Binary Linear Codes With Three Weights

Kelan Ding and Cunsheng Ding

***Abstract*—In this paper, a class of binary three-weight linear codes is constructed. Their dual codes are also studied. The dual codes are either optimal or almost optimal. These codes have applications in authentication codes, secret sharing schemes, and association schemes, in addition to their applications in consumer electronics and communication and data storage systems.**

***Index Terms*—Association schemes, authentication codes, linear codes, permutation polynomial, secret sharing schemes.**

I. Introduction

THROUGHOUT this paper, let $q = 2^m$ for some positive integer m, and let GF(q) denote the finite field with q elements. An $[n, k]$ binary code $\mathcal{C}$ is a k-dimensional subspace of GF(2)^n. An $[n, k, d]$ binary code $\mathcal{C}$ is a k-dimensional subspace of GF(2)^n with minimum (Hamming) distance d.

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 $1 + A_1 z + A_2 z^2 + \ldots + A_n z^n$. The *weight distribution* $(1, A_1, \ldots, A_n)$ is an important research topic in coding theory, as it contains crucial information as to estimate the error correcting capability and the probability of error detection and correction with respect to some algorithms. A code $\mathcal{C}$ is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1, A_2, \cdots, A_n)$ is equal to t. An $[n, k, d]$ binary code $\mathcal{C}$ is called *optimal* if its parameters n, k and d meet a bound on linear codes [13, Chapter 2]. An $[n, k, d]$ binary code $\mathcal{C}$ is called *almost optimal* if $[n, k, d + 1]$ meets a bound on linear codes [13, Chapter 2].

Let $D = \{d_1, d_2, \ldots, d_n\} \subseteq$ GF(q)*. Let Tr denote the trace function from GF(q) onto GF(2) throughout this paper. We define a linear code of length n over GF(2) by

$$\mathcal{C}_D = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) : x \in \mathrm{GF}(q)\}, \quad (1)$$

and call D the *defining set* of this code $\mathcal{C}_D$. Different orderings of the elements of D result in different codes $\mathcal{C}_D$, but the codes are permutation equivalent [13, p. 20]. Permutation equivalent codes have the same length, dimension and weight distribution. Hence, any indexing of the elements of the defining set D will not affect the conclusions of the code $\mathcal{C}_D$ in the theorems of this paper.

Manuscript received August 19, 2014; revised September 20, 2014; accepted September 26, 2014. Date of publication October 3, 2014; date of current version November 7, 2014. The work of C. Ding was supported by the Hong Kong Research Grants Council under Grant 601013. The associate editor coordinating the review of this paper and approving it for publication was M. Baldi.

K. Ding is with the Institute of Information Engineering, The Chinese Academy of Sciences, Beijing 100864, China (e-mail: dingkelan@iie.ac.cn).

C. Ding is with the Department of Computer Science and Engineering, School of Engineering, The Hong Kong University of Science and Technology, Kowloon, Hong Kong (e-mail: cding@ust.hk).

Digital Object Identifier 10.1109/LCOMM.2014.2361516

TABLE I
THE WEIGHT DISTRIBUTION OF THE CODES OF THEOREM 1

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

This construction approach is generic in the sense that many classes of known codes could be produced by selecting the defining set $D \subseteq$ GF(q). It was employed in [9] and [10] for obtaining linear codes with a few weights.

The objective of this paper is to construct a class of binary linear codes with three nonzero weights and new parameters using this generic construction approach. The duals of the linear codes with three weights obtained in this paper are either optimal or almost optimal. The binary linear codes with three weights presented in this paper have applications in secret sharing schemes [1], authentication codes [11], and association schemes [2], in addition to their applications in consumer electronics, communication and data storage systems.

II. The Binary Linear Codes and Their Parameters

We only describe the binary codes and introduce their parameters in this section. The proofs of their parameters will be presented later.

Let h be an integer with $1 \le h < m/2$, where m is a positive integer. Define $\ell = \gcd(m, h)$. In this paper, the defining set D of the code $\mathcal{C}_D$ of (1) is given by

$$D = \left\{ x \in \mathrm{GF}(q)^* : \mathrm{Tr}\left(x^{2^h+1}\right) = 0 \right\}. \quad (2)$$

Theorem 1: Let m/ℓ be odd, and let D be defined in (2). Then the set $\mathcal{C}_D$ of (1) is a $[2^{m-1} - 1, m]$ binary code with the weight distribution in Table I.

