Advances in Social Science, Education and Humanities Research, volume 550
Proceedings of the 1st International Conference on Mathematics and Mathematics Education (ICMMED 2020)

LCD Codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$

Faldy Tita[1*], Djoko Suprijanto[2]

[1,2] *Combinatorial Mathematics Research Group, Institut Teknologi Bandung, Bandung, Indonesia*
[*]*Email: tita.faldy@gmail.com*

ABSTRACT

In this article, we study linear codes with complementary dual (LCD codes) over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$, where $q = p^s$; p is an odd prime, s is a positive integer, and $v^m = v$; which generalize the observation of Melakhessou et al. (2018). We give necessary and sufficient conditions on the existence of LCD codes and present a method of construction of LCD codes from a combinatorial object, namely from weighing matrices. Several concrete examples are also provided.

Keywords: *Dual codes, Gray map, Linear codes, LCD codes.*

1. INTRODUCTION

"When introducing the dual code $C^\perp$ of a linear code C in his excellent textbook on coding theory [1], van Lint is quick to warn the reader to 'be careful not think of $C^\perp$ as an orthogonal complement in the sense of vector spaces over $\mathbb{R}$. In the case of a finite field $\mathbb{F}_q$, the subspace C and $C^\perp$ can have an intersection larger than $\{\mathbf{0}\}$ and in fact they can even be equal' [[1],p.34]. The purpose of this paper is to explore the fate that awaits one who, daring to ignore this savage advice, chooses to consider only those linear codes C for which the dual code $C^\perp$ can be thought of as a genuine orthogonal complement, i.e., for which $C \cap C^\perp = \{\mathbf{0}\}$."([2],p. 337)

The above quotation from Massey shows that in the beginning the motivation to investigate the linear codes with a complementary dual or linear complementary dual code (LCD codes for short) is purely algebraic in general [3-6]. However, since the last five years the LCD codes become a very active research area since their application to cryptography, in particular to protect an information against so-called "side-channel attacks (SCA)" or "fault non-invasive attacks", as shown by Carlet and Guilley [7].

LCD codes were first considered by Massey [2] over a finite field $\mathbb{F}_q$, where q is a prime power. It is well-known that a finite field is a special commutative finite ring. Recently Melakhessou et al. [3] generalized it by considering LCD codes over a finite non-chain ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$. Our aim is to further generalize the study of Melakhessou et al. [3], namely to study the LCD codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$, where $q = p^s$, p is odd prime, s is a positive integer, and $v^m = v$.

The paper is organized as follows. Section 2 recalls some preliminary results on the structure of $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ and introduced the Gray map. In Section 3 we present some results of linear codes and the relation between the dual and Gray image of codes. Section 4 considers LCD codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$. Necessary and sufficient conditions on the existence of LCD codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ are given, and LCD codes are constructed from a combinatorial object, in this case is a weighing matrix. Several concrete examples of LCD codes over certain finite fields constructed from weighing matrices are provided in the last subsection.

2. PRELIMINARIES

From now on, $\boldsymbol{R}$ denotes the finite non-chain ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$, where $q = p^s$, s is a positive integer, p is an odd prime, and $v^m = v$. The ring $\boldsymbol{R}$ is equivalent to the ring $\frac{\mathbb{F}_q[v]}{\langle v^m - v\rangle}$.

Since p is prime, $q = p^s$ and $(m-1)|(p-1)$, it follows that $v^m - v = v(v-v_1)(v-v_2)\dots(v-v_{m-1})$ with all v_i's in $\mathbb{F}_p$. For $a,b \in \mathbb{Z}_{\geq 0}$, with $a < b$, let $[a,b] := \{a, a+1, a+2, \dots, b-1, b\}$. Let $f_i = v - v_i$ and $\widehat{f_i} = \frac{v^m - v}{f_i}$, where $i \in [0, m-1]$. Then there exist $a_i, b_i \in \boldsymbol{R}[v]$ such that $a_i f_i + b_i \widehat{f_i} = 1$. Let $e_i = b_i \widehat{f_i}$, then $e_i^2 = e_i$, $e_i e_j = 0$ and $\sum_{i=0}^{m-1} e_i = 1$, where $i, j \in [0, m-1]$ and $i \neq j$. Therefore,

