Bull. Aust. Math. Soc. **98** (2018), 167–174
doi:10.1017/S0004972718000291

FEW-WEIGHT CODES FROM TRACE CODES OVER R_k

MINJIA SHI✉, YUE GUAN, CHENCHEN WANG and PATRICK SOLÉ

(Received 11 February 2018; accepted 12 March 2018; first published online 3 May 2018)

Abstract

We construct two families of few-weight codes for the Lee weight over the ring R_k based on two different defining sets. For the first defining set, taking the Gray map, we obtain an infinite family of binary two-weight codes which are in fact 2^k-fold replicated MacDonald codes. For the second defining set, we obtain two infinite families of few-weight codes. These few-weight codes can be used to implement secret-sharing schemes.

2010 *Mathematics subject classification*: primary 94B05; secondary 94B15.

Keywords and phrases: few-weights codes, trace codes, Gray may, defining set.

1. Introduction

Few-weight codes were studied first for their intrinsic mathematical appeal. For instance, two-weight codes over fields have been investigated for more than 40 years because of their interplay with strongly regular graphs, difference sets and finite geometry [2, 4]. In recent years, a cryptographic motivation has been added connected with Massey's secret-sharing scheme [12]. In general, a secret-sharing scheme is a protocol that allows a privileged person (the so-called 'dealer') to share a secret with a number of users, by giving each one a share of the secret. Only selected subsets of users may combine their shares to gain access to the secret. This is called the access structure of the scheme. The advantage of few-weight codes arises from a numerical condition on the weights that determines the access structure of the scheme [1]. This condition is easier to check for few-weight codes than for codes with a complex weight distribution.

One important construction technique for few-weight codes is to use trace codes. For example the simplex code, a one-weight code, can be constructed as a trace code by using finite field extensions [11]. In recent years, this technique has been refined by using ring extensions of a finite field coupled with a linear Gray map [13–15]. The

This research is supported by the 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) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008).

smallest such extension of $\mathbb{F}_2$ is $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$, a polynomial analogue of $\mathbb{Z}_4$. A fourth degree extension of $\mathbb{F}_2$ is $R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. More generally, an extension of degree 2^k of $\mathbb{F}_2$, denoted by R_k, was introduced in [7], along with a linear Gray map. In this paper we consider trace codes over R_k, and thus generalise our previous work [14, 15]. In some cases, we obtain a concatenation of the MacDonald code of type 13 (see [10]) with a repetition code. In other cases we obtain two new infinite families of two-weight codes. In both cases, we explore a potential application to a secret-sharing scheme. It is worth observing that, while most standard constructions of few-weight codes use cyclic codes [6, 8, 9], our construction uses codes that are abelian but not obviously cyclic.

The article is organised as follows. We collect some basic information in Section 2. The trace codes are proved to be abelian in Section 3 and their weight distributions are computed in Section 4. In Section 5, we prove that all these codewords are minimal and describe an application to a secret-sharing scheme.

2. Notations and definitions

2.1. Rings. For any integer $k \geq 1$, denote the integer range $\{1, 2, \ldots, k\}$ by $[k]$.

Define the ring $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/I_k$, where I_k is the polynomial ideal generated by the relations $u_i^2 = 0$ for i in $[k]$ and $u_i u_j = u_j u_i$ for i, j in $[k]^2$. The ring R_k can also be described recursively by

$$R_k = R_{k-1}[u_k]/\langle u_k^2 = 0 \text{ and } u_k u_j = u_j u_k \text{ for } j \text{ in } [k-1]\rangle.$$

This ring is the ring of Boolean functions in k variables [3]. For convenience, set $u_A := \prod_{i\in A} u_i$ for any subset $A \subseteq [k]$, with the convention $u_A = 1$ when $A = \emptyset$. Thus, $r \in R_k$ can be written as $r = \sum_A c'_A u_A$ with $c'_A \in \mathbb{F}_2$. If $\sum_A c'_A u_A$ and $\sum_B d'_B u_B$ with $A, B \subseteq [k]$ are two elements of the ring R_k, then their product is $(\sum_A c'_A u_A)(\sum_B d'_B u_B) = \sum_{A,B\subseteq[k], A\cap B=\emptyset} c'_A d'_B u_{A\cup B}$.