Example 1: Let $(m, h) = (5, 1)$. Then $m/\ell = 5$, and the code $\mathcal{C}_D$ has parameters [15, 5, 6] and weight enumerator $1 + 10z^6 + 15z^8 + 6z^{10}$. This code is almost optimal, as the optimal one has parameters [15, 5, 7] by the Griesmer bound.

Example 2: Let $(m, h) = (6, 2)$. Then $m/\ell = 3$, and the code $\mathcal{C}_D$ has parameters [31, 6, 12] and weight enumerator $1 + 10z^{12} + 47z^{16} + 6z^{20}$.

Theorem 2: Let m/ℓ be even, and let D be defined in (2). Then the binary code $\mathcal{C}_D$ of (1) has parameters

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

and the weight distribution in Table II.

Example 3: Let $(m, h) = (8, 1)$. Then $m/\ell = 8$, and the code $\mathcal{C}_D$ has parameters [111, 8, 48] and weight enumerator $1 + 36z^{48} + 192z^{56} + 27z^{64}$.

TABLE II
THE WEIGHT DISTRIBUTION OF THE CODES OF THEOREM 2

Weight w	Multiplicity A_w
0	1
2^{m-2}	$2^{m-2\ell-1}-1-(-1)^{\frac{m}{2\ell}}2^{\frac{m}{2}-\ell-1}$
$2^{m-2}-(-1)^{\frac{m}{2\ell}}2^{\frac{m}{2}+\ell-2}$	$2^m-2^{m-2\ell}$
$2^{m-2}-(-1)^{\frac{m}{2\ell}}2^{\frac{m}{2}+\ell-1}$	$2^{m-2\ell-1}+(-1)^{\frac{m}{2\ell}}2^{\frac{m}{2}-\ell-1}$

Example 4: Let $(m,h)=(8,2)$. Then $m/\ell=4$. The code $\mathcal{C}_D$ has parameters [95, 8, 32] and weight enumerator $1+10z^{32}+240z^{48}+5z^{64}$.

III. THE PROOFS OF THE MAIN RESULTS

Our task in this section is to prove Theorems 1 and 2. Before doing this, we need to do some preparations. We start with group characters.

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

$$\chi_b(c)=(-1)^{\mathrm{Tr}(bc)} \quad \text{for all } c\in \mathrm{GF}(q) \tag{3}$$

defines an additive character of GF(q). When $b=0$, $\chi_0(c)=1$ for all $c\in \mathrm{GF}(q)$, and is called the *trivial additive character* of GF(q). The character χ_1 in (3) is called the *canonical additive character* of GF(q). It is known that every additive character of GF(q) can be written as $\chi_b(x)=\chi_1(bx)$ [16, Theorem 5.7].

For any a and b in GF(q), we define the following exponential sum

$$S_h(a,b)=\sum_{x\in \mathrm{GF}(q)}\chi_1\left(ax^{2^h+1}+bx\right). \tag{4}$$

To prove the weight distributions of the codes in Theorems 1 and 2, we need the values of the sum $S_h(a,b)$.

We now define a constant as follows. Let

$$n_0=\left|\left\{x\in \mathrm{GF}(q):\mathrm{Tr}\left(x^{2^h+1}\right)=0\right\}\right|.$$

By definition, the length n of the code $\mathcal{C}_D$ of (1) is equal to n_0-1. We have

$$\begin{aligned} n_0&=\frac{1}{2}\sum_{y\in \mathrm{GF}(2)}\sum_{x\in \mathrm{GF}(q)}(-1)^{y\mathrm{Tr}\left(x^{2^h+1}\right)}\\ &=\frac{1}{2}\sum_{y\in \mathrm{GF}(2)}\sum_{x\in \mathrm{GF}(q)}\chi_1\left(yx^{2^h+1}\right)\\ &=2^{m-1}+\frac{1}{2}\sum_{x\in \mathrm{GF}(q)}\chi_1\left(x^{2^h+1}\right). \end{aligned} \tag{5}$$

To prove Theorems 1 and 2, we also define the following parameter

$$N_b=\left|\left\{x\in \mathrm{GF}(q):\mathrm{Tr}\left(x^{2^h+1}\right)=0 \text{ and } \mathrm{Tr}(bx)=0\right\}\right|,$$