$$\begin{aligned}\boldsymbol{R} &= e_0\boldsymbol{R} \oplus e_1\boldsymbol{R} \oplus \cdots \oplus e_{m-1}\boldsymbol{R} \\ &= e_0\mathbb{F}_q \oplus e_1\mathbb{F}_q \oplus \cdots \oplus e_{m-1}\mathbb{F}_q\end{aligned}$$

and

$$\begin{aligned}\boldsymbol{R} &\cong \frac{\boldsymbol{R}}{\langle v \rangle} \times \frac{\boldsymbol{R}}{\langle v - v_1 \rangle} \times \cdots \times \frac{\boldsymbol{R}}{\langle v - v_{m-1} \rangle} \\ &\cong \underbrace{\mathbb{F}_q \times \mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{\boldsymbol{m}}\end{aligned}$$

A code $\mathcal{C}$ of length n over $\boldsymbol{R}$ is subset of $\boldsymbol{R}^n$. $\mathcal{C}$ is linear if and only if $\mathcal{C}$ is an $\boldsymbol{R}$-submodule of $\boldsymbol{R}^n$. An element of $\mathcal{C}$ is called a codeword of $\mathcal{C}$ and matrix whose generated code $\mathcal{C}$ is a generator matrix. In this paper, we always assume that $\mathcal{C}$ is a linear code of length n over $\boldsymbol{R}$.

Generalizing [3], we define a Gray map as follows. Let $GL_m(\mathbb{F}_q)$ be the general linear group of degree m over $\mathbb{F}_q$. Let $r = e_0 r_0 + e_1 r_1 + \cdots + e_{m-1} r_{m-1} \in \boldsymbol{R}$, the element r can be viewed as the vector of length m over $\mathbb{F}_q$, that is $\boldsymbol{r} = (r_0, r_1, \dots, r_{m-1})$.

Define the Gray map

$$\begin{aligned}\phi : \boldsymbol{R} &\longrightarrow \mathbb{F}_q^m \\ \boldsymbol{r} = (r_0, r_1, \dots, r_{m-1}) &\mapsto (r_0, r_1, \dots, r_{m-1})M\end{aligned}$$

for any matrix $M \in GL_m(\mathbb{F}_q)$. Similarly, the Gray map ϕ can be extended to the map Φ from $\boldsymbol{R}^n$ to $\mathbb{F}_q^{mn}$

$$\begin{aligned}\Phi : \boldsymbol{R}^n &\longrightarrow \mathbb{F}_q^{mn} \\ (c_0, c_1, \dots, c_{n-1}) &\mapsto (c_0 M, c_1 M, \dots, c_{n-1} M).\end{aligned}$$

The Hamming weight $W_H(\boldsymbol{v})$ of a vector $\boldsymbol{v}$ is the number of nonzero components in $\boldsymbol{v}$. Let $\boldsymbol{r} = (r_0, r_1, \dots, r_{m-1})$ be an element of $\boldsymbol{R}$. The Gray weight of $\boldsymbol{r}$, denoted by $W_G(\boldsymbol{r})$, is defined as the Hamming weight of the vector $\boldsymbol{r}M$, i.e. $W_G(\boldsymbol{r}) = W_H(\boldsymbol{r}M)$.

For any vector $\boldsymbol{c} = (c_0, c_1, \dots, c_{n-1}) \in \boldsymbol{R}^n$, the Gray weight of $\boldsymbol{c}$ is defined as

$$W_G(c) = \sum_{i=0}^{n-1} W_G(c_i).$$

For any element $\boldsymbol{c_1}, \boldsymbol{c_2} \in \boldsymbol{R}^n$, the Gray distance between $\boldsymbol{c_1}$ and $\boldsymbol{c_2}$ is defined naturally by $d_G(\boldsymbol{c_1}, \boldsymbol{c_2}) = W_G(\boldsymbol{c_1} - \boldsymbol{c_2})$. The minimum Gray weight of code $\mathcal{C}$ is the smallest nonzero Gray weight among all codewords. If $\mathcal{C}$ linear, then the minimum Gray distance is the same as the minimum Gray weight.

