Five-weight codes from three-valued correlation of M-sequences *

Minjia Shi

School of Mathematical Sciences, Anhui University, China

Liqin Qian

Department of Mathematics, Nanjing University of Aeronautics and Astronautics, China

Tor Helleseth

The Selmer Center, Department of Informatics, University of Bergen, Bergen, Norway

Patrick Solé

I2M,CNRS, Centrale Marseille, University of Aix-Marseille, Marseilles, France

Abstract: In this paper, for each of six families of three-valued m-sequence correlation, we construct an infinite family of five-weight codes from trace codes over the ring $R = \mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$. The trace codes have the algebraic structure of abelian codes. Their Lee weight distribution is computed by using character sums. Their support structure is determined. An application to secret sharing schemes is given. The parameters of the binary image are $[2^{m+1}(2^m - 1), 4m, 2^m(2^m - 2^r)]$ for some explicit r.

Key words: Secret sharing schemes; Five-weight codes; M-sequence; Correlation; Trace codes.

*This research is supported by National Natural Science Foundation of China (61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), the Academic Fund for Outstanding Talents in Universities (gxbjZD03) and by The Research Council of Norway (247742/O70). Minjia Shi (Corresponding author: smjwcl.good@163.com)

1 Introduction

Few weight codes form an important topic in secret sharing schemes [4, 7, 25]. When using Massey's secret sharing scheme [7], the minimality of codewords for support inclusion is a crucial question, which is easier to elucidate in codes with a small number of explicit weights, using the Ashikmin-Barg criterion [1].

A classical construction of codes over finite fields called **trace codes** is as follows

$$C := \{(tr(d_1x), \dots, tr(d_nx)) \mid x \in F\},$$

where F is some extension of the alphabet field, tr is the trace function from F down to the alphabet, and the set $L = \{d_1, \dots, d_n\} \subseteq F$ is the **defining set**. Many few-weight codes can be produced by this method [25, 7].

In recent papers [20, 19, 21, 22, 24], the notion of trace codes has been extended from finite fields alphabets to a ring R. Then a linear Gray map constructs codes over a finite field from codes over R. The **Lee weight** over R is the Hamming weight of the Gray image. They are part of a general research program where a variety of few weight codes are obtained by varying the base ring and the defining set. Let $\mathbb{F}_q$ denote a finite field with q elements. We can summarize the outcome of this research program as shown below:
[20]: $L = \mathcal{R}_m^*, R = \mathbb{F}_2 + u\mathbb{F}_2; u^2 = 0$
[19]: $L = \mathcal{R}_m^*, R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2; u^2 = v^2 = 0; uv = vu;$
[21]: $L = D + u\mathbb{F}_{p^m}, (p-1)|[\mathcal{R}_m^* : L], R = \mathbb{F}_p + u\mathbb{F}_p; D \subseteq \mathbb{F}_{p^m};$
[22]: $[\mathcal{R}_m^* : L] = 2, R = \mathbb{F}_p + u\mathbb{F}_p;$
[24]: $L = \mathcal{R}_m^*, R = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2;$
Here, L is called the defining set of trace codes, $\mathcal{R}_m$ denotes an m-extension of the ring R with $m > 1$ and $\mathcal{R}_m^*$ its set of units. The symbol $[A : B]$ denotes the index of the subgroup A of B.

In the present paper, we define a trace code by replacing the linear form d_ix in the above definition by a binomial (a polynomial with exactly two monomials) in x. In particular, we use the binomials of the form $x + x^d$ (the integer d is called the **decimation**) that occur in the evaluation of pairs of m-sequences with a three-valued correlation. Seven infinite families of such binomials are known [3, 5, 9, 12, 16, 18], and they are conjectured to be the only ones. See [10, 13] for a survey on low correlation sequences. In this paper, we manage to give a unified proof that six of them yield five-weight binary codes when $R = \mathbb{F}_2 + u\mathbb{F}_2$, and $L = \mathcal{R}_m^*$. In contrast with most constructions of few-weight codes our trace codes are not visibly cyclic [2], but they are provably abelian.

The manuscript is organized as follows. Basic notations and definitions are provided in Section 2. Section 3 shows that the codes and their binary images are abelian. The main result, the Lee weight distribution of these codes, is presented in Section 4. Some results on the dual distance and on the support structure of the binary images and an application to secret sharing schemes are given in Section 5 and Section 6.

2 Preliminaries

We consider the local ring $\mathbb{F}_2 + u\mathbb{F}_2$ denoted by R, with $u^2 = 0$. For any positive integer m, we construct an extension of degree m of R as $\mathcal{R}_m = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ with again $u^2 = 0$. This is a local ring with maximal ideal (u), and a chain ring of depth two. Furthermore, there is a *conjugacy map* F which maps $z = \alpha + \beta u$ onto $F(z) = \alpha^2 + \beta^2 u$ for $\alpha, \beta \in \mathbb{F}_{2^m}$. The *Trace* of z, denoted by $Tr(z)$ is then defined as the sum of its conjugates.

$$Tr(z) = \sum_{j=0}^{m-1} F^j(z).$$

The connection with the standard trace $tr()$ of $\mathbb{F}_{2^m}$ down to $\mathbb{F}_2$ is as follows

$$Tr(\alpha + \beta u) = tr(\alpha) + tr(\beta)u,$$

for all $\alpha, \beta \in \mathbb{F}_{2^m}$. The trace from $\mathbb{F}_{2^m}$ to a subfield $\mathbb{F}_{2^s}$ will be denoted by $tr_s^m()$ and sometimes by $tr_m()$ if $s = 1$.

For convenience, let M denote the maximal ideal of $\mathcal{R}_m$, i.e.,

$$M = (u) = \{\beta u \mid \beta \in \mathbb{F}_{2^m}\},$$

and let M^* denote the nonzero elements of M. The group of units in $\mathcal{R}_m$ is

$$\mathcal{R}_m^* = \{\alpha + \beta u \mid \alpha \in \mathbb{F}_{2^m}^*, \beta \in \mathbb{F}_{2^m}\},$$

where $\mathbb{F}_{2^m}^*$ is the the set of nonzero elements in $\mathbb{F}_{2^m}$. It is easy to check $\mathcal{R}_m^* \cong \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$ and $|\mathcal{R}_m^*| = (2^m - 1)2^m$. Hence, $\mathcal{R}_m^*$ is not a cyclic group and $\mathcal{R}_m = \mathcal{R}_m^* \cup M$.

A **linear code** C over R of length n is an R-submodule of R^n. If $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ are two elements of R^n, their standard inner product is defined by $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$, where the operation is performed in R. The **dual code** of C is denoted by $C^{\perp}$ and defined as $C^{\perp} = \{y \in R^n \mid \langle x, y\rangle = 0, \forall x \in C\}$.

