ON SOME CLASSES OF CODES WITH A FEW WEIGHTS

YIWEI LIU
School of Computer Science & Technology
Beijing Institute of Technology, Beijing 100081, China

ZHUI LIU
Department of Mathematics, Beijing Key Laboratory on MCAACI
Beijing Institute of Technology, Beijing 100081, China

(Communicated by Jens Zumbraegel)

Abstract. We generalize the code constructed recently by Wang et al, and obtain many classes of codes with a few weights. The weight distribution of these codes is completely determined, and the minimum distance of the duals of these codes is determined. We also show that some subclasses of the duals of these codes are optimal. Furthermore, some parameters of the generalized Hamming weight of these codes are calculated in certain cases.

1. Introduction

Throughout this paper, let \( m \) be a positive integer, and let \( r \) be a prime such that \( 2 \) is a primitive root modulo \( r^m \), that is, \( 2 \) is a generator of the multiplicative group of integers modulo \( r^m \). Let \( q = 2^{\phi(r^m)} \), where \( \phi \) is the Euler function. Let \( \gamma \) be a primitive element of \( F_q \), where \( F_q \) denotes the finite field with \( q \) elements.

An \([n, k, d]\) binary linear code \( C \) is a \( k \)-dimensional subspace of \( F_2^n \) with minimum Hamming distance \( d \). Let \( A_i \) denote the number of codewords with Hamming weight \( i \) in a code \( C \) of length \( n \). The weight enumerator of \( C \) is defined by \( 1 + A_1 y + A_2 y^2 + \cdots + A_n y^n \). The sequence \((A_1, A_2, \cdots, A_n)\) is called the weight distribution of the code \( C \). The weight distribution of a code gives information about the error correcting capability and the probability of error detection and correction with respect to some decoding algorithms.

A code \( C \) is \( t \)-weight if the number of nonzero \( A_i \) in the sequence \((A_1, A_2, \cdots, A_n)\) is equal to \( t \). An \([n, k, d]\) code \( C \) is called optimal if no \([n, k, d+1]\) code exists, and is called almost optimal if the code \([n, k, d+1]\) is optimal [6, Chapter 2].

Let \( \text{Tr} \) denote the trace function from \( F_q \) onto \( F_2 \). For any set \( A = \{a_1, a_2, \cdots, a_n\} \subseteq F_q^* \), we define a linear code of length \( n \) over \( F_2 \) by

\[
C_A = \{(\text{Tr}(xa_1), \text{Tr}(xa_2), \cdots, \text{Tr}(xa_n)): x \in F_q\},
\]

and call \( A \) the defining set of \( C_A \). It is a basic fact that different orderings of the elements of \( A \) result in equivalent codes [6, p.20]. Since equivalent codes have the same weight distribution, we will not specify the ordering of the elements in \( A \) when we study the weight distribution of \( C_A \).

2010 Mathematics Subject Classification: 94B05.

Key words and phrases: Weight distribution, trace function, secret sharing scheme, primitive root, generalized Hamming weight.

This work was supported by The National Science Foundation of China (No. 11171366).

* Corresponding author: Zihui Liu.
This construction of $C_A$ is generic in the sense that many classes of known codes can be produced by selecting the defining set $A \subseteq \mathbb{F}_q^*$ properly [3], [9], and these codes are useful in secret sharing schemes [1], [2], [13] and authentication codes [4].

The aim of this paper is to generalize the code-constructing method in [9] and [10], and then obtain many new classes of two-weight and three-weight codes, whose duals are either optimal or almost optimal. We will completely determine the weight distribution of these two-weight and three-weight codes, and study the duals of these codes, and further determine the optimal duals of these codes. We will also compute the generalized Hamming weight of these two-weight and three-weight codes in some cases. To get these new results, we will have to develop new techniques which are much different from that in [9] and [10], and these new techniques and new results are main contributions of the paper.

2. Preliminaries and problem formulation

In this section, we present some results of group characters and exponential sums for later use, please see [7] for details. An additive character $\chi$ of $\mathbb{F}_q$ is a function from $\mathbb{F}_q$ to the set of complex numbers of absolute value 1 such that $\chi(x + y) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{F}_q$. For each $b \in \mathbb{F}_q$, the function

\[
\chi_b(c) = (-1)^{\text{Tr}(bc)}, \forall c \in \mathbb{F}_q
\]

defines an additive character of $\mathbb{F}_q$, and every additive character of $\mathbb{F}_q$ can be obtained in this way. When $b = 1$, the character $\chi_1$ in (1) is called the canonical additive character of $\mathbb{F}_q$. It is obvious that $\chi_b(x) = \chi_1(bx)$.

Let $\alpha = \gamma \frac{r-1}{\phi(r^m)}$, and for any $a, b \in \mathbb{F}_q$, define the following exponential sum

\[
S(a, b) := \sum_{x \in \mathbb{F}_q^*} \chi_1(ax \frac{r-1}{\phi(r^m)} + bx).
\]

Then,

\[
S(a, 0) = q - 1 \cdot \frac{r-1}{\phi(r)} S(a),
\]

where

\[
S(a) = \sum_{i=0}^{r^m-1} \chi_1(aa^i).
\]

Since 2 is a primitive root modulo $r^m$, the $r^m$th cyclotomic polynomial is irreducible and is the minimal polynomial of $\alpha = \gamma \frac{r-1}{\phi(r^m)}$, then $\mathbb{F}_q = \mathbb{F}_2(\alpha)$. Express $a \in \mathbb{F}_q$ in basis $(\alpha, \alpha^2, \cdots, \alpha^{\phi(r^m)})$, say

\[
a = \sum_{j=1}^{\phi(r^m)} a_j \alpha^j
\]

where $a_j \in \mathbb{F}_2$ for all $j = 1, \cdots, \phi(r^m)$. For $i = 0, 1, \cdots, r^m-1-1$, we denote by $a^{(i)}$ the following subvector of length $r - 1$ of the coordinate vector $a = (a_1, a_2, \cdots, a_{\phi(r^m)})$ of $a$:

\[
a^{(i)} = (a_{r^m-1-i}, a_{2r^m-1-i}, \cdots, a_{(r-1)r^m-1-i}).
\]

Let $wt(x)$ denote the Hamming weight of the binary vector $x$. We get the following two useful lemmas.
Lemma 1. ([8], Theorem 1 and Theorem 3) Let $a \in \mathbb{F}_q$. Then
\[ S(a) = \sum_{i=0}^{r^m-1} (-1)^{\text{wt}(a^{(i)})} \left( r - 2\text{wt}(a^{(i)}) \right). \]
Moreover, there exists a $b \in \mathbb{F}_q$ such that each subvector $b^{(i)}$ is of even weight and $S(a) = r^m - 2\text{wt}(b)$. $S(a)$ ranges over $r^m - 4j$, $j = 1, 2, \ldots, \phi(r^m)/2$, when $a \in \mathbb{F}_q^n$.

