


The weight distribution of a class of two-weight linear codes derived from Kloosterman sums

Pan Tan^{1,3} · Zhengchun Zhou¹ · Deng Tang¹  · Tor Helleseth²

Received: 28 October 2016 / Accepted: 8 March 2017 / Published online: 15 March 2017
© Springer Science+Business Media New York 2017

Abstract Linear codes with few weights have applications in data storage systems, secret sharing schemes, and authentication codes. In this paper, a class of p -ary two-weight linear codes is constructed using a generic construction developed by Ding et al. recently, where p is a prime. Their length and weight distribution are closed-form expressions of Kloosterman sums over prime finite fields, and are completely determined when $p = 2$ and $p = 3$. The dual of this class of linear codes is also studied and is shown to be optimal or almost optimal in the binary case.

Keywords Linear codes · Optimal codes · Secret sharing schemes · Authentication codes · Kloosterman sums

Mathematics Subject Classification (2010) 06E30 · 11T71 · 94A60

✉ Deng Tang
dtang@foxmail.com

Pan Tan
lanqingfeixue@my.swjtu.edu.cn

Zhengchun Zhou
zzc@home.swjtu.edu.cn

Tor Helleseth
tor.helleseth@ii.uib.no

¹ School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China

² Department of Informatics, University of Bergen, N-5020 Bergen, Norway

³ State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

1 Introduction

Let $q = p^m$ and \mathbb{F}_q denote the finite field with q elements, where p is a prime and m is a positive integer. An $[n, k, d]$ linear code \mathcal{C} over \mathbb{F}_p is a k -dimensional subspace of \mathbb{F}_p^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

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

Accordingly, the sequence $(1, A_1, \dots, A_n)$ is called the weight distribution of \mathcal{C} . Clearly, the weight distribution gives the minimum distance of the code, and thus the error correcting capability. Moreover, the weight distribution of a code allows the computation of the error probability of error detection and correction with respect to some error detection and error correction algorithms (see [14] for details). Thus the study of the weight distribution of a linear code is important in both theory and applications.

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 . Linear codes with few weights have applications in secret sharing schemes [1, 3, 18], authentication codes [5, 6], and association schemes [2], in addition to their applications in consumer electronics, communication and data storage systems. They are also closely related with strongly regular graphs and combinatorial design. An $[n, k, d]$ linear code \mathcal{C} is called optimal if its parameters n, k and d meet a bound on linear codes [13]. An $[n, k, d]$ linear code \mathcal{C} is called almost optimal if $[n, k, d + 1]$ meets a bound on linear codes [13].

Design of (almost) optimal linear codes with few weights has been an interesting research topic in coding theory. Much progress has been made in recent years. One of known approaches for obtaining such linear codes is based on subsets of a finite field and the trace function over this field. Specifically, let $D = \{d_1, d_2, \dots, d_n\}$ be a subset of \mathbb{F}_q^* , a linear code of length n over \mathbb{F}_p can be obtained as

$$C_D = \{(\text{Tr}_1^m(ad_1), \text{Tr}_1^m(ad_2), \dots, \text{Tr}_1^m(ad_n)) : a \in \mathbb{F}_q\}, \tag{1}$$

where Tr_1^m is the absolute trace function from \mathbb{F}_q to \mathbb{F}_p and D is called the defining set of this code. It turns out in [7, 8] that this approach is very promising in the sense that it can generate many (almost) optimal linear codes with a few weights if the subset D is appropriately chosen. This is further confirmed by a number of recent papers [11, 12, 17].

An objective of this paper is to construct a class of two-weight linear codes over \mathbb{F}_p with new parameters using the approach mentioned above. They are optimal or almost optimal linear codes in many cases. Another objective of this paper is to study the weight distribution and the dual of this class of linear codes. Thanks to some known results on Kloosterman sums over finite fields, the length and weight distribution of this class of linear codes have a closed-form expression, and are completely determined when $p = 2$ and $p = 3$. The parameters of its dual are also determined which are optimal or almost optimal in the binary case.

