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 $\{0\}$ 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 sage 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 $C \cap C^\perp = \{0\}$.*(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 an 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, $R$ 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 $R$ is equivalent to the ring $\mathbb{F}_q[v]/(v^m-v)$.
Since \( p \) is prime, \( q = p^x \) and \((m-1)(p-1), \) it follows that \( p^m - v = v(v - v_1)(v - v_2)\ldots(v - v_{m-1}) \) with all \( v_i \)'s in \( \mathbb{F}_p. \) For \( a, b \in \mathbb{Z}_{\geq 0}, \) with \( a < b, \) let \( \{a, b\} = (a, a+1, a+2, \ldots, b-1, b). \) Let \( f_i = v - v_i \) and \( f = \sum f_i \), where \( i \in [0, m-1]. \) Then there exist \( a_i, b_i \in \mathbb{R}(v) \) such that \( a_i f_i + b_i f = 1. \) Let \( e_1, e_2, \ldots, e_m \) be the \( \in \mathbb{R} \times \mathbb{R} - \{0, m-1\} \) where \( i, f_i \in \{0, m-1\} \) and \( i \neq j. \) Therefore,

\[
R = e_0R \oplus e_1R \oplus \cdots \oplus e_{m-1}R
\]

and

\[
R \cong \frac{R}{(v)} \times \frac{R}{(v-v_1)} \times \cdots \times \frac{R}{(v-v_{m-1})} \cong \mathbb{F}_q \oplus \mathbb{F}_q \oplus \cdots \oplus \mathbb{F}_q.
\]

A code \( C \) of length \( n \) over \( R \) is a subset of \( R^n. \) A code \( C \) is linear if and only if \( C \) is an \( R \)-submodule of \( R^n. \) An element of \( C \) is called a codeword of \( C \) and \( C \) is a generator matrix. In this paper, we always assume that \( C \) is a linear code of length \( n \) over \( R \).

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 \( r = e_0r_0 + e_1r_1 + \cdots + e_{m-1}r_{m-1} \in R, \) the element \( r \) can be viewed as the vector of length \( m \) over \( \mathbb{F}_q, \) that is \( r = (r_0, r_1, \ldots, r_{m-1}). \)

Define the Gray map

\[
\phi : R \rightarrow \mathbb{F}_q^n
\]

\[
r = (r_0, r_1, \ldots, r_{m-1}) \mapsto (r_0, r_1, \ldots, r_{m-1})M
\]

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

\[
\Phi : R^n \rightarrow \mathbb{F}_q^{mn}
\]

\[
(c_0, c_1, \ldots, c_{m-1}) \mapsto (c_0M, c_1M, \ldots, c_{m-1}M).
\]

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

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

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

For any element \( c_1, c_2 \in R^n, \) the Gray distance between \( c_1 \) and \( c_2 \) is defined naturally by \( d_G(c_1, c_2) = W_G(c_1 - c_2). \) The minimum Gray weight of code \( C \) is the smallest nonzero Gray weight among all codewords. If \( C \) 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 \( R. \) By definition of a Gray weight and a linearity of \( \Phi, \) it is easy to derive the following property.

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

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

Let \( C \) be a linear code of length \( n \) over \( R. \) Define

\[
C_i = \{ x_i \in \mathbb{F}_q^n : \exists x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{m-1} \in \mathbb{F}_q, e_0x_0 + e_1x_1 + \cdots + e_{m-1}x_{m-1} \in C \}
\]

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

Furthermore, we also have

\[
\mathcal{G} = e_0G_0 \oplus e_1G_1 \oplus \cdots \oplus e_{m-1}G_{m-1}.
\]

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

\[
G = \begin{bmatrix}
G_0 & e_1G_1 & \ldots & e_{m-1}G_{m-1}
\end{bmatrix}
\]

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

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

\[
x \cdot y = xy^T = \sum_{i=0}^{n-1} x_iy_i.
\]

The dual code \( C^\perp \) for code \( C \) is defined as

\[
C^\perp = \{ x \in R^n : x \cdot y = 0, \forall y \in C \}
\]

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

**Proposition 2.** Let \( C = e_0G_0 \oplus e_1G_1 \oplus \cdots \oplus e_{m-1}G_{m-1} \) be a linear code of length \( n \) over \( R. \) Then

\[
C^\perp = e_0G_0^\perp \oplus e_1G_1^\perp \oplus \cdots \oplus e_{m-1}G_{m-1}^\perp.
\]

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

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

**Proposition 4.** Let $C$ be a linear code of length $n$ over $R$. 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 $C$ is a self-dual, then $\Phi(C)$ is a self-dual code of length $mn$ over $\mathbb{F}_q$.