Lemma 2. ([8], Theorem 7) Let $a, b \in \mathbb{F}_q^*$, and let $c = ab^{-\frac{q+1}{r^m}}$. Then
\[ S(a, b) = (-1)^{\text{wt}(c^{(i)})} \sqrt{q} - \frac{\sqrt{q} + 1}{r^m} S(c). \]

For the defining set
\[ A' = \{ x \in \mathbb{F}_q^* : \text{Tr}(x^{\frac{q+1}{r^m}} + bx) = 0 \}, \quad b \in \mathbb{F}_q. \]
Wang et al. [9] [10] have recently studied the code $C_{A'}$ and determined the weight distribution the code $C_A$ and the minimum distance of the dual of $C_A$. Motivated by this result, we will study the code $C_A$, where the defining set $A$ is given by
\[ (4) \quad A = \{ x \in \mathbb{F}_q^* : \text{Tr}(ax^{\frac{q+1}{r^m}} + bx) = 0 \}, \quad \forall (a, b) \in \mathbb{F}_q \times \mathbb{F}_q. \]
Obviously, $C_{A'}$ is a special case of $C_A$ by taking $a = 1$ in (4).

In order to obtain the weight distribution of $C_{A'}$, by Lemmas 1 and 2, Wang et al. [9] [10] skillfully used the coordinate vector $1$ of $a = 1$ and computed $S(1, b)$ directly by discussing the value taken by $b$. Such a direct computation can’t work because of the complexity when the parameter $a$ varies in $\mathbb{F}_q^*$. Our contributions are to find new techniques to overcome the above difficulties, and our techniques will avoid the tedious computation of $S(a)$ and $S(a, b)$ and obtain a complete description of the code $C_A$.

The paper is organized as follows: in Section 3, we will determine the weight distribution of $C_A$ for any pair $(a, b)$. In Section 4, we show that for any pair $(a, b)$, the minimum distance of the dual $C_A^\perp$ of $C_A$ is equal to 3, and present some subclasses of the dual code $C_A^\perp$ which are optimal. In Section 5, we will study the generalized Hamming weight of $C_A$ for any pair $(a, b)$, and determine some parameters of the generalized Hamming weight in some cases, and then the conclusion in Section 6.

3. The Weight Distribution of $C_A$

Let $r$, $m$, $q$ ($= 2^{\phi(r^m)}$), $\gamma$, $\alpha$ and $S(a)$ be defined as before. We will determine the weight distribution of $C_A$ in this section.

Define
\[ n_0 := \left| \{ x \in \mathbb{F}_q : \text{Tr}(ax^{\frac{q+1}{r^m}} + bx) = 0 \} \right|, \]
\[ N_d := \left| \{ x \in \mathbb{F}_q : \text{Tr}(ax^{\frac{q+1}{r^m}} + bx) = 0 \text{ and } \text{Tr}(dx) = 0 \} \right|. \]
Then $n_0 - 1$ is the codeword length of $C_A$, and for $d \in \mathbb{F}_q^*$, the Hamming weight of the nonzero codeword
\[ c_d = (\text{Tr}(da_1), \text{Tr}(da_2), \ldots, \text{Tr}(da_{n_0-1})) \quad (a_i \in A, i = 1, \ldots, n_0 - 1) \]
is equal to $n_0 - N_d$. 
By calculating and using the notation $S(a, b)$ in Section 2, we get

$$n_0 = \frac{1}{2} \sum_{x \in F_q} \left( 1 + (-1)^{\text{Tr} \left( \frac{x - 1}{r^{m}} + bx \right)} \right)$$

(6)

$$= \frac{q + 1}{2} + \frac{1}{2} S(a, b)$$

and

$$N_d = \frac{1}{4} \sum_{x \in F_q} \left( 1 + (-1)^{\text{Tr} \left( \frac{x - 1}{r^{m}} + bx \right)} \right) \left( 1 + (-1)^{\text{Tr} (dx)} \right)$$

$$= \frac{1}{4} \left( q + 2 + S(a, b) + S(a, b + d) \right), \ d \in F_q^*.$$

Thus,

(7) \quad \text{wt}(c_d) = n_0 - N_d = \frac{1}{4} \left( q + S(a, b) - S(a, b + d) \right), \ d \in F_q^*.$$

According to (7), we have to compute $S(a, b)$ and $S(a, b + d)$ in order to get the weight distribution of $C_A$. For the special cases $(a, b) = (1, 0)$ and $(a, b) = (1, 1)$, using Lemmas 1 and 2, Wang et al [9] [10] obtained $S(1, d)$ and $S(1, 1 + d)$ by tedious computation according to the value of $d \in F_q^*$, and they also remark in [10] that for any $(a, b) = (1, b)$, $b \in F_q$, their method is also effective. However, such computation method is difficult and complicated to be carried out to obtain $S(a, b + d)$ for any pair $(a, b) \in F_q^2$ and any $d \in F_q^*$. To overcome this difficulty, our technique is to use the following basic observations.

**Lemma 3.** For any integer $k$ and $a \in F_q$, it holds that $S(\alpha k a) = S(a)$.

**Proof.** For any integer $k$, since $\alpha$ has order $r^m$, it follows from (3) that

$$S(\alpha^k a) = \sum_{i=0}^{r^m-1} \chi_1(a \alpha^i + k) = \sum_{i=0}^{r^m-1} \chi_1(a \alpha^i) = S(a).$$

**Lemma 4.** Let $a, b \in F_q$, $a \neq 0$, and let $c = ab^{-\frac{r^m}{r^{m^2}}} + 1$ if $b \neq 0$. Then,

$$S(a, b) = \begin{cases} 
\frac{q - 1}{r^m} S(a), & b = 0; \\
\left(-1\right)^{\text{wt}(c^{(0)})} \sqrt{q} - \frac{\sqrt{q} + 1}{r^m} S(a), & b \neq 0.
\end{cases}$$

**Proof.** For $b = 0$, the result is by (2). For $b \neq 0$, assume $b = \gamma^{-k}$ for some integer $k$, then $c = ab^{-\frac{r^m}{r^{m^2}}} = a\alpha^k$, and thus $S(c) = S(a)$ by Lemma 3, then the result follows by Lemma 2.

