, e_\ell\}$. By assumption we have that $|ED| = |E||D|$. Up to column permutations, every codeword $\hat{\mathbf{c}}_x$ in $\mathcal{C}_{\hat{D}}$ can be expressed as

$$\hat{\mathbf{c}}_x = (e_1\mathbf{c}_x, e_2\mathbf{c}_x, \dots, e_\ell\mathbf{c}_x),$$

where \mathbf{c}_x is the corresponding codeword in \mathcal{C}_D . It then follows that $\text{wt}(\hat{\mathbf{c}}_x) = \ell\text{wt}(\mathbf{c}_x)$. In addition, $\hat{\mathbf{c}}_x$ is the zero codeword in $\mathcal{C}_{\hat{D}}$ if and only if \mathbf{c}_x is the zero codeword in \mathcal{C}_D . The desired conclusions then follow. □

It should be noticed that the condition $|ED| = |E||D|$ in Theorem 1 is necessary. Without this condition, there may be no specific relation among the parameters of the two codes \mathcal{C}_D and $\mathcal{C}_{\hat{D}}$.

Theorem 1 can be employed to derive parameters of a shortened or expanded code of a linear code obtained from this generic construction in some special cases. We now demonstrate this possibility in the rest of this section.

Corollary 1 *Let $\hat{D} = \text{GF}(q)^*$, $E = \text{GF}(p)^*$, and let D be the coset representatives of the quotient group $\text{GF}(q)^*/\text{GF}(p)^*$. Then $\hat{D} = ED$, and \mathcal{C}_D is a one-weight code with parameters $[(q - 1)/(p - 1), m]$ and weight enumerator $1 + (p^m - 1)z^{p^{m-1}}$.*

Proof Note that $\hat{D} = \text{GF}(q)^*$. For every $x \in \text{GF}(q)^*$, the codeword \hat{c}_x has Hamming weight $(p - 1)p^{m-1}$. Hence, $\mathcal{C}_{\hat{D}}$ is a $[p^m - 1, m]$ code over $\text{GF}(p)$ with the only nonzero weight $(p - 1)p^{m-1}$. The desired conclusions on \mathcal{C}_D then follow from Theorem 1. \square

The code \mathcal{C}_D in Corollary 1 is the well-known simplex code. The purpose of presenting this code is to demonstrate that it is a shortened version of the code $\mathcal{C}_{\hat{D}}$ obtained from the generic construction. In addition, in the next corollary, we will show that this code can be extended into many ways so that many one-weight linear codes can be obtained.

Corollary 2 *Let D be the coset representatives of the quotient group $\text{GF}(q)^*/\text{GF}(p)^*$. Let E be any subset of $\text{GF}(p)^*$. Define $\tilde{D} = ED$. Then $\mathcal{C}_{\tilde{D}}$ is a one-weight code with parameters $[\ell(q - 1)/(p - 1), m]$ and weight enumerator $1 + (p^m - 1)z^{\ell p^{m-1}}$, where ℓ is the cardinality of E and $1 \leq \ell \leq p - 1$.*

Proof It was proved in Corollary 1 that \mathcal{C}_D is a one-weight code with parameters $[(q - 1)/(p - 1), m]$ and weight enumerator $1 + (p^m - 1)z^{p^{m-1}}$. By the definition of D , we have that $|ED| = |E||D|$. The desired conclusions on the code $\mathcal{C}_{\tilde{D}}$ then follow from Theorem 1. \square

The codes $\mathcal{C}_{\tilde{D}}$ in Corollary 2 are extensions and generalizations of the codes from skew sets presented in [9]. Since the total number of nonempty sets of $\text{GF}(p)^*$ is $2^{p-1} - 1$, the construction in Corollary 2 yields $2^{p-1} - 1$ one-weight codes over $\text{GF}(p)$.

We inform that the technique of shortening a linear code obtained from this generic construction was already employed in [14]. Theorem 1 is a formal description and generalization of this technique.

5 Combining two linear codes obtained from this generic construction

5.1 A method for combining two codes

Theorem 2 *Let $D_1 \subset \text{GF}(q)$ and $D_2 \subset \text{GF}(q)$ with $D_1 \cap D_2 = \emptyset$. Define $D = D_1 \cup D_2$. Let $n_i = |D_i|$ for $i \in \{1, 2\}$. Assume that \mathcal{C}_D is an $[n_1 + n_2, k]$ one-weight code over $\text{GF}(p)$ with nonzero-weight w , and \mathcal{C}_{D_i} has also dimension k for each i . Then \mathcal{C}_{D_1} has weight enumerator*

$$1 + A_1z + A_2z^2 + \dots + A_{n_1}z^{n_1}$$

if and only if \mathcal{C}_{D_2} has weight enumerator

$$1 + A_1z^{w-1} + A_2z^{w-2} + \dots + A_{n_1}z^{w-n_1}.$$

Proof By assumption, $D_1 \cap D_2 = \emptyset$. It follows that up to coordinate permutations every codeword \mathbf{c}_x in \mathcal{C}_D can be expressed as

$$\mathbf{c}_x = (\mathbf{c}_x^{(1)}, \mathbf{c}_x^{(2)}),$$

where $\mathbf{c}_x^{(i)}$ is the codeword in \mathcal{C}_{D_i} . It then follows that $\text{wt}(\mathbf{c}_x) = \text{wt}(\mathbf{c}_x^{(1)}) + \text{wt}(\mathbf{c}_x^{(2)})$. By the assumptions of this theorem, all three codes have the same dimension. Hence, \mathbf{c}_x is the zero codeword in \mathcal{C}_D if and only if $\mathbf{c}_x^{(1)}$ and $\mathbf{c}_x^{(2)}$ are the zero codeword in \mathcal{C}_{D_1} and \mathcal{C}_{D_2} respectively. The desired conclusions then follow. \square

It should be pointed out that the condition $D_1 \cap D_2 = \emptyset$ in Theorem 2 is necessary for the correctness of the conclusion. This is implied by the proof of Theorem 2 above.

