Bull. Korean Math. Soc. **0** (2019), No. 0, pp. 1–0
https://doi.org/10.4134/BKMS.b181173
pISSN: 1015-8634 / eISSN: 2234-3016

ON LCD CODES OVER FINITE CHAIN RINGS

Yilmaz Durğun

Abstract. Linear complementary dual (LCD) codes are linear codes that intersect with their dual trivially. LCD cyclic codes have been known as reversible cyclic codes that had applications in data storage. Due to a newly discovered application in cryptography, interest in LCD codes has increased again. Although LCD codes over finite fields have been extensively studied so far, little work has been done on LCD codes over chain rings. In this paper, we are interested in structure of LCD codes over chain rings. We show that LCD codes over chain rings are free codes. We provide some necessary and sufficient conditions for an LCD code C over finite chain rings in terms of projections of linear codes. We also showed the existence of asymptotically good LCD codes over finite chain rings.

1. Introduction

A linear code with a complementary dual (an LCD) is defined to be a linear code C satisfying $C \cap C^{\perp} = \{0\}$. The LCD code which is also known as reversible code was first introduced by Massey in [13]. Following his first study, Massey also showed the existence of asymptotically good LCD codes in [14]. The LCD codes were later shown to meet the asymptotic Gilbert-Varshamov bound using the hull dimension spectra of linear codes by Sendrier in [19]. Furthermore, Yang and Massey in [22] provided a necessary and sufficient condition under which a cyclic code to have a complementary dual. Quasi-cyclic LCD codes were then analyzed by Esmaeili and Yari in [5] and their asymptotic behaviors were explored by Güneri et al. in [7]. Recently, several constructions of LCD codes were presented together with their applications against side-channel attacks (SCA) by Carlet and Guilley [2]. Following, Mesnager et al. [16] investigated the construction of algebraic geometry LCD codes which could be resistant against SCA. In [10], Jin constructed some families of Maximum Distance Separable (MDS) codes with complementary duals, through generalized Reed-Solomon codes. Dougherty et al. [4] provided a linear programming bound on the largest size of an LCD code of given length and minimum distance. In [3], Carlet et al. completely determined all LCD codes

Received December 3, 2018; Revised April 23, 2019; Accepted October 10, 2019.
2010 *Mathematics Subject Classification.* Primary 94B05, 11T71.
Key words and phrases. LCD codes, projections of linear codes, finite chain rings.

over finite fields F_q for $q > 3$. There are many recent studies on LCD codes over finite fields [11, 20, 23].

All the mentioned studies above have investigated the LCD codes over finite fields. LCD codes over chain rings, instead, were examined by Liu and Liu in [12]. Their study, which inspired our paper, provided a necessary condition for an LCD code over finite chain rings, see [12, Theorem 3.4]. We improved this result by giving necessary and sufficient conditions for an LCD code over finite chain rings. Besides, in terms of a generator matrix, they provided a sufficient condition for a linear code C over a chain ring to be LCD code, see [12, Theorem 3.5]. Following this result, they gave an example to show that the given sufficient condition is not necessary, see [12, Example 2]. We showed that the given example is incorrect and the provided sufficient condition is, indeed, necessary. Furthermore, the authors introduced a new condition, in addition to the existing one, to show the converse of [12, Theorem 3.9]. However, we showed that the new condition itself is already necessary and sufficient for a linear code to be LCD.

This paper is organized as follows. Section 2 provides a background knowledge on finite chain rings. In Section 3, we generalize some results for linear codes given in [18]. The depicted results in Section 3 are then applied to give sufficient and necessary conditions for LCD code linear codes over a finite chain ring in Section 4. Our results provided in Section 4 are as follows. An LCD code over a finite chain ring is a free code (Proposition 4.1). A linear code C with generator matrix G in standard form is LCD code if and only if the $k \times k$ matrix GG^{tr} is invertible, where k is the number of rows of G (Corollary 4.2). For a linear code C over a chain ring R with γ a fixed generator of the maximal ideal of R and ν the nilpotency index of γ, C is an LCD code over R if and only if $\psi_t(C)$ is an LCD code and $\psi_t(C) = \psi_t((C : \gamma^{\nu-t}))$ over $R/\gamma^t R$ for some $1 \leq t < \nu$, ψ_t being the canonical projections $R \to R/\gamma^t R$ and $(C : r) = \{e \in R^n \mid re \in C\}$, if and only if $\gamma^{j-1}v$ does not belong to $C \cap C^{\perp}$ for any nonzero $v = (v_1, \ldots, v_n) \in F_q^n$, where F_q is the residue field of R (Theorem 4.5, Theorem 4.8).

