Trace codes over Z 4 , and Boolean functions

Minjia Shi, Yan Liu, Hugues Randriambololona, Lin Sok, Patrick Sole

Designs, Codes and Cryptography (2019) 87:1447–1455
https://doi.org/10.1007/s10623-018-0542-x

Trace codes over $\mathbb{Z}_4$, and Boolean functions

Minjia Shi[1,2] · Yan Liu[2] · Hugues Randriam[3] · Lin Sok[2,4] · Patrick Solé[5]

Received: 20 July 2017 / Revised: 6 April 2018 / Accepted: 10 August 2018 / Published online: 25 August 2018

Abstract
We construct trace codes over $\mathbb{Z}_4$ based on Boolean functions and their support. The Lee weight distribution of these codes is studied by using the Walsh–Hadamard transform of the Boolean functions, and exponential character sums. We obtain few weights codes. In particular, bent and semi-bent functions give three-weight codes.

Keywords Galois rings · Boolean functions · Character sums

Mathematics Subject Classification 94B05 · 10G99

1 Introduction

Most trace codes have their coordinate sets indexed by the elements of a finite field, or in the case of $\mathbb{Z}_4$-codes by the Teichmüller set of a Galois ring [6]. This is the case, for instance, of the quaternary Kerdock codes [3]. Recently, Ding investigated a different way of constructing

Communicated by T. Helleseth.

✉ Lin Sok
sok.lin@rupp.edu.kh

Minjia Shi
smjwcl.good@163.com

Yan Liu
liuyan2612@126.com

Hugues Randriam
randriam@enst.fr

Patrick Solé
sole@math.univ-paris13.fr

1 Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, Anhui University, No.3 Feixi Road, Hefei 230039, Anhui, China

2 School of Mathematical Sciences, Anhui University, Hefei 230601, Anhui, China

3 LTCI/Telecom ParisTech, 46 rue Barrault, 75013 Paris, France

4 Department of Mathematics, Royal University of Phnom Penh, Phnom Penh 12156, Cambodia

5 CNRS/LAGA, University of Paris 8, 2, rue de la Liberté, 93 526 Saint-Denis, France

trace codes by indexing their coordinate places by the elements of a difference set [1], and in some cases, the support of a Boolean function [1, §VI].

In this paper we generalize Ding's approach to $\mathbb{Z}_4$-codes. The support S_f of a Boolean function f is mapped to a subset of a Teichmüller set by inverse reduction modulo 2. The Lee weight distribution of the code is studied by means of a variant of the Walsh–Hadamard transform, which is in fact the Walsh–Hadamard transform for a family of Boolean functions. In fact some of our codes (§4.1) will have the codes of [1] both as residue codes and as torsion codes. Another approach, with a different defining set, yields three-weight codes.

The material is organized as follows. The next section sets up the basic notations and definitions. Section 3 gives a character sum approach to the weight distribution of our trace codes. Section 4 discusses the two families of codes we mentioned and give, for the second family, its weight distributions when the Boolean function is bent or semi-bent. Section 5 recapitulates the obtained results and makes some conjectures for future research.

2 Preliminaries

2.1 Rings

In this subsection, we recall several basic facts on the algebraic structure of the Galois ring $GR(4, m)$ and fix several basic notations. For more knowledge on Galois rings we refer to Wan's book [9]. For simplicity, let $\mathcal{R} = GR(4, m)$. Denote by $\mathcal{R}^*$ the group of units. In $\mathcal{R}$ with maximal ideal $I = \langle 2 \rangle$, there exists a nonzero element ξ of order $2^m - 1$, which is a root of a basic primitive polynomial $h(x)$ of degree m over $\mathbb{Z}_4$ and $\mathcal{R} = \mathbb{Z}_4[\xi]$. Let $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$. It can be shown that any element $c \in \mathcal{R}$ can be written uniquely as $c = a + 2b$ with $a, b \in \mathcal{T}$. It can be also shown that $\mathcal{T} \equiv \mathbb{F}_{2^m} \pmod 2$. Recall that the *trace* map tr from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is defined by $tr(a) = \sum_{i=0}^{m-1} a^{2^i}$ for all $a \in \mathbb{F}_{2^m}$. Define the *generalized trace* map Tr from $\mathcal{R}$ to $\mathbb{Z}_4$ by $Tr(c) = tr(a) + 2tr(b)$ for all $c = a + 2b \in \mathcal{R}$.