For a given positive integer $m \geq 2$, let $\mathcal{R}$ be the ring obtained by replacing $\mathbb{F}_2$ by $\mathbb{F}_{2^m}$ in the definition of R_k. The elements of $\mathcal{R}$ have the form $\sum_{A\subseteq[k]} c_A u_A$ with $c_A \in \mathbb{F}_{2^m}$. An element of $\mathcal{R}$ is a unit if $c_\emptyset \neq 0$. Let $\mathcal{R}^*$ be the set of all the units of $\mathcal{R}$ and let M denote its maximal ideal.

The Frobenius operator F maps $\sum_{A\subseteq[k]} c_A u_A$ to $\sum_{A\subseteq[k]} c_A^2 u_A$. Let Tr denote the *Trace function*, defined by $\mathrm{Tr} = \sum_{j=0}^{m-1} F^j$. It is obvious that $\mathrm{Tr}(\sum_A c_A u_A) = \sum_A u_A \mathrm{tr}(c_A)$, where $A \subseteq [k]$ and tr denotes the standard trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.

2.2. The Lee weight and the Gray map. Define the Lee weight w_L as the Hamming weight of the image of a codeword under the Gray map ϕ_k. A recursive definition of ϕ_k is given in [7]. Suppose $\bar{c} \in R_k^n$ is represented as $\bar{c}_1 + u_k\bar{c}_2$ with $\bar{c}_1, \bar{c}_2 \in R_{k-1}^n$. Then $\phi_k(\bar{c}) = (\phi_{k-1}(\bar{c}_2), \phi_{k-1}(\bar{c}_1) + \phi_{k-1}(\bar{c}_2))$. Furthermore, ϕ_k is a distance-preserving map from R_k^n to $\mathbb{F}_2^{2^k n}$.

2.3. The weight formula of C_D. Let α be a fixed primitive element of $\mathbb{F}_{2^m}$ and N_0 a positive integer such that $N_0|(2^m - 1)$. Define $D = C_0^{N_0} = \langle \alpha^{N_0}\rangle \subseteq \mathbb{F}_{2^m}$, where $\langle \alpha^{N_0}\rangle$ denotes the subgroup of $\mathbb{F}_{2^m}^* = \langle\alpha\rangle$ generated by α^{N_0}.

https://doi.org/10.1017/S0004972718000291 Published online by Cambridge University Press

Let ϕ, χ denote the canonical additive characters of $\mathbb{F}_2$ and $\mathbb{F}_{2^m}$, respectively, and let λ, ψ denote the multiplicative characters of $\mathbb{F}_2$ and $\mathbb{F}_{2^m}$, respectively. The Gauss sums over $\mathbb{F}_2$ and $\mathbb{F}_{2^m}$ are $G(\lambda, \phi) = \sum_{x \in \mathbb{F}_2^*} \lambda(x)\phi(x)$ and $G(\psi, \chi) = \sum_{x \in \mathbb{F}_{2^m}^*} \psi(x)\chi(x)$.

Let $C_D = \{(\mathrm{tr}(x\alpha^0), \mathrm{tr}(x\alpha^{N_0}), \ldots, \mathrm{tr}(x\alpha^{N_0(f-1)})) : x \in \mathbb{F}_{2^m}\}$. For a nonzero codeword $c_b = (\mathrm{tr}(b\alpha^0), \mathrm{tr}(b\alpha^{N_0}), \ldots, \mathrm{tr}(b\alpha^{N_0(f-1)})) \in C_D$, with $b \in \mathbb{F}_{2^m}^*$, let $w_H(c_b)$ denote its Hamming weight. Then $w_H(c_b) = f - N(b)$, where

$$N(b) = |\{1 \le j \le f : \mathrm{tr}(b\alpha^{N_0(j-1)}) = 0\}|.$$

By basic facts on additive characters,

$$2N(b) = \sum_{i=1}^{f} \sum_{y \in \mathbb{F}_2} \phi(y\mathrm{tr}(b\alpha^{N_0(j-1)})) = f + \sum_{i=1}^{f} \chi(b\alpha^{N_0(j-1)}) = f + \frac{1}{N_0} \sum_{x \in \mathbb{F}_{2^m}^*} \chi(bx^{N_0})$$
$$= f + \frac{1}{N_0(2^m - 1)} \sum_{\psi \in \widehat{\mathbb{F}_{2^m}^*}} G(\bar{\psi}, \chi)\psi(b) \sum_{x \in \mathbb{F}_{2^m}^*} \psi(x^{N_0}).$$