Let $D \subset \text{GF}(q)$. Starting from now on, let \bar{D} denote the complement $\text{GF}(q) \setminus D$ of D . As a corollary of Theorem 2, we have the following.

Corollary 3 *Let $D \subset \text{GF}(q)$. Assume that \mathcal{C}_D is an $[n, m]$ linear code with*

$$\max_{\mathbf{c} \in \mathcal{C}_D} \text{wt}(\mathbf{c}) < (p - 1)p^{m-1}$$

and weight enumerator

$$1 + A_1z + A_2z^2 + \dots + A_nz^n.$$

Then $\mathcal{C}_{\bar{D}}$ has parameters $[q - n, m]$ and weight enumerator

$$1 + A_1z^{(p-1)p^{m-1}-1} + A_2z^{(p-1)p^{m-1}-2} + \dots + A_nz^{(p-1)p^{m-1}-n}.$$

Proof Note that $\mathcal{C}_{\text{GF}(q)}$ is a $[q, m]$ linear code over $\text{GF}(p)$, and has the only nonzero weight $(p - 1)p^{m-1}$. By definition, up to column permutations, every codeword \mathbf{c} in $\mathcal{C}_{\text{GF}(q)}$ can be expressed as $\mathbf{c} = (\mathbf{c}_x^{(1)}, \mathbf{c}_x^{(2)})$, where $\mathbf{c}_x^{(1)}$ and $\mathbf{c}_x^{(2)}$ are the corresponding codewords in \mathcal{C}_D and $\mathcal{C}_{\bar{D}}$, respectively. Since \mathcal{C}_D has dimension m , \mathbf{c}_x is the zero codeword in $\mathcal{C}_{\text{GF}(q)}$ if and only if $\mathbf{c}_x^{(1)}$ is the zero codeword in \mathcal{C}_D . Note that $\mathcal{C}_{\text{GF}(q)}$ is a one-weight code with nonzero weight $(p - 1)p^{m-1}$ and $\max_{\mathbf{c} \in \mathcal{C}_D} \text{wt}(\mathbf{c}) < (p - 1)p^{m-1}$. \mathbf{c}_x is a nonzero codeword in $\mathcal{C}_{\text{GF}(q)}$ if and only if $\mathbf{c}_x^{(2)}$ is a nonzero codeword in $\mathcal{C}_{\bar{D}}$. We then deduce that the dimension of $\mathcal{C}_{\bar{D}}$ is also m . The rest of the desired conclusions follows from Theorem 2. \square

It is noticed that the condition $\max_{\mathbf{c} \in \mathcal{C}_D} \text{wt}(\mathbf{c}) < (p - 1)p^{m-1}$ in Corollary 3 is necessary. Without this condition, the dimension of $\mathcal{C}_{\bar{D}}$ may be less than m .

Corollary 3 could be employed to determine the weight enumerator of many classes of linear codes $\mathcal{C}_{\bar{D}}$ from those of the code \mathcal{C}_D . In the next subsections, we will demonstrate this with a few examples.

5.2 A class of one-weight and two-weight codes

Let $f(x)$ be a function from $\text{GF}(q)$ to $\text{GF}(q)$. We define

$$D(f) := \{f(x) : x \in \text{GF}(q)\} \setminus \{0\}.$$

A polynomial f over $\text{GF}(q)$ of the form

$$f(x) = \sum_{i \in I} \sum_{j \in J} a_{i,j} x^{p^i + p^j} \tag{5}$$

is called a *quadratic form* over $\text{GF}(q)$, where $a_{i,j} \in \text{GF}(q)$, and I and J are subsets of $\{0, 1, 2, \dots, m - 1\}$.

Note that $\text{GF}(q)$ is a vector space of dimension m over $\text{GF}(p)$. The rank of the quadratic form f over $\text{GF}(q)$ is defined to be the codimension of the $\text{GF}(p)$ -vector space

$$V_f = \{x \in \text{GF}(q) : f(x + z) - f(x) - f(z) = 0 \text{ for all } z \in \text{GF}(q)\}.$$

That is $|V_f| = p^{m-r}$, where r denotes the rank of f .

It is still very difficult to determine the length n_f of the code $\mathcal{C}_{D(f)}$ for general quadratic forms f , let alone the weight distribution of the code $\mathcal{C}_{D(f)}$. However, under certain conditions the weight distribution of $\mathcal{C}_{D(f)}$ can be worked out [9]. Below we derive a general result on the code $\mathcal{C}_{\overline{D(f)}}$ from known results on the code $\mathcal{C}_{D(f)}$.