3. BASIC PROPERTIES OF LINEAR CODE OVER *R*

In this section, we present some basic results of linear codes over $\boldsymbol{R}$. By definition of a Gray weight and a linearity of Φ, it is easy to derive the following property.

Lemma 1. *If $\mathcal{C}$ is a linear code of length n over $\boldsymbol{R}$, then its Gray image $\Phi(\mathcal{C})$ is a linear code of length mn over $\mathbb{F}_q$. Furthermore, the Gray map Φ is a distance-preserving map from $\mathcal{C}$ to $\Phi(\mathcal{C})$.*

Proof. Similar to the proof of Lemma 1 in [3].

Let $\mathcal{C}$ be a linear code of length n over $\boldsymbol{R}$. Define

$$\begin{aligned}C_i = \{\mathbf{x}_i \in \mathbb{F}_q^n :\ \exists \mathbf{x}_0, \dots, \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, \dots, \mathbf{x}_{m-1} \in \mathbb{F}_q^n; \\ e_0\mathbf{x}_0 + e_1\mathbf{x}_1 + \cdots + e_{m-1}\mathbf{x}_{m-1} \in \mathcal{C}\}.\end{aligned}$$

where $i \in [0, m-1]_{\mathbb{Z}}$. It is clear that for every $i \in [0, m-1]_{\mathbb{Z}}$, C_i is a linear code over $\mathbb{F}_q^n$.

Furthermore, we also have

$$\mathcal{C} = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1}.$$

Let $\mathcal{G}$ be a generator matrix of $\mathcal{C}$ over $\boldsymbol{R}$. For every $i \in [0, m-1]_{\mathbb{Z}}$, since C_i is a linear code over $\mathbb{F}_q$ then the generator matrix $\mathcal{G}$ can be expressed as

$$\mathcal{G} = \begin{bmatrix} e_0 G_0 \\ e_1 G_1 \\ \vdots \\ e_{m-1} G_{m-1} \end{bmatrix} \qquad (1)$$

where $G_0, G_1, \dots, G_{m-1}$ are generator matrices of $C_0, C_1, \dots, C_{m-1}$, respectively.

Let $\mathbf{x} = (x_0, x_1, \dots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, \dots, y_{n-1})$ be any two elements of R^n. The inner product of $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$\mathbf{x} \cdot \mathbf{y} = \mathbf{x}\mathbf{y}^T = \sum_{i=0}^{n-1} x_i y_i.$$

The dual code $\mathcal{C}^\perp$ for code $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbf{R}^n : \mathbf{x} \cdot \mathbf{y} = 0, \forall \mathbf{y} \in \mathcal{C}\}.$$

If $\mathcal{C} \subseteq \mathcal{C}^\perp$, then $\mathcal{C}$ is said to be a self-orthogonal code, and $\mathcal{C}$ is said to be a self-dual code if $\mathcal{C} = \mathcal{C}^\perp$. The following two propositions can be easily derived.

Proposition 2. *Let $\mathcal{C} = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1}$ be a linear code of length n over $\boldsymbol{R}$. Then*

$$\mathcal{C}^\perp = e_0 C_0^\perp \oplus e_1 C_1^\perp \oplus \cdots \oplus e_{m-1} C_{m-1}^\perp.$$

Moreover, $\mathcal{C}$ is a self-dual code over R if and only if $C_0, C_1, \dots, C_{m-1}$ are all self-dual codes over $\mathbb{F}_q$.