For $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_2^n, d_H(x, y) = |\{i \mid x_i \neq y_i\}|$ is called the **Hamming distance** between x and y and $w_H(x) = d_H(x, 0)$, the Hamming weight of x. The Hamming weight of $c = (c_1, c_2, \dots, c_n)$ of $\mathbb{F}_2^n$ can also be equivalently defined as the number of nonzero components of c.

For any $x = \alpha + \beta u \in R$, we define the **Gray map** $\Phi : R \to \mathbb{F}_2^2$, $\Phi(\alpha + \beta u) = (\beta, \alpha + \beta)$, where $\alpha, \beta \in \mathbb{F}_2$. This map can be extended to R^n in the natural way [20]. From the definition of Gray map, we know that Φ is a bijection and linear. Then Φ is a weight-preserving map from (R^n, Lee weight) to ($\mathbb{F}_2^{2n}$, Hamming weight), that is, $w_L(x) = w_H(\Phi(x)), x \in R^n$.

Given a finite abelian group G, a code over R is said to be **abelian** if it is an ideal of the group ring $R[G]$. In other words, the coordinates of C are indexed by elements of G and G acts regularly on this set. In the special case when G is cyclic, the code is a cyclic code in the usual sense [17].

3 Symmetry

For $a, b \in \mathcal{R}_m$, we define the vector $Ev(a, b)$ by the following evaluation map:

$$Ev(a, b) = (Tr(ax + bx^d))_{x \in \mathcal{R}_m^*}.$$

Define the code $T_d(m)$ by the formula

$$T_d(m) = \{Ev(a, b) \mid a, b \in \mathcal{R}_m\}.$$

Thus $T_d(m)$ is a code of length $|\mathcal{R}_m^*|$ over R.

Proposition 3.1 The group of units $\mathcal{R}_m^*$ acts regularly on the coordinates of $T_d(m)$.
Proof. For any $v', u' \in \mathcal{R}_m^*$ the change of variables $x \mapsto (u'/v')x$ permutes the coordinates of $T_d(m)$, and maps v' to u'. Such a permutation is unique, given v', u'. $\square$

The code $T_d(m)$ is thus an *abelian code* with respect to the group $\mathcal{R}_m^*$. In other words, it is an ideal of the group ring $R[\mathcal{R}_m^*]$. As observed in the previous section, $\mathcal{R}_m^*$ is not a cyclic group, and thus $T_d(m)$ may not be cyclic. The next result shows that its binary image is also abelian.

Proposition 3.2 A degree two extension of $\mathcal{R}_m^*$ of size $2|\mathcal{R}_m^*|$ acts regularly on the coordinates of $\Phi(T_d(m))$.

Proof. It is similar to the proof in [20], and we omit it here. □

4 The values of the Lee Weight

In this section we determine, for some specific values of d, the Lee weight distribution of the code $T_d(m)$ of length $|\mathcal{R}_m^*|$ over R defined by

$$T_d(m) = \{Ev(a,b) \mid a, b \in \mathcal{R}_m\},$$

where the evaluation map $Ev(a,b)$ is given by

$$Ev(a,b) = (Tr(ax + bx^d))_{x \in \mathcal{R}_m^*}.$$

The Lee weight distribution has so far not been determined for $T_d(m)$ for any d. The determination of the Lee weight distribution of $T_d(m)$ over R also determines the Hamming weight distribution of the binary code $\Phi(T_d(m))$ of length $2|\mathcal{R}_m^*|$.

We consider the following seven values of d (called decimations) given by d_i, $i = 1, 2, \cdots, 7$,

1) $d_1 = 2^k + 1$, where $\frac{m}{\gcd(k,m)}$ is odd.

2) $d_2 = 2^{2k} - 2^k + 1$, where $\frac{m}{\gcd(k,m)}$ is odd.

3) $d_3 = 2^{\frac{m-1}{2}} + 3$, where m is odd.

4) $d_4 = 2^{\frac{m-1}{2}} + 2^{\frac{m-1}{4}} - 1$, where $m \equiv 1 \pmod 4$.

5) $d_5 = 2^{\frac{m-1}{2}} + 2^{\frac{3m-1}{4}} - 1$, where $m \equiv 3 \pmod 4$.

6) $d_6 = 2^{\frac{m}{2}} + 2^{\frac{m+2}{4}} + 1$, where $m \equiv 2 \pmod 4$.

7) $d_7 = 2^{\frac{m}{2}+1} + 3$, where $m \equiv 2 \pmod 4$.

Note that it is well known that $\gcd(d_i, 2^m - 1) = 1$ for $i = 1, 2, \cdots, 7$.

The main result in this paper is to show that each of the codes $T_d(m)$ have five Lee weights and to determine their Lee weight distributions for any $d \in D^* = \{d_1, d_2, d_3, d_4, d_5, d_6\}$. The last value of $d = d_7$ does not lead to a five weight code $T_d(m)$. Actually to find the Lee weight distribution of T_{d_7} appears to be a very hard open problem and is left as a challenge to the reader.

In the following we define a family of binary codes $B_d(m)$ of length $2^m - 1$ that are related to the family of codes $T_d(m)$ of length $|\mathcal{R}_m^*|$ over R. Let $B_d(m)$ be the binary code

$$B_d(m) = \{v(a,b) \mid a, b \in \mathbb{F}_{2^m}\},$$

where

$$v(a,b) = (tr(ax + bx^d))_{x \in \mathbb{F}_{2^m}^*}.$$

.

Let

$$C_d(a,b) = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{tr(ax+bx^d)}.$$

The exponential sum $C_d(a,b)$ is fundamental for determination of the cross correlation between two binary m-sequences of period $2^m - 1$ that differ by a decimation d.

The weight distribution of the code $B_d(m)$ is completely determined by the values taken on by the exponential sum $C_d(a,b), a, b \in \mathbb{F}_{2^m}$ since $w_H(v(a,b)) = \frac{2^m-1-C(a,b)}{2}$. Let $D = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7\}$ and note that the following lemma shows that $d \in D$ are all the known values for $C_d(a,b)$ to take on three different values when $a, b \in \mathbb{F}_{2^m}$. In particular, it follows that the corresponding binary codes $B_d(m)$ have only three nonzero Hamming weights for $d \in D$. It has been conjectured by Dobbertin [8] that the set D of seven families of decimations gives all three-valued $C_d(a,b)$.

To find values of d leading to a three-valued $C(a,b)$ has been a research problem for more than 50 years [9, 12, 14]. These results have numerous applications in communication systems, sequence designs, coding theory and cryptology [10]. In particular, this has led to families of sequences applied in GPS, and in many other mobile communication standards [13].

The important role of $d \in D$ to construct binary codes with few weights of period $2^m - 1$ make these decimations good candidates for finding other codes with few weights among the codes $T_d(m)$ of length $|\mathcal{R}_m^*| = 2^m(2^m - 1)$.