Corollary 4 *Let f be a quadratic form of rank r over $\text{GF}(q)$ such that*

- $f(0) = 0$ and $f(x) \neq 0$ for all $x \in \text{GF}(q)^*$; and
- f is e -to-1 on $\text{GF}(q)^*$ (i.e. $f(x) = u$ has either e solutions $x \in \text{GF}(q)^*$ or no solution for each $u \in \text{GF}(q)^*$), where e is a positive integer.

If r is odd and $e > 1$, then $\mathcal{C}_{\overline{D(f)}}$ is a one-weight code over $\text{GF}(p)$ with parameters

$$\left[\frac{(e-1)q+1}{e}, m, \frac{(e-1)(p-1)q}{ep} \right].$$

If $r \geq 2$ is even and $e > 1$, then $\mathcal{C}_{\overline{D(f)}}$ is a two-weight code over $\text{GF}(p)$ with parameters

$$\left[\frac{(e-1)q+1}{e}, m, \frac{(p-1)((e-1)q-p^{m-r/2})}{ep} \right]$$

and weight enumerator

$$1 + \frac{q-1}{2} z^{\frac{(p-1)((e-1)q-p^{m-r/2})}{ep}} + \frac{q-1}{2} z^{\frac{(p-1)((e-1)q+p^{m-r/2})}{ep}}.$$

Proof The parameters of the code $\mathcal{C}_{D(f)}$ were determined in [9]. In addition, it is easily verified that the conditions of Corollary 3 were satisfied by $\mathcal{C}_{D(f)}$. The desired conclusions on the code $\mathcal{C}_{\overline{D(f)}}$ then follow from Corollary 3 and Theorem 3 in [9]. □

Example 1 $f(x) = x^{p^\ell+1}$ is a quadratic form over $\text{GF}(q)$ satisfying the conditions of Corollary 4, if $e = \text{gcd}(q-1, p^\ell+1) > 1$.

Example 2 $f(x) = x^{10} - ux^6 - u^2x^2$ is a quadratic form over $\text{GF}(3^m)$ satisfying the conditions of Corollary 4, where $u \in \text{GF}(3^m)$, m is odd, and $e = 2$.

5.3 The parameters of some binary codes

Let f be a Boolean function from $\text{GF}(2^m)$ to $\text{GF}(2)$. The *support* of f is defined to be

$$D_f = \{x \in \text{GF}(2^m) : f(x) = 1\} \subseteq \text{GF}(2^m).$$

Recall that $n_f = |D_f|$.

The Walsh transform of f is defined by

$$\hat{f}(w) = \sum_{x \in \text{GF}(2^m)} (-1)^{f(x) + \text{Tr}(wx)} \tag{6}$$

where $w \in \text{GF}(2^m)$. The Walsh spectrum of f is the following multiset

$$\left\{ \left\{ \hat{f}(w) : w \in \text{GF}(2^m) \right\} \right\}.$$

It is in general a very hard to determine the weight distribution of the binary code \mathcal{C}_{D_f} with length n_f and dimension at most m . However, in a number of special cases, this can be done. Below we describe the weight distribution of the code \mathcal{C}_{D_f} by making use of some results on the binary code \mathcal{C}_{D_f} obtained in [9].

The main result of this section is described in the following corollary.

Corollary 5 *Let symbols and notation be the same as above. If $2n_f \neq \hat{f}(w)$ for all $w \in \text{GF}(2^m)^*$ and*

$$\max_{w \in \text{GF}(2^m)} \hat{f}(w) < 2(2^m - n_f), \tag{7}$$

then \mathcal{C}_{D_f} is a binary linear code with length $2^m - n_f$ and dimension m , and its weight distribution is given by the following multiset:

$$\left\{ \left\{ \frac{2(2^m - n_f) - \hat{f}(w)}{4} : w \in \text{GF}(2^m)^* \right\} \right\} \cup \{\{0\}\}. \tag{8}$$

Proof According to Theorem 9 in [9], the code \mathcal{C}_{D_f} has dimension m and the maximum nonzero Hamming weight of codewords in \mathcal{C}_{D_f} is

$$\max_{w \in \text{GF}(2^m)} \frac{2n_f + \hat{f}(w)}{4} < 2^{m-1}$$

due to the condition of (7). The desired conclusions then follow from Corollary 3 and Theorem 9 in [9]. □

For all the two-weight and three-weight codes \mathcal{C}_{D_f} from bent, semibent and almost bent functions described in [9], the corresponding binary codes \mathcal{C}_{D_f} are also two-weight and three-weight codes with the weight distribution given in Corollary 5. We omit the details of the weight distributions here.

5.4 A class of ternary codes

In this subsection, we determine the parameters of a class of ternary codes.

Our main result of this section is the following.

Theorem 3 *Let h be an odd positive integer and let $m = 3h \geq 3$. Let $\ell = 3^{2h} - 3^h + 1$. Define*

$$D = \left\{ \alpha^t : \text{Tr}_{3^m/3}(\alpha^t + \alpha^{t\ell}) = 0, 0 \leq t \leq (3^m - 3)/2 \right\}, \tag{9}$$

where α is a generator of $\text{GF}(3^m)^$.*

Then the ternary code $\mathcal{C}_{\overline{D}}$ has parameters

$$\left[\frac{5 \times 3^{3h-1} + 1}{2}, 3h, 5 \times 3^{3h-2} - 3^{2h-2} \right]$$

and the weight distribution of Table 1.