Proposition 3. *Let M be an invertible matrix of size m over $\mathbb{F}_q$, $\mathcal{C}$ is a linear code of length n with the minimum Gray distance d_G over $\boldsymbol{R}$. If $\mathcal{C}$ has generator matrix $\mathcal{G}$ as (1) and $|\mathcal{C}| = p^{\sum_{i=0}^{m-1} k_i}$, then $\Phi(\mathcal{C})$ is a*

$[mn, \sum_{i=0}^{m-1} k_i, d_G]$ linear code over $\mathbb{F}_q$, where k_i's are the respective dimensions of the C_i's.

The proposition below shows that the linearity of the code $\mathcal{C}$ over the ring $\boldsymbol{R}$ implies the linearity of the code over $\mathbb{F}_q$ which is the Gray image of $\mathcal{C}$.

Proposition 4. *Let $\mathcal{C}$ be a linear code of length n over $\boldsymbol{R}$. Let $M \in GL_m(\mathbb{F}_q)$ and $MM^T = \lambda I_m$, where $\lambda \in \mathbb{F}_q \setminus \{0\}$, I_m is the identity matrix of size m over $\mathbb{F}_q$. If $\mathcal{C}$ is a self-dual, then $\Phi(\mathcal{C})$ is a self-dual code of length mn over $\mathbb{F}_q$.*

Proof. For any two elements $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$, $\mathbf{d} = (d_0, d_1, \dots, d_{n-1}) \in \Phi(\mathcal{C})$, there exist two elements $\mathbf{x} = (x_0, x_1, \dots, x_{n-1})$, $\mathbf{y} = (y_0, y_1, \dots, y_{n-1}) \in \mathcal{C}$ such that

$$\mathbf{c} = (x_0M, x_1M, \dots, x_{n-1}M)$$

and

$$\mathbf{d} = (y_0M, y_1M, \dots, y_{n-1}M)$$

Therefore, we have

$$\begin{aligned}\mathbf{c} \cdot \mathbf{d} &= \mathbf{c}\mathbf{d}^T \\ &= (x_0M, x_1M, \dots, x_{n-1}M) \cdot (y_0M, y_1M, \dots, y_{n-1}M) \\ &= \sum_{i=0}^{n-1} x_i MM^T y_i^T\end{aligned}$$

Since $MM^T = \lambda I_m$, we have $\mathbf{c} \cdot \mathbf{d} = \lambda \sum_{i=0}^{n-1} x_i y_i^T$. If $\mathcal{C}$ is a self-dual code, then $\mathbf{x} \cdot \mathbf{y} = \lambda \sum_{i=0}^{n-1} x_i y_i^T = 0$. Hence $\mathbf{c} \cdot \mathbf{d} = 0$, then $\Phi(\mathcal{C})$ is a self-dual code.

Example 5. For $q = 11$ and $m = 6$, we take for M the block diagonal matrix of size 6×6 with three block equal to $\begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}$. In this case $\lambda = 2$. The generator matrix $\mathcal{G}$ of the Gray image becomes

$$\Phi(\mathcal{G}) = \begin{bmatrix} -G_0 & -G_0 & 0 & 0 & 0 & 0 \\ -G_1 & G_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -G_2 & -G_2 & 0 & 0 \\ 0 & 0 & -G_3 & G_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & -G_4 & -G_4 \\ 0 & 0 & 0 & 0 & -G_5 & G_5 \end{bmatrix}.$$

4. LCD CODES OVER *R*

A linear code with complementary dual (LCD) is defined as a linear code $\mathcal{C}$ whose dual code $\mathcal{C}^\perp$ satisfies

$$\mathcal{C} \cap \mathcal{C}^\perp = \{0\}.$$

LCD code have been shown to provide an optimum linear coding solution [2]. In this section we first show the existence of LCD codes over $\boldsymbol{R}$. We then introduce a method to construct LCD codes over $\boldsymbol{R}$ as well as LCD codes over $\mathbb{F}_q$ from weighing matrices.

4.1. Existence of LCD Codes over R

For LCD codes over $\boldsymbol{R}$, we have the following result.