Let ψ_0 denote the trivial character of $\mathbb{F}_{2^m}$. By the orthogonality property of multiplicative characters [9],

$$\sum_{x \in \mathbb{F}_{2^m}^*} \psi(x^{N_0}) = \begin{cases} 2^m - 1 & \text{if } \psi^{N_0} = \psi_0, \\ 0 & \text{otherwise.} \end{cases}$$

Hence,

$$2N(b) = f + \frac{1}{N_0} \sum_{j=0}^{N_0 - 1} G(\bar{\varphi}^j, \chi)\varphi^j(b), \tag{2.1}$$

where φ is a multiplicative character of order N_0 in $\widehat{\mathbb{F}_{2^m}^*}$, the multiplicative character group of $\mathbb{F}_{2^m}^*$.

3. Symmetry

Let $L_0 \subseteq \mathcal{R}^*$. A binary linear code over R_k is defined by $C_{L_0} = \{(\mathrm{Tr}(xd)_{d \in L_0} : x \in \mathcal{R}\}$. Here L_0 is called the *defining set* of C_{L_0}. This construction is very powerful: many optimal few-weight codes can be obtained by choosing different defining sets L_0 [8, 9].

We will study two different defining sets: $L = \mathcal{R}^* = \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m} \times \cdots \times \mathbb{F}_{2^m}$ and $L' = D \times \underbrace{\mathbb{F}_{2^m} \times \cdots \times \mathbb{F}_{2^m}}_{2^k - 1}$. For $a \in \mathcal{R}$, define the vector $ev(a)$ (respectively $ev'(a)$) by the evaluation map $ev(a) = (\mathrm{Tr}(ax))_{x \in L}$ (respectively $ev'(a) = (\mathrm{Tr}(ax))_{x \in L'}$). The codes C and C' are defined respectively by $C = \{ev(a) : a \in \mathcal{R}\}$ and $C' = \{ev'(a) : a \in \mathcal{R}\}$. Thus, the length of the code C (respectively C') is $n = |L| = (2^m - 1)2^{m(2^k - 1)}$ (respectively $n' = |L'| = 2^{m(2^k - 1)}f$) and the code length of codes $\phi_k(C)$ (respectively $\phi_k(C')$) is $N = 2^k n$ (respectively $N' = 2^k n'$).

Similar to [15, Proposition 3.1], we have the following result.

https://doi.org/10.1017/S0004972718000291 Published online by Cambridge University Press

TABLE 1. Weight distribution of $\phi_k(C)$.

Weight	Frequency
0	1
$w_1 = 2^{m(2^k-1)+k-1}(2^m-1)$	$2^{m2^k}-2^m$
$w_2 = 2^{m(2^k-1)+k-1}2^m$	2^m-1

PROPOSITION 3.1. *The group L (respectively L') acts regularly on the coordinates of C (respectively C'). Thus, the code C (respectively C') is an abelian code based on the group L.*

4. Weight distribution of trace codes

Before calculating the weight distributions of C and C', we recall some classic facts.

LEMMA 4.1 [11, (6), page 412]. *If $y = (y_1, y_2, \ldots, y_s) \in \mathbb{F}_2^s$, the Hamming weight satisfies $2w_H(y) = s - \sum_{i=1}^{s}(-1)^{y_i}$.*

LEMMA 4.2 [11, Lemma 9, page 143]. *For any $z \in \mathbb{F}_{2^m}^*$, we have $\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{tr}(zx)} = 0$.*

4.1. Lee weight distribution of the trace code C.

THEOREM 4.3. *For $a \in \mathcal{R}$, the weight distribution of the trace code C is as follows.*