Proof According to Theorem 15 in [9], the ternary code \mathcal{C}_D has dimension $m = 3h$ and the maximum nonzero Hamming weight of codewords in \mathcal{C}_{D_f} is

$$3^{3h-2} + 3^{2h-2} < 2 \times 3^{3h-1}.$$

The desired conclusions then follow from Corollary 3 and Theorem 15 in [9]. □

We remark that the code $\mathcal{C}_{\overline{D}}$ of Theorem 3 has more than three nonzero weights if h is even.

5.5 Other two-weight and three-weight codes

Corollary 3 can be employed to obtain many linear codes with a few weights. For instances, it can be applied to all the codes in [13, 14, 17] to obtain two-weight and three-weight codes.

6 A class of binary linear codes and their parameters

The objective of this section is to present a class of three-weight binary codes and consider their application in secret sharing. In this section, let $p = 2$ and we consider only binary codes \mathcal{C}_D within the generic construction of this paper.

6.1 The description of the codes

In this subsection, we only describe the binary codes and introduce their parameters, but will present the proofs of their parameters in the next subsection.

In this subsection, the defining set D of the code \mathcal{C}_D of (2) is given by

$$D = \{x \in \text{GF}(2^m)^* : \text{Tr}(x^3 + x) = 0\}. \tag{10}$$

Since $0 \notin D$, the minimum distance d^\perp of the dual code \mathcal{C}_D^\perp of \mathcal{C}_D cannot be 1. Note that the elements in D are pairwise distinct, the minimum distance d^\perp of the dual code \mathcal{C}_D^\perp cannot be 2. Hence, we have the following lemma.

Lemma 1 *The minimum distance d^\perp of the dual code \mathcal{C}_D^\perp of \mathcal{C}_D is at least 3 if $n = |D| \geq 3$.*

Table 1 The weight distribution of the codes of Theorem 3

Weight w	Multiplicity A_w
0	1
$5 \times 3^{3h-2} + 3^{2h-2}$	$3^{2h} + 3^h$
$5 \times 3^{3h-2}$	$3^{3h} - 2 \times 3^{2h} - 1$
$5 \times 3^{3h-2} - 3^{2h-2}$	$3^{2h} - 3^h$

Table 2 The weight distribution of the codes \mathcal{C}_D of Theorem 4

Weight w	Multiplicity A_w
0	1
$2^{m-2} + \left[(-1)^{\frac{m^2-1}{8}} - 1\right] 2^{\frac{m-3}{2}}$	$2^{m-2} + 2^{\frac{m-3}{2}} - \frac{1}{2}[1 + (-1)^{\frac{m^2-1}{8}}]$
$2^{m-2} + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-3}{2}}$	2^{m-1}
$2^{m-2} + \left[(-1)^{\frac{m^2-1}{8}} + 1\right] 2^{\frac{m-3}{2}}$	$2^{m-2} - 2^{\frac{m-3}{2}} + \frac{1}{2}[-1 + (-1)^{\frac{m^2-1}{8}}]$

Theorem 4 Let $m \geq 5$ be odd, and let D be defined in (10). Then the set \mathcal{C}_D of (2) is a $[2^{m-1} - 1 + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-1}{2}}, m]$ binary code with the weight distribution in Table 2. The dual code \mathcal{C}_D^\perp has parameters

$$\left[2^{m-1} - 1 + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-1}{2}}, 2^{m-1} - 1 + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-1}{2}} - m, d^\perp\right],$$

where $d^\perp \geq 3$.

Example 3 Let $m = 5$. Then the code \mathcal{C}_D has parameters $[11, 5, 4]$ and weight enumerator $1 + 10z^4 + 16z^6 + 5z^8$. This code is optimal. Its dual \mathcal{C}_D^\perp has parameters $[11, 6, 3]$ and is almost optimal.

Example 4 Let $m = 7$. Then the code \mathcal{C}_D has parameters $[71, 7, 32]$ and weight enumerator $1 + 35z^{32} + 64z^{36} + 28z^{40}$. Its dual \mathcal{C}_D^\perp has parameters $[71, 64, 3]$ and is optimal.

Theorem 5 Let $m \geq 4$ be even, and let D be defined in (10). Then the set \mathcal{C}_D of (2) is a $[2^{m-1} - 1, m]$ binary code with the weight distribution in Table 3 when $m \equiv 2 \pmod{4}$, and a $[2^{m-1} - 1 - 2^{\frac{m}{2}}(-1)^{\frac{m}{4}}, m]$ binary code with the weight distribution in Table 4 when $m \equiv 0 \pmod{4}$.

The dual code \mathcal{C}_D^\perp has parameters $[2^{m-1} - 1, 2^{m-1} - 1 - m, d^\perp \geq 3]$ when $m \equiv 2 \pmod{4}$, and parameters

$$[2^{m-1} - 1 - 2^{\frac{m}{2}}(-1)^{\frac{m}{4}}, 2^{m-1} - 1 - 2^{\frac{m}{2}}(-1)^{\frac{m}{4}} - m, d^\perp \geq 3]$$

when $m \equiv 0 \pmod{4}$.

Example 5 Let $m = 6$. Then the code \mathcal{C}_D has parameters $[31, 6, 12]$ and weight enumerator $1 + 10z^{12} + 47z^{16} + 6z^{20}$. Its dual \mathcal{C}_D^\perp has parameters $[31, 25, 3]$ and is almost optimal.