2. Preliminaries

2.1. Finite chain rings

We begin with the definition and some properties of finite chain rings, based on mainly [15].

Definition. A finite commutative ring with identity $1 \neq 0$ is called a finite chain ring if its ideals are linearly ordered by inclusion.

A chain ring has a unique maximal ideal, i.e., that is a local ring. While not all chain rings are commutative, we shall assume that all rings in this paper are commutative. It is well known, and not difficult to prove, that a ring is a finite chain ring if and only if it is a finite local principal ideal ring. A simple

example of a finite chain ring is the ring Z_{p^a} of integers modulo p^a, for some prime p and $a \geq 1$.

Let R be a finite chain ring, $\mathbf{m}$ the unique maximal ideal of R, and let γ be a generator of the unique maximal ideal $\mathbf{m}$. Then $\mathbf{m} = \langle\gamma\rangle = R\gamma$, where $R\gamma = \langle\gamma\rangle = \{\beta\gamma \,|\, \beta \in R\}$. We have

$$\cdots \subseteq \langle\gamma^i\rangle \subseteq \cdots \subseteq \langle\gamma^1\rangle \subseteq \langle\gamma^0\rangle = R.$$

It is well known that there exists i such that $\langle\gamma^i\rangle = 0$. Let ν be the minimal number such that $\langle\gamma^\nu\rangle = 0$. We will call ν the nilpotency index of γ.

Let $F_q \cong R/\mathbf{m} = R/\gamma R$ be the residue field with characteristic p, where p is a prime number. This implies that there exist integers q and r such that $|F_q| = q = p^r$. The cardinality of R is $|R| = |F_q|^\nu$; see for example [18, Lemma 2.4]. *Throughout this paper, R denotes a finite chain ring with $1 \neq 0$, γ a fixed generator of the maximal ideal of R, ν the nilpotency index of γ. We set $\alpha = \gamma^{\nu-1}$.*

The proof of the following lemma is illustrated in [15, p. 340].

Lemma 2.1. *For any $0 \neq a \in R$ there is a unique integer i; $0 \leq i \leq \nu$ such that $a = u\gamma^i$, with u a unit. The unit u is unique modulo $\gamma^{\nu-i}$ only.*

Corollary 2.2. *If $1 \leq i < j \leq \nu$ and $\gamma^i c \in \gamma^j R$, then $c \in \gamma^{j-i}R$. In particular, if $\gamma^i c = 0$, then $c \in \gamma^{\nu-i}R$.*

There is a canonical projection homomorphism from R onto $F_q \cong R/\gamma R$. Denote by $\overline{r}$ the image of an element $r \in R$ under this projection. In [18], Norton and Sălăgean proved the following lemma.

Lemma 2.3. *Let $V \subseteq R$ be a set of representatives for the equivalence classes of R under congruence modulo γ. (Equivalently, we can define V to be a maximal subset of R with the property that $\overline{r_1} \neq \overline{r_2}$ for all $r_1, r_2 \in R$, $r_1 \neq r_2$.) Then,*

1. *for any $v \in R$ there exist unique $r_0, \ldots, r_{\nu-1} \in V$ such that $v = \sum_{i=0}^{\nu-1} r_i\gamma^i$;*
2. *$|V| = |R/\gamma R| = |F_q|$;*
3. *$|R/\gamma^j R| = |\langle\gamma^j\rangle| = |F_q|^{\nu-j}$ for $0 \leq j \leq \nu - 1$.*