2.2 Codes

A *linear code* C over $\mathbb{Z}_4$ of length n is a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$. Such a code is of *type* $4^{k_1}2^{k_2}$ if, as an abelian group it is isomorphic to $\mathbb{Z}_4^{k_1} \times \mathbb{Z}_2^{k_2}$. For any two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_4^n$, the Euclidean inner product of $\mathbf{x}$ and $\mathbf{y}$ is defined by $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i$, where the operation is performed in $\mathbb{Z}_4$. The *dual code* of C is denoted by $C^\perp$ and defined as $C^\perp = \{\mathbf{y} \in \mathbb{Z}_4^n : \langle \mathbf{x}, \mathbf{y} \rangle = 0, \forall \mathbf{x} \in C\}$. By definition, $C^\perp$ is also a linear code over $\mathbb{Z}_4$. The *residue code* $Res(C)$ of C is the binary code defined as $Res(C) = \{\mathbf{x} \in \mathbb{F}_2^n : \exists \mathbf{y} \in C, \mathbf{y} \equiv \mathbf{x} \pmod 2\}$. The *torsion code* $Tor(C)$ is the binary code defined as $Tor(C) = \{\mathbf{x} \in \mathbb{F}_2^n : \exists \mathbf{y} \in C, \mathbf{y} = 2\mathbf{x}\}$. The *Lee weight* $w_L(\mathbf{x})$ of $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is defined as $w_L(\mathbf{x}) = n_1(\mathbf{x}) + 2n_2(\mathbf{x}) + n_3(\mathbf{x})$, where $n_i(\mathbf{x})$ denote the number of occurences of a i symbol in $\mathbf{x}$. The *Lee distance* d_L of C is the minimum Lee weight of its nonzero vectors. The parameters of linear $\mathbb{Z}_4$-code are denoted compactly as $(n, 4^{k_1}2^{k_2}, d_L)$.

For any $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_4^n$ with $x_i = r_i + 2q_i$, the *Gray map* ϕ from $\mathbb{Z}_4^n$ to $\mathbb{F}_2^{2n}$ is given by $\phi(\mathbf{x}) = (q(\mathbf{x}), r(\mathbf{x}) + q(\mathbf{x}))$, where $r(\mathbf{x}) = (r_1, r_2, \ldots, r_n), q(\mathbf{x}) =$

$(q_1, q_2, \ldots, q_n)$ are binary vectors. Then ϕ is a weight-preserving map from ($\mathbb{Z}_4^n$, Lee weight) to ($\mathbb{F}_2^{2n}$, Hamming weight), that is, $w_L(\mathbf{x}) = w_H(\phi(\mathbf{x}))$, where $w_H(\phi(\mathbf{x}))$ denotes the number of nonzero positions in the binary vector $\phi(\mathbf{x})$.

3 Trace codes

3.1 Description of trace codes

Let $D = \{d_1, d_2, \ldots, d_n\} \subseteq \mathcal{R}\backslash\{0\}$. We define a linear code of length n over $\mathbb{Z}_4$ by $C_D = \{c_a = (Tr(ad_1), Tr(ad_2), \ldots, Tr(ad_n)) : a \in \mathcal{R}\}$, and call D the defining set of this code C_D. In [1], a similar class of binary codes was introduced as

$$\mathcal{C}_{\bar{D}} = \{c_b = (tr(b\bar{d}_1), \ldots, tr(b\bar{d}_n)) : b \in \mathbb{F}_{2^m}\},$$

for some $\bar{D} = \{\bar{d}_1, \bar{d}_2, \ldots, \bar{d}_n\} \subseteq \mathbb{F}_{2^m}\backslash\{0\}$. The following result is immediate and given without proof.

Proposition 1 *With the above notation, identifying $D \subseteq \mathcal{T}$ with its finite field image, we have*

$$Res(C_D) = Tor(C_D) = \mathcal{C}_D.$$

This implies directly that

$$d_H(\mathcal{C}_D) \leq d_L(C_D) \leq 2d_H(\mathcal{C}_D).$$

3.2 The weights of C_D

The weight enumeration of C_D is facilitated by using character sums of the type $E(a) = \sum_{d\in D} i^{Tr(ad)}$. As is well-known in $\mathbb{Z}_4$-codes studies [3,9], we have

$$w_L(c_a) = n - \Re(E(a)), \tag{1}$$

where $\Re(E(a))$ stands for the real part of $E(a)$.