**Table 1.** The weight distribution of the code $C_A$ in Theorem 5

| Weight | Multiplicity |
|--------|-------------|
| $0$    | $1$         |
| $\frac{q + \sqrt{q}}{2} + \frac{q + \sqrt{q}}{4} S(a)$ | $\frac{q - 1}{2} - \frac{q - 1}{2r^m} S(a)$ |
| $\frac{q - \sqrt{q}}{4} + \frac{q + \sqrt{q}}{4} S(a)$ | $\frac{q - 1}{2} + \frac{q - 1}{2r^m} S(a)$ |
For any \((a,b) \in \mathbb{F}_q^2\) with \(a = 0\), it can be checked that the corresponding \(C_A\) is a constant-weight code whose weight distribution is clear. We wonder what the weight distribution of \(C_A\) is for any \((a,b) \in \mathbb{F}_q^* \times \mathbb{F}_q\), and we divide the analysis into two cases.

**(Case i.)** \(b = 0\), that is, \((a,b) = (a,0)\).

In this case, our main result is

**Theorem 5.** Assume \(r^m \geq 9\). Then, the code \(C_A\) is a \(\left\lfloor \frac{q-1}{2} + \frac{q-1}{2^m} S(a), r^m-1(r-1) \right\rfloor\) binary code with weight distribution described in Table 1.

**Proof.** Since the length of the code \(C_A\) is equal to \(n_0 - 1\), we get by substituting \(b = 0\) into (6) that

\[
n_0 - 1 = \frac{q+1}{2} + \frac{1}{2} S(a,0) - 1
= \frac{q-1}{2} + \frac{q-1}{2^m} S(a). \quad \text{(by Lemma 4)}
\]

According to (7), for \(b = 0\), each nonzero codeword \(c_d \in C_A\) with \(d \in \mathbb{F}_q^*\) has Hamming weight

\[
wt(c_d) = \frac{1}{4} (q + S(a,0) - S(a,d))
= \frac{1}{4} \left( q + \frac{q-1}{r^m} S(a) - \left( \pm \sqrt{q} - \frac{\sqrt{q} + 1}{r^m} S(a) \right) \right) \quad \text{(by Lemma 4)}
= \frac{q \pm \sqrt{q}}{4} + \frac{q + \sqrt{q}}{4} S(a).
\]

Define

\[
w_1 = \frac{q + \sqrt{q}}{4} + \frac{q + \sqrt{q}}{4^m} S(a),
w_2 = \frac{q - \sqrt{q}}{4} + \frac{q + \sqrt{q}}{4^m} S(a),
\]

and assume the number of codewords with weight \(w_1\) and \(w_2\) is \(B_1\) and \(B_2\), respectively. It suffices to compute \(B_1\) and \(B_2\) in order to get the weight distribution of \(C_A\).

Note that \(wt(c_d) > 0\) for each nonzero codeword \(c_d\) with \(d \in \mathbb{F}_q^*\) by virtue of \(r^m \geq 9\), thus, the dimension of the code \(C_A\) is \(\phi(r^m) = r^m-1(r-1)\).

Since the minimum distance of the dual code \(C_A^\perp\) of \(C_A\) is at least 3, it follows from the first two Pless Power Moments [6, p.260] that the following system equations hold

\[
\begin{cases}
B_1 + B_2 = 2^{\phi(r^m)} - 1 \\
w_1 B_1 + w_2 B_2 = \left( \frac{q-1}{2} + \frac{q-1}{2^m} S(a) \right) 2^{\phi(r^m)} - 1.
\end{cases}
\]

Solving this system of equations yields the weight distribution in Table 1. \(\square\)

**Remark 6.** The result in [9] is a special case of Theorem 5 by taking \((a,0) = (1,0)\) and by using the fact \(S(1) = r^m - 2(r-1)\).

Since by Lemma 1 \(S(a)\) ranges over \(r^m - 4j, j = 1, 2, \ldots, \phi(r^m)/2\), when \(a \in \mathbb{F}_q^*\), Table 1 yields altogether \(\phi(r^m)/2\) classes of two-weight codes. The following examples show that many of them are optimal.
Example 7. Let $m = 2, r = 3, a = 1$. Then $q = 2^6$, $S(a) = 5$, the code $C_A$ has parameters $[49, 6, 24]$ and weight enumerator $1 + 49y^{24} + 14y^{28}$. The code is optimal.

Example 8. Let $m = 2, r = 3, a = 1 + \alpha + \alpha^2$. Then $q = 2^6, S(a) = -3$, the code $C_A$ has parameters $[21, 6, 8]$ and weight enumerator $1 + 21y^8 + 42y^{12}$. The code is optimal.

Example 9. Let $m = 2, r = 3, a = 1 + \alpha$. Then $q = 2^6$, $S(a) = 1$, the code $C_A$ has parameters $[35, 6, 16]$ and weight enumerator $1 + 35y^{16} + 28y^{20}$. The code is optimal.

Table 2. The weight distribution of the code $C_A$ in Theorem 10

| Weight | Multiplicity |
|--------|-------------|
| 0      | 1           |
| $q$    | $\frac{g}{2} + (-1)^{wt(c)} \sqrt{q}$ |
| $\sqrt{q} - \frac{g + \sqrt{q} S(a)}{4m}$ | 1 |

(Case ii.) $b \neq 0$, that is, $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$.

In this case, our main result is

Theorem 10. Assume $r^m \geq 5$ and let $c = ab^{-\frac{r-1}{r^m}}$. Then, the code $C_A$ is a $[\frac{g + (-1)^{wt(c)} \sqrt{q} - 1}{2r^m} S(a), r^m - 1]$ binary code with weight distribution described in Table 2.