For any two elements a and b of a ring, we will write $a \mid b$ for a divides b. For any constant $r \in R$ and any $c \in R^n$ we denote by rc the usual multiplication of a vector by a scalar. Also, for a set $C \subseteq R^n$ we write rC for the set $\{rc \,|\, c \in C\}$. We will say that a vector $c \in R^n$ is divisible by a constant $r \in R$, and write $r \mid c$, if all entries of c are divisible by r. Lemma 2.1 implies that for any $c \in R^n$ there is a unique i such that $c = \gamma^i e$, $0 \leq i \leq \nu - 1$, $e \in R^n$ and $\gamma \nmid e$. The R-module αR^n also has the structure of F_q-vector space, with multiplication of a vector $\alpha c \in \alpha R^n$ by $b \in F_q$ defined as usual to be $a\alpha c$ where $a \in R$ is an element for which $\bar{a} = b$.

Lemma 2.4 ([18, Lemma 2.9])**.** *Let $0 \leq i \leq \nu - 1$. The map $\varphi_i : \gamma^i R^n \to (R/\gamma^{v-i}R)^n$ given by $\varphi_i(\gamma^i c) = (c_1 + \gamma^{v-i}R, c_2 + \gamma^{v-i}R, \ldots, c_n + \gamma^{v-i}R)$ for*

any $c = (c_1, c_2, \ldots, c_n) \in R^n$ is an isomorphism of R and of $R/\gamma^{v-i}R$-modules. In particular $\varphi : \alpha R^n \to F_q^n$ given by $\varphi(\alpha c) = \bar{c}$ is an isomorphism of F_q-vector spaces.

2.2. Linear algebra over R

The set of all $m \times l$ matrices over R will be represented by $M_{m\times l}(R)$. For $A \in M_{m\times l}(R)$, we denote the transpose of the matrix A by A^{tr}. Given matrices A of size $m \times l$ and B of size $m \times l$, we use $\begin{pmatrix} A & B \end{pmatrix}$ to denote the matrix of size $m \times (l + l)$ formed by concatenating A and B. If C is another matrix of size $m \times l$, the $(m + m) \times l$ matrix $\binom{A}{C}$ is similarly defined (by concatenating vertically). We also let 0 denote the zero matrix, where the size will either be obvious from the context or specified whenever necessary. Similarly, we denote the $m \times m$ identity matrix by I_m, or simply I if the size is clear from the context.

Definition ([6])**.** For any integer $t \geq 1$, let $a_i = (a_{i1}, \ldots, a_{in}) \in R^n$, where $i = 1, \ldots, t$. The vectors $a_1, \ldots, a_t$ are said to be linearly dependent if there exists $(b_1, \ldots, b_t)$ in the set difference $R^t \setminus \{0\}$ such that $b_1a_1 + \cdots + b_ta_t = 0$; otherwise, $a_1, \ldots, a_t$ are said to be linearly independent.

Definition ([6])**.** Let $A = (a_{ij})_{m\times l}$ be in $M_{m\times l}(R)$.

(1) If the rows of A are linearly independent, then we say that A is a full-row-rank (FRR) matrix.
(2) If there is an $l \times m$ matrix B over R such that $AB = I$, then we say that A is right-invertible and B is a right inverse of A.
(3) If $m = l$ and the determinant $\det A$ is a unit of R, then we say that A is non-singular.

The following corollary follows from a typical linear algebra argument.

Corollary 2.5 ([6, Corollary 2.8])**.** *Let $A = (a_{ij})_{m\times l}$ be in $M_{m\times l}(R)$. Then, A is invertible if and only if A is non-singular if and only if A is FRR.*

2.3. Codes over R

Let $n \geq 1$ be a fixed natural number. By a (block) code of length n over R_ν we will mean a nonempty subset of R_ν^n. We will only consider codes that are different from 0, and n will always denote the length of the code. The code is called linear if it is an R_ν-submodule of R_ν^n. From now on, by "code" we mean "linear code".