Lemma 4.1 [1, 3, 8, 5, 9, 12, 13, 16, 18] Let $D = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7\}$, then the seven values $d \in D$ have the property that $\gcd(d, 2^m - 1) = 1$. The distribution of

$$C_d(a,1) = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{tr(ax+x^d)},$$

when a runs through $\mathbb{F}_{2^m}^*$, is three-valued and has the following distribution:

$$\begin{array}{ccll} -1 & \text{occurs} & M_0 & \text{times,} \\ -1+2^r & \text{occurs} & M_+ & \text{times,} \\ -1-2^r & \text{occurs} & M_- & \text{times,} \end{array}$$

where $r = \frac{m+e}{2}$, $M_0 = 2^m - 2^{m-e} - 1$, $M_+ = 2^{m-e-1} + 2^{\frac{m-e-2}{2}}$, $M_- = 2^{m-e-1} - 2^{\frac{m-e-2}{2}}$.

Furthermore, $e = \gcd(m,k)$ for the cases d_1 and d_2, $e = 1$ for the cases d_3, d_4 and d_5, and finally $e = 2$ for the cases d_6 and d_7.

Note that since $\gcd(d, 2^m - 1) = 1$ for $d \in D$, then $C_d(a,b) = C_d(ab^{-\frac{1}{d}}, 1)$.

In the analysis of the Lee weight distribution of $T_d(m)$ it is important to know $\gcd(d-1, 2^m-1)$ that is given in the following lemma.

Lemma 4.2 The following holds:

1) $\gcd(d_i - 1, 2^m - 1) = 1$ for $i = 1, 3, 4, 5$.

2) $\gcd(d_2 - 1, 2^m - 1) = 2^{\gcd(k,m)} - 1$.

3)

$$\gcd(d_6 - 1, 2^m - 1) = \left\{ \begin{array}{lll} 1 & \text{if} & m \equiv 2 \pmod 8, \\ 3 & \text{if} & m \equiv 6 \pmod 8). \end{array} \right.$$

4) $\gcd(d_7 - 1, 2^m - 1) = 2^{\frac{m}{2}} + 1$.

Proof. We only provide a short proof for the cases involving d_4 and d_5 and omit the other and more trivial cases.

Consider the case $d_4 = 2^{\frac{m-1}{2}} + 2^{\frac{m-1}{4}} - 1$, $m \equiv 1 \pmod 4$. Let $x = 2^{(m-1)/4}$ and observe that $d_4 - 1 = x^2 + x - 2$ and $\gcd(d_4 - 1, 2^m - 1) = \gcd(x^2 + x - 2, 2x^4 - 1)$. The extended Euclidean algorithm leads to

$$31 = (10x + 21)(2x^4 - 1) - (20x^3 + 22x^2 + 18x + 26)(x^2 + x - 2),$$

and therefore $\gcd(d_4 - 1, 2^m - 1)$ divides 31 .

Let $t = (m-1)/4$. If 31 divides $2^m - 1 = 2^{4t+1} - 1$, we have $t \equiv 1 \pmod 5$. In this case, $d_4 - 1 = 2^{2t} + 2^t - 2 \equiv 4 \not\equiv 0 \pmod{31}$, and thus $\gcd(d_4 - 1, 2^m - 1) = 1$.

Consider the case $d_5 = 2^{\frac{m-1}{2}} + 2^{\frac{3m-1}{4}} - 1$, $m \equiv 3 \pmod 4$. Let $x = 2^{(m+1)/4}$ and observe that in this case $\gcd(d_5 - 1, 2^m - 1) = \gcd(\frac{x^3}{2} + \frac{x^2}{2} - 2, \frac{x^4}{2} - 1)$. We obtain

$$62 = (9x^2 + 20x + 21)(x^4 - 2) - (9x^3 + 11x^2 + 10x + 26)(x^3 + x^2 - 4)$$

and thus $\Delta = \gcd(d_5 - 1, 2^m - 1)$ divides 31.

If $\Delta = 31$ then $x^4 \equiv 2 \pmod{31}$ and $x^3 + x^2 \equiv 4 \pmod{31}$. The first equation has only the two solutions $x = \pm 2^4$. Inserting the value $x = 2^4$ in the second equation gives

$$x^3 + x^2 \equiv (2^4)^3 + (2^4)^2 \equiv 4 + 8 = 12 \not\equiv 4 \pmod{31}.$$

Then we try $x = -2^4 \equiv 15 \pmod{31}$ which is impossible since $x = 2^{\frac{m+1}{4}} \not\equiv 15 \pmod{31}$. Hence, we conclude that $\gcd(d_5 - 1, 2^m - 1) = 1$. □

We first recall the following classic lemmas, which play an important role in determining the Lee weight distribution of $T_d(m)$.

Lemma 4.3 [17, (6) p.412] If $y = (y_1, y_2, \cdots, y_n) \in \mathbb{F}_2^n$, then $2w_H(y) = n - \sum\limits_{i=1}^{n} (-1)^{y_i}$.

Lemma 4.4 [17, Lemma 9 p.143] If $z \in \mathbb{F}_{2^m}^*$, then $\sum\limits_{x \in \mathbb{F}_{2^m}} (-1)^{tr(zx)} = 0$.

We next will discuss the Lee weight distribution of $T_d(m)$ for $d \in D^*$. Note that the Lee weight distribution of two codes $T_d(m)$ can be different even though the corresponding two codes $B_d(m)$ have the same Hamming weight distribution. This implies that the determination of the Lee weight distribution of $T_d(m)$ is not solely a direct function of the Hamming weight distribution of $B_d(m)$.

Theorem 4.5 Let $a, b \in \mathcal{R}_m$, and let $d \in D^* = \{d_1, d_2, d_3, d_4, d_5, d_6\}$. Let (e, r, M_+, M_0, M_-) be as given in Lemma 4.1. Furthermore, let s be defined by $\gcd(d-1, 2^m-1) = 2^s - 1$ which by Lemma 4.2 holds for all d in D^* for some s depending on d. Let $A_i(x)$ denote the number of codewords of Lee weight i in $T_d(m)$ coming from case x.

(i) If $a = 0, b = 0$, then $w_L(Ev(a, b)) = 0$ and $A_0(i) = 1$.

(ii) If $b = 0, a \neq 0$,
1) $a \in M^*$, then $w_L(Ev(a, b)) = 2^{2m}$ and $A_{2^{2m}}(ii, 1) = 2^m - 1$.
2) $a \in \mathcal{R}_m^*$, then $w_L(Ev(a, b)) = (2^m - 1)2^m$ and $A_{2^m(2^m-1)}(ii, 2) = 2^m(2^m - 1)$.