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

$$\begin{aligned} N_b&=\frac{1}{4}\sum_{x\in \mathrm{GF}(q)}\left(\sum_{y\in \mathrm{GF}(2)}(-1)^{y\mathrm{Tr}\left(x^{2^h+1}\right)}\right)\left(\sum_{z\in \mathrm{GF}(2)}(-1)^{z\mathrm{Tr}(bx)}\right)\\ &=\frac{1}{4}\sum_{x\in \mathrm{GF}(q)}(-1)^{\mathrm{Tr}(bx)}+\frac{1}{4}\sum_{x\in \mathrm{GF}(q)}(-1)^{\mathrm{Tr}\left(x^{2^h+1}\right)}\\ &\quad+\frac{1}{4}\sum_{x\in \mathrm{GF}(q)}(-1)^{\mathrm{Tr}\left(x^{2^h+1}+bx\right)}+2^{m-2}\\ &=\frac{1}{4}\left(\sum_{x\in \mathrm{GF}(q)}\left(\chi_1\left(x^{2^h+1}\right)+\chi_1\left(x^{2^h+1}+bx\right)\right)+2^m\right). \end{aligned} \tag{6}$$

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

$$\mathbf{c}_b=(\mathrm{Tr}(xd_1),\mathrm{Tr}(xd_2),\ldots,\mathrm{Tr}(xd_n)) \tag{7}$$

of the code $\mathcal{C}_D$ of (1) is equal to n_0-N_b.

A. The Proof of Theorem 1

It is well known that

$$\gcd(2^h+1,2^m-1)=\begin{cases}1 & \text{if } m/\ell \text{ is odd},\\ 2^\ell+1 & \text{if } m/\ell \text{ is even}.\end{cases} \tag{8}$$

Hence, x^{2^h+1} is a permutation polynomial over GF(q). Thus, we have the following lemma [5].

Lemma 3: When m/ℓ is odd, we have

$$\sum_{x\in \mathrm{GF}(q)}\chi_1\left(ax^{2^h+1}\right)=0$$

for each $a\in \mathrm{GF}(q)^*$.

We will need the following lemma [5].

Lemma 4: Let $b\in \mathrm{GF}(q)^*$ and suppose m/ℓ is odd. Then $S_h(a,b)=S_h(1,bc^{-1})$, where $c\in \mathrm{GF}(q)^*$ is the unique element satisfying $c^{2^h+1}=a$. Further, we have

$$S_h(1,b)=\begin{cases}0 & if\ \mathrm{Tr}_\ell(b)\neq 1,\\ \pm 2^{(m+\ell)/2} & if\ \mathrm{Tr}_\ell(b)=1,\end{cases}$$

where and hereafter Tr_ℓ is the trace function from GF(q) to GF(2^ℓ).

We are now ready to prove Theorem 1. Let m/ℓ be odd. It follows from (5) and Lemma 3 that the length n of the code $\mathcal{C}_D$ in Theorem 1 is equal to $2^{m-1}-1$, as $n_0=2^{m-1}$.

It follows from (6), Lemmas 3 and 4 that

$$N_b\in\left\{2^{m-2},2^{m-2}\pm 2^{\frac{m+\ell-4}{2}}\right\}$$

for any $b\in \mathrm{GF}(q)^*$. Hence, the weight $\mathrm{wt}(\mathbf{c}_b)$ of the codeword $\mathbf{c}_b$ in (7) satisfies

$$\mathrm{wt}(\mathbf{c}_b)=n_0-N_b\in\left\{2^{m-2},2^{m-2}\pm 2^{\frac{m+\ell-4}{2}}\right\}.$$

It will be proved that the minimum weight of the dual code $\mathcal{C}_D^\perp$ is at least 3 (see Theorem 7). Define

$w_1{=}2^{m-2}-2^{(m+\ell-4)/2}$, $w_2{=}2^{m-2}$, $w_3{=}2^{m-2}+2^{(m+\ell-4)/2}$.