For a code C, we define the rank of C, denoted by $\mathrm{rank}(C)$, to be the minimum number of generators of C and the *free rank* of C, denoted by $\mathrm{free\ rank}(C)$, to be the maximum of the ranks of free R-submodules of C. Codes where the rank is equal to the free rank are called free codes. For any vector over R_ν, we define the Hamming weight to be the number of non-zero coordinates. We denote by d the minimum Hamming weight of the code, which is the smallest of all the Hamming weights of all non-zero vectors in the code. We attach

to the ambient space the following inner product: for $v = (v_1, \ldots, v_n)$ and $w = (w_1, \ldots, w_n)$ in R^n, let $[v, w] = \sum_{i=1}^{n} v_i w_i$. The *dual* (*orthogonal*) *of the code*, denoted by $C^{\perp}$, is defined by

$$C^{\perp} = \{w \in R^n \mid [v, w] = 0, \forall v \in C\}.$$

It is evident that $C^{\perp}$ is linear. We know from [21] that $|C||C^{\perp}| = |R|^n$ if R is a Frobenius ring, where $|R|$ denotes the cardinality of R. We also know that any chain ring is Frobenius.

The structure of codes for $R = Z_{p^a}$, is described in [1, p. 22]. The following structural results for codes over finite chain rings can be found in [18].

Definition (Generator matrix)**.** Let C be a code over R. A matrix G is called a generator matrix for C if the rows of G span C and none of them can be written as a linear combination of the other rows of G.

G is called a generator matrix for C in standard form if after a suitable permutation of the coordinates,

$$(1) \quad G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \ldots & A_{0,t-1} & A_{0,\nu} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \ldots & \gamma A_{1,\nu-1} & \gamma A_{1,\nu} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \ldots & \gamma^2 A_{2,\nu-1} & \gamma^2 A_{2,\nu} \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & \gamma^{\nu-1} I_{k_{\nu-1}} & \gamma^{\nu-1} A_{\nu-1,\nu} \end{pmatrix},$$

where the columns are grouped into blocks of sizes $k_0, k_1, \ldots, k_{\nu-1}, n - \sum_{i=0}^{\nu-1} k_i$ with $k_i \geq 0$. Note that all the entries in $\gamma^i A_{i,j}$ $(0 \leq i \leq \nu - 1, 1 \leq j \leq \nu)$ are in $\langle \gamma^i \rangle$. A code with generator matrix of this form is said to be have type $\{k_0, k_1, \ldots, k_{\nu-1}\}$.

The generator matrix in standard form G is associated to the matrix A, where

$$(2) \quad A = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \ldots & A_{0,\nu-1} & A_{0,\nu} \\ 0 & I_{k_1} & A_{1,2} & A_{1,3} & \ldots & A_{1,\nu-1} & A_{1,\nu} \\ 0 & 0 & I_{k_2} & A_{2,3} & \ldots & A_{2,\nu-1} & A_{2,\nu} \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & I_{k_{\nu-1}} & A_{\nu-1,\nu} \end{pmatrix} = \begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{\nu-1} \end{pmatrix}.$$

Note that any rows in A can not be divided by γ.

For the following results, see [18].

Theorem 2.6. *Any linear code C has a generator matrix in standard form. All generator matrices in standard form for a linear code C have the same parameters $k_0, k_1, \ldots, k_{\nu-1}$ and $|C| = |F_q|^{\sum_{i=0}^{\nu-1}(\nu-i)k_i}$.*

This theorem justifies the following notation.

Definition. Let C be a linear code. We denote by $k(C)$ the number of rows of a generating matrix G in standard form for C, and for $i = 0, \ldots, \nu - 1$ we

denote by $k_i(C)$ the number of rows of G that are divisible by γ^i but not by γ^{i+1}. Clearly, $k(C) = \sum_{i=0}^{\nu-1} k_i(C)$.

We define $k_\nu = n - \sum_{i=0}^{\nu-1} k_i$. The following lemma is immediate, see [9] or [18].

Lemma 2.7. *Let C be a code of type $\{k_0, k_1, \ldots, k_{\nu-1}\}$. Then $C^\perp$ is a code of type $\{k_\nu, k_{\nu-1}, \ldots, k_1\}$.*

A linear code is called free if it is a free R-submodule.