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

$$c = (x_0 M, x_1 M, \ldots, x_{n-1} M)$$

and

$$d = (y_0 M, y_1 M, \ldots, y_{n-1} M)$$

Therefore, we have

$$c \cdot d = cd^T = (x_0 M, x_1 M, \ldots, x_{n-1} M) \cdot (y_0 M, y_1 M, \ldots, y_{n-1} M)$$

$$= \sum_{i=0}^{n-1} x_i M M^T y_i^T$$

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

**Example 5.** For $q = 11$ and $m = 6$, we take for $M$ the block diagonal matrix of size $6 \times 6$ with three block equal to $[-1 \ 1 \ 0 \ \cdots \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]$ $[-1 \ 0 \ 0 \ \cdots \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]$. In this case $\lambda = 2$. The generator matrix $G$ of the Gray image becomes

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

4. LCD Codes over $R$

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

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

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 $R$. We then introduce a method to construct LCD codes over $R$ as well as LCD codes over $\mathbb{F}_q$ from weighing matrices.

4.1. Existence of LCD Codes over $R$

For LCD codes over $R$, we have the following result.

**Theorem 6.** A code $C = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1}$ of length $n$ over $R$ is an LCD code if and only if $C_0, C_1, \ldots, C_{m-1}$ are LCD codes over $\mathbb{F}_q$.

**Proof.** Let a linear code $C = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1}$ has dual code $C^\perp = e_0 C_0^\perp \oplus e_1 C_1^\perp \oplus \cdots \oplus e_{m-1} C_{m-1}^\perp$. We have that

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

Thus, $C$ is an LCD code over $R$ 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 $C = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1}$ is an LCD code over $R$. If $C$ is an LCD code of length $n$ over $R$, then $\Phi(C)$ 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 $\Phi(C)$ is a self-dual code. Since $\Phi$ is a bijective linear transformation and $C$ is an LCD code where $C \cap C_i = \{0\}$, the $\Phi(C)$ 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 $R$. 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 $G$ is a generator matrix of linear code $C$ over $R$, then $C$ is an LCD code if and only if $GG^T$ is nonsingular.

**Proof.** From Equation (1), the generator matrix of $C$ can be expressed as

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

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

$$GG^T = \begin{bmatrix}
e_0 G_0 G_0^T & 0 & \cdots & 0 \\
e_0 G_1 G_1^T & \ddots & \vdots & \vdots \\
\vdots & \ddots & \ddots & \vdots \\
e_0 G_{m-1} G_{m-1}^T & \cdots & 0 & 0
\end{bmatrix}$$

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 $G_i G_i^T$ for $i \in [0, m-1]_\mathbb{Z}$ are nonsingular. Thus, $GG^T$ is nonsingular.
4.2. LCD Codes from Weighing Matrices

In this subsection we construct LCD codes over $\mathbb{F}_q$ and over $\mathbb{R}$ 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 $k \leq n$. 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 $\alpha$ be a nonzero element of $\mathbb{F}_q$, such that $\alpha^2 + k \neq 0$ mod $q$. Then the matrix

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

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

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

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

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

$$GG^T = [\alpha I_n | W_{n,k}] [\alpha I_n^T | W_{n,k}^T]$$

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

$$GG^T = [\alpha I_n | \beta I_n + W_{n,k}] [\beta I_n^T + W_{n,k}^T]$$

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

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

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

**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 matrices.

**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, $G = [2I_4 | W_{4,3}]$ 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

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

Thus, $G = [4I_{10} | W_{10,9}]$ 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

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

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

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

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

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

81
5. CONCLUSION

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

ACKNOWLEDGMENTS

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

REFERENCES