2 Preliminaries

Throughout this paper, we adopt the following notations unless otherwise stated:

- p is a prime and $m = 2k$, where k is a positive integer with $k > 2$.
- $q = p^m$ and $r = p^k$.
- $\text{Tr}_{\ell_1}^{\ell_2}(x)$ is the trace function from the finite field $\mathbb{F}_{p^{\ell_2}}$ to $\mathbb{F}_{p^{\ell_1}}$ for any positive integers $\ell_1 | \ell_2$.

- χ is the canonical additive character on \mathbb{F}_q , i.e., $\chi(x) = e^{2\pi\sqrt{-1}\text{Tr}_1^m(x)/p}$ for any $x \in \mathbb{F}_q$.
- For any positive integer $\ell|m$, χ_ℓ is the canonical additive character on \mathbb{F}_{p^ℓ} , i.e., $\chi_\ell(x) = e^{2\pi\sqrt{-1}\text{Tr}_1^\ell(x)/p}$ for any $x \in \mathbb{F}_{p^\ell}$.

Let α be a generator of \mathbb{F}_q^* and $\beta = \alpha^{r-1}$. Let Δ be the cyclic group generated by β and $\Gamma = \{\alpha^j : 0 \leq j \leq r\}$. The following results will be useful to prove our main results.

Fact 1 *With notations defined above, we have*

1. $\{v^{r-1} : v \in \Gamma\} = \Delta$; and
2. for each $x \in \mathbb{F}_q^*$, it has a unique decomposition as $x = uv$, where $u \in \mathbb{F}_r^*$ and $v \in \Gamma$.

Lemma 1 *For any given $a \in \mathbb{F}_q^*$, there is one and only one $v_a \in \Gamma$ such that*

$$\text{Tr}_k^m(av_a) = 0.$$

Proof By Fact 1, x has a unique decomposition as $x = uv$, where $u \in \mathbb{F}_r^*$ and $v \in \Gamma$. Therefore $\text{Tr}_k^m(x) = \text{Tr}_k^m(uv) = u\text{Tr}_k^m(v)$ which implies that the number of solutions $x \in \mathbb{F}_q^*$ to $\text{Tr}_k^m(x) = 0$ is $r-1$ times as the number of solutions $v \in \Gamma$ to $\text{Tr}_k^m(v) = 0$. The conclusion then follows from the fact that the equation $\text{Tr}_k^m(x) = 0$ has $q^{m-k} - 1 = r-1$ solutions in \mathbb{F}_q^* . \square

The length and weights of the linear code proposed in this paper will be expressed by means of the Kloosterman sums over finite field. For any $a \in \mathbb{F}_{p^\ell}$, the Kloosterman sum over \mathbb{F}_{p^ℓ} at the point a is defined by

$$K_\ell(a) = \sum_{x \in \mathbb{F}_{p^\ell}^*} \chi_\ell\left(ax + \frac{1}{x}\right),$$

where ℓ is a positive integer with $\ell|m$. The following bound on $|K_\ell(a)|$ will be needed in the sequel.

Lemma 2 [16] *With notations as above, we have*

$$|K_\ell(a)| \leq 2\sqrt{p^\ell}$$

for any nonzero $a \in \mathbb{F}_{p^\ell}$.

The following result on an incomplete exponential sum was firstly proven in [15] in the binary case and was extended to the nonbinary case by the last author in [10].

Lemma 3 *For any $a \in \mathbb{F}_q^*$, we have*

$$\sum_{x \in \Delta} \chi(ax) = -K_k(a^2).$$

The following lemma is due to Carlitz [4] and will be needed in the sequel.

Lemma 4 *For any $a \in \mathbb{F}_q^*$,*

$$K_k(a) = - \sum_{t=0}^{\lfloor k/2 \rfloor} (-1)^{k-t} \frac{k}{k-t} \binom{k-t}{t} p^t (K_1(a))^{k-2t}.$$

3 A Class of Two-Weight Linear Codes

In this section, we shall study a class of linear codes with two weights. Following the notations in Section 2, let D be a subset of \mathbb{F}_q^* given by

$$D = \left\{ x \in \mathbb{F}_q^* : \text{Tr}_1^m(x^{r-1}) = 0 \right\}. \tag{2}$$

According to (1), we naturally obtain a class of linear codes by using such D as the defining set. The following are the main results of this paper.