Proof. As in the statement at the beginning of this section, the length of $C_A$ should be equal to $n_0 - 1$. According to (6), we get

$$n_0 - 1 = \frac{q + 1}{2} + \frac{1}{2} S(a, b) - 1$$
$$= \frac{q - 1}{2} + \frac{1}{2} (-1)^{wt(c)} \sqrt{q} - \frac{\sqrt{q} + 1}{r^m} S(a) \quad \text{(by Lemma 4)}$$
$$= \frac{q + (-1)^{wt(c)} \sqrt{q} - 1}{2r^m} - \frac{\sqrt{q} + 1}{r^m} S(a).$$

According to (7) and Lemma 4, each nonzero codeword $c_d \in C_A$ with $d \in \mathbb{F}_q^*$ has Hamming weight

$$wt(c_d) = \frac{1}{4} (q + S(a, b) - S(a, b + d)).$$

Thus, if $b + d = 0$,

$$wt(c_d) = \frac{1}{4} \left( q + S(a, b) \right).$$
$$= \frac{1}{4} \left( q + (-1)^{wt(c)} \sqrt{q} - \frac{\sqrt{q} + 1}{r^m} S(a) - \frac{q - 1}{r^m} S(a) \right)$$
$$= \frac{1}{4} \left( q + (-1)^{wt(c)} \sqrt{q} - \frac{\sqrt{q} + q}{r^m} S(a) \right);$$
Solving this system of equations yields the weight distribution in Table 2. The weight distribution of the code constructed in [10] may be considered as a special case of Theorem 10 with \(a = 1\). Note that there exist two coinciding weights in Theorem 10 when \(r^m = 5\) and \(S(a) = 1\) or \(r^m = 9\) and \(S(a) = 1\), the three-weight code in Theorem 10 is in fact two-weight in the above two special cases.

**Example 12.** Let \(m = 2\), \(r = 3\), \(a = 1\), \(b = 1\). Then \(q = 2^6\), \(S(a) = 5\), \(wt(c^{(0)}) = 2\), and \(C_A\) is a three-weight code with parameters \([33, 6, 8]\) and weight enumerator \(1 + y^8 + 48y^{16} + 14y^{20}\).

4. **The dual code \(C_A^\perp\) of \(C_A\)**

In Section 3, we showed that for any pair \((a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q\), the corresponding code \(C_A\) is two-weight or three-weight. In this section, we will give two results about the dual of \(C_A\). One contribution is that we will show all the binary codes \(C_A^\perp\) have

\[
\begin{align*}
\text{wt}(c_d) &= \frac{1}{4} (q + S(a, b) - S(a, b + d)) \\
&= \frac{1}{4} \left( q + (-1)^{\text{wt}(c^{(0)})} \sqrt{q} - \frac{\sqrt{q} + 1}{q^m} S(a) \right) \\
&= \frac{1}{4} \left( q + (-1)^{\text{wt}(c^{(0)})} \sqrt{q} \pm \frac{\sqrt{q} + 1}{q^m} S(a) \right) \\
&= \begin{cases} \\
q + (-1)^{\text{wt}(c^{(0)})} \frac{2\sqrt{q}}{4}, & \text{or, } q + (-1)^{\text{wt}(c^{(0)})} \frac{2\sqrt{q}}{4}. \\
\end{cases}
\end{align*}
\]

Define

\[
\begin{align*}
w_1 &= \frac{q}{4} \\
w_2 &= \frac{q + (-1)^{\text{wt}(c^{(0)})} 2\sqrt{q}}{4} \\
w_3 &= \frac{1}{4} \left( q + (-1)^{\text{wt}(c^{(0)})} \sqrt{q} - \frac{\sqrt{q} + q}{q^m} S(a) \right).
\end{align*}
\]

Then, \(w_1\), \(w_2\) and \(w_3\) are all the possible weights of the code \(C_A\). Assume the number of codewords with weight \(w_1\), \(w_2\) and \(w_3\) is \(B_1\), \(B_2\) and \(B_3\), respectively. It suffices to compute \(B_1\), \(B_2\) and \(B_3\) in order to get the weight distribution of \(C_A\).

As in the proof of Theorem 5, since \(wt(c_d) > 0\) for each nonzero codeword \(c_d\) with \(d \in \mathbb{F}_q^*\) by virtue of \(r^m \geq 5\), the dimension of the code \(C_A\) is \(\phi(r^m) = r^{m-1}(r - 1)\).

The same arguments as in the proof of Theorem 5 lead to the first three Pless Power Moments [6, p.260] equations

\[
\begin{align*}
B_1 + B_2 + B_3 &= 2\phi(r^m) - 1 \\
w_1 B_1 + w_2 B_2 + w_3 B_3 &= \left( \frac{q + (-1)^{\text{wt}(c^{(0)})} \sqrt{q} - \frac{\sqrt{q} + 1}{q^m} S(a)}{2} \right) 2\phi(r^m) - 1 \\
w_2^2 B_1 + w_2^2 B_2 + w_3^2 B_3 &= \left( \frac{q + (-1)^{\text{wt}(c^{(0)})} \sqrt{q} - \frac{\sqrt{q} + 1}{q^m} S(a)}{2} \right) \left( \frac{q + (-1)^{\text{wt}(c^{(0)})} \sqrt{q} + 1}{2} \right) 2\phi(r^m) - 2.
\end{align*}
\]

Solving this system of equations yields the weight distribution in Table 2.

**Remark 11.** The weight distribution of the code constructed in [10] may be considered as a special case of Theorem 10 with \(a = 1\). Note that there exist two coinciding weights in Theorem 10 when \(r^m = 5\) and \(S(a) = 1\) or \(r^m = 9\) and \(S(a) = 1\), the three-weight code in Theorem 10 is in fact two-weight in the above two special cases.

The dual code \(C_A^\perp\) of \(C_A\).
minimum distance 3. The other contribution is by using Lemma 4 to determine some subclasses of \( C_A \) which are optimal.

Due to the Sphere Packing Bound [6, Theorem 1.12.1], the minimum weight of the dual \( C_A^\perp \) is at most 4. Note that the minimum weight of \( C_A^\perp \) is at least equal to 3, thus, all the binary codes \( C_A^\perp \) are optimal or almost optimal. In fact, we will show in this section that all the binary codes \( C_A^\perp \) have minimum distance 3, which has already been set up for \( C_A^\perp \) in [9] [10] with \((a, b) = (1, 0)\) and \((a, b) = (1, 1)\).

Note that when \((a, b) = (1, 0)\), the minimum distance of \( C_A^\perp \) being equal to 3 may be set up by using the properties of subfields of \( F_q \) [9].