(iii) If $a = 0, b \neq 0$,
1) $b \in M^*$, then $w_L(Ev(a, b)) = 2^{2m}$ and $A_{2^{2m}}(iii, 1) = 2^m - 1$.
2) $b \in \mathcal{R}_m^*$, then $w_L(Ev(a, b)) = (2^m - 1)2^m$ and $A_{2^m(2^m-1)}(iii, 2) = 2^m(2^m - 1)$.

(iv) If $a \neq 0, b \neq 0$,
1) $a \in M^*, b \in M^*$, then $w_L(Ev(a, b)) = 2^{2m}, 2^{2m} - 2^{r+m}$ or $2^{2m} + 2^{r+m}$ and

$A_{2^{2m}}(iv,1)=(2^m-1)M_0$, $A_{2^{2m}+2^{r+m}}(iv,1)=(2^m-1)M_-$ and $A_{2^{2m}-2^{r+m}}(iv,1)=(2^m-1)M_+$.

2) $a\in M^*, b\in\mathcal{R}_m^*$, then $w_L(Ev(a,b))=(2^m-1)2^m$ and $A_{2^m(2^m-1)}(iv,2)=(2^m-1)^2 2^m$.

3) $a\in\mathcal{R}_m^*, b\in M^*$, then $w_L(Ev(a,b))=(2^m-1)2^m$ and $A_{2^m(2^m-1)}(iv,3)=(2^m-1)^2 2^m$.

4) $a\in\mathcal{R}_m^*, b\in\mathcal{R}_m^*$, then $w_L(Ev(a,b))=2^m(2^m-1), 2^m(2^m-2^s)$ or 2^{2m} and $A_{2^m(2^m-1)}(iv,4)=2^{2m}(2^m-1)\frac{2^m-1}{2^s-1}(2^s-2)$, $A_{2^{2m}}(iv,4)=(2^m-1)^2 2^{2m-s}$ and $A_{2^m(2^m-2^s)}(iv,4)=\frac{(2^m-1)^2 2^{2m-s}}{2^s-1}$.

Proof. (i) If $a=0,b=0$ then $Ev(a,b)=(\underbrace{0,0,\cdots,0}_{|\mathcal{R}_m^*|})$. So $w_L(Ev(a,b))=0$.

Hence, this case contributes with $A_0(i)=1$.

(ii) Let $b=0, a\neq 0$.

1) For $a\in M^*$, let $a=a_1u, a_1\in\mathbb{F}_{2^m}^*,\ x=x_0+x_1u\in\mathcal{R}_m^*, x_0\in\mathbb{F}_{2^m}^*$. So we have $ax=a_1x_0u, Tr(ax)=tr(a_1x_0)u$. Taking Gray map yields

$$\Phi(Ev(a,b))=(tr(a_1x_0),tr(a_1x_0))_{x_0,x_1}.$$

Using Lemma 4.3 and Lemma 4.4 we have

$$\begin{aligned}2|\mathcal{R}_m^*|-2w_L(Ev(a,b)) &= 2\sum_{x_0\in\mathbb{F}_{2^m}^*}\sum_{x_1\in\mathbb{F}_{2^m}}(-1)^{tr(a_1x_0)}\\ &= -2^{m+1}.\end{aligned}$$

Then $w_L(Ev(a,b))=|\mathcal{R}_m^*|+2^m=2^{2m}$.

Therefore this case contributes with $A_{2^{2m}}(ii,1)=2^m-1=|M^*|$.

2) For $a\in\mathcal{R}_m^*$, let $a=a_0+a_1u\in\mathcal{R}_m^*,\ x=x_0+x_1u\in\mathcal{R}_m^*$. So we have $ax=(a_0+a_1u)(x_0+x_1u)=a_0x_0+(a_0x_1+a_1x_0)u, Tr(ax)=tr(a_0x_0)+tr(a_0x_1+a_1x_0)u$. Taking Gray map yields

$$\Phi(Ev(a,b))=(tr(a_0x_1+a_1x_0),tr(a_0x_0)+tr(a_0x_1+a_1x_0))_{x_0,x_1}.$$

From Lemma 4.3 and Lemma 4.4, and the fact that $a_0\neq 0$, we have

$$\begin{aligned}2|\mathcal{R}_m^*|-2w_L(Ev(a,b)) &= \sum_{x_0\in\mathbb{F}_{2^m}^*}\sum_{x_1\in\mathbb{F}_{2^m}}(-1)^{tr(a_0x_1+a_1x_0)}+\\ &\quad \sum_{x_0\in\mathbb{F}_{2^m}^*}\sum_{x_1\in\mathbb{F}_{2^m}}(-1)^{tr(a_0x_0)+tr(a_0x_1+a_1x_0)}\\ &= 0.\end{aligned}$$

Then $w_L(Ev(a,b)) = |\mathcal{R}_m^*| = (2^m-1)2^m$.

The contribution from this case is therefore $A_{2^m(2^m-1)}(ii,2) = 2^m(2^m-1) = |\mathcal{R}_m^*|$.

(iii) In the case $a = 0$ and $b \neq 0$.

1) For $b \in M^*$, let $b = b_1u$, $b_1 \in \mathbb{F}_{2^m}^*$, $x = x_0 + x_1u \in \mathcal{R}_m^*$, $x_0 \neq 0$. So we have $T(bx^d) = tr(b_1x_0^d)u$. Taking Gray map yields

$$\Phi(Ev(a,b)) = (tr(b_1x_0^d), tr(b_1x_0^d))_{x_0,x_1}.$$

From Lemma 4.3 and Lemma 4.4, we have since $b_1 \neq 0$, and $\gcd(d, 2^m-1) = 1$ that

$$\begin{aligned} 2|\mathcal{R}_m^*| - 2w_L(Ev(a,b)) &= 2\sum_{x_0\in\mathbb{F}_{2^m}^*}\sum_{x_1\in\mathbb{F}_{2^m}}(-1)^{tr(b_1x_0^d)} \\ &= -\ 2^{m+1}. \end{aligned}$$

Then $w_L(Ev(a,b)) = |\mathcal{R}_m^*| + 2^m = 2^{2m}$.

Therefore this case contributes with $A_{2^{2m}}(iii,1) = 2^m - 1 = |M^*|$.