Theorem 1 *Let \mathcal{C}_D be the linear code with defining set D in (2). Then \mathcal{C}_D is a two-weight linear code with parameters $[n, m]$ and weight distribution in Table 1, where*

$$n = \frac{(p^k - 1)(p^k + 1 + S)}{p} \tag{3}$$

and

$$S = \sum_{t=0}^{\lfloor k/2 \rfloor} (-1)^{k-t} \frac{k}{k-t} \binom{k-t}{t} p^t \sum_{y \in \mathbb{F}_p^*} (K_1(y^2))^{k-2t}. \tag{4}$$

Proof Define

$$n = \left| \left\{ x \in \mathbb{F}_q^* : \text{Tr}_1^m(x^{r-1}) = 0 \right\} \right|.$$

By definition, the length of the code \mathcal{C}_D is equal to n which can be expressed in terms of character sums as

$$n = \frac{1}{p} \sum_{x \in \mathbb{F}_q^*} \sum_{y \in \mathbb{F}_p} \zeta_p^{y \text{Tr}_1^m(x^{r-1})} = \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_q^*} \chi(yx^{r-1}).$$

Using Fact 1 and the fact that $u^{r-1} = 1$ for each $u \in \mathbb{F}_r^*$, we have

$$\begin{aligned} n &= \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{u \in \mathbb{F}_r^*} \sum_{v \in \Gamma} \chi(yv^{r-1}) \\ &= \frac{p^k - 1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in \Delta} \chi(yx) \\ &= \frac{p^k - 1}{p} \left(p^k + 1 + \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \Delta} \chi(yx) \right), \end{aligned}$$

where the last identity followed from the orthogonal property of the additive character χ . Applying Lemmas 3 and 4, we immediately get the formula in (3) for the length n of \mathcal{C}_D .

Table 1 Weight distribution of \mathcal{C}_D

Weight w	No. of codewords A_w
0	1
$p^{k-2}(p-1)(p^k+1+S) - p^{k-1}(p-1)$	$\frac{(p^k-1)(p^k+1+S)}{p}$
$p^{k-2}(p-1)(p^k+1+S)$	$\frac{(p^k-1)((p^k+1)(p-1)-S)}{p}$

We now calculate the Hamming weight of the codewords in \mathcal{C}_D . Note that the codewords in \mathcal{C}_D are

$$\mathbf{c}_a = (\text{Tr}_1^m(ad_1), \text{Tr}_1^m(ad_2), \dots, \text{Tr}_1^m(ad_n)), a \in \mathbb{F}_q.$$

By definition, the Hamming weight of a codeword \mathbf{c}_a is equal to $n - N_a$, where

$$N_a = \left| \left\{ x \in \mathbb{F}_q^* : \text{Tr}_1^m(x^{r-1}) = 0 \text{ and } \text{Tr}_1^m(ax) = 0 \right\} \right|.$$

Clearly, $N_a = n$ if $a = 0$, and otherwise N_a can be expressed in terms of character sums as

$$\begin{aligned} N_a &= \frac{1}{p^2} \sum_{x \in \mathbb{F}_q^*} \left(\sum_{y \in \mathbb{F}_p} \zeta_p^{y \text{Tr}_1^m(x^{r-1})} \right) \left(\sum_{z \in \mathbb{F}_p} \zeta_p^{z \text{Tr}_1^m(ax)} \right) \\ &= \frac{1}{p^2} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_q^*} \chi(yx^{r-1} + zax). \end{aligned}$$

By Fact 1 again, we have

$$\begin{aligned} N_a &= \frac{1}{p^2} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \sum_{v \in \Gamma} \chi(yv^{r-1}) \sum_{u \in \mathbb{F}_r^*} \chi(zauv) \\ &= \frac{1}{p^2} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \sum_{v \in \Gamma} \chi(yv^{r-1}) \left(\sum_{u \in \mathbb{F}_r} \chi(zauv) - 1 \right). \end{aligned}$$