Table 3 The weight distribution of the codes \mathcal{C}_D of Theorem 5 when $m \equiv 2 \pmod{4}$

Weight w	Multiplicity A_w
0	1
2^{m-2}	$3 \cdot 2^{m-2} - 1$
$2^{m-2} + 2^{\frac{m-2}{2}}$	$2^{m-3} - 2^{\frac{m-4}{2}}$
$2^{m-2} - 2^{\frac{m-2}{2}}$	$2^{m-3} + 2^{\frac{m-4}{2}}$

Table 4 The weight distribution of the codes C_D of Theorem 5 when $m \equiv 0 \pmod{4}$

Weight w	Multiplicity A_w
0	1
$2^{m-2} - (-1)^{\frac{m}{4}} 2^{\frac{m-2}{2}}$	$3 \cdot 2^{m-2}$
$2^{m-2} - [(-1)^{\frac{m}{4}} + 1] 2^{\frac{m-2}{2}}$	$2^{m-3} + 2^{\frac{m-4}{2}} + \frac{1}{2}[(-1)^{\frac{m}{4}} - 1]$
$2^{m-2} - [(-1)^{\frac{m}{4}} - 1] 2^{\frac{m-2}{2}}$	$2^{m-3} - 2^{\frac{m-4}{2}} - \frac{1}{2}[(-1)^{\frac{m}{4}} + 1]$

Example 6 Let $m = 10$. Then the code C_D has parameters $[511, 10, 240]$ and weight enumerator $1 + 136z^{240} + 767z^{256} + 120z^{272}$. Its dual C_D^\perp has parameters $[511, 501, 3]$.

Example 7 Let $m = 4$. Then the code C_D has parameters $[11, 4, 4]$ and weight enumerator $1 + 2z^4 + 12z^6 + z^8$. This code is almost optimal. Its dual C_D^\perp has parameters $[11, 7, 3]$ and is optimal.

Example 8 Let $m = 8$. Then the code C_D has parameters $[111, 8, 48]$ and weight enumerator $1 + 36z^{48} + 192z^{56} + 27z^{64}$. Its dual C_D^\perp has parameters $[111, 103, 3]$ and is almost optimal.

6.2 The proofs of Theorems 4 and 5

For any a and b in $\text{GF}(q)$, we define the following exponential sum

$$S(a, b) = \sum_{x \in \text{GF}(q)} \chi_1(ax^3 + bx). \tag{11}$$

To prove the weight distributions of the codes in Theorems 4 and 5, we need the values of the sum $S(a, b)$.

We now define a constant as follows. Let

$$n_0 = \left| \left\{ x \in \text{GF}(q) : \text{Tr}(x^3 + x) = 0 \right\} \right|.$$

By definition, the length n of the code C_D of (2) is equal to $n_0 - 1$. We have

$$\begin{aligned} n_0 &= \frac{1}{2} \sum_{y \in \text{GF}(2)} \sum_{x \in \text{GF}(q)} (-1)^{y\text{Tr}(x^3+x)} \\ &= \frac{1}{2} \sum_{y \in \text{GF}(2)} \sum_{x \in \text{GF}(q)} \chi_1(yx^3 + yx) \\ &= 2^{m-1} + \frac{1}{2} \sum_{x \in \text{GF}(q)} \chi_1(x^3 + x). \end{aligned} \tag{12}$$

To prove Theorems 4 and 5, we also define the following parameter

$$N_b = \left| \left\{ x \in \text{GF}(q) : \text{Tr}(x^3 + x) = 0 \text{ and } \text{Tr}(bx) = 0 \right\} \right|,$$

where $b \in \text{GF}(q)^*$. By definition and the basic facts of additive characters, for any $b \in \text{GF}(q)^*$ we have

$$\begin{aligned}
 N_b &= \frac{1}{4} \sum_{x \in \text{GF}(q)} \left(\sum_{y \in \text{GF}(2)} (-1)^{y\text{Tr}(x^3+x)} \right) \left(\sum_{z \in \text{GF}(2)} (-1)^{z\text{Tr}(bx)} \right) \\
 &= \frac{1}{4} \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}(bx)} + \frac{1}{4} \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}(x^3+x)} \\
 &\quad + \frac{1}{4} \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}(x^3+(b+1)x)} + 2^{m-2} \\
 &= \frac{1}{4} \left(\sum_{x \in \text{GF}(q)} \left(\chi_1(x^3+x) + \chi_1(x^3+(b+1)x) \right) + 2^m \right). \tag{13}
 \end{aligned}$$

For any $b \in \text{GF}(q)^*$, the Hamming weight $\text{wt}(\mathbf{c}_b)$ of the following codeword

$$\mathbf{c}_b = (\text{Tr}(bd_1), \text{Tr}(bd_2), \dots, \text{Tr}(bd_n)) \tag{14}$$

of the code \mathcal{C}_D of (2) is equal to $n_0 - N_b$.

Let $m \geq 4$ be odd. It is well known that $\text{Tr}(x^3)$ is a semibent function from $\text{GF}(q)$ to $\text{GF}(2)$. Thus, we have

$$\sum_{x \in \text{GF}(q)} \chi_1(x^3 + (b+1)x) \in \{0, 2^{\frac{m+1}{2}}, -2^{\frac{m+1}{2}}\} \tag{15}$$

for each $b \in \text{GF}(q)^*$.

The following lemma is proved in Theorem 2 of [5].