2) For $b \in \mathcal{R}_m^*$, let $b = b_0 + b_1u \in \mathcal{R}_m^*$, $b_0 \neq 0$. Let $x = x_0 + x_1u \in \mathcal{R}_m^*$. So we have $bx^d = (b_0+b_1u)(x_0^d + dx_0^{d-1}x_1u) = b_0x_0^d + (b_1x_0^d + b_0dx_0^{d-1}x_1)u$. Hence, since d is odd then $Tr(bx^d) = tr(b_0x_0^d) + tr(b_1x_0^d + b_0x_0^{d-1}x_1)u$. Taking Gray map yields

$$\Phi(Ev(a,b)) = (tr(b_1x_0^d + b_0x_0^{d-1}x_1), tr(b_0x_0^d + b_1x_0^d + b_0x_0^{d-1}x_1))_{x_0,x_1}.$$

From Lemma 4.3 and Lemma 4.4, we have since $b_0 \neq 0$, that

$$\begin{aligned} 2|\mathcal{R}_m^*| - 2w_L(Ev(a,b)) &= \sum_{x_0\in\mathbb{F}_{2^m}^*}\sum_{x_1\in\mathbb{F}_{2^m}}(-1)^{tr(b_1x_0^d+b_0x_0^{d-1}x_1)} + \\ &\quad \sum_{x_0\in\mathbb{F}_{2^m}^*}\sum_{x_1\in\mathbb{F}_{2^m}}(-1)^{tr(b_0x_0^d)+tr(b_1x_0^d+b_0x_0^{d-1}x_1)} \\ &= 0. \end{aligned}$$

Then $w_L(Ev(a,b)) = |\mathcal{R}_m^*| = (2^m-1)2^m$.

The contribution from this case is therefore $A_{2^m(2^m-1)}(iii,2) = 2^m(2^m-1) = |\mathcal{R}_m^*|$.

(iv) In this case $a \neq 0, b \neq 0$.

1) For $a \in M^*, b \in M^*$, let $a = a_1u, b = b_1u, a_1, b_1 \in \mathbb{F}_{2^m}^*, x = x_0 + x_1u \in R_m^*$, $x_0 \neq 0$. Therefore we have

$$\begin{aligned} ax + bx^d &= a_1u(x_0 + x_1u) + b_1u(x_0 + x_1u)^d \\ &= (a_1x_0 + b_1x_0^d)u. \end{aligned}$$

Hence,

$$Tr(ax+bx^d)=tr(a_1x_0+b_1x_0^d)u.$$

Taking Gray map yields

$$\Phi(Ev(a,b))=(tr(a_1x_0+b_1x_0^d),tr(a_1x_0+b_1x_0^d))_{x_0,x_1}.$$

Combined with Lemma 4.3 and Lemma 4.4, we have

$$\begin{aligned} 2|\mathcal{R}_m^*|-2w_L(Ev(a,b)) &= 2\sum_{x_0\in\mathbb{F}_{2^m}^*}\sum_{x_1\in\mathbb{F}_{2^m}}(-1)^{tr(a_1x_0+b_1x_0^d)} \\ &= 2^{m+1}\sum_{x_0\in\mathbb{F}_{2^m}^*}(-1)^{tr(a_1x_0+b_1x_0^d)}. \end{aligned}$$

This means that $w_L(Ev(a,b))=|\mathcal{R}_m^*|-2^mC_d(a_1,b_1)=2^m(2^m-1-C_d(a_1,b_1))$. Therefore Lemma 4.1 implies that $w_L(Ev(a,b))=2^{2m},2^{2m}\pm2^{r+m}$.

Since $C_d(a_1,b_1)=C_d(c,1)$ where $c^d=a_1^d/b_1$ it follows that c runs through all elements in $\mathbb{F}_{2^m}^*$ exactly 2^m-1 times when a_1,b_1 run through $\mathbb{F}_{2^m}^*$.

Hence, it follows from the cross correlation distribution in Lemma 4.1 that the contribution to the weight distribution in this case is: $A_{2^{2m}}(iv,1)=(2^m-1)M_0$, $A_{2^{2m}+2^{r+m}}(iv,1)=(2^m-1)M_-$ and $A_{2^{2m}-2^{r+m}}(iv,1)=(2^m-1)M_+$.

2) For $a\in M^*,b\in\mathcal{R}_m^*$, let $a=a_1u,a_1\in\mathbb{F}_{2^m}^*,b=b_0+b_1u\in\mathcal{R}_m^*,\ x=x_0+x_1u\in\mathcal{R}_m^*$. Thus we have $b_0,x_0\in\mathbb{F}_{2^m}^*$ and since d is odd we obtain

$$\begin{aligned} ax+bx^d &= a_1u(x_0+x_1u)+(b_0+b_1u)(x_0+x_1u)^d \\ &= b_0x_0^d+(a_1x_0+b_1x_0^d+b_0x_0^{d-1}x_1)u, \\ Tr(ax+bx^d) &= tr(b_0x_0^d)+tr(a_1x_0+b_1x_0^d+b_0x_0^{d-1}x_1)u. \end{aligned}$$

Taking Gray map yields

$$\Phi(Ev(a,b))=(tr(a_1x_0+b_1x_0^d+b_0x_0^{d-1}x_1),tr(b_0x_0^d)+tr(a_1x_0+b_1x_0^d+b_0x_0^{d-1}x_1))_{x_0,x_1}.$$

In the light of Lemma 4.3 and Lemma 4.4, it follows from $b_0\neq0$ and $x_0\neq0$, that

$$\begin{aligned} 2|\mathcal{R}_m^*|-2w_L(Ev(a,b)) &= \sum_{x_0\in\mathbb{F}_{2^m}^*}\sum_{x_1\in\mathbb{F}_{2^m}}(-1)^{tr(a_1x_0+b_1x_0^d+b_0x_0^{d-1}x_1)}+ \\ &\quad \sum_{x_0\in\mathbb{F}_{2^m}^*}\sum_{x_1\in\mathbb{F}_{2^m}}(-1)^{tr(b_0x_0^d)+tr(a_1x_0+b_1x_0^d+b_0x_0^{d-1}x_1)} \\ &= 0. \end{aligned}$$

Thus, $w_L(Ev(a,b)) = |\mathcal{R}_m^*| = 2^m(2^m-1)$.

Hence, this case contributes with $A_{2^m(2^m-1)}(iv,2) = (2^m-1)^2 2^m = |M^*||\mathcal{R}_m^*|$.