We now determine the number A_{w_i} of codewords with weight w_i in $\mathcal{C}_D$. The first three Pless Power Moments [13, p. 260] lead to the following system of equations:

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} = 2^m - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} = n2^{m-1}, \\ w_1^2 A_{w_1} + w_2^2 A_{w_2} + w_3^2 A_{w_3} = n(n+1)2^{m-2}, \end{cases} \tag{9}$$

where $n = 2^{m-1} - 1$. Solving the system of equations in (9) yields the weight distribution of Table I. The dimension of the code $\mathcal{C}_D$ is m, as $\mathrm{wt}(\mathbf{c}_b) > 0$ for each $b \in \mathrm{GF}(q)^*$. This completes the proof of Theorem 1.

B. The Proof of Theorem 2

Let m/ℓ be even. To prove Theorem 2, we need the next two lemmas proved by Coulter [5].

Lemma 5: Let m/ℓ be even so that $m = 2e$. Then

$$S_h(a,0) = \begin{cases} (-1)^{e/\ell} 2^e \ if \ a \neq g^{t(2^\ell+1)} \ for \ any \ t, \\ -(-1)^{e/\ell} 2^{e+\ell} \ if \ a = g^{t(2^\ell+1)} \ for \ some \ t, \end{cases}$$

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

Lemma 6: Let $b \in \mathrm{GF}(q)^*$ and suppose m/ℓ is even so that $m = 2e$ for some integer e. Let $f(x) = a^{2^h} x^{2^{2h}} + ax \in \mathrm{GF}(q)[x]$. There are two cases.

(i) If $a \neq g^{t(2^\ell+1)}$ for any t, then f is a permutation polynomial of $\mathrm{GF}(q)$.Let x_0 be the unique element satisfying $f(x_0) = b^{2^h}$. Then

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

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

$$S_h(a,b) = \begin{cases} -(-1)^{e/\ell} 2^{e+\ell} \chi_1\left(a x_0^{2^h+1}\right) & if \ \mathrm{Tr}_\ell(a) = 0, \\ (-1)^{e/\ell} 2^e \chi_1\left(a x_0^{2^h+1}\right) & if \ \mathrm{Tr}_\ell(a) \neq 0, \end{cases}$$

where Tr_ℓ is the trace function from $\mathrm{GF}(q)$ to $\mathrm{GF}(2^\ell)$.

We are now ready to prove Theorem 2. Recall that m/ℓ is even. It follows from (5) and Lemma 5 that the length n of the code $\mathcal{C}_D$ in Theorem 2 is given by

$$n = n_0 - 1 = 2^{m-1} - (-1)^{\frac{m}{2\ell}} 2^{\frac{m}{2}+\ell-1} - 1. \tag{10}$$

Since $1 \leq h < m/2$, $\gcd(2h, m) < m$. We know that the equation $x^{2^{2h}} + x = b^{2^h}$ must have a solution for some $b \in \mathrm{GF}(q)^*$. Note that $\mathrm{Tr}_\ell(1) = 0$, as m/ℓ is even. It then follows from (6), Lemmas 5 and 6 that

$$N_b \in \left\{2^{m-2}, 2^{m-2} - (-1)^{e/\ell} 2^{e+\ell-2}, 2^{m-2} - (-1)^{e/\ell} 2^{e+\ell-1}\right\}$$

for any $b \in \mathrm{GF}(q)^*$ and N_b takes on all the three values in the set above. Hence, the weight $\mathrm{wt}(\mathbf{c}_b)$ of (7) satisfies

$$\mathrm{wt}(\mathbf{c}_b) = n_0 - N_b \in \left\{2^{m-2}, 2^{m-2} - (-1)^{e/\ell} 2^{e+\ell-2}, 2^{m-2} - (-1)^{e/\ell} 2^{e+\ell-1}\right\},$$

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

It will be proved that the minimum weight of the dual code $\mathcal{C}_D^\perp$ is at least 3 (see Theorem 7). Define $u = -(-1)^{e/\ell} 2^{e+\ell-2}$ and

$$w_1 = w_2 + u, \ w_2 = 2^{m-2} + a, \ w_3 = w_2 - a.$$

We now determine the number A_{w_i} of codewords with weight w_i in $\mathcal{C}_D$. The first three Pless Power Moments [13, p. 260] lead to the following system of equations:

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} = 2^m - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} = n2^{m-1}, \\ w_1^2 A_{w_1} + w_2^2 A_{w_2} + w_3^2 A_{w_3} = n(n+1)2^{m-2}, \end{cases} \tag{11}$$

where n is given in (10). Solving the system of equations in (11) proves the weight distribution of the code $\mathcal{C}_D$ in Table II. The dimension of the code $\mathcal{C}_D$ is m, as $\mathrm{wt}(\mathbf{c}_b) > 0$ for each $b \in \mathrm{GF}(q)^*$. This completes the proof of Theorem 2.