(i) *If $a = 0$, then $w_L(ev(a)) = 0$.*

(ii) *Assume $a \in M \setminus \{0\}$. If $a = c_{[k]}u_{[k]}$ and $c_{[k]} \in \mathbb{F}_{2^m}^*$, then $w_L(ev(a)) = 2^{2^k m+k-1}$. If $a \in M \setminus \{0, c_{[k]}u_{[k]}\}$, then $w_L(ev(a)) = (2^m-1)2^{m(2^k-1)+k-1}$.*

(iii) *If $a \in \mathcal{R}^*$, then $w_L(ev(a)) = (2^m-1)2^{m(2^k-1)+k-1}$.*

PROOF. Part (i) is clear.

For part (ii), assume $a \in M \setminus \{0\}$. Suppose $a = c_{[k]}u_{[k]}$ with $c_{[k]} \in \mathbb{F}_{2^m}^*$ and let $x = \sum_{B\subseteq[k]} d_B u_B \in L$. Then $ax = \sum_{B\subseteq[k]} c_{[k]}u_{[k]}d_B u_B = c_{[k]}d_\emptyset u_{[k]}$, where $d_\emptyset \in \mathbb{F}_{2^m}^*$. Thus, $\mathrm{Tr}(ax) = \mathrm{tr}(c_{[k]}d_\emptyset)u_{[k]}$. It follows that $\phi_k(ev(a)) = (\mathrm{tr}(c_{[k]}d_\emptyset), \ldots, \mathrm{tr}(c_{[k]}d_\emptyset)) \in \mathbb{F}_2^{2^k}$. By Lemma 4.1, $w_L(ev(a)) = 2^{2^k m+k-1}$.

On the other hand, if $a \in M \setminus \{0, c_{[k]}u_{[k]}\}$, suppose $a = c_{\{1\}}u_{\{1\}}$ with $c_{\{1\}} \in \mathbb{F}_{2^m}^*$ and $x = \sum_{B\subseteq[k]} d_B u_B \in L$. Then $ax = \sum_{B\subseteq\{2,\ldots,k\}} c_{\{1\}}d_B u_{\{1\}\cup B}$. Every component of the vector $\phi_k(ev(a))$ contains $\mathrm{tr}(c_{\{1\}}d_{\{2,\ldots,k\}})$ and this implies that $2^k|L| - 2w_L(ev(a)) = 0$. For $a \in M \setminus \{0, u_{\{1\}}, u_{[k]}\}$, the Lee weight equals $2^{k-1}|L|$.

For (iii), suppose $a \in \mathcal{R}^*$. Let $a = \sum_{A\subseteq[k]} c_A u_A$, where $c_{A\setminus\emptyset} \in \mathbb{F}_{2^m}$ and $c_\emptyset \in \mathbb{F}_{2^m}^*$. Moreover, $x = \sum_{B\subseteq[k]} d_B u_B$, where $d_{B\setminus\emptyset} \in \mathbb{F}_{2^m}$ and $d_\emptyset \in \mathbb{F}_{2^m}^*$. By a series calculation, $w_L(ev(a)) = 2^{k-1}|L|$. □

Therefore, we have obtained a binary two-weight code of length $(2^m-1)2^{m(2^k-1)+k}$ and dimension $2^k m$. The weight distribution is shown in Table 1.

https://doi.org/10.1017/S0004972718000291 Published online by Cambridge University Press

REMARK 4.4. We can compare the two-weight code $\phi_k(C)$ with the MacDonald codes in [10]. It can be seen as a concatenation of the MacDonald code of type 13 (with $k = 2^k m, u = 2^k m - m$) in [10, Table 6, page 54] and a length 2^k repetition. In fact, it is equivalent to the code obtained by the Gray map from a simplex code over R_k. Note that the parameters in Table 1 include [14, 15] as special cases.