Theorem 6. *A code $\mathcal{C} = e_0\mathcal{C}_0 \oplus e_1\mathcal{C}_1 \oplus \cdots \oplus e_{m-1} \mathcal{C}_{m-1}$ of length n over $\boldsymbol{R}$ is an LCD code if and only if $\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_{m-1}$ are LCD codes over $\mathbb{F}_q$.*

Proof. Let a linear code $\mathcal{C} = e_0\mathcal{C}_0 \oplus e_1\mathcal{C}_1 \oplus \cdots \oplus e_{m-1}\mathcal{C}_{m-1}$ has dual code $\mathcal{C}^\perp = e_0\mathcal{C}_0^\perp \oplus e_1\mathcal{C}_1^\perp \oplus \cdots \oplus e_{m-1}\mathcal{C}_{m-1}^\perp$. We have that

$$\mathcal{C} \cap \mathcal{C}^\perp = e_0(\mathcal{C}_0 \cap \mathcal{C}_0^\perp) \oplus e_1(\mathcal{C}_1 \cap \mathcal{C}_1^\perp) \oplus \cdots \oplus e_{m-1}(\mathcal{C}_{m-1} \cap \mathcal{C}_{m-1}^\perp).$$

Due the direct sum we have

$$\mathcal{C} \cap \mathcal{C}^\perp = \{0\} \Leftrightarrow C \cap C_i^\perp = \{0\}, i \in [0, m-1]_{\mathbb{Z}}$$

Thus, $\mathcal{C}$ is an LCD code over $\boldsymbol{R}$ if and only if for all $i \in [0, m-1]_{\mathbb{Z}}$, C_i is an LCD code over $\mathbb{F}_q$.

Theorem 7. *If C is an LCD code over $\mathbb{F}_q$, then $\mathcal{C} = e_0C \oplus e_1C \oplus \cdots \oplus e_{m-1}C$ is an LCD code over $\boldsymbol{R}$. If $\mathcal{C}$ is an LCD code of length n over $\boldsymbol{R}$, then $\Phi(\mathcal{C})$ is an LCD code of length mn over $\mathbb{F}_q$.*

Proof. The first part is deduced from Theorem 6. From Proposition 4, we have that $\Phi(\mathcal{C})$ is a self-dual code. Since Φ is a bijective linear transformation and $\mathcal{C}$ is an LCD code where $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$, the $\Phi(\mathcal{C})$ is an LCD code of length mn over $\mathbb{F}_q$.

Next, we give a necessary and sufficient condition on the existence of LCD codes over $\boldsymbol{R}$. First we require the following result due to Massey [2].

Proposition 8. *If G is a generator matrix for an $[n, k]$ linear code C over $\mathbb{F}_q$, then C is an LCD code if and only if the $k \times k$ matrix GG^T is nonsingular.*

Theorem 9. *If $\mathcal{G}$ is a generator matrix of linear code $\mathcal{C}$ over $\boldsymbol{R}$, then $\mathcal{C}$ is an LCD code if and only if $\mathcal{G}\mathcal{G}^T$ is nonsingular.*

Proof. From Equation (1), the generator matrix of $\mathcal{C}$ can be expressed as

$$\mathcal{G} = \begin{bmatrix} e_0G_0 \\ e_1G_1 \\ \vdots \\ e_{m-1}G_{m-1} \end{bmatrix}$$

Since $e_i, i \in [0, m-1]_{\mathbb{Z}}$ are orthogonal idempotents, a simple calculation gives

$$\mathcal{G}\mathcal{G}^T = \begin{bmatrix} e_0G_0G_0^T & 0 & \cdots & 0 \\ 0 & e_1G_1G_1^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e_{m-1}G_{m-1}G_{m-1}^T \end{bmatrix}$$

From Proposition 8, a necessary and sufficient condition for a code over $\mathbb{F}_q$ with generator matrix G_i to be LCD is that $G_iG_i^T$ for $i \in [0, m-1]_{\mathbb{Z}}$ be nonsingular. Thus, $\mathcal{G}\mathcal{G}^T$ is nonsingular.