For \((a, b) = (1, 1)\), the codeword length of \( C_A \) is greater than \( \frac{q}{2} \) by Theorem 10, and by using such a fact and the Pigeonhole principle, it was shown in [10] that the corresponding binary code \( C_A^\perp \) has minimum distance 3.

The Pigeonhole principle, however, can no longer apply to other values taken by \((a, b)\). For, the codeword length of \( C_A \), which by Theorems 5 and 10 is determined by the values of \((a, b)\), may not be greater than \( \frac{q}{2} \).

We thus have to find a new general proving method to obtain that any binary code \( C_A^\perp \) corresponding to any value of \((a, b)\) \((a \in F_q^*, b \in F_q)\) has minimum distance 3.

To this end, we first need a lemma. Recall that for any \((a, b) \in F_q^* \times F_q\), the defining set \( A \) is defined as

\[
A = \{ x \in F_q^* : \text{Tr}(ax^{q-1} + bx) = 0 \}.
\]

Define

\[
A_1 := \{ x \in F_q^* : \text{Tr}(ax^{q-1}) = 0 \text{ and } \text{Tr}(bx) = 0 \}; \\
A_2 := \{ x \in F_q^* : \text{Tr}(ax^{q-1}) = 1 \text{ and } \text{Tr}(bx) = 1 \}.
\]

Then, \( A = A_1 \cup A_2 \) and \( A_1 \cap A_2 = \emptyset \).

**Lemma 13.** If \( r^m \geq 9 \), then for any \((a, b) \in F_q^* \times F_q\), \( A_1 \neq \emptyset \).

**Proof.** It suffices to show the size \(|A_1|\) of \( A_1 \) satisfies \(|A_1| > 0\). We have

\[
|A_1| = |\{ x \in F_q^* : \text{Tr}(ax^{q-1} + bx) = 0 \}| - 1 - |A_2| \\
= n_0 - 1 - |A_2| \\
= n_0 - 1 - \frac{1}{4} \sum_{x \in F_q} \left( (1 - (-1)^{\text{Tr}(ax^{q-1})})(1 - (-1)^{\text{Tr}(bx)}) \right) \\
= n_0 - 1 - \frac{1}{4} \left( q + S(a, b) - S(a, 0) - \sum_{x \in F_q} (-1)^{\text{Tr}(bx)} \right) \\
= \frac{q - 2}{4} + \frac{1}{4} S(a, b) + \frac{1}{4} S(a, 0) + \frac{1}{4} \sum_{x \in F_q} (-1)^{\text{Tr}(bx)} \quad \text{(by (6))} \\
= \begin{cases} 
\frac{q-1}{2} + \frac{1}{2} S(a, 0), & b = 0 \\
\frac{2}{3} - \frac{1}{3} S(a, b) + \frac{1}{3} S(a, 0), & b \neq 0.
\end{cases}
\]

Since \( S(a) \) ranges over \( r^m - 4j, j = 1, 2, \cdots, \phi(r^m)/2 \), when \( a \in F_q^* \) by Lemma 1, we obtain \(|A_1| > 0\) by Lemma 4 and the assumption \( r^m \geq 9 \). \( \square \)

**Theorem 14.** Assume \( r^m \geq 9 \). Then, each dual code \( C_A^\perp \) is a binary code with minimum distance 3.
Let \( \text{Theorem 15.} \)

Consider the set

\[
S := \{ y : y \in \mathbb{F}_q, y^{\frac{q-1}{2}} = 1 \text{ and } \text{Tr}(bx_0y) = 0 \} = \{ y : y \in \mathbb{F}_q, y^{\frac{q-1}{2}} = 1 \} \cap \{ y : y \in \mathbb{F}_q, \text{Tr}(bx_0y) = 0 \}.
\]

Since 2 is a primitive root modulo \( r^m \), we have

\[ q = 2^{\phi(r^m)} = 2^{(r-1)r^{m-1}} \equiv 1 \pmod{r^m}, \]

thus, \( 2^{\frac{(r-1)r^{m-1}}{2}} \equiv -1 \pmod{r^m} \).

And thus,

\[
2^{\frac{(r-1)r^{m-1}}{2}} - 1 \equiv \frac{q-1}{r^m}.
\]

Then, for any \( y \in \mathbb{F}_2^r \subset \mathbb{F}_q \), where \( t = \frac{(r-1)r^{m-1}}{2} \), we have \( y^{\frac{q-1}{2}} = 1 \). Or equivalently,

\[
\mathbb{F}_2^r \subset \{ y : y \in \mathbb{F}_q, y^{\frac{q-1}{2}} = 1 \}.
\]

By (8), we obtain

\[
S \supset (\mathbb{F}_2^r \cap \{ y : y \in \mathbb{F}_q, \text{Tr}(bx_0y) = 0 \}) = (\mathbb{F}_2^r \cap \{ y : y \in \mathbb{F}_q, \text{Tr}(bx_0y) = 0 \}) \setminus \{0\}.
\]

Since \( \mathbb{F}_2^r \) and \( \{ y : y \in \mathbb{F}_q, \text{Tr}(bx_0y) = 0 \} \) can be considered as \( t \)-dimensional and at least \( (\phi(r^m) - 1) \)-dimensional subspaces of \( \mathbb{F}_q \) over \( \mathbb{F}_2 \), respectively, it follows that \( \mathbb{F}_2^r \cap \{ y : y \in \mathbb{F}_q, \text{Tr}(bx_0y) = 0 \} \) is also a subspace of \( \mathbb{F}_q \) over \( \mathbb{F}_2 \) and

\[
\dim(\mathbb{F}_2^r \cap \{ y : y \in \mathbb{F}_q, \text{Tr}(bx_0y) = 0 \}) \geq t - 1.
\]

This and the assumption \( r^m \geq 9 \) yield that there exist two distinct elements \( y_1, y_2 \in S \) and \( y_1 + y_2 \in S \) such that \( y_1 + y_2 \in S \). Then, it holds that \( x_0y_1 \in A_1, x_0y_2 \in A_1 \) and \( x_0y_1 + x_0y_2 = x_0(y_1 + y_2) \in A_1 \). Equivalently, the dual code \( C_A^\perp \) has minimum distance 3.

Like the code \( C_A \), we state that many codes among \( C_A^\perp \) are optimal, as the following theorem says.