3) Now we deal with the case $a \in \mathcal{R}_m^*$ and $b \in M^*$ with $a = a_0 + a_1 u \in \mathcal{R}_m^*, b = b_1 u, a_0, b_1 \in \mathbb{F}_{2^m}^*, x = x_0 + x_1 u \in \mathcal{R}_m^*$, $x_0 \in \mathbb{F}_{2^m}^*$. Deduce from computing

$$\begin{aligned} ax + bx^d &= (a_0 + a_1 u)(x_0 + x_1 u) + b_1 u (x_0 + x_1 u)^d \\ &= a_0 x_0 + (a_1 x_0 + a_0 x_1 + b_1 x_0^d) u \end{aligned}$$

that $Tr(ax + bx^d) = tr(a_0x_0) + tr(a_1x_0 + a_0x_1 + b_1x_0^d)u$. Taking Gray map yields

$$\Phi(Ev(a,b)) = (tr(a_1x_0 + a_0x_1 + b_1x_0^d), tr(a_0x_0) + tr(a_1x_0 + a_0x_1 + b_1x_0^d))_{x_0,x_1}.$$

According to Lemma 4.3 and Lemma 4.4, we have since $a_0 \neq 0$,

$$\begin{aligned} 2|\mathcal{R}_m^*| - 2w_L(Ev(a,b)) &= \sum_{x_0 \in \mathbb{F}_{2^m}^*} \sum_{x_1 \in \mathbb{F}_{2^m}} (-1)^{tr(a_1x_0 + a_0x_1 + b_1x_0^d))} + \\ &\quad \sum_{x_0 \in \mathbb{F}_{2^m}^*} \sum_{x_1 \in \mathbb{F}_{2^m}} (-1)^{tr(a_0x_0) + tr(a_1x_0 + a_0x_1 + b_1x_0^d))} \\ &= 0. \end{aligned}$$

Then $w_L(Ev(a,b)) = |\mathcal{R}_m^*| = 2^m(2^m-1)$.

Hence, this case contributes with $A_{2^m(2^m-1)}(iv,3) = (2^m-1)^2 2^m = |M^*||\mathcal{R}_m^*|$.

4) For $a \in \mathcal{R}_m^*, b \in \mathcal{R}_m^*$, let $a = a_0 + a_1 u \in \mathcal{R}_m^*, b = b_0 + b_1 u \in \mathcal{R}_m^*, x = x_0 + x_1 u \in \mathcal{R}_m^*$, $a_0, b_0, x_0 \in \mathbb{F}_{2^m}^*$. So we have since d is odd that

$$\begin{aligned} ax + bx^d &= (a_0 + a_1 u)(x_0 + x_1 u) + (b_0 + b_1 u)(x_0 + x_1 u)^d \\ &= (a_0x_0 + b_0x_0^d) + (a_0x_1 + a_1x_0 + b_1x_0^d + b_0 d x_0^{d-1} x_1) u, \\ Tr(ax + bx^d) &= tr(a_0x_0 + b_0x_0^d) + tr(a_0x_1 + a_1x_0 + b_1x_0^d + b_0x_0^{d-1}x_1)u. \end{aligned}$$

Taking Gray map yields $\Phi(Ev(a,b)) = (tr(a_0x_1 + a_1x_0 + b_1x_0^d + b_0x_0^{d-1}x_1), tr(a_0x_0 + b_0x_0^d) + tr(a_0x_1 + a_1x_0 + b_1x_0^d + b_0x_0^{d-1}x_1))_{x_0,x_1}$. Using Lemma 4.3 and Lemma 4.4, we obtain

$$\begin{aligned} 2|\mathcal{R}_m^*| - 2w_L(Ev(a,b)) &= \sum_{x_0 \in \mathbb{F}_{2^m}^*} \sum_{x_1 \in \mathbb{F}_{2^m}} (-1)^{tr(a_0x_1 + a_1x_0 + b_1x_0^d + b_0x_0^{d-1}x_1)} + \\ &\quad \sum_{x_0 \in \mathbb{F}_{2^m}^*} \sum_{x_1 \in \mathbb{F}_{2^m}} (-1)^{tr(a_0x_0 + b_0x_0^d) + tr(a_0x_1 + a_1x_0 + b_1x_0^d + b_0x_0^{d-1}x_1)}. \end{aligned}$$

Observe that

$$\begin{aligned} 2|\mathcal{R}_m^*| - 2w_L(Ev(a,b)) &= \sum_{x_0\in\mathbb{F}_{2^m}^*} (-1)^{tr(a_1x_0+b_1x_0^d)} \sum_{x_1\in\mathbb{F}_{2^m}} (-1)^{tr((a_0+b_0x_0^{d-1})x_1)} + \\ & \sum_{x_0\in\mathbb{F}_{2^m}^*} (-1)^{tr((a_1+a_0)x_0+(b_1+b_0)x_0^d)} \sum_{x_1\in\mathbb{F}_{2^m}} (-1)^{tr((a_0+b_0x_0^{d-1})x_1)} \\ &= 2^m \sum_{x_0\in U} (-1)^{tr(a_1x_0+b_1x_0^d)} (1+(-1)^{tr(a_0x_0+b_0x_0^d)}) \\ &= 2^{m+1} \sum_{x_0\in U} (-1)^{tr(a_1x_0+b_1x_0^d)} \end{aligned}$$

where $U = \{x \in \mathbb{F}_{2^m}^* \mid a_0 + b_0x^{d-1} = 0\}$. Since $\gcd(d-1, 2^m-1) = 2^s-1$ for any $d \in D^*$, it follows that x^{d-1} and x^{2^s-1} run through the same nonzero elements in $\mathbb{F}_{2^m}^*$ when x runs through $\mathbb{F}_{2^m}^*$ and therefore

$$U = \{x \in \mathbb{F}_{2^m}^* \mid x^{2^s-1} = \frac{a_0}{b_0}\}.$$

Note that U depends on a_0 and b_0.

First, consider the case $U = \emptyset$ that occurs if and only if $\frac{a_0}{b_0} \neq \gamma^{2^s-1}$ for any $\gamma \in \mathbb{F}_{2^m}^*$. In this case

$$w_L(Ev(a,b)) = |\mathcal{R}_m^*| = 2^m(2^m-1).$$

The number of choices of $a_1, b_1 \in \mathbb{F}_{2^m}$ and $a_0, b_0 \in \mathbb{F}_{2^m}^*$ with the condition $\frac{a_0}{b_0} \neq \gamma^{2^s-1}$ for any $\gamma \in \mathbb{F}_{2^m}^*$ is $2^{2m}(2^m-1)\frac{2^m-1}{2^s-1}(2^s-2)$. Hence, this contributes

$$A_{2^m(2^m-1)}(iv, 4) = 2^{2m}(2^m-1)\frac{2^m-1}{2^s-1}(2^s-2).$$

Note that this case never occurs for $s = 1$.

Next consider the case $U \neq \emptyset$, then $\frac{a_0}{b_0} = \gamma^{2^s-1}$ for some $\gamma \in \mathbb{F}_{2^m}^*$, and we have

$$U = \{x \in \mathbb{F}_{2^m}^* \mid x = \gamma\delta, \text{ where } \delta \in \mathbb{F}_{2^s}^*\},$$

since $x^{2^s-1} = \gamma^{2^s-1}\delta^{2^s-1} = \gamma^{2^s-1} = \frac{a_0}{b_0}$ for any $\delta \in \mathbb{F}_{2^m}^*$.