4.2. Lee weight distribution of the trace code C'.

THEOREM 4.5. *Let m be even. If $1 < N_0 < 2^{m/2} + 1$, then C' is an $(|L'|, 2^{m2^k}, d_L)$ linear code over R_k which has at most $N_0 + 1$ different nonzero Lee weights, where*

$$\frac{1}{N_0} 2^{m(2^k-1)+k-1}[2^m - (N_0 - 1)2^{m/2}] \le d_L \le \frac{1}{N_0} 2^{m(2^k-1)+k-1}(2^m - 1).$$

PROOF. Assume that $x = \sum_{B\subseteq[k]} d_B u_B \in L'$ and $a = c_{[k]}u_{[k]}$ with $c_{[k]} \in \mathbb{F}_{2^m}^*$. Then we have $\mathrm{Tr}(ax) = \mathrm{tr}(c_{[k]}d_\emptyset)u_{[k]}$. Taking the Gray map, $\phi_k(ev'(a)) = (\mathrm{tr}(c_{[k]}d_\emptyset), \ldots, \mathrm{tr}(c_{[k]}d_\emptyset))$ in $\mathbb{F}_2^{2^k}$. Consequently, $w_L(ev'(a)) = w_H(\phi_k(ev'(a))) = 2^{m(2^k-1)+k}(f - N(c_{[k]}))$ where $N(c_{[k]}) = |\{1 \le j \le f : \mathrm{tr}(d_j c_{[k]}) = 0\}|$, and by (2.1),

$$f - N(c_{[k]}) = \frac{2^m}{2N_0} - \frac{1}{2N_0} \sum_{j=1}^{N_0-1} G(\bar{\varphi}^j, \chi)\varphi^j(c_{[k]}).$$

Since $\left| \sum_{j=1}^{N_0-1} G(\bar{\varphi}^j, \chi)\varphi^j(c_{[k]}) \right| \le (N_0 - 1)2^{m/2}$ and $N_0 < 2^{m/2} + 1$,

$$2^{m(2^k-1)+k-1} \frac{2^m - (N_0 - 1)2^{m/2}}{N_0} \le w_L(ev'(a)) \le 2^{m(2^k-1)+k-1} \frac{2^m + (N_0 - 1)2^{m/2}}{N_0}.$$

In this case, there are at most N_0 nonzero weights.

Now let $a \in \mathcal{R} \setminus \{0, c_{[k]}u_{[k]}\}$. This case is similar to the last two cases in the proof of Theorem 4.3. Thus, $w_L(ev'(a)) = \frac{1}{2}N' = 2^{m(2^k-1)+k-1}(2^m - 1)/N_0$. In conclusion, the codeword C' has at most $N_0 + 1$ different nonzero Lee weights. Since

$$\frac{1}{N_0} 2^{m(2^k-1)+k-1}(2^m - 1) < \frac{1}{N_0} 2^{m(2^k-1)+k-1}(2^m + (N_0 - 1)2^{m/2}),$$

it follows that

$$\frac{1}{N_0} 2^{m(2^k-1)+k-1}[2^m - (N_0 - 1)2^{m/2}] \le d_L(C') \le \frac{1}{N_0} 2^{m(2^k-1)+k-1}(2^m - 1). \qquad \square$$

THEOREM 4.6. *Let m be an even number and $N_0 > 2$ with $N_0|(2^m - 1)$. Assume that there exists a positive integer l such that $2^l \equiv -1 \pmod{N_0}$ and set $t = m/2l$. The linear code $\phi_k(C')$ is a three-weight code provided that $2^{m/2} + (-1)^t(N_0 - 1) > 0$ and its weight distribution is given in Table 2.*

PROOF. Let $a = c_{[k]}u_{[k]}$ and $c_{[k]} \in \mathbb{F}_{2^m}^*$. From Theorem 4.5, there are at most N_0 different nonzero weights in this case, and these weights are

$$2^k 2^{m(2^k-1)} \left(\frac{2^m - 1}{2N_0} - \frac{1}{2N_0} \sum_{j=0}^{N_0-1} G(\bar{\varphi}^j, \chi)\varphi^j(c_{[k]}) \right).$$

https://doi.org/10.1017/S0004972718000291 Published online by Cambridge University Press

Table 2. Weight distribution of $\phi_k(C')$.