We shall use sometimes, following [1], a notation inspired by the tradition of difference sets. Let $\chi = i^{Tr()}$ be the canonical additive character of $GR(4, m)$, and let aD denotes the set $\{ad : d \in D\}$. We write $\chi(S) = \sum_{x\in S} \chi(x)$ for any subset S of $GR(4, m)$. With this notation $E(a) = \chi(aD)$.

4 Construction of $\mathbb{Z}_4$-codes by Boolean functions

Let f be a Boolean function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. The support of f is defined to be

$$S_f = \{x \in \mathbb{F}_{2^m} : f(x) = 1\} \subseteq \mathbb{F}_{2^m}.$$

Take a set $\bar{S}_f \subseteq \mathcal{T}$ such that $\bar{S}_f \equiv S_f \pmod 2$. Let the size of set S_f be n_f, that is, $n_f = |S_f| = |\bar{S}_f|$. The Walsh–Hadamard transform of f is defined by

$$W_f(w) = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{f(x)+tr(wx)}, \tag{2}$$

where $w \in \mathbb{F}_{2^m}$. By [1], the Walsh spectrum of f is the following multiset

$$\{\{W_f(w) : w \in \mathbb{F}_{2^m}\}\}.$$

4.1 Case of $D = \bar{S}_f$

Define $\Gamma(w) = \sum_{x \in \mathcal{T}} i^{Tr(wx)}$ with $w \in \mathcal{R}$. Thus $\Gamma(w)$ is $E(w)$ when D is $\mathcal{T}$. In this case $D = \bar{S}_f$, the weight distribution of $C_{\bar{S}_f}$ can be worked out in this subsection. To this end, we need the following lemma [10].

Lemma 1 *Let ϵ be the primitive 8th root of unity, given by $\epsilon = \frac{(1+i)}{\sqrt{2}}$. For any $w = r + 2s \in \mathcal{R}$ with $r(\neq 0), s \in \mathcal{T}$, we have*

$$\Gamma(w) = i^{-Tr(\frac{s}{r})}\Gamma(1)$$

with $\Gamma(1) = \begin{cases} \sqrt{2^m}\epsilon^m, & \text{if } m \text{ is odd,} \\ -\sqrt{2^m}\epsilon^m, & \text{if } m \text{ is even.} \end{cases}$

Now, define $Q(x) = \sum_{\substack{i,j=0 \\ j>i}}^{m-1} x^{2^i+2^j}$ and $\hat{f}(w) = 2^{-m} \sum_{x \in \mathcal{R}} i^{2f(\bar{x})+Tr(wx)}$, where $w \in \mathcal{R}$ and $f(\bar{x}) = 1$ if $x \in \bar{S}_f$, otherwise 0. The main result of this subsection is then described in the following theorem.

Theorem 1 *Let symbols and notations be as above. Let $w = r + 2s \in \mathcal{R}$ with $r, s \in \mathcal{T}$. Then $C_{\bar{S}_f}$ is a linear code over $\mathbb{Z}_4$ with length n_f and its Lee weight distribution is given by the following multiset:*

$$\left\{\left\{\frac{4n_f - 2\Re(\Gamma(w)) + W_{f_r}(\bar{s}) + W_{f_r}(\bar{r}+\bar{s})}{4}\right\}\right\} \cup \left\{\left\{\frac{2n_f + W_f(\bar{s})}{2}\right\}\right\} \cup \{\{0\}\}, \tag{3}$$

with $f_r(x) = f(x) + Q(rx)$.

Proof It is trivial that $w_L(c_0) = 0$. As defined previously, we have $2^m \hat{f}(w) = \sum_{x \in \mathcal{R}} i^{2f(\bar{x})+Tr(wx)}$, where $f(\bar{x}) = 1$ if $x \in \bar{S}_f$, and $f(\bar{x}) = 0$ if $x \notin \bar{S}_f$. Let $w = 2s \in I$ with $s \in \mathcal{T}\backslash\{0\}$. From the previous discussion in the Sects. 2 and 3, we have

$$\begin{aligned} 2^m \hat{f}(w) &= \sum_{\substack{x=y+2z \in \mathcal{R} \\ x \in \mathcal{T}+2\mathcal{T}}} i^{2f(\bar{x})+Tr(wx)} \\ &= 2^m \sum_{y \in \mathcal{T}} (-1)^{f(\bar{y})+tr(\bar{s}\bar{y})} \\ &= 2^m W_f(\bar{s}). \end{aligned}$$