Lemma 2 *When m is odd, we have*

$$S(1, 1) = \sum_{x \in \text{GF}(q)} \chi_1(x^3 + x) = (-1)^{\frac{m^2-1}{8}} 2^{\frac{m+1}{2}}.$$

We are now ready to prove Theorem 4. Let $m \geq 4$ be odd.

It follows from (12) and Lemma 2 that the length n of the code \mathcal{C}_D in Theorem 4 is equal to $2^{m-1} + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-1}{2}} - 1$, as $n_0 = 2^{m-1} + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-1}{2}}$.

It follows from (13), (15) and Lemma 2 that

$$N_b \in \left\{ 2^{m-2} + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-3}{2}}, 2^{m-2} + [(-1)^{\frac{m^2-1}{8}} \pm 1] 2^{\frac{m-3}{2}} \right\}$$

for any $b \in \text{GF}(q)^*$. Hence, the weight $\text{wt}(\mathbf{c}_b)$ of the codeword \mathbf{c}_b in (14) satisfies

$$\text{wt}(\mathbf{c}_b) = n_0 - N_b \in \left\{ 2^{m-2} + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-3}{2}}, 2^{m-2} + [(-1)^{\frac{m^2-1}{8}} \mp 1] 2^{\frac{m-3}{2}} \right\}.$$

Define

$$\begin{aligned}
 w_1 &= 2^{m-2} + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-3}{2}}, \\
 w_2 &= 2^{m-2} + \left[(-1)^{\frac{m^2-1}{8}} - 1 \right] 2^{\frac{m-3}{2}}, \\
 w_3 &= 2^{m-2} + \left[(-1)^{\frac{m^2-1}{8}} + 1 \right] 2^{\frac{m-3}{2}}.
 \end{aligned}$$

We now determine the number A_{w_i} of codewords with weight w_i in \mathcal{C}_D . By Lemma 1, the minimum weight of the dual code \mathcal{C}_D^\perp is at least 3. The first three Pless Power Moments [15, p.260] lead to the following system of equations:

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} &= 2^m - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} &= n2^{m-1}, \\ w_1^2 A_{w_1} + w_2^2 A_{w_2} + w_3^2 A_{w_3} &= n(n + 1)2^{m-2}, \end{cases} \tag{16}$$

where $n = 2^{m-1} + (-1)^{\frac{m^2-1}{8}} 2^{\frac{m-1}{2}} - 1$. Solving the system of equations in (16) yields the weight distribution of Table 2. The dimension of the code \mathcal{C}_D is m , as $\text{wt}(\mathbf{c}_b) > 0$ for each $b \in \text{GF}(q)^*$. The conclusions on the dual code \mathcal{C}_D^\perp then follow on the length and the dimension of \mathcal{C}_D and Lemma 1. This completes the proof of Theorem 4.

Below we prove Theorem 5

Let $m \geq 4$ be even. To prove Theorem 5, we need the next two lemmas proved by Coulter [6].

Lemma 3 *Let $m \geq 4$ be even and $a \in \text{GF}(q)^*$. Then*

$$S(a, 0) = \begin{cases} (-1)^{\frac{m}{2}} 2^{\frac{m}{2}} & \text{if } a \neq g^{3t} \text{ for any } t, \\ -(-1)^{\frac{m}{2}} 2^{\frac{m}{2}+1} & \text{if } a = g^{3t} \text{ for some } t, \end{cases}$$

where g is a generator of $\text{GF}(q)^*$.

Lemma 4 *Let $m \geq 4$ be even, $b \in \text{GF}(q)^*$, $f(x) = a^2x^4 + ax \in \text{GF}(q)[x]$, and let g be a generator of $\text{GF}(q)^*$. There are the following two cases.*

- (i) *If $a \neq g^{3t}$ for any t , then f is a permutation polynomial of $\text{GF}(q)$. Let x_0 be the unique element satisfying $f(x_0) = b^2$. Then*

$$S(a, b) = (-1)^{\frac{m}{2}} 2^{\frac{m}{2}} \chi_1(ax_0^3) = (-1)^{\frac{m}{2}} 2^{\frac{m}{2}} (-1)^{\text{Tr}(ax_0^3)}.$$

- (ii) *If $a = g^{3t}$ for some t , then $S(a, b) = 0$ unless the equation $f(x) = b^2$ is solvable. If this equation is solvable, with solution x_0 say, then*

$$S(a, b) = \begin{cases} -(-1)^{\frac{m}{2}} 2^{\frac{m}{2}+1} (-1)^{\text{Tr}(ax_0^3)} & \text{if } \text{Tr}(a) = 0, \\ (-1)^{\frac{m}{2}} 2^{\frac{m}{2}} (-1)^{\text{Tr}(ax_0^3)} & \text{if } \text{Tr}(a) \neq 0, \end{cases}$$

where Tr is the trace function from $\text{GF}(q)$ onto $\text{GF}(2)$.

According to [7, p.29], the following lemma can be easily proved.

Lemma 5 *Let $m \geq 4$ be even and $f(x) = a^2x^4 + ax \in \text{GF}(q)[x]$. If $a = 1 = g^{3t}$ for some t , then the equation $f(x) = 1$ is solvable if and only if $m \equiv 0 \pmod{4}$, where g is a generator of $\text{GF}(q)^*$.*

The next lemma will be employed later.