Weight	Frequency
0	1
$w'_1 = (2^{m(2^k-1)+k-1}[2^m + (-1)^t(N_0-1)2^{m/2}])/N_0$	$(2^m-1)/N_0$
$w'_2 = (2^{m(2^k-1)+k-1}(2^m-1))/N_0$	$2^{2^k m} - 2^m$
$w'_3 = (2^{m(2^k-1)+k-1}[2^m - (-1)^t 2^{m/2}])/N_0$	$(N_0-1)(2^m-1)/N_0$

By Lemma 2.4 and the proof of Theorem 4.1 in [9], the set of these weights gives two values which are equal to $(2^{m(2^k-1)+k-1}[2^m + (-1)^t(N_0-1)2^{m/2}])/N_0$ and $(2^{m(2^k-1)+k-1}[2^m - (-1)^t 2^{m/2}])/N_0$. Next, let $a \in \mathcal{R} \setminus \{0, c_{[k]}u_{[k]}\}$. This case only gives one nonzero weight, namely, $\frac{1}{2}N' = (2^{m(2^k-1)+k-1}(2^m-1))/N_0$. □

Remark 4.7. The choice of the defining set L' is motivated from [9], but $\phi_k(C')$ is different from the codes constructed in [9]. Since the length, minimum distance and weight distribution of the three-weight code $\phi_k(C')$ are determined by the values of N_0, k and m, it is difficult to compare $\phi_k(C')$ with other three-weight codes.

Remark 4.8. When $N_0 = 1$, the code constructed in Theorem 4.6 is the same as the code constructed in Theorem 4.3, because $L' = L$ in that case.

Remark 4.9. In general, different choices of the defining sets lead to linear codes with different parameters. However, this is not always the case. Let Q denote the set of squares in $\mathbb{F}_{2^m}$. If the defining set is $Q \times \mathbb{F}_{2^m} \times \cdots \times \mathbb{F}_{2^m}$, the code we get is the same as the previous one where $L = \mathcal{R}^*$ because the elements in $\mathbb{F}_{2^m}^*$ are all squares which means $Q = \mathbb{F}_{2^m}^*$.

5. Application to secret-sharing schemes

In general, the access structure of the secret-sharing scheme constructed from a linear code is hard to determine. However, if all the codewords of the linear code are minimal, we can use its dual code to construct an interesting secret-sharing scheme.

5.1. Minimal codewords. A codeword of a binary code is called minimal if its support does not properly contain the support of another nonzero codeword. The following lemma gives a useful way of finding minimal codewords.

Lemma 5.1 (Ashikhmin–Barg, [1]). *Let w_0 and w_∞ denote the smallest and largest nonzero weights of a binary code. If $w_0/w_\infty > \frac{1}{2}$, then every nonzero codeword of this binary code is minimal.*

We apply this lemma to the codes under scrutiny.

https://doi.org/10.1017/S0004972718000291 Published online by Cambridge University Press

THEOREM 5.2.

(1) *For $m \geq 2$, all the nonzero codewords of $\phi_k(C)$, are minimal.*
(2) *Keep the same conditions as Theorem 4.6. When t is odd, all nonzero codewords of $\phi_k(C')$ are minimal for $2 < N_0 < \frac{1}{2}(2^{m/2} + 1)$; when t is even, all nonzero codewords of $\phi_k(C')$ are minimal for $2 < N_0 < 2^{m/2} - 1$.*

PROOF. (1) By Theorem 4.3 and Lemma 5.1, $w_0 = w_1$ and $w_\infty = w_2$. Rewriting the inequality of Lemma 5.1 as $2w_1 - w_2 > 0$ gives $2^{k-1}2^{m(2^k-1)}(2^m - 2) > 0$, which is satisfied for $m \geq 2$. We can prove (2) similarly. □

5.2. The dual code. The dual code $C^\perp$ of C is defined by

$$C^\perp = \Big\{ \sum_B d_B u_B : \Big(\sum_A c_A u_A \Big) \Big(\sum_B d_B u_B \Big) = 0, \text{ for all } \sum_A c_A u_A \in C \Big\}.$$

LEMMA 5.3. *For $a \in \mathcal{R}$, if $\mathrm{Tr}(ax) = 0$, then $x = 0$.*

The following result determines the dual Lee distance of the two-Lee-weight code C. The proof is similar to those in [14, 15] and is omitted here.