On the other hand,

$$\begin{aligned}
2^m \hat{f}(w) &= \sum_{\substack{x=y+2z\in\mathcal{R}\\ x\in\mathcal{T}+2\mathcal{T}}} i^{2f(\bar{x})+Tr(wx)} \\
&= \sum_{\substack{x=y+2z\\ x\in\bar{S}_f+2\mathcal{T}}} i^{2f(\bar{x})+Tr(wx)} \\
&\quad + \sum_{\substack{x=y+2z\\ x\in(\mathcal{T}\setminus\bar{S}_f)+2\mathcal{T}}} i^{2f(\bar{x})+Tr(wx)} \\
&= \sum_{z\in\mathcal{T}}\sum_{y\in\bar{S}_f} i^{2f(\bar{y})+Tr(wy)} \\
&\quad + \sum_{z\in\mathcal{T}}\sum_{y\in\mathcal{T}\setminus\bar{S}_f} i^{2f(\bar{y})+Tr(wy)} \\
&= 2^m\Big(-\sum_{y\in\bar{S}_f} i^{Tr(wy)} + \sum_{y\in\mathcal{T}\setminus\bar{S}_f} i^{Tr(wy)}\Big) \\
&= -2^{m+1}\chi(w\bar{S}_f),
\end{aligned}$$

where the last equality follows by $\sum_{y\in\mathcal{T}} i^{Tr(wy)} = \sum_{y\in\mathbb{F}_2^m} (-1)^{tr(\bar{s}\bar{y})} = 0$ with $s \neq 0$. It then follows from Eq. (1) that the Lee weight of the codeword c_w with $w \in I\setminus\{0\}$ is equal to $\frac{2n_f+\Re(W_f(\bar{s}))}{2}$.

It remains to consider $w = r + 2s$ with $r \neq 0$. Now consider $E(w) = \sum_{d\in\bar{S}_f} i^{Tr(wd)} = \sum_{x\in\mathcal{T}} \frac{1-(-1)^{f(\bar{x})}}{2} i^{Tr(wx)}$, which implies $w_L(c_w) = n_f - \Re(E(w))$. So it is necessary to analyze the exponential sum $E(w)$. By a simple calculation, we have

$$\begin{aligned}
2E(w) &= \sum_{x\in\mathcal{T}} i^{Tr(wx)} - \sum_{x\in\mathcal{T}} (-1)^{f(\bar{x})} i^{Tr(wx)} \\
&= \Gamma(w) - \sum_{x\in\mathcal{T}} (-1)^{f(\bar{x})+tr(\bar{s}\bar{x})} i^{Tr(rx)} \\
&= \Gamma(w) - \sum_{x\in\mathcal{T}} (-1)^{f(\bar{x})+tr(\bar{s}\bar{x})+Q(\bar{r}\bar{x})} i^{tr(\bar{r}\bar{x})}
\end{aligned}$$

where the last equality follows by $Tr(rx) = tr(\bar{r}\bar{x}) + 2Q(\bar{r}\bar{x})$ given in [6]. Furthermore, letting $f_r(\bar{x}) = f(\bar{x}) + Q(\bar{r}\bar{x})$, and using the identity

$$\forall a \in \{0,1\},\ i^a = \frac{1+(-1)^a}{2} + \frac{1-(-1)^a}{2} i,$$

with $a = tr(\bar{r}\bar{x})$, we get $\Re(E(w)) = \frac{1}{2}\Re(\Gamma(w)) - \frac{1}{4}\Re(W_{f_r}(\bar{s}) + W_{f_r}(\bar{r}+\bar{s}))$. Hence, the Lee weight distribution of $C_{\bar{S}_f}$ is given by the multiset in (3). This completes the proof. □

Example 2 In this example, we construct trace codes over $\mathbb{Z}_4$ from bent, semi-bent and formally self-dual [5] and boolean functions of $m = 4$ variables and compare their minimum distance with that of residue and torsion codes in Table 1.