**Theorem 15.** Assume \( r^m \geq 9 \). Then,

i) For any \( (a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q \) with \( b = 0 \), the dual code \( C_A^\perp \) is optimal provided \( S(a) > 0 \).

ii) For any \( (a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q \) with \( b \neq 0 \), the dual code \( C_A^\perp \) is optimal provided \( wt(c^{(0)}) \) is even.

**Proof.**

i) Assume that the dual code \( C_A^\perp \) with parameters \([n, n - \phi(r^m), 3] \) is not optimal, where \( n = \frac{a_2}{2} + \frac{q-1}{2} S(a) \). Then, there exists an \([n, n - \phi(r^m), 4] \) code. Let \( k' \) be the maximum dimension among all the binary codes with length \( n \) and minimum distance at least 4. Then, \( k' \geq n - \phi(r^m) \), and by [6, Theorem 2.1.2], \( k' \) should also be the maximum dimension among all the binary codes with length...
n − 1 and minimum distance at least 3. Then, by the Sphere Packing Bound [6, Theorem 1.12.1], we have

\[ 2^{k'} \leq \frac{2^{n-1}}{1 + (n-1)} = \frac{2^{n-1}}{n}. \]

Thus,

\[ 2^{n-\phi(r^m)} \leq \frac{2^{n-1}}{n}, \]

that is,

\[ 2^{\phi(r^m)-1} = \frac{q}{2} \geq n = \frac{q-1}{2} + \frac{q-1}{2r^m} S(a), \]

which is nonsense when \( S(a) > 0 \). Thus, \( C_A^\perp \) is optimal.

ii) Note that in this case

\[ n = \frac{q + (-1)^{wt(c^{(0)})}\sqrt{q} - 1}{2} - \frac{\sqrt{q} + 1}{2r^m} S(a) \]

since \( wt(c^{(0)}) \) is even. Similarly to the proof as in i), if the code \( C_A^\perp \) is not optimal, then we get

\[ \frac{q}{2} \geq n. \]

Then, we further get

\[ S(a) \geq \frac{\sqrt{q} - 1}{\sqrt{q} + 1} r^m, \]

which is a contradiction to Lemma 1. Thus, the code \( C_A^\perp \) is optimal. \( \square \)

**Example 16.** Let \( m = 2, r = 3, a = 1, b = 0 \). Then \( q = 2^6, S(a) = 5 \), the code \( C_A^\perp \) has parameters \([49, 29, 3]\) and is optimal.

**Example 17.** Let \( m = 2, r = 3, a = 1 + \alpha, b = 0 \). Then \( q = 2^6, S(a) = 1 \), the code \( C_A^\perp \) has parameters \([33, 27, 3]\) and is optimal.

**Example 18.** Let \( m = 2, r = 3, a = 1, b = 1 \). Then \( q = 2^6, S(a) = 5, wt(c^{(0)}) = 2 \), the code \( C_A^\perp \) has parameters \([33, 27, 3]\) and is optimal.

**Example 19.** Let \( m = 2, r = 3, a = 1 + \alpha + \alpha^2, b = 1 \). Then \( q = 2^6, S(a) = -3, wt(c^{(0)}) = 2 \), the code \( C_A^\perp \) has parameters \([37, 31, 3]\) and is optimal.

5. **The Generalized Hamming Weight of \( C_A \)**

In this section, we will study the support weight of the subcodes of \( C_A \). Our aim along this direction is to determine the generalized Hamming weight (GHW) of \( C_A \) in certain cases by using Lemma 4.

Let \( C \) be a \( k \)-dimensional linear code. Then, the support of a subcode \( D \) is defined as the set of the coordinate positions where not all the codewords of \( D \) are zeroes, and the size of the support of \( D \), denoted by \( w(D) \), is called the support weight of \( D \).

The GHW of the code \( C \) is defined as the ordered sequence

\[ (w_{1}^{\min}, w_{2}^{\min}, \ldots, w_{k}^{\min}), \]
where

\[ w_i^{\min} := \min \{ w(\mathcal{D}) : \mathcal{D} \text{ is a } i\text{-dimensional subcode} \}. \]

The GHW of a linear code was introduced by Wei [11], and it is useful in the wire-tap channel II with the coset coding scheme [11] and the analysis of the trellis complexity of a code [5]. Determining the GHW of a linear code is an interesting research problem [12].

Since the map from an element \( d \in \mathbb{F}_q \) to the codeword of \( C_A \) defined by (5) is one-to-one on condition \( r^m \geq 9 \), we may identify the subcode of \( C_A \) with the subspace of \( \mathbb{F}_q \) over \( \mathbb{F}_2 \). In the following text, we always assume \( r^m \geq 9 \) and identify a \( \theta \)-dimensional subcode of \( C_A \) with a \( \theta \)-dimensional subspace of \( \mathbb{F}_q \) over \( \mathbb{F}_2 \).

We first obtain a formula describing the support weight of a \( \theta \)-dimensional subcode \( \mathcal{V}_\theta \) of \( C_A \), and then use this formula to determine the GHW of \( C_A \) in certain cases.

Assume \( d_i, 1 \leq i \leq \theta \), are basis elements of \( \mathcal{V}_\theta \) (considered as a subspace of \( \mathbb{F}_q \)) over \( \mathbb{F}_2 \), and Define

\[ N_{\mathcal{V}_\theta} = \left\{ x \in \mathbb{F}_q : \text{Tr} \left( ax + bx \right) = 0 \text{ and } \text{Tr}(d_i x) = 0, 1 \leq i \leq \theta \right\}. \]

Then,

\[ N_{\mathcal{V}_\theta} = \frac{1}{2^\theta+1} \sum_{x \in \mathbb{F}_q} \left[ (1 + (-1)^{\text{Tr}(ax + bx)}) \prod_{i=1}^{\theta} (1 + (-1)^{\text{Tr}(d_i x)}) \right] \]

\[ = \frac{1}{2^\theta+1} \sum_{x \in \mathbb{F}_q} \left[ (1 + (-1)^{\text{Tr}(ax + bx)}) \sum_{d \in \mathcal{V}_\theta} (-1)^{\text{Tr}(d x)} \right] \]

\[ = \frac{1}{2^\theta+1} \sum_{d \in \mathcal{V}_\theta} \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(d x)} + \frac{1}{2^\theta+1} \sum_{d \in \mathcal{V}_\theta} \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ax + bx + (b+d)x)} \]

\[ = \frac{q}{2^\theta+1} + \frac{1}{2^\theta+1} \sum_{d \in \mathcal{V}_\theta} \left( 1 + \sum_{x \in \mathbb{F}_q^*} (-1)^{\text{Tr}(ax + bx + (b+d)x)} \right) \]

\[ = \frac{q+2^\theta}{2^\theta+1} + \frac{1}{2^\theta+1} \sum_{d \in \mathcal{V}_\theta} \sum_{x \in \mathbb{F}_q^*} (-1)^{\text{Tr}(ax + bx + (b+d)x)} \]

\[ = \frac{q+2^\theta}{2^\theta+1} + \frac{1}{2^\theta+1} \sum_{d \in \mathcal{V}_\theta} S(a, b + d). \]