THEOREM 5.4. *For $k \geq m \geq 2$, the dual Lee distance d' of both the codes C and C' is 2.*

5.3. Massey's secret-sharing scheme. Massey's scheme [12], is a secret-sharing scheme based on coding theory. When all nonzero codewords are minimal, it was shown in [5] that there is the following alternative, depending on d'.

(i) If $d' \geq 3$, then the secret-sharing scheme is '*democratic*', that is, every user belongs to the same number of coalitions.
(ii) If $d' = 2$, then the secret-sharing scheme is '*dictatorial*', that is, there are users who belong to every coalition (the '*dictators*').

By Theorem 5.2, the secret-sharing schemes built on $\phi_k(C)$ and $\phi_k(C')$ are dictatorial.

References

[1] A. Ashikhmin and A. Barg, 'Minimal vectors in linear codes', *IEEE Trans. Inform. Theory* **44** (1998), 2010–2017.
[2] R. Calderbank and W. M. Kantor, 'The geometry of two-weight codes', *Bull. Lond. Math. Soc.* **18** (1986), 97–122.
[3] C. Carlet, 'Boolean functions for cryptography and error correcting codes', in: *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (eds. Yves Crama and P. L. Hammer) (Cambridge University Press, New York, 2010), 257–397.
[4] P. Delsarte, 'Weights of linear codes and strongly regular normed spaces', *Discrete Math.* **3** (1972), 47–64.
[5] C. Ding and J. Yuan, 'Covering and secret sharing with linear codes', *Springer LNCS* **2731** (2003), 11–25.
[6] K. Ding and C. Ding, 'A class of two-weight and three-weight codes and their applications in secret sharing', *IEEE Trans. Inform. Theory* **61** (2015), 5835–5842.
[7] S. T. Dougherty, B. Yildiz and S. Karadeniz, 'Codes over R_k, Gray maps and their binary images', *Finite Fields Appl.* **17** (2011), 205–219.

https://doi.org/10.1017/S0004972718000291 Published online by Cambridge University Press

[8] Z. Heng and Q. Yue, 'A class of binary linear codes with at most three weights', *IEEE Commun. Lett.* **19** (2015), 1488–1491.
[9] Z. Heng and Q. Yue, 'A class of q-ary linear codes derived from irreducible cyclic codes', Preprint, 2015, arXiv:1511.09174vl.
[10] J. E. MacDonald, 'Design methods for maximum minimum-distance error-correcting codes', *IBM J. Res. Develop.* **4** (1960), 43–57.
[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).
[12] J. L. Massey, 'Minimal codewords and secret sharing', in: *Proc. 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden* (Institutionen for informationsteori, Tekniska hogsk., Lund, Sweden, 1993), 276–279.
[13] M. Shi, Y. Guan and P. Solé, 'Two new families of two-weight codes', *IEEE Trans. Inform. Theory* **63** (2017), 6240–6246.
[14] M. Shi, Y. Liu and P. Solé, 'Optimal two-weight codes from trace codes over $\mathbb{F}_2 + u\mathbb{F}_2$', *IEEE Commun. Lett.* **20** (2016), 2346–2349.
[15] M. Shi, Y. Liu and P. Solé, 'Optimal binary codes from trace codes over a non-chain ring', *Discrete Appl. Math.* **219** (2017), 176–181.

MINJIA SHI,
Key Laboratory of Intelligent Computing and Signal Processing,
Ministry of Education, Anhui University, No. 3 Feixi Road,
Hefei, Anhui Province 230039, PR China
and
School of Mathematical Sciences,
Anhui University, Hefei, Anhui, 230601, PR China
e-mail: smjwcl.good@163.com

YUE GUAN, School of Mathematical Sciences,
Anhui University, Hefei, Anhui, 230601, PR China
e-mail: guanyueeee@163.com

CHENCHEN WANG, School of Mathematical Sciences,
Anhui University, Hefei, Anhui, 230601, PR China
e-mail: wangchenchen233@163.com

PATRICK SOLÉ, CNRS/LAGA,
Université Paris 8, 93 526 Saint-Denis, France
e-mail: sole@enst.fr

https://doi.org/10.1017/S0004972718000291 Published online by Cambridge University Press