Table 1 Comparison of minimum distances for C_D, $Res(C_D)$ and $Tor(C_D)$

C_D	$d_H(Res(C_D)) \le d_L(C_D) \le 2d_H(Tor(C_D))$
$C_{\bar{S}_{f_1}}$	$2 \le 4 \le 4$
$C_{\bar{S}_{f_2}}$	$2 \le 3 \le 4$
$C_{\bar{S}_{f_3}}$	$6 \le 6 \le 12$
$C_{\bar{S}_{f_4}}$	$2 \le 2 \le 4$

- Boolean function
  $f_1(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_4 + x_1 + x_2x_4 + x_3 + x_4 + 1$ gives a $(7, 4^4 2^0, 4)$ code whose Gray image is a $(14, 2^8, 4)$ binary code which is optimal by [2].
- Formally self-dual function
  $f_2(x_1, x_2, x_3, x_4) = x_1x_2x_4 + x_1x_2 + x_1x_3x_4 + x_1x_4 + x_2$ gives a $(6, 4^4 2^0, 3)$ code whose Gray image is a $(12, 2^8, 3)$ binary code which is optimal by [2].
- Semi-bent function
  $f_3(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_4 + x_1 + x_2x_3 + x_2 + x_3x_4 + x_3 + x_4$ gives a $(12, 4^6 2^0, 6)$ code whose Gray image is a $(24, 2^{12}, 6)$ binary code.
- Bent function
  $f_4(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_1 + x_2x_3 + x_2x_4 + x_3x_4$ gives $(6, 4^4 2^0, 2)$ code whose Gray image is a $(12, 2^8, 2)$ binary code.

The rank of a quadratic form g in m Boolean variables is defined to be the codimension of its radical $V_g = \{x \in \mathbb{F}_{2^m} \mid \forall z \in \mathbb{F}_{2^m},\ g(x+z) - g(x) - g(z) = 0\}$, or in terms of the bilinear form $B_g(x, y) = g(x + y) - g(x) - g(y)$, $V_g = \{x \in \mathbb{F}_{2^m} \mid \forall z \in \mathbb{F}_{2^m},\ B_g(x, z) = 0\}$,

Proposition 2 *Let $h = \lfloor \frac{m}{2} \rfloor$. Then the rank of $Q(x)$ is equal to $2h$.*

Proof With the above notation, the bilinear form $B_Q(x, y)$ attached to Q is

$$\begin{aligned} B_Q(x, y) &= \sum_{\substack{i,j=0 \\ j \neq i}}^{m-1} x^{2^i} y^{2^j} \\ &= tr(x)tr(y) + tr(xy) \\ &= tr(tr(x)y + xy). \end{aligned}$$

Now $x \in V_Q$ iff

$$\forall z \in \mathbb{F}_{2^m}, tr(z(tr(x) + x)) = 0.$$

By the non-degeneresccence of the trace form [4, Lemma 3.8.5], this yields $tr(x) = x$, hence $x \in \mathbb{F}_2$. But $tr(1) = m$, which is zero or one depending on the parity of m. □

Let f be an affine function. Without loss of generality, let $f(x) = tr(ax) + b$ with $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_2$. Using Eq. (2), for any $s \in \mathbb{F}_{2^m}^*$, we have

$$W_f(s) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{tr(ax)+b+tr(sx)} = (-1)^b 2^m \delta_{a,s}, \tag{4}$$

where $\delta_{a,s}$ is equal to 1 if $a = s$, and 0 if not. We are now ready for a connection with affine functions. To this end, we need the following classical lemma [7, vol. 2, p. 1802].

Lemma 2 *Let f be a Boolean degree 2 and let $2h$ be the rank of the associated quadratic Boolean function. Its Walsh–Hadamard transform takes values in $\{0, \pm 2^{m-h}\}$.*

The following corollary introduces a connection between affine functions and a class of linear code $C_{\bar{S}_f}$ over $\mathbb{Z}_4$. And the Lee weight distribution of the linear code $C_{\bar{S}_f}$ is established.

Corollary 1 *Let $m \geq 2$ be a positive integer. If $f(x) = tr(ax) + b$ is an affine function in m variables with $a \in \mathbb{F}_{2^m}^*$, $b \in \mathbb{F}_2$, then $C_{\bar{S}_f}$ is a linear code with parameters $(n_f, 4^m)$ with $n_f = 2^{m-1}$, and its Lee weight distribution is $\{0\} \cup \{2^{m-1}, 2^{m-1} + (-1)^b 2^{m-1}\} \cup \{2^{m-1} - \frac{1}{2}\Re(\Gamma(w)), 2^{m-1} - \frac{1}{2}\Re(\Gamma(w)) \pm 2^{m-h-2}, 2^{m-1} - \frac{1}{2}\Re(\Gamma(w)) \pm 2^{m-h-1}\}$.*

Proof It is not hard to get $n_f = 2^{m-1}$ when f is an affine function. The result follows by Theorem 1, Lemma 2 and Eq. (4). □

Example 3 For $m = 4$ and $b = 1$, we have $\Re(\Gamma(w)) = \pm 4$, and we obtain the Lee distance $d_L = 4$. After Gray map we obtain a $(16, 2^8, 4)_2$ code, which is quasi-optimal by [2].