Then, let $c = (a_1 + b_1\frac{a_0}{b_0})\gamma$, we observe that when a_1, b_1 run through $\mathbb{F}_{2^m}$ and a_0, b_0 run through $\mathbb{F}_{2^m}^*$ with the condition $\frac{a_0}{b_0} = \gamma^{2^s-1}$ for some $\gamma \in \mathbb{F}_{2^m}^*$, then each value of $c \in \mathbb{F}_{2^m}$ occurs equally often with multiplicity

$$2^m(2^m-1)\frac{2^m-1}{2^s-1}.$$

The continuation of the calculations above gives,

$$\begin{aligned}
w_L(Ev(a,b)) &= |\mathcal{R}_m^*| - 2^m \sum_{x_0\in U}(-1)^{tr(a_1x_0+b_1x_0^d)} \\
&= |\mathcal{R}_m^*| - 2^m \sum_{x_0\in U}(-1)^{tr((a_1+b_1x_0^{d-1})x_0)} \\
&= |\mathcal{R}_m^*| - 2^m \sum_{x_0\in U}(-1)^{tr((a_1+b_1\frac{a_0}{b_0})\gamma\delta)} \\
&= |\mathcal{R}_m^*| - 2^m \sum_{\delta\in\mathbb{F}^*_{2^s}}(-1)^{tr_m(c\delta)} \\
&= 2^m(2^m-1-\sum_{\delta\in\mathbb{F}^*_{2^s}}(-1)^{tr_s(\delta tr_s^m(c))}).
\end{aligned}$$

Note that, well-known properties of the trace function give

$$\sum_{\delta\in\mathbb{F}^*_{2^s}}(-1)^{tr_s(\delta tr_s^m(c)} = \begin{cases} -1 & \text{if} \quad Tr_s^m(c)\neq 0 \quad \text{that occurs} \quad 2^m-2^{m-s} \quad \text{times,} \\ 2^s-1 & \text{if} \quad Tr_s^m(c)=0 \quad \text{that occurs} \quad 2^{m-s} \quad \text{times.}\end{cases}$$

These two values of the trace function lead to Lee weights 2^{2m} and $2^m(2^m-2^s)$ and the final contributions to the weight distribution in this case becomes:

$$A_{2^{2m}}(iv,4) = (2^m-1)^2 2^{2m-s},$$

$$A_{2^m(2^m-2^s)}(iv,4) = \frac{(2^m-1)^2 2^{2m-s}}{2^s-1}.$$

The discussion above shows that the code has the following five nonzero weights:

$$\{2^{2m}-2^{m+r}, 2^m(2^m-2^s), 2^m(2^m-1), 2^{2m}, 2^{2m}+2^{m+r}\}.$$

Furthermore, the number of codewords of each Lee weight from each case above has been determined. □

The complete Lee weight distribution for $T_d(m)$ follows easily in the following corollary by adding up the information in the previous theorem .

Corollary 4.6 Let (e, r, M_+, M_0, M_-) be as given in Lemma 4.1 and furthermore let s be defined by $\gcd(d-1, 2^m-1) = 2^s-1$ which by Lemma 4.2 holds for all d in D^* for some s depending on d. Let A_i denote the number of codewords of Lee weight i in $T_d(m)$. The Lee weight distribution of the code $T_d(m)$ over R for $d \in D^* = \{d_1, d_2, d_3, d_4, d_5, d_6\}$ is given by:

$A_0 = 1,$

$A_{2^{2m}-2^{m+r}} = (2^m - 1)M_+,$

$A_{2^m(2^m-2^s)} = (2^m - 1)^2 \ \frac{2^{2m-s}}{2^s-1},$

$A_{2^m(2^m-1)} = 2^{2m}(2^m - 1)(2 + (2^m - 1)\frac{2^s-2}{2^s-1}),$

$A_{2^{2m}} = (2^m - 1)(M_0 + 2 + (2^m - 1)2^{2m-s}),$

$A_{2^{2m}+2^{m+r}} = (2^m - 1)M_-.$

In particular the code $\Phi(T_d(m))$ has parameters $[2^{m+1}(2^m - 1), 4m, 2^m(2^m - 2^r)]$.

Proof. This result is a simple consequence of the previous theorem that study several cases and determine, in each case, the number of codewords in $T_d(m)$ of Lee weight i in case x, denoted by $A_i(x)$. Adding the number of codewords of weight i in each case completes the proof. □

A concrete example is as follows.

Example 4.7 Let $m = 5$, $e = 1$, $r = 3$, $s = 1$. Then we obtain a binary code of parameters $[1984, 20, 768]$. The weights are $\{768, 960, 992, 1024, 1280\}$.

5 Dual distance

Proposition 5.2 The dual distance of $T_d(m)$ is 2.

Proof. We exhibit a codeword of weight 2 in $T_d(m)^\perp$ supported by $x, y \in L$. Assume $y = (1 + u)x$. Because d is odd, we have $y^d = (1 + u)x^d$. Hence the relation

$$(x, x^d)^t + (1 + u)(y, y^d)^t = 0.$$

Thus there is a codeword of shape $(1, 1+u, 0^{n-2})$ in $T_d(m)^\perp$. Since $w_L((1, 1+u)) = 2$, the result follows. □

We construct a projective code related to $T_d(m)$, by removing half the columns of its generator matrix. Write $L = L' \cup (1 + u)L'$ (this writing is non unique). Define a trace code $HT_d(m)$, of defining set L' by the relation

$$HT_d(m) = \{(Tr(ax + bx^d)_{x\in L'} \mid a, b \in \mathcal{R}_m\}.$$

Proposition 5.3 The dual distance of $HT_d(m)$ is ≥ 3. Each weight in $HT_d(m)$ is half the weight of some weight in $T_d(m)$ with the same frequency.

Proof. By construction the codewords of weight 2 in $HT_d(m)^\perp$, similar to those described in Proposition 5.2 cannot occur. It is easy to exclude the shapes $(u, 0^{n-1})$

or $(1, 1, 0^{n-2})$. Hence the dual distance of $HT_d(m)$ is ≥ 3. The relation between the weights of $HT_d(m)$ and those of $T_d(m)$ is immediate. □

6 Application to secret sharing schemes

In this section, we first introduce the support structure. Let q be a prime power, and n an integer. Let $\mathbb{F}_q$ denote the finite field of order q. The **support** $s(x)$ of a vector x in $\mathbb{F}_q^n$ is defined as the set of indices where it is nonzero. We say that a vector x covers a vector y if $s(x)$ contains $s(y)$. A **minimal codeword** of a linear code C is a nonzero codeword that does not cover any other nonzero codeword. In general determining the minimal codewords of a given linear code is a difficult task. However, there is a numerical condition, derived in [1], bearing on the weights of the code, that is easy to check.