Thus,

\[ w(\mathcal{V}_\theta) = n_0 - N_{\mathcal{V}_\theta} = \frac{q+1}{2} + \frac{1}{2} S(a, b) - \left( \frac{q+2^\theta}{2^\theta+1} + \frac{1}{2^\theta+1} \sum_{d \in \mathcal{V}_\theta} S(a, b + d) \right) \]

\[ = \frac{2^\theta q}{2^\theta+1} + \left( \frac{1}{2} - \frac{1}{2^\theta+1} \right) S(a, b) - \frac{1}{2^\theta+1} \sum_{d \in \mathcal{V}_\theta, d \neq 0} S(a, b + d). \]
Formula (10) may be used to determine the GHW of the code $C_A$ in certain cases. We state our results according to whether $b = 0$ or $b \neq 0$ in the pair $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q$.

**Theorem 20.** For any pair $(a, b) = (a, 0)$ such that $wt(a^{(0)})$ is even, the corresponding code $C_A$ satisfies

\[ w_{\min}^a = \frac{2^\theta - 1}{2^\theta + 1} \left( q - \sqrt{q} + \frac{q + \sqrt{q}}{r_m} S(a) \right) \]

for any $\theta$ with $1 \leq \theta \leq \phi(r^m)/2$.

**Proof.** If $(a, b) = (a, 0)$, then for any $\theta$-dimensional subspace $\mathcal{V}_\theta$, it follows from (10) and Lemma 4 that

\[ w(\mathcal{V}_\theta) = \frac{2^\theta q - q}{2^\theta + 1} + \left( \frac{1}{2} - \frac{1}{2^\theta + 1} \right) S(a, 0) - \frac{1}{2^{\theta+1}} \sum_{d \in \mathcal{V}_\theta, d \neq 0} S(a, d) \]

\[ = \frac{2^\theta q - q}{2^\theta + 1} + \left( \frac{1}{2} - \frac{1}{2^\theta + 1} \right) S(a) - \frac{1}{2^\theta + 1} \sum_{d \in \mathcal{V}_\theta, d \neq 0} (\pm \sqrt{q} - \frac{\sqrt{q} + 1}{r_m} S(a)) \]

\[ \geq \frac{2^\theta - 1}{2^\theta + 1} \left( q - \sqrt{q} + \frac{q + \sqrt{q}}{r_m} S(a) \right). \]

(11)

To proceed the proof, it suffices to find a $\theta$-dimensional subspace $\mathcal{V}_\theta \subset \mathbb{F}_q$ over $\mathbb{F}_2$ such that $w(\mathcal{V}_\theta)$ achieves the lower bound in (11).

Recall that $\mathbb{F}_{2^t}$, $t = \phi(r^m)/2$, is a subfield of $\mathbb{F}_q$ such that $d^{\frac{q-1}{2^t}} = 1$ for any $d \in \mathbb{F}_{2^t}$ (see (9) in Section 4). It follows that

\[ S(a, d) = (-1)^{wt(a^{(0)})} \sqrt{q} - \frac{\sqrt{q} + 1}{r_m} S(a) = \sqrt{q} - \frac{\sqrt{q} + 1}{r_m} S(a) \]

for any $d \in \mathbb{F}_{2^t}$ by Lemma 4 and $wt(a^{(0)})$ being even. Now we take any $\theta$-dimensional subspace $\mathcal{V}_0$ with $\mathcal{V}_0 \subset \mathbb{F}_{2^t}$, then it follows from (11) and (12) that

\[ w(\mathcal{V}_\theta) = \frac{2^\theta - 1}{2^\theta + 1} \left( q - \sqrt{q} + \frac{q + \sqrt{q}}{r_m} S(a) \right). \]

(12)

Theorem 20 is particularly applied to the special case $(a, b) = (1, 0)$, which corresponds to the code $C_A$ studied in [9]. Since $wt(1^{(0)}) = r - 1$ is even and $S(a) = r^m - 2(r - 1)$ [9], we obtain

**Corollary 21.** For $(a, b) = (1, 0)$, the corresponding code $C_A$ satisfies

\[ w_{\min}^a = \frac{2^\theta - 1}{2^\theta + 1} \left( q - \sqrt{q} + \frac{q + \sqrt{q}}{r_m} S(1) \right) \]

\[ = \frac{2^\theta - 1}{2^\theta} \left( q - \frac{r - 1}{r_m} (q + \sqrt{q}) \right) \]

for any $\theta$ with $1 \leq \theta \leq \phi(r^m)/2$.
For the general pair \((a, b)\) with \(b \neq 0\), the result is a little more complicated, and our main result is

**Theorem 22.** For any \((a, b)\) with \(b \neq 0\), let \(c = ab^{-\frac{q-1}{r}}\), and assume \(\text{wt}(c^{(0)})\) is even. Then, the code \(C_{\theta}\) satisfies

\[
\begin{align*}
\omega_{\min} &= \min \left\{ \frac{2^\theta q - q}{2^{\theta+1}} + \frac{1}{2^{\theta+1}} \sqrt{q} - \frac{1}{2^{\theta+1}} \frac{q + \sqrt{q}}{r^m} S(a), \frac{2^\theta q - q}{2^{\theta+1}} \right\}
\end{align*}
\]

for any \(\theta\) with \(1 \leq \theta \leq \phi(r^m)/2\).

**Proof.** Since \(b \neq 0\), the map \(y \mapsto by\), \(y \in \mathbb{F}_q\), is one-to-one from \(\mathbb{F}_q\) to itself. For any \(\theta\) with \(1 \leq \theta \leq \phi(r^m)/2\), the map is a permutation of the \(\theta\)-dimensional subspaces of \(\mathbb{F}_q\) over \(\mathbb{F}_2\). We simply denote the image of a \(\theta\)-dimensional subspace \(\mathcal{V}_\theta\) under this map by \(b\mathcal{V}_\theta\).