4.2 Case of $D = \bar{S}_f + 2\mathcal{T}$

In the light of Theorem 1, the linear code $C_{\bar{S}_f}$ can have many weights. In order to get fewer weights, we change the defining set of C_D. In this subsection, the defining set of C_D is $D = \{d = x + 2y : x \in \bar{S}_f, y \in \mathcal{T}\}$. The main result of this subsection is described in the following theorem.

Theorem 4 *Let symbols and notations be as above. Let $w = r + 2s \in \mathcal{R}$ with $r, s \in \mathcal{T}$. Then C_D is a linear code over $\mathbb{Z}_4$ with length $2^m n_f$ and its weight distribution is given by the following multiset:*

$$\begin{aligned}\left\{\left\{2^m n_f\right\}\right\} \cup &\left\{\left\{2^m n_f + 2^{m-1}\Re(W_f(\bar{s}))\right\}\right\} \\ &\cup \{\{0\}\}. \end{aligned} \tag{5}$$

Proof It is trivial that $w_L(c_0) = 0$. Let $w = r + 2s \in \mathcal{R}$ with $r, s \in \mathcal{T}$ and $(r, s) \neq (0, 0)$. By a simple calculation, we have

$$\begin{aligned}\chi(wD) &= \sum_{d=x+2y\in D} i^{Tr(wd)} \\ &= \sum_{x\in\bar{S}_f}\sum_{y\in\mathcal{T}} (-1)^{tr(\bar{r}\bar{y})} i^{Tr(wx)} \\ &= 2^m \delta_{r,0} \sum_{x\in\bar{S}_f} i^{Tr(wx)},\end{aligned}$$

where $\delta_{r,0} = 1$ if $r = 0$ and $\delta_{r,0} = 0$ if $r \neq 0$.
As defined previously, if $w \in \mathcal{R}^*$, we get $w_L(c_w) = |D| = 2^m n_f$. Now, suppose that $w = 2s$ with $s \in \mathcal{T}\backslash\{0\}$, then

$$\begin{aligned}\chi(wD) &= 2^m \sum_{x\in\bar{S}_f} (-1)^{tr(\bar{s}\bar{x})} \\ &= 2^m \sum_{x\in\mathcal{T}} \frac{1 - (-1)^{f(\bar{x})}}{2} (-1)^{tr(\bar{s}\bar{x})} \\ &= -2^{m-1} W_f(\bar{s}).\end{aligned}$$

Applying Eq. (1), for any $w = 2s \in I\backslash\{0\}$, the Lee weight of the codeword c_w is equal to $2^m n_f + 2^{m-1}\Re(W_f(\bar{s}))$. Hence, the weight distribution of C_D is given by the multiset in (5). This completes the proof. □

Theorem 4 established a connection between Boolean functions and a class of linear codes over $\mathbb{Z}_4$. In order to determine the weight distribution of the linear code C_D, it is equivalent to analyze the Walsh spectrum. We are now ready for a connection with bent functions.

Corollary 2 *Let $m > 2$ be an even integer. If f is a bent Boolean function in m variables, then C_D is a linear code with parameters $(2^m n_f, 4^m)$, with $n_f = 2^{m-1} \pm 2^{\frac{m-2}{2}}$, and non-zero Lee weights $2^m n_f \pm 2^{\frac{3m-2}{2}}$ and $2^m n_f$.*

Proof The length is estimated as in the binary case [1, (17)]. Since, by the definition of a bent function, the Walsh transform takes values in $\{\pm 2^{\frac{m}{2}}\}$, the result follows by Theorem 4. □

Example 5 For $m = 4$, the bent function $f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$ gives a code over $\mathbb{Z}_4$ with parameters $(96, 4^4 2^0, 64)$ and its Hamming distance and Lee distance is 32 and 64 respectively. Its Gray image is a binary code with parameters $(192, 2^8, 64)$.