Lemma 6 *Let $m \geq 4$ be even. Then*

$$S(1, 1) = \begin{cases} 0 & \text{if } m \equiv 2 \pmod{4}, \\ -(-1)^{\frac{m}{4}} 2^{\frac{m}{2}+1} & \text{if } m \equiv 0 \pmod{4}. \end{cases}$$

Proof Let $m \geq 4$ be even. It is well known that $\gcd(3, 2^m - 1) = 3$. Hence, there exists $t = \frac{2^m-1}{3}$ such that $g^{3t} = 1$. Note that $\text{Tr}(1) = 0$, as m is even. It then follows from Lemmas 4 and 5 that

$$\begin{aligned}
 S(1, 1) &= \begin{cases} 0 & \text{if } m \equiv 2 \pmod{4} \\ -2^{\frac{m}{2}+1}(-1)^{\text{Tr}(x_0^3)} & \text{if } m \equiv 0 \pmod{4} \end{cases} \\
 &= \begin{cases} 0 & \text{if } m \equiv 2 \pmod{4} \\ -2^{\frac{m}{2}+1}(-1)^{\frac{m}{4} \pmod{2}} & \text{if } m \equiv 0 \pmod{4} \end{cases} \\
 &= \begin{cases} 0 & \text{if } m \equiv 2 \pmod{4}, \\ -2^{\frac{m}{2}+1}(-1)^{\frac{m}{4}} & \text{if } m \equiv 0 \pmod{4}, \end{cases}
 \end{aligned}$$

where x_0 is a solution of the equation $x^4 + x = 1$ when $m \equiv 0 \pmod{4}$. This completes the proof. \square

We are now ready to prove Theorem 5. Recall that $m \geq 4$ is even. It follows from (12) and Lemma 6 that the length n of the code \mathcal{C}_D in Theorem 5 is given by

$$n = \begin{cases} 2^{m-1} - 1 & \text{if } m \equiv 2 \pmod{4}, \\ 2^{m-1} - 2^{\frac{m}{2}}(-1)^{\frac{m}{4}} - 1 & \text{if } m \equiv 0 \pmod{4}. \end{cases} \tag{17}$$

Since $\gcd(3, 2^m - 1) = 3$, there exists $t = \frac{2^m-1}{3}$ such that $g^{3t} = 1$. Note that $\text{Tr}(1) = 0$, as m is even. It follows from Lemmas 3 and 4 that

$$S(1, b + 1) \in \left\{ 0, \pm(-1)^{\frac{m}{2}} 2^{\frac{m}{2}+1} \right\} \tag{18}$$

for any $b \in \text{GF}(q)^*$.

It then follows from (13), (18) and Lemma 6 that

$$N_b \in \{u_1, \pm u_2 + u_1\}$$

when $m \equiv 2 \pmod{4}$, and

$$N_b \in \left\{ u_1 - (-1)^{\frac{m}{4}} u_2, (-(-1)^{\frac{m}{4}} \pm 1) u_2 + u_1 \right\}$$

when $m \equiv 0 \pmod{4}$, for any $b \in \text{GF}(q)^*$, where $u_1 = 2^{m-2}$ and $u_2 = 2^{\frac{m}{2}-1}$. Hence, the weight $\text{wt}(\mathbf{c}_b)$ of the codeword of (14) satisfies

$$\text{wt}(\mathbf{c}_b) = n_0 - N_b \in \begin{cases} \{u_1, u_1 \pm u_2\} & \text{if } m \equiv 2 \pmod{4} \\ \{u_1 - (-1)^{\frac{m}{4}} u_2, u_1 - ((-1)^{\frac{m}{4}} \pm 1) u_2\} & \text{if } m \equiv 0 \pmod{4} \end{cases}$$

and the code \mathcal{C}_D has all the three weights in the set above.

Define $u_1 = 2^{m-2}$, $u_2 = 2^{\frac{m}{2}-1}$, $u = u_1 - (-1)^{\frac{m}{4}} u_2$ and

$$\begin{cases} w_1 = u_1, w_2 = u_1 + u_2, w_3 = u_1 - u_2 & \text{if } m \equiv 2 \pmod{4} \\ w_1 = u, w_2 = u - u_2, w_3 = u + u_2 & \text{if } m \equiv 0 \pmod{4}. \end{cases}$$

We now determine the number A_{w_i} of codewords with weight w_i in \mathcal{C}_D . By Lemma 1, the minimum weight of the dual code \mathcal{C}_D^\perp is at least 3. The first three Pless Power Moments [15, p.260] lead to the following system of equations:

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} &= 2^m - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} &= n 2^{m-1}, \\ w_1^2 A_{w_1} + w_2^2 A_{w_2} + w_3^2 A_{w_3} &= n(n + 1) 2^{m-2}, \end{cases} \tag{19}$$

where n is given in (17). Solving the system of equations in (19) proves the weight distribution of the code \mathcal{C}_D in Tables 3 and 4. The dimension of the code \mathcal{C}_D is m , as $\text{wt}(\mathbf{c}_b) > 0$

for each $b \in \text{GF}(q)^*$. The conclusions on the dual code \mathcal{C}_D^\perp then follow on the length and the dimension of \mathcal{C}_D and Lemma 1. This completes the proof of Theorem 5.