Note that for any $z \in \mathbb{F}_p, u \in \mathbb{F}_r^*, v \in \Gamma$ and $a \in \mathbb{F}_q^*$,

$$\chi(zauv) = \chi_k(\text{Tr}_k^m(zauv)) = \chi_k(zu \text{Tr}_k^m(av)).$$

We then arrive at $N_a = N_{a,1} - N_{a,2}$, where

$$N_{a,1} = \frac{1}{p^2} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \sum_{v \in \Gamma} \chi(yv^{r-1}) \sum_{u \in \mathbb{F}_r} \chi_k(zu \text{Tr}_k^m(av))$$

and

$$\begin{aligned} N_{a,2} &= \frac{1}{p^2} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \sum_{v \in \Gamma} \chi(yv^{r-1}) \\ &= \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{v \in \Gamma} \chi(yv^{r-1}) \\ &= \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in \Delta} \chi(yx). \end{aligned} \tag{5}$$

Using the orthogonal property of the nontrivial additive characters and Fact 1, we have

$$\begin{aligned}
 p^{2-k}N_{a,1} &= \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \sum_{\substack{v \in \Gamma \\ z \text{Tr}_k^m(av)=0}} \chi(yv^{r-1}) \\
 &= \sum_{y \in \mathbb{F}_p} \sum_{v \in \Gamma} \chi(yv^{r-1}) + \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p^*} \sum_{\substack{v \in \Gamma \\ z \text{Tr}_k^m(av)=0}} \chi(yv^{r-1}) \\
 &= \sum_{y \in \mathbb{F}_p} \sum_{v \in \Gamma} \chi(yv^{r-1}) + (p-1) \sum_{y \in \mathbb{F}_p} \sum_{\substack{v \in \Gamma \\ \text{Tr}_k^m(av)=0}} \chi(yv^{r-1}) \\
 &= \sum_{y \in \mathbb{F}_p} \sum_{x \in \Delta} \chi(yx) + (p-1) \sum_{y \in \mathbb{F}_p} \chi(yv_a^{r-1}) \\
 &= \sum_{y \in \mathbb{F}_p} \sum_{x \in \Delta} \chi(yx) + (p-1) \sum_{y \in \mathbb{F}_p} \chi_1(y \text{Tr}_1^m(v_a^{r-1})),
 \end{aligned}
 \tag{6}$$

where v_a is the only one element in Γ such that $\text{Tr}_k^m(av_a) = 0$ due to Lemma 1. It then follows from (5) and (6) that

$$\begin{aligned}
 N_a &= \frac{p^{k-1}-1}{p} \left(p^k + 1 + \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \Delta} \chi(yx) \right) + p^{k-2}(p-1) \sum_{y \in \mathbb{F}_p} \chi_1(y \text{Tr}_1^m(v_a^{r-1})) \\
 &= \frac{(p^{k-1}-1)(p^k+1+S)}{p} + p^{k-2}(p-1) \sum_{y \in \mathbb{F}_p} \chi_1(y \text{Tr}_1^m(v_a^{r-1})),
 \end{aligned}
 \tag{7}$$

where the second identity followed from Lemmas 3 and 4, and S is given by (4). Note that the weight of the codeword \mathbf{c}_a is equal to $n - N_a$. By (7), the weight of \mathbf{c}_a takes the value

$$w_1 = p^{k-2}(p-1)(p^k+1+S) - p^{k-1}(p-1)$$

if $\text{Tr}_1^m(v_a^{r-1}) = 0$, and otherwise takes the value

$$w_2 = p^{k-2}(p-1)(p^k+1+S).$$

Note that $w_2 > w_1$ and S is an integer due to (3). In order to prove that the dimension of \mathcal{C}_D is equal to m , it is only necessary to prove that $w_1 > 0$ which is equivalent to proving that $p^k + 1 + S - p > 0$. According to Lemma 3,

$$S = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \Delta} \chi(yx) = - \sum_{y \in \mathbb{F}_p^*} K_k(y^2).$$