Corollary 2.8 ([18])**.** *Let C be a linear code. The following assertions are equivalent*:

(1) *C is a free code.*
(2) *Any generator matrix in standard form for C is of the form $(I_{k(C)}|M)$ for some matrix M.*
(3) *$k(C) = k_0(C)$.*

3. Projections and lifts of codes over R

In this section, some results for linear codes over a finite chain ring given in [18] are generalized. Recall that R stands for a finite chain ring with $1 \neq 0$, γ a fixed generator of the maximal ideal of R, ν the nilpotency index of γ and $F_q \cong R/\gamma R$. Let $T^*(R) := \{b \in R : b \neq 0, b^q = b\}$. The set $T(R) = T^*(R) \cup \{0\}$ is called Teichmüller set of R. For every element $a \in R$, there exists unique $(a_0, a_1, \ldots, a_{\nu-1}) \in T(R)^{\nu-1}$ such that $a = a_0 + a_1\gamma + \cdots + a_{\nu-1}\gamma^{\nu-1}$ (see [8]). The operations over R are presented as

$$\sum_{l=0}^{\nu-1} a_l\gamma^l + \sum_{l=0}^{\nu-1} b_l\gamma^l = \sum_{l=0}^{\nu-1}(a_l + b_l)\gamma^l,$$
$$\sum_{l=0}^{\nu-1} a_l\gamma^l . \sum_{l'=0}^{\nu-1} b_{l'}\gamma^{l'} = \sum_{s=0}^{\nu-1}(\sum_{l+l'=s} a_l b_{l'})\gamma^s.$$

For a positive integers $t < \nu$, we define a map as follows:

$$\psi_t : R \to R/\gamma^t R,$$
$$\sum_{l=0}^{\nu-1} a_l\gamma^l \to \sum_{l=0}^{t-1} a_l\gamma^l + \gamma^t R.$$

In this case, it can be seen that

$$\psi_t(a+b) = \psi_t(a) + \psi_t(b),\ \psi_t(ab) = \psi_t(a)\psi_t(b)$$

for any $a, b \in R$. The map ψ_t is said to be a canonical projection from R to $R/\gamma^t R$. Note that the map ψ_t can also be extended naturally from R^n to $(R/\gamma^t R)^n$.

For any code C and any $r \in R$, $(C : r)$ is the *submodule quotient* $(C : r) = \{e \in R^n \,|\, re \in C\}$.

Definition. To any code C over R, we associate the tower of codes

$$C = (C : \gamma^0) \subseteq (C : \gamma^1) \subseteq \cdots \subseteq (C : \gamma^{\nu-1})$$

over R and its projection to $R/\gamma^t R$ for $1 \leq t < j < \infty$,

$$\psi_t(C) = \psi_t((C : \gamma^0)) \subseteq \psi_t((C : \gamma^1)) \subseteq \cdots \subseteq \psi_t((C : \gamma^{\nu-1})).$$

For a particular case, $t = 1$, the projection of the towers were introduced in [18] and denoted as $\psi_1((C : \gamma^l)) = \overline{(C : \gamma^l)}$.

The following result appears in [18, Lemma 3.4] for the particular case $t = 1$.

Lemma 3.1. *Let C be a code over R with generator matrix G in standard form and let A be as in* (2)*. Then for $1 \leq t < \nu < \infty$, $0 \leq i \leq \nu - t$, $\psi_t((C : \gamma^i))$ has a generator matrix*

$$\begin{pmatrix} \psi_t(A_0) \\ \psi_t(A_1) \\ \vdots \\ \psi_t(A_i) \\ \psi_t(\gamma A_{i+1}) \\ \vdots \\ \psi_t(\gamma^{t-1} A_{t-1+i}) \end{pmatrix}$$

over $R/\gamma^t R$ and $k(\psi_t((C : \gamma^i))) = k_0(C) + k_1(C) + \cdots + k_{t-1+i}(C)$.

Proof. For completeness, we give a proof which is similar to the one given for Lemma 3.4 in [18].