4.2. LCD Codes from Weighing Matrices

In this subsection we construct LCD codes over $\mathbb{F}_q$ and over $\boldsymbol{R}$ from weighing matrices. So, we start with the following definition.

Definition 10. *A* weighing matrix $W_{n,k}$ of order n *and weight k is an $n \times n$ $(0,1,-1)$-matrix such that*

$$WW^T = kI_n$$

where $k \le n$. A weighing matrix $W_{n,n}$ and $W_{n.n-1}$ is called a Hadamard matrix and conference matrix respectively. A matrix W is symmetric if $W = W^T$and W is skew-symmetric if $W = -W^T$.

Proposition 11. *Let $W_{n,k}$ be weighing matrix of order n and weight k. Then the followings hold.*

(i) *Let α be a nonzero element of $\mathbb{F}_q$, such that $\alpha^2 + k \neq 0$ mod q. Then the matrix*

$$G = [\alpha I_n \mid W_{n,k}]$$

generates a $[2n, n]$ LCD code over $\mathbb{F}_q$.

(ii) *Let $W_{n,k}$ be a skew-symmetric of order n, α and β nonzero elements of $\mathbb{F}_q$, such that $\alpha^2 + \beta^2 + k \neq 0$ mod q. Then the matrix*

$$G = [\alpha I_n \mid \beta I_n + W_{n,k}]$$

generates a $[2n, n]$ LCD code over $\mathbb{F}_q$.

Proof. From Definition 10 and Proposition 8, then we sufficiently prove that GG^T is nonsingular.

In the first case we have

$$\begin{aligned} GG^T &= [\alpha I_n \mid W_{n,k}] \begin{bmatrix} \alpha I_n \\ W_{n,k}^T \end{bmatrix} \\ &= [(\alpha^2 + k) I_{2n}] \end{aligned}$$

Since $\alpha^2 + k \neq 0$, then GG^T is nonsingular. And for second case, we have

$$\begin{aligned} GG^T &= [\alpha I_n \mid \beta I_n + W_{n,k}] \begin{bmatrix} \alpha I_n \\ \beta I_n + W_{n,k}^T \end{bmatrix} \\ &= [(\alpha^2 + \beta^2 + k) I_{2n}] \end{aligned}$$

Since $\alpha^2 + \beta^2 + k \neq 0$, then GG^T is nonsingular.

Thus, a matrix G is a generator matrix of a $[2n, n]$ LCD code over $\mathbb{F}_q$.

Theorem 12. *Under the condition of Proposition 11, the matrix*

$$\mathcal{G} = \begin{bmatrix} e_0 G \\ e_1 G \\ \vdots \\ e_{m-1} G \end{bmatrix}$$

is a generator matrix of a $[2n, n]$ LCD code over $\boldsymbol{R}$.

Proof. The result follows from Proposition 11 and Theorem 9.

4.3. Some Example

In this subsection we provide several examples of LCD codes over certain finite fields constructed from weighing matrix.

Example 13. Let $q = 3, n = 4, k = 3$, and $\alpha = 2$ so that $\alpha^2 + 3 \neq 0$ mod 3. Then for the weighing matrix given by

$$W_{4,3} = \begin{bmatrix} 1 & -1 & -1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 0 & -1 & 1 & 1 \end{bmatrix}$$

Thus, $G = [2I_4 \mid W_{4,3}]$ generates a [8,4] LCD code over $\mathbb{F}_3$ by Proposition 11 (i).

Example 14. Let $q = 11, n = 10, k = 9$, and $\alpha = 4$ so that $\alpha^2 + 9 \neq 0$ mod 11. Then for the weighing matrix given by

$$W_{10,9} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 0 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 0 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 0 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 0 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 0 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & 1 & 0 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 0 & 1 \\ -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 0 \end{bmatrix}$$

Thus, $G = [4I_{10} \mid W_{10,9}]$ generates a [20,10] LCD code over $\mathbb{F}_{11}$ by Proposition 11 (i).