6.3 Applications of the binary codes in secret sharing

Any linear code over $\text{GF}(p)$ can be employed to construct secret sharing schemes [1, 4, 18]. In order to obtain secret sharing schemes with interesting access structures, one would like to have linear codes \mathcal{C} such that $w_{\min}/w_{\max} > \frac{p-1}{p}$ [18], where w_{\min} and w_{\max} denote the minimum and maximum nonzero weight of the linear code.

When $m \equiv 2 \pmod{4}$ and $m \geq 6$, the code \mathcal{C}_D of Section 6.1 satisfies that

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{m-2} - 2^{(m-2)/2}}{2^{m-2} + 2^{(m-2)/2}} > \frac{1}{2}.$$

When $m \equiv 4 \pmod{8}$ and $m > 4$, the code \mathcal{C}_D of Section 6.1 satisfies that

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

When $m \equiv 0 \pmod{8}$ and $m \geq 8$, the code \mathcal{C}_D of Section 6.1 satisfies that

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

When $m \equiv \pm 1 \pmod{8}$ and $m \geq 7$, the code \mathcal{C}_D of Section 6.1 satisfies that

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{m-2}}{2^{m-2} + 2^{(m-1)/2}} > \frac{1}{2}.$$

When $m \equiv \pm 3 \pmod{8}$ and $m > 5$, the code \mathcal{C}_D of Section 6.1 satisfies that

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{m-2} - 2^{(m-1)/2}}{2^{m-2}} > \frac{1}{2}.$$

Hence, the linear codes \mathcal{C}_D of Section 6.1 satisfy the condition that $w_{\min}/w_{\max} > \frac{1}{2}$ when $m \geq 6$, and can thus be employed to obtain secret sharing schemes with interesting access structures using the framework in [18]. Note that binary linear codes can be employed for secret sharing bit by bit. Hence, a secret of any size can be shared with a secret sharing scheme based on a binary linear code. We remark that the dimension of the code \mathcal{C}_D of this paper is small compared with its length and this makes it suitable for the application in secret sharing.

7 Concluding remarks

In this paper, we established a few relations among the parameters of a few subclasses of linear codes \mathcal{C}_D (i.e., Theorem 1, Corollaries 1 and 2, Theorem 2, Corollary 5). With these relations, a number of classes of one-weight, two-weight and three-weight codes are derived from some known classes of one-weight, two-weight and three-weight codes. Instead of writing down all these codes, we documented a few classes of them as examples in this paper. We also constructed a class of three-weight binary codes described in Theorems 4 and 5.

The codes presented in this paper are interesting, as one-weight codes, two-weight codes and three-weight codes have applications in secret sharing [1, 4, 18], authentication codes [12], combinatorial designs and graph theory [2, 3], and association schemes [2].

Every linear code over a finite field is generated by a generator matrix. Different ways of constructing the generator matrix give different constructions of linear codes. Similarly, different ways of constructing the defining set D for the generic construction of linear codes in this paper are different constructions of the linear codes \mathcal{C}_D . There are a huge number of ways of constructing the defining D , and thus many different constructions of the codes \mathcal{C}_D . The difficulty is the selection of D so that the code \mathcal{C}_D has good parameters. Note that the generic construction of linear codes \mathcal{C}_D of this paper is different from the one in [4].

References

1. Anderson, R., Ding, C., Helleseht, T., Kløve, T.: How to build robust shared control systems. Des. Codes Cryptogr. **15**(2), 111–124 (1998)
2. Calderbank, A.R., Goethals, J.M.: Three-weight codes and association schemes. Philips J. Res. **39**, 143–152 (1984)
3. Calderbank, A.R., Kantor, W.M.: The geometry of two-weight codes. Bull. London Math. Soc. **18**, 97–122 (1986)
4. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inf. Theory **51**(6), 2089–2102 (2005)
5. Carlitz, L.: Explicit evaluation of certain exponential sums. Mathematica Scandinavica **44**, 5–16 (1979)
6. Coulter, R.S.: On the evaluation of a class of Weil sums in characteristic 2. New Zealand J. of Math. **28**, 171–184 (1999)
7. Dickson, L.E.: Linear Groups with an Exposition of the Galois Field Theory. Dover, New York (1958)
8. Ding, C.: A class of three-weight and four-weight codes. In: Xing, C., et al. (eds.) Proc. of the Second International Workshop on Coding Theory and Cryptography, Lecture Notes in Computer Science, vol. 5557, pp. 34–42. Springer, Berlin (2009)
9. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **60**(6), 3265–3275 (2015)
10. Ding, C., Luo, J., Niederreiter, H.: Two weight codes punctured from irreducible cyclic codes. In: Li, Y., Ling, S., Niederreiter, H., Wang, H., Xing, C., Zhang, S. (eds.) Proc. of the First International Workshop on Coding Theory and Cryptography, pp. 119–124. World Scientific, Singapore (2008)
11. Ding, C., Niederreiter, H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory **53**(6), 2274–2277 (2007)
12. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**, 81–99 (2005)
13. Ding, K., Ding, C.: Binary linear codes with three weights. IEEE Commun. Lett. **18**(11), 1879–1882 (2014)
14. Ding, K., Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing, to appear in IEEE Trans. Inf. Theory. arXiv:1503.06512
15. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
16. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1997)
17. Wang, Q., Ding, K., Xue, R.: Binary linear codes with two weights. IEEE Commun. Lett. **19**, 1097–1100 (2015)
18. Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**(1), 206–212 (2006)