It is easy to check that $\psi_t((C : \gamma^i))$ contains the module spanned by the rows of the given matrix. Let $e \in \psi_t((C : \gamma^i))$ and let $g \in (C : \gamma^i)$ be such that $\psi_t(g) = e$. As $\gamma^i g \in C$ and G is a generating matrix for C, there are $v_j \in R^{k_j}$ such that

$$\begin{aligned} \gamma^i g = (&v_0, v_0 A_{0,1} + \gamma v_1, \ldots, v_0 A_{0,\nu-1} + v_1 \gamma A_{1,\nu-1} + \cdots + \gamma^{\nu-1} v_{\nu-1}, \\ &v_0 A_{0,\nu} + \cdots + \gamma^{\nu-1} v_{\nu-1} A_{\nu-1,\nu}). \end{aligned}$$

Here, $\gamma^i g$ is divisible by γ^i, therefore $v_0 = \gamma^i w_0$ for some $w_0 \in R^{k_0}$. The second block of entries of $\gamma^i g$ becomes $\gamma^i w_0 A_{0,1} + \gamma v_1$, hence $v_1 = \gamma^{i-1} w_1$ for some $w_1 \in R^{k_1}$. By following the same steps, we get $v_j = \gamma^{i-j} w_j$ for some $w_j \in R^{k_j}$ for $j = 0, 1, \ldots, \nu - 1$. Accordingly, $\gamma^i g = \sum_{j=0}^{i} \gamma^i w_j A_j + \sum_{j=i+1}^{\nu-1} \gamma^j v_j A_j$ and $g \equiv \sum_{j=0}^{i} w_j A_j + \sum_{j=i+1}^{\nu-1} \gamma^{j-i} v_j A_j \pmod{\gamma^{\nu-i}}$ by Corollary 2.2, thus $e = \psi_t(g) = \sum_{j=0}^{i} \psi_t(w_j)\psi_t(A_j) + \sum_{j=i+1}^{t-1+i} \psi_t(v_j)\psi_t(\gamma^{j-i} A_j) + \gamma^t R$, i.e., $\psi_t((C : \gamma^i))$ is generated by the required matrix. Since $k(\psi_t(A_l)) = k_l(C)$ for each $l \in \{0, \ldots, i\}$ and $k(\psi_t(\gamma^{i+l} A_{l+i})) = k_{i+l}(C)$ for each $l \in \{1, \ldots, t-1\}$, $k(\psi_t((C : \gamma^i))) = k_0(C) + k_1(C) + \cdots + k_{t-1+i}(C)$. □

The following result also appears in [18, Theorem 3.10] for the particular case $t = 1$.

Lemma 3.2. *Let C be a code over R with generator matrix G in standard form as in* (1)*. Then for $1 \leq t < \nu < \infty$, $0 \leq i \leq \nu - t$, $\psi_t((C^\perp : \gamma^i)) = (\psi_t((C : \gamma^{\nu-t-i})))^\perp$ over $R/\gamma^t R$.*

Proof. We will first prove that $\psi_t((C^\perp : \gamma^i)) \perp \psi_t((C : \gamma^{\nu-t-i}))$. Let $b \in (C^\perp : \gamma^i)$ and let $e \in (C : \gamma^{\nu-t-i})$. In this case, $\gamma^i b \in C^\perp$ and $\gamma^{\nu-t-i}e \in C$, thus $\gamma^{\nu-t}be^{tr} = 0$, i.e., $\psi_t(be^{tr}) = 0$. Then $\psi_t((C^\perp : \gamma^i)) \subseteq (\psi_t((C : \gamma^{\nu-t-i})))^\perp$. Note that $k_0(C^\perp) = n - k(C)$ and $k_i(C^\perp) = k_{\nu-i}(C)$ for all $0 < i \leq \nu - 1$, [18, Theorem 3.10]. $\psi_t((C : \gamma^{\nu-t-i}))$ is a code of type $\{k_0 + k_1 + \cdots + k_{\nu-t-i}, k_{\nu-t-i+1}, \ldots, k_{\nu-1-i}\}$ by Lemma 3.1 thus implying $(\psi_t((C : \gamma^{\nu-t-i})))^\perp$ is a code of type $\{n-(\sum_{j=0}^{\nu-1-i} k_j), k_{\nu-1-i}, \ldots, k_{\nu-t-i+1}\}$ by Lemma 2.7. Applying the similar procedure, we obtain that $\psi_t((C^\perp : \gamma^i))$ is a code of type $\{n - (\sum_{j=0}^{\nu-1-i} k_j), k_{\nu-i-1}, \ldots, k_{\nu-t+1-i}\}$. Because $\psi_t((C^\perp : \gamma^i))$ and $(\psi_t((C : \gamma^{\nu-t-i})))^\perp$ are codes of same type and $\psi_t((C^\perp : \gamma^i)) \subseteq (\psi_t((C : \gamma^{\nu-t-i})))^\perp$, $\psi_t((C^\perp : \gamma^i)) = (\psi_t((C : \gamma^{\nu-t-i})))^\perp$ over $R/\gamma^t R$ by [18, Corollary 3.7]. □