Example 15. Let $q = 7, n = 8, k = 5, \alpha = 4$ and $\beta = 2$ so that $\alpha^2 + \beta^2 + 5 \neq 0$ mod 7. Then for the weighing matrix given by

$$W_{8,5} = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ -1 & 0 & 0 & -1 & 0 & -1 & -1 & 1 \\ -1 & 0 & 0 & 1 & 1 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 & 1 & -1 & 0 & -1 \\ -1 & 0 & -1 & -1 & 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 1 & -1 & 0 & 0 & 1 \\ -1 & 1 & 1 & 0 & -1 & 0 & 0 & -1 \\ -1 & -1 & 0 & 1 & 0 & -1 & 1 & 0 \end{bmatrix}$$

Thus, $G = [4I_8 \mid 2I_8 + W_{8,5}]$ generates a [16,8] LCD code over $\mathbb{F}_7$ by Proposition 11 (ii).

Example 16. Let $\boldsymbol{R} = \mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3 + v^3\mathbb{F}_3$, with $v^4 = v$. From Example 13 we can construct generator matrix

$$\mathcal{G} = \begin{bmatrix} e_0 G \\ e_1 G \\ e_2 G \\ e_3 G \end{bmatrix}$$

where $e_i, i \in [0,3]$ are orthogonal idempotent elements in $\boldsymbol{R}$ and $G = [2I_4 \mid W_{4,3}]$. Thus, $\mathcal{G}$ generates a [8,4] LCD code over $\boldsymbol{R}$.

5. CONCLUSION

In this article, we investigate linear codes with complementary dual (LCD codes) over the ring $\boldsymbol{R} = \mathbb{F}_q + \boldsymbol{v}\mathbb{F}_q + \boldsymbol{v}^2\mathbb{F}_q + \cdots + \boldsymbol{v}^{m-1}\mathbb{F}_q$, where $q = p^s$; p is odd prime, $\boldsymbol{s}$ is positive integer, and $\boldsymbol{v}^m = \boldsymbol{v}$. We describe the conditions on the existence of LCD codes and present construction of LCD codes over ring $\boldsymbol{R}$ from weighing matrices. Further, it should be possible to obtain a linear programming bound for codes over $\boldsymbol{R}$.

ACKNOWLEDGMENTS

This research is supported by Kementerian Riset dan Teknologi/ Badan Riset dan Inovasi Nasional (Kemenristek/ BRIN).

REFERENCES

[1] J. H. van Lint, Introduction to Coding Theory, Springer, Berlin, Heidelberg, 1965.

[2] J. L. Massey, Linear codes with complementary duals, Journal of Discrete Mathematics vol.106-107, Elsevier, Amsterdam, 1992, pp 337-342. DOI: https://doi.org/10.1016/0012-365X(92)90563-U

[3] A. Melakhessou, K. Guenda, T. A. Gulliver, M. Shi, P. Sole, On codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, Journal of Applied Mathematics and Computing vol. 57, Springer, Berlin, Heidelberg, 2018, pp 375-391. DOI: https://doi.org/10.1007/s12190-017-1111-6

[4] J. Gao, Some results on linear codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$, Journal of Applied Mathematics and Computing vol. 47, Springer, Berlin, Heidelberg, 2015, pp 473-485. DOI: https://doi.org/10.1007/s12190-014-0786-1

[5] M. Shi, T. Yao, A. Alahmadi, P. Sole, Skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, Journal of IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences vol. E98-A(8), The IEICE, Tokyo, 2015, pp 1845-1848. DOI: https://doi.org/10.1587/transfun.E98.A.1845

[6] M. Shi, T. Yao, P. Sole, Skew cyclic codes over a non-chain ring, Chinese Journal of Electronics vol. 26(3), The Institution of Engineering and Technology (IET), UK(China), 2017, pp 544-547. DOI: https://doi.org/10.1049/cje.2017.03.008

[7] C. Carlet, S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, Advances in Mathematics of Communications vol. 10(1), American Institute of Mathematical Sciences, Springfield, 2016, pp 131-150. DOI: https://doi.org/10.3934/amc.2016.10.131