It then follows from Lemma 2 that

$$|S| \leq \sum_{y \in \mathbb{F}_p^*} |K_k(y^2)| \leq 2(p-1)\sqrt{p^k}.$$

This together with the fact that S is an integer means that

$$p^k + 1 + S - p \geq p^k + 1 - p - 2(p-1)\sqrt{p^k}.$$

When $k = 3$, it is easily verified that $p^k + 1 + S - p > 0$. When $k > 3$, we have

$$p^k + 1 + S - p \geq (\sqrt{p^k} - p)^2 + 2\sqrt{p^k} - p^2 - p + 1 > 0.$$

Therefore, $w_1 > 0$ for any $k \geq 3$. The discussion above shows that the dimension of \mathcal{C}_D is equal to m . It will be proved in Theorem 2 that the minimum weight of the dual code of \mathcal{C}_D is at least 2. By the Pless Power Moments (see [13], p. 259), we have

$$\begin{cases} A_{w_1} + A_{w_2} = p^m - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} = (p - 1)p^{m-1}n, \end{cases}$$

where A_{w_1} and A_{w_2} denote the number of codewords with weight w_1 and w_2 in \mathcal{C}_D , respectively. Solving this simple equation system gives the weight distribution of \mathcal{C}_D in Table 1. This completes the proof. □

Remark 1 In Theorem 1, we get closed-form expressions of the length and weight distribution of \mathcal{C}_D using Kloosterman sums. One point that should be mentioned is that the defining set of \mathcal{C}_D has been used in [12]. In this sense, the linear code \mathcal{C}_D is not new. However, thanks to some known results on Kloosterman sums, we can determine the weight distribution of \mathcal{C}_D in the binary and ternary cases as shown below.

Remark 2 According to Theorem 1, in order to completely establish the weight distribution of \mathcal{C}_D , it is sufficient to determine the value of the inner exponential sum in (4). It may be very hard in general. However, this can be done when p is small. In particular, when $p = 2$ and $p = 3$, we can get a more elegant expression for S . Note that $K_1(1) = 1$ when $p = 2$ and $K_1(1) = -1$ when $p = 3$. By (4), we immediately have

$$S = \sum_{t=0}^{\lfloor k/2 \rfloor} (-1)^{k-t} \frac{k}{k-t} \binom{k-t}{t} 2^t$$

when $p = 2$, and

$$S = -2 \sum_{t=0}^{\lfloor k/2 \rfloor} (-1)^t \frac{k}{k-t} \binom{k-t}{t} 3^t$$

when $p = 3$. Plugging these values of S into Table 1, we then completely determine the weight distribution of the code \mathcal{C}_D in the binary and ternary cases.

The numerical experiments by Magma in the following examples agree with the weight distribution in Table 1.

Example 1 Let $p = 2$ and $k = 4$. Then the code \mathcal{C}_D has parameters [135, 8, 64] and weight enumerator $1 + 135y^{64} + 120y^{72}$. It is almost optimal due to [9].

Example 2 Let $p = 3$ and $k = 3$. Then $m = 6$ and $q = 3^6$, the code \mathcal{C}_D has parameters [104, 6, 54] and weight enumerator $1 + 104y^{54} + 624y^{72}$. According to [9], the minimum distance of the best known linear codes with length 104 and dimension 6 is 56.

Example 3 Let $p = 3$ and $k = 4$. Then the code \mathcal{C}_D has parameters $[2560, 8, 1674]$ and weight enumerator $1 + 2560y^{1674} + 4000y^{1728}$.

4 The Dual of \mathcal{C}_D

In this section, we shall discuss the dual code of the two-weight code in Theorem 1. The following theorem is the main result of this section.

Theorem 2 *Let \mathcal{C}_D^\perp be the dual of the code \mathcal{C}_D . Then \mathcal{C}_D^\perp is a linear code with parameters $[n, n - m, d^\perp]$, where $d^\perp = 3$ if $p = 2$ and $d^\perp = 2$ if p is an odd prime.*

Proof The dimension of the code \mathcal{C}_D^\perp follows from Theorem 1. By definition, D does not contain the zero element of \mathbb{F}_q , thus the minimum distance of \mathcal{C}_D^\perp cannot be one.

When $p = 2$, any two distinct elements d_i and d_j in D satisfy $d_i + d_j \neq 0$, where $1 \leq i \neq j \leq n$. This means that the minimum distance of \mathcal{C}_D^\perp cannot be 2. Note that $\text{Tr}_1^m(1) = 0$ as m is even. Therefore, $\text{Tr}_1^m(x^{r-1}) = \text{Tr}_1^m(1) = 0$ for any $x \in \mathbb{F}_r^*$ which further implies that $\mathbb{F}_r^* \subset D$. According to the basic properties of finite fields, there exist two distinct elements $x_1, x_2 \in \mathbb{F}_r^*$ such that $x_1 + x_2 \in \mathbb{F}_r^*$. Hence, $\{x_1, x_2, x_1 + x_2\} \subset D$ which means that the minimum distance of \mathcal{C}_D^\perp is 3.