Example 3.3. Let $R = Z_{3^3}$. By [8, p. 227], $T(R) = \{0, 1, -1\}$. Let C be a code over R with generator matrix $G = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 3 & 6 & 15 \\ 0 & 0 & 9 & 18 \end{pmatrix}$. Then $A_0 = \begin{pmatrix} 1 & 0 & 2 & 0 \end{pmatrix}$, $A_1 = \begin{pmatrix} 0 & 1 & 2 & 5 \end{pmatrix}$, $A_2 = \begin{pmatrix} 0 & 0 & 1 & 2 \end{pmatrix}$. The code $(C : 3)$ is generated by $G_1 = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 5 \\ 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 9 \end{pmatrix}$. For $t = 2$, $\psi_2(15) = \psi_2(6) = -3$, $\psi_2(18) = \psi_2(9) = \psi_2(0) = 0$, $\psi_2(5) = -4$, $\psi_2(1) = 1$, $\psi_2(2) = 2$. The codes $\psi_2((C : 3^0))$ and $\psi_2((C : 3^1))$ are generated over $R/3^2R$ respectively by $\begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 3 & -3 & -3 \end{pmatrix} = \begin{pmatrix} \psi_2(A_0) \\ \psi_2(3A_1) \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & -4 \\ 0 & 0 & 3 & -3 \end{pmatrix} = \begin{pmatrix} \psi_2(A_0) \\ \psi_2(A_1) \\ \psi_2(3A_2) \end{pmatrix}$. Moreover, $k(\psi_2((C : 3^0)) = 2 = k_0 + k_1$ and $k(\psi_2((C : 3^1)) = 3 = k_0 + k_1 + k_2$.

In particular, the code $C^\perp$ is generated by $\begin{pmatrix} 25 & 20 & 1 & 1 \\ 21 & 3 & 3 & 9 \\ 0 & 9 & 0 & 9 \end{pmatrix}$, and $\psi_2(C^\perp)$ is generated by $\begin{pmatrix} -2 & 2 & 1 & 1 \\ 3 & 3 & 3 & 0 \end{pmatrix}$ by the fact that $\psi_2(25) = -2$, $\psi_2(20) = 2$, $\psi_2(21) = 3$. Clearly $\psi_2(C^\perp) \perp \psi_2(C : 3)$, as indicated in Lemma 3.2.

Let C be a code with generator matrix G as in (1). The following matrix H

$$(3) \quad \begin{pmatrix} B_{0,\nu} & B_{0,\nu-1} & \cdots & B_{0,1} & I_{n-k(C)} \\ \gamma B_{1,\nu} & \gamma B_{1,\nu-1} & \cdots & \gamma I_{k_{\nu-1}(C)} & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \gamma^{\nu-1} B_{\nu-1,\nu} & \gamma^{\nu-1} I_{k_1(C)} & \cdots & 0 & 0 \end{pmatrix} = \begin{pmatrix} B_0 \\ \gamma B_1 \\ \vdots \\ \gamma^{\nu-1} B_{\nu-1} \end{pmatrix}$$

is a generator matrix for $C^\perp$ and a parity check matrix for C, where $B_{i,j} = -\sum_{k=i+1}^{j-1} B_{i,k} A_{\nu-j,\nu-k}^{tr} - A_{\nu-j,\nu-i}^{tr}$ for $0 \leq i < j \leq \nu$, (see [18, Theorem 3.10]).