IV. The Duals of the Codes $\mathcal{C}_D$

For the dual $\mathcal{C}_D^\perp$ of the three-weight codes $\mathcal{C}_D$ of this paper, we have the following conclusion.

Theorem 7: Let $m \geq 5$. The dual $\mathcal{C}_D^\perp$ of the three-weight code $\mathcal{C}_D$ is a binary code with parameters $[n, n-m, d^\perp]$, where $n = 2^{m-1} - 1$ if m/ℓ is odd and $n = 2^{m-1} - (-1)^{\frac{m}{2\ell}} 2^{\frac{m}{2}+\ell-1} - 1$ if m/ℓ is even; and $d^\perp = 3$ if m is even and $3 \leq d^\perp \leq 4$ if m is odd.

Proof: The dimension of the code $\mathcal{C}_D^\perp$ follows from Theorems 1 and 2. Since D does not contain the zero element of $\mathrm{GF}(q)$, the minimum distance of $\mathcal{C}_D^\perp$ cannot be one. Similarly, since D is not a multiset, any two elements d_i and d_j of D must be distinct if $i \neq j$. Hence, the minimum distance $\mathcal{C}_D^\perp$ cannot be 2.

When m is even, $1 \in D$. Since $m \geq 5$, $n \geq 2$, then there is another element $b \in D$ such that $b \neq 1$. We have then

$$\mathrm{Tr}\left((1+b)^{2^h+1}\right) = \mathrm{Tr}(1) + \mathrm{Tr}\left(b^{2^h+1}\right) + \mathrm{Tr}\left(b^{2^h}\right) + \mathrm{Tr}(b) = 0.$$

Hence, $\{1, b, 1+b\} \subseteq D$. Therefore, the minimum distance of $\mathcal{C}_D^\perp$ is 3.

When m is odd, $n = 2^{m-1} - 1$. Let $D = \{d_1, d_2, \ldots, d_n\}$. Consider all the sums $d_i + d_j$ with $i \neq j$. The total number of such sums is equal to $(2^{m-1} - 1)(2^{m-2} - 1) > 2^m$ when $m \geq 5$. Hence, there must be four distinct integers i_1, i_2, i_3, i_4 in $\{1, 2, \ldots, n\}$ such that $d_{i_1} + d_{i_2} = d_{i_3} + d_{i_4}$. Hence, $\mathcal{C}_D^\perp$ has a codeword with Hamming weight 4. It then follows that $3 \leq d^\perp \leq 4$. □

We remark that the code $\mathcal{C}_D^\perp$ is at least almost optimal when m is odd, as the minimum weight of any binary code with length $2^{m-1} - 1$ and dimension $2^{m-1} - 1 - m$ is at most 4 due to the sphere packing bound.

Example 5: Let $(m, h) = (5, 1)$. Then the binary code $\mathcal{C}_D^\perp$ has parameters [15, 10, 3] and is almost optimal, while the optimal binary code has parameters [15, 10, 4].

Example 6: Let $(m, h) = (6, 1)$. Then the binary code $\mathcal{C}_D^\perp$ has parameters [39, 33, 3] and is optimal.

Example 7: Let $(m, h) = (6, 2)$. Then the binary code $\mathcal{C}_D^{\perp}$ has parameters [31, 25, 3] and is almost optimal, while the optimal binary code has parameters [31, 25, 4].

V. Concluding Remarks

There is a recent survey on three-weight cyclic codes [8]. Some interesting three-weight codes were presented in [2], [4], [6], [12], [14], [15], [18], and [19]. We did not find the parameters of the three-weight codes of this paper in these references.

The construction of linear codes in this paper is quite different from those in [3] and [19] due to the following:

1) First of all, the codes constructed in [3] and [19] are over GF(p) where p must be odd, while the codes of this paper are binary.
2) Secondly, the codes constructed in [3] and [19] have length $p^m - 1$, while the binary codes of this paper have length $2^{m-1} - 1$ if m is odd and $2^{m-1} - (-1)^{\frac{m}{2t}} 2^{\frac{m}{2}+\ell-1} - 1$ if m is even. Consequently, the formats of the lengths of the codes are not similar.
3) Most differently, the codes constructed in [3] and [19] have dimension $2m$, while the codes of this paper have dimension m.