When p is an odd prime, it is clear that $-x \in D$ for any $x \in D$ since $r - 1$ is even. Choose some $x_1 \in D$ and set $x_2 = -x_1$, then $x_1 \neq x_2$ and $\{x_1, x_2\} \subset D$. This implies that the minimum distance of \mathcal{C}_D^\perp is 2. □

We remark that the linear code \mathcal{C}_D^\perp is bad when $p > 2$ since its minimum distance is only 2. However, it is at least almost optimal when $p = 2$ since any binary linear code with length n in (3) and dimension m has minimum distance at most 4 due to the sphere packing bound [13].

Example 4 Let $p = 2$ and $k = 3$. Then the binary code \mathcal{C}_D^\perp has parameters $[49, 43, 3]$. It is optimal due to [9].

Example 5 Let $p = 2$ and $k = 4$. Then the binary code \mathcal{C}_D^\perp has parameters $[135, 127, 3]$. It is optimal due to [9].

5 Concluding Remarks

In this paper, we studied a class of two-weight linear codes, and gave closed-form expressions of their length and weight distributions thanks to some known results on Kloosterman sums. The dual of the linear codes was proved to be optimal or almost optimal in the binary case. Finally, we mentioned that our linear code can be employed to construct secret sharing schemes with nice access structures under the framework developed in [3].

Acknowledgments The authors are very grateful to the reviewers and the Editor for their valuable comments that improved the presentation of this paper. Special thanks go to one of the reviewers for pointing out [12] and one family of two-weight linear codes. This work was supported by the National Natural Science Foundation of China (Grant Nos. 61672028, 61602394) and the Fundamental Research Funds for the Central Universities of China (Grant No. 2682016CX113).

References

1. Anderson, R.J., Ding, C., Helleseht, T., Kløve, T.: How to build robust shared control systems. *Des. Codes Cryptography* **15**(2), 111–124 (1998)
2. Calderbank, A., Goethals, J.: Three-weight codes and association schemes. *Philips J. Res.* **39**(4-5), 143–152 (1984)
3. 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)
4. Carlitz, L.: Kloosterman sums and finite field extensions. *Acta Arithmetica* **16**(2), 179–194 (1969)
5. Ding, C., Helleseht, T., Kløve, T., Wang, X.: A generic construction of cartesian authentication codes. *IEEE Trans. Inf. Theory* **53**(6), 2229–2235 (2007)
6. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. *Theor. Comput. Sci.* **330**(1), 81–99 (2005)
7. Ding, K., Ding, C.: Binary linear codes with three weights. *IEEE Commun. Lett.* **18**(11), 1879–1882 (2014)
8. 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)
9. Grassl, M.: Bounds on the minimum distance of linear codes. Online available at <http://www.codetables.de>, Accessed on pp. 08–20 (2008)
10. Helleseht, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Trans. Inf. Theory* **52**(5), 2018–2032 (2006)
11. Heng, Z., Yue, Q.: A class of binary linear codes with at most three weights. *IEEE Commun. Lett.* **19**(9), 1488–1491 (2015)
12. Heng, Z., Yue, Q.: Two classes of two-weight linear codes. *Finite Fields Appl.* **38**, 72–92 (2016)
13. Huffman, W.C., Pless, V.: *Fundamentals of error-correcting codes*. Cambridge University Press (2003)
14. Kløve, T.: *Codes for Error Detection*. In: World Scientific (2007)
15. Leander, N.G.: Monomial bent functions. *IEEE Trans. Inf. Theory* **52**(2), 738–743 (2006)
16. Lidl, R., Niederreiter, H.: *Finite fields*, vol. 20. Cambridge University Press (1997)
17. Qi, Y., Tang, C., Huang, D.: Binary linear codes with few weights. *IEEE Commun. Lett.* **20**(2), 208–211 (2016)
18. Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. *IEEE Trans. Inf. Theory* **52**(1), 206–212 (2006)