Recall that f is a **semi-bent function** of m variables iff its Walsh–Hadamard transform takes three values, namely

- $\{0, \pm 2^{\frac{m+1}{2}}\}$, if m is odd
- $\{0, \pm 2^{\frac{m+2}{2}}\}$, if m is even.

We have, by [1, Cor. 11] the following result. The proof is analogous to that of Corollary 2 and is omitted.

Corollary 3 *Let $m > 3$ be an integer. If f is a semi-bent Boolean function in m variables, then C_D is a linear code with parameters $(2^m n_f, 4^m)$, with*

$$n_f = \begin{cases} 2^{m-1}, & if\ \hat{f}(0) = 0, \\ 2^{m-1} - 2^{\frac{m-1}{2}}, & if\ \hat{f}(0) = 2^{\frac{m+1}{2}}, \\ 2^{m-1} + 2^{\frac{m-1}{2}}, & if\ \hat{f}(0) = -2^{\frac{m+1}{2}}. \end{cases}$$

Its non-zero Lee weights are $\begin{cases} 2^m n_f - 2^{\frac{3m-1}{2}}, 2^m n_f + 2^{\frac{3m-1}{2}}, 2^m n_f \text{ if } m \text{ is odd}, \\ 2^m n_f - 2^{\frac{3m}{2}}, 2^m n_f + 2^{\frac{3m}{2}}, 2^m n_f \text{ if } m \text{ is even}. \end{cases}$

Example 6 In this example we construct trace codes over $\mathbb{Z}_4$ for $m = 4, 5$.

- For $m = 4$, the semi-bent function $f(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_4 + x_1 + x_2x_3 + x_2 + x_3x_4 + x_3 + x_4$ gives a code over $\mathbb{Z}_4$ with parameters $(192, 4^4 2^0, 192)$ and its Hamming distance and Lee distance is 96 and 192 respectively. Its Gray image is a binary code with parameters $(384, 2^8, 192)$, which is optimal by Griesmer's bound.
- For $m = 5$, the semi-bent function $f(x_1, x_2, x_3, x_4, x_5) = x_1x_4 + x_1x_5 + x_2x_3 + x_3x_4 + x_3x_5 + x_3 + x_4 + 1$ gives a code over $\mathbb{Z}_4$ with parameters $(512, 4^5 2^0)$ and its Hamming distance and Lee distance is 192 and 384 respectively. Its Gray image is a binary code with parameters $(1024, 2^{10}, 384)$.

5 Conclusion

In the present work we have studied a family of linear codes over the ring $\mathbb{Z}_4$. Given a classical Boolean function, or, equivalently its support we have discussed two different constructions of Trace codes. Building on the results in [1], we give upper and lower bounds on the minimum Lee distance. However, the weight distribution is difficult to analyze in general, and we could give only partial results when the Boolean function is affine. The second construction is easier to analyze, and yields three-weight codes.

There is ample room for variation on these themes. Using difference sets or relative difference sets might give more powerful results. Another path of inquiry would be to use a similar approach for $\mathbb{Z}_4$ valued Boolean functions like those studied in [8].

Acknowledgements This research is supported by National Natural Science Foundation of China (61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133), Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008) and China Postdoctoral Science Foundation (Grant No. 2016M601991).

References

1. Ding C.S.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015).
2. Grassl M.: Bounds on the minimum distance of linear codes and quantum codes. http://www.codetables.de.
3. Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inf. Theory **40**(2), 301–319 (1994).
4. Huffman W.C., Pless V.: Fundamentals of Error Correcting Codes. Cambridge University Press, Cambridge (2003).
5. Hyun J.Y., Lee H., Lee Y.: MacWilliams duality and gleason-type theorem on self-dual bent functions. Des. Codes Cryptogr. **63**(3), 295–304 (2012).
6. Kumar P.V., Helleseth T.: An expansion for the coordinates of the trace function over Galois rings. AAECC **8**(5), 353–361 (1998).
7. Pless V.S., Huffman W.C.: Handbook of Coding Theory. North Holland, Amsterdam (1998).
8. Solé P., Tokareva N.: Connections between quaternary and binary bent functions. IACR Cryptology Eprint Archive (2009).
9. Wan Z.X.: Quaternary Codes. World Scientific, Singapore (1997).
10. Yang K., Helleseth T., Kumar P.V., Shanbhag A.G.: On the weight hierarchy of kerdock codes over $\mathbb{Z}_4$. IEEE Trans. Inf. Theory **42**(5), 1587–1593 (1996).