The three-weight codes $\mathcal{C}_D$ of this paper may yield association schemes with the framework introduced in [2]. Any linear code over GF(p) can be employed to construct secret sharing schemes [1], [3], [17]. In order to obtain secret sharing schemes with interesting access structures, we would like to have linear codes $\mathcal{C}$ such that $w_{\min}/w_{\max} > \frac{p-1}{p}$ [17], where $w_{\min}$ and $w_{\max}$ denote the minimum and maximum nonzero weight of the linear code.

Let m be odd and $\ell = 1$. Then for the code $\mathcal{C}_D$ of Theorem 1 we have

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{m-2} - 2^{(m-3)/2}}{2^{m-2} + 2^{(m-3)/2}} > \frac{1}{2}$$

if $m \geq 5$. Hence, the linear codes $\mathcal{C}_D$ of this paper satisfy the condition that $w_{\min}/w_{\max} > \frac{1}{2}$ under certain conditions, and can be employed to obtain secret sharing schemes with interesting access structures using the framework in [17]. 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.

Acknowledgment

The authors would like to thank the reviewers and the Editor, Dr. Marco Baldi, for their comments that improved the presentation and quality of this paper.

References

[1] R. Anderson, C. Ding, T. Helleseth, and T. Kløve, "How to build robust shared control systems," *Designs, Codes Cryptography*, vol. 15, no. 2, pp. 111–124, Nov. 1998.
[2] A. R. Calderbank and J. M. Goethals, "Three-weight codes and association schemes," *Philips J. Res.*, vol. 39, no. 4/5, pp. 143–152, 1984.
[3] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2089–2102, Jun. 2005.
[4] S.-T. Choi, J.-Y. Kim, J.-S. No, and H. Chung, "Weight distribution of some cyclic codes," in *Proc. Int. Symp. Inf. Theory*, 2012, pp. 2911–2913.
[5] R. S. Coulter, "On the evaluation of a class of Weil sums in characteristic 2," *New Zealand J. of Math.*, vol. 28, pp. 171–184, 1999.
[6] B. Courteau and J. Wolfman, "On triple-sum-sets and two or three weight codes," *Discrete Math.*, vol. 50, no. 1, pp. 179–189, 1884.
[7] C. Ding, T. Helleseth, T. Kløve, and X. Wang, "A general construction of authentication codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2229–2235, Jun. 2007.
[8] C. Ding, C. Li, N. Li, and Z. Zhou, *Three-Weight Cyclic Codes and Their Weight Distributions*, submitted for publication.
[9] C. Ding, J. Luo, and H. Niederreiter, "Two weight codes punctured from irreducible cyclic codes," in *Proc. 1st Int. Workshop Coding Theory Cryptography*, Y. Li, S. Ling, H. Niederreiter, H. Wang, C. Xing, and S. Zhang, Eds., Singapore, 2008, pp. 119–124.
[10] C. Ding and H. Niederreiter, "Cyclotomic linear codes of order 3," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2274–2277, Jun. 2007.
[11] C. Ding and X. Wang, "A coding theory construction of new systematic authentication codes," *Theoretical Comput. Sci.*, vol. 330, no. 1, pp. 81–99, Jan. 2005.
[12] K. Feng and J. Luo, "Value distribution of exponential sums from perfect nonlinear functions and their applications," *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pp. 3035–3041, Sep. 2007.
[13] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[14] C. Li, Q. Yue, and F. Li, "Weight distributions of cyclic codes with respect to pairwise coprime order elements," *Finite Fields Appl.*, vol. 28, pp. 94–114, Jul. 2014.
[15] C. Li, Q. Yue, and F. Li, "Hamming weights of the duals of cyclic codes with two zeros," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 3895–3902, Jul. 2014.
[16] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1997.
[17] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 206–212, Jan. 2006.
[18] Y. Xia, X. Zeng, and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d=(p^n+1)/(p+1)+(p^n-1)/2$," *Appl. Algebra Eng. Commun. Comput.*, vol. 21, no. 5, pp. 329–342, 2010.
[19] Z. Zhou and C. Ding, "A class of three-weight codes," *Finite Fields Appl.*, vol. 25, pp. 79–93, Jan. 2014.