Using (10), we get

\[
\begin{align*}
\omega(\mathcal{V}_\theta) &= \frac{2^\theta q - q}{2^{\theta+1}} + \left(\frac{1}{2} - \frac{1}{2^{\theta+1}}\right) S(a, b) - \frac{1}{2^{\theta+1}} \sum_{d \in \mathcal{V}_\theta, d \neq 0} S(a, b + d) \\
&= \left\{ \begin{array}{ll}
\frac{2^\theta q - q}{2^{\theta+1}} + \left(\frac{1}{2} - \frac{1}{2^{\theta+1}}\right) S(a, b) - \frac{1}{2^{\theta+1}} S(a, 0) - \\
\frac{1}{2^{\theta+1}} \sum_{d \in \mathcal{V}_\theta, d \neq 0} S(a, b + d), & b \in \mathcal{V}_\theta \\
\frac{2^\theta q - q}{2^{\theta+1}} + \left(\frac{1}{2} - \frac{1}{2^{\theta+1}}\right) S(a, b) - \frac{1}{2^{\theta+1}} \sum_{d \in \mathcal{V}_\theta, d \neq 0} S(a, b + d), & b \notin \mathcal{V}_\theta \\
\frac{2^\theta q - q}{2^{\theta+1}} + \left(\frac{1}{2} - \frac{1}{2^{\theta+1}}\right) S(a, b) - \frac{1}{2^{\theta+1}} S(a, 0) - \\
\frac{2^\theta q - q}{2^{\theta+1}} + (\sqrt{q} - \frac{\sqrt{q} + 1}{r^m}) S(a), & b \in \mathcal{V}_\theta \\
\frac{2^\theta q - q}{2^{\theta+1}} + (\sqrt{q} - \frac{\sqrt{q} + 1}{r^m}) S(a) - \frac{2^\theta q - 1}{2^{\theta+1}} (\sqrt{q} - \frac{\sqrt{q} + 1}{r^m}) S(a), & b \notin \mathcal{V}_\theta \\
\end{array} \right.
\end{align*}
\]

If \(\text{wt}(c^{(0)})\) is even, then these two lower bounds can be modified to

\[
\begin{align*}
\omega(\mathcal{V}_\theta) &\geq \left\{ \begin{array}{ll}
\frac{2^\theta q - q}{2^{\theta+1}} + \frac{1}{2^{\theta+1}} \sqrt{q} - \frac{1}{2^{\theta+1}} \frac{q + \sqrt{q}}{r^m} S(a), & b \in \mathcal{V}_\theta \\
\frac{2^\theta q - q}{2^{\theta+1}} + \frac{1}{2^{\theta+1}} \sqrt{q} - \frac{1}{2^{\theta+1}} \frac{q + \sqrt{q}}{r^m} S(a), & b \notin \mathcal{V}_\theta \\
\end{array} \right.
\end{align*}
\]

Similar to the arguments as in the proof of Theorem 20, it suffices to find the subspaces which can achieve the lower bounds in (13). To this end, we take any \(\theta\)-dimensional subspace \(\mathcal{V}_\theta \subset \mathbb{F}_2^t\) \((t = \phi(r^m)/2)\) such that \(1 \in \mathcal{V}_\theta\), then, it can be checked that \(\omega(b\mathcal{V}_\theta)\) achieves the first lower bound in (13). Similarly, we take any \(\theta\)-dimensional subspace \(\mathcal{V}_\theta \subset \mathbb{F}_2^t\) such that \(1 \notin \mathcal{V}_\theta\), then, it can be checked that \(\omega(b\mathcal{V}_\theta)\) achieves the second lower bound in (13). We thus finish the proof of the theorem.  

\[\square\]
6. Conclusion

In this paper, we obtained many classes of two-weight and three-weight codes by generalizing the constructing method introduced by Wang et al. The weight distributions of these two-weight and three-weight codes were completely determined, and the minimum distance of the duals of these codes was determined. We also showed that some subclasses of the duals of these codes were optimal. Furthermore, some parameters of the generalized Hamming weight of these codes were calculated in certain cases. We remarked that these two-weight and three-weight codes can be employed in secret sharing schemes using the framework in [14].

References

[1] A. R. Anderson, C. Ding, T. Helleseth and T. Kløve, How to build robust shared control systems, Des., Codes Cryptogr., 15 (1998), 111–124.
[2] C. Carlet, C. Ding and J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Trans. Inf. Theory, 51 (2005), 2089–2102.
[3] K. Ding and C. Ding, Binary linear codes with three weights, IEEE Commun. Lett., 18 (2014), 1879–1882.
[4] C. Ding, T. Helleseth, T. Kløve and X. Wang, A general construction of authentication codes, IEEE Trans. Inf. Theory, 53 (2007), 2229–2235.
[5] G. D. Forney, Dimension/length profiles and trellis complexity of linear block codes, IEEE Trans. Inf. Theory, 40 (1994), 1741–1752.
[6] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[7] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[8] M. Moisio, Explicit evaluation of some exponential sums, Finite Fields Their Appl., 15 (2009), 644–651.
[9] Q. Wang, K. Ding and R. Xue, Binary linear codes with two weights, IEEE Commun. Lett., 19 (2015), 1097–1100.
[10] Q. Wang, K. Ding, D. D. Lin and R. Xue, A kind of three-weight linear codes, Cryptogr. Commun., 9 (2017), 315–322.
[11] V. K. Wei, Generalized Hamming weights for linear codes, IEEE Trans. Inf. Theory, 37 (1991), 1412–1418.
[12] M. H. Yang, J. Li, K. Q. Feng and D. D. Lin, Generalized Hamming weights of irreducible cyclic codes, IEEE Trans. Inf. Theory, 61 (2015), 4905–4913.
[13] J. Yuan and C. Ding, Secret sharing schemes from two-weight codes, Electronic Notes in Discrete Mathematics, 15 (2003), P232.
[14] J. Yuan and C. Ding, Secret sharing schemes from three classes of linear codes, IEEE Trans. Inf. Theory, 52 (2006), 206–212.

Received June 2017; revised February 2018.

E-mail address: 1192338547@qq.com
E-mail address: lzhui@bit.edu.cn