Lemma 6.1 (Ashikmin-Barg) Denote by w_0 and w_∞ the minimum and maximum nonzero weights, respectively. If

$$\frac{w_0}{w_\infty} > \frac{q-1}{q},$$

then every nonzero codeword of C is minimal.

We can infer from this the support structure for the codes of this paper.

Proposition 6.2 All the nonzero codewords of $\Phi(T_d(m))$, and of $\Phi(HT_d(m))$, for $m > 2$ and m is odd, are minimal.

Proof. Based on the introduction of Lemma 6.1, then $w_0 = \omega_1$, $w_\infty = \omega_5$ and $q = 2$. Next we need to prove the inequality $\frac{w_1}{w_5} > \frac{1}{2}$ is true for $m > 2$. Thus, we obtain

$$\begin{aligned} 2\omega_1 - \omega_5 &= 2(2^{2m} - 2^{\frac{3m+1}{2}}) - (2^{2m} + 2^{\frac{3m+1}{2}}) \\ &= 2^{2m}(1 - 3 \cdot 2^{1-m}) > 0. \end{aligned}$$

Hence the statement on $\Phi(T_d(m))$, is proved. The analogous statement on $\Phi(HT_d(m))$, follows similarly by Proposition 5.3. □

A secret sharing scheme (SSS) is a protocol involving a dealer and S users. **Massey's scheme** is a construction of such a scheme where a code C of length n over $\mathbb{F}_p$ gives rise to a SSS with $S = n - 1$. See [25] for a detailed explanation of the mechanism of that scheme.

Now, the coalition structure is related to the support structure of C. In the special case when all nonzero codewords are minimal, it was shown in [7] that there is the following alternative, depending on the dual distance d':

- If $d' \geq 3$, then the SSS is *"democratic"*: every user belongs to the same number of coalitions.
- If $d' = 2$, then there are users who belong to every coalition: the *"dictators"*.

Depending on the application, one or the other situation might be more suitable. By the results of the preceding section we see that $\Phi(T_d(m))$ leads to a dictatorial scheme, and $\Phi(HT_d(m))$ to a democratic one.

7 Conclusion and open problems

In this paper, we have studied a family of trace codes over $\mathbb{F}_2 + u\mathbb{F}_2$, based on six of the seven known families of decimations leading to three-valued cross correlation of m-sequences. These codes are provably abelian, but not visibly cyclic. Using a character sum approach, we have been able to determine their Lee weight distribution of $T_d(m)$, and we have obtained a family of abelian binary five-weight codes by the Gray map. The same study for the seventh decimation is challenging, and is likely to lead to binary codes with many more than five weights.

References

[1] Ashikmin, A., Barg, A.: Minimal vectors in linear codes, IEEE Transactions on Information Theory, 1998, **44**(5): 2010–2017.

[2] Brouwer, A.E., Haemers, W.H.: *Spectra of Graphs.* Springer New York, 2012.

[3] Canteaut, A., Charpin, P., Dobbertin, H.: Binary m-sequences with three valued crosscorrelation: A proof of Welch's conjecture, IEEE Transactions on Information Theory, 2000, **46**(1): 4-7.

[4] Carlet C., Ding C. and Yuan J., Linear codes from highly nonlinear functions and their secret sharing schemes, IEEE Transactions on Information Theory, 2005, **51**(6): 2089–2102.

[5] Cusick, T. W., Dobbertin, H.: Some new three-valued crosscorrelation functions for binary m-sequences, IEEE Transactions on Information Theory, 1996, **42**(4): 1238-1240.

[6] Ding, C., Luo, J., Niederreiter, H.: Two-Weight Codes Punctured from Irreducible Cyclic Codes. Proceedings of the First International Workshop Wuyi Mountain, Fujian, China, 11 C 15 June 2007 World Scientific, Series on Coding Theory & Cryptology, 2008, 4:288.

[7] Ding C., Yuan J.: Covering and Secret Sharing with Linear Codes. Lecture Notes in Computer Science, 2003, 2731:11-25.

[8] Dobbertin, H.: Almost perfect power functions on $GF(2^n)$: The Welch case, IEEE Transactions on Information Theory, 1999, **45**(4): 1271-1275.

[9] Gold, R.: Maximal recursive sequences with 3-valued cross-correlation functions, IEEE Transactions on Information Theory, 1968, **14**(1): 154-156.

[10] Golomb, S.W., Guang, G.: *Signal design for good correlation for wireless communication, cryptography, and radar*. Cambridge University Press, (2005).

[11] Griesmer, J.H.: A Bound for Error-Correcting Codes. IBM Journal of Research & Development, 1960, **4**(5): 532-542.

[12] Helleseth, T.: Some results about the cross-correlation between two maximal linear sequences, Discrete Mathematics, 1976, **16**(3): 209-232.

[13] Helleseth, T., Kumar, P.V.: Sequences with low correlation, in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998, 1765-1853.

[14] Pursley, M., Sarwate, D. : Crosscorrelation properties of pseudorandom and related sequences,Proceedings of the IEEE, 1980, **vol. 68**, no. 5, 593–619.

[15] Huffman, W.C., Pless, V.: *Fundamentals of Error Correcting Codes*, Cambridge University Press, 2003.

[16] Kasami, T.: The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, Information and Control, 1971, **18**(4): 369-394.

[17] MacWilliams, F.J., Sloane, N.J.A.: *The theory of error-correcting codes*. North-Holland Pub. Co, 1977.

[18] Niho, Y.: Multivalued Cross-Correlation Functions between Two Maximal Linear Recursive Sequences, Ph.D. dissertation, Univ. Southern Calif., Los Angeles, 1972.

[19] Shi, M.J., Liu, Y., Solé, P.: Optimal binary codes from trace codes over a non-chain ring, Discrete Applied Mathematics, **219**(2017), 176–181.

[20] Shi, M.J., Liu, Y., Solé, P.: Optimal two weight codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Communications Letters, 2016, **20**(12): 2346–2349.

[21] Shi, M.J., Liu, Y., Solé, P.: Trace Codes with Few Weights over $\mathbb{F}_p + u\mathbb{F}_p$, `https://arxiv.org/pdf/1612.00128.pdf`

[22] Shi, M.J., Wu ,R.S., Liu, Y., Solé, P.: Two and three weight codes over $\mathbb{F}_2+u\mathbb{F}_2$, Cryptography and Communications, 2017, **9**(5):637–646.

[23] Shi, M.J., Zhu, S.X., Yang, S.L.: A class of optimal p-ary codes from one-weight codes over $\mathbb{F}_p[u]/(u^m)$, Journal of the Franklin Institute, 2013, **350**(5):929-937.

[24] Shi, M.J., Zhu, H.W., Solé, P.: Three-weight codes and the cubic construction, Appl. Comput. Math, 2018, **17**(2):175–184.

[25] Yuan J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Transactions on Information Theory, 2006, **52**(1), 206–212.