We associate the following matrix B to H, where B is defined as

$$\begin{pmatrix} B_0 \\ B_1 \\ \vdots \\ B_{\nu-1} \end{pmatrix}. \tag{4}$$

Corollary 3.4. *Let C be a code over R with generator matrix G as in (1), parity check matrix H as in (3) and let A, B be associated to G, H as in (2) and (4). Then, for $1 \leq t < \nu < \infty$, $\psi_t(C)$ has a generator matrix and a parity check matrix*

$$\begin{pmatrix} \psi_t(A_0) \\ \psi_t(\gamma A_1) \\ \vdots \\ \psi_t(\gamma^{t-1} A_{t-1}) \end{pmatrix}, \begin{pmatrix} \psi_t(B_0) \\ \psi_t(B_1) \\ \vdots \\ \psi_t(B_{\nu-t}) \\ \psi_t(\gamma B_{\nu-t+1}) \\ \vdots \\ \psi_t(\gamma^{t-1} B_{\nu-1}) \end{pmatrix}$$

over $R/\gamma^t R$, respectively.

We close this section with the following result.

Corollary 3.5. *Let C be a code over R_ν with generator matrix G as in (1). The following assertions are equivalent:*

1. *C is a free code;*
2. *$\psi_t(C) = \psi_t((C : \gamma^0)) = \psi_t((C : \gamma^1)) = \cdots = \psi_t((C : \gamma^{\nu-t}))$ over $R/\gamma^t R$ for all $1 \leq t < \nu < \infty$;*
3. *$\psi_t(C) = \psi_t((C : \gamma^0)) = \psi_t((C : \gamma^1)) = \cdots = \psi_t((C : \gamma^{\nu-t}))$ over $R/\gamma^t R$ for some $1 \leq t < \nu < \infty$.*

Proof. (1) $\Rightarrow$ (2) follows by Lemma 3.1 and Corollary 2.8, (2) $\Rightarrow$ (3) is clear. For (3) $\Rightarrow$ (1), pick an arbitrary $t \in \{1, \ldots, \nu-1\}$ and assume $\psi_t(C) = \psi_t((C : \gamma^0)) = \psi_t((C : \gamma^1)) = \cdots = \psi_t((C : \gamma^{\nu-t}))$ over $R/\gamma^t R$. Then, by Lemma 3.1, $k_t = \cdots = k_{\nu-1} = 0$. Now, we will show that $k_i = 0$ for all $i \in \{1, \ldots, t-1\}$. By Lemma 3.1, $\psi_t(C)$ and $\psi_t((C : \gamma^1))$ have generator matrices

$$\begin{pmatrix} \psi_t(A_0) \\ \psi_t(\gamma A_1) \\ \vdots \\ \psi_t(\gamma^{t-1} A_{t-1}) \end{pmatrix}, \begin{pmatrix} \psi_t(A_0) \\ \psi_t(A_1) \\ \psi_t(\gamma A_2) \\ \vdots \\ \psi_t(\gamma^{t-2} A_{t-1}) \\ \psi_t(\gamma^{t-1} A_t) \end{pmatrix}$$

over $R/\gamma^t R$, respectively. Then now, $\psi_t(C)$ and $\psi_t((C : \gamma^1))$ are codes of types $\{k_0, k_1, \ldots, k_{t-1}\}$ and $\{k_0 + k_1, k_2, \ldots, k_{t-1}, k_t\}$, respectively. However, since

by our assumption $\psi_t(C) = \psi_t((C : \gamma^1))$, $k_0 = k_0 + k_1$, $k_1 = k_2$, ..., $k_{t-1} = k_t$, so that $k_i = 0$ for all $i \in \{1, \ldots, t\}$. $k(C)$ must then be equal to $k_0(C)$ implying C is a free code by Corollary 2.8. □

Example 3.6. Let R be as in Example 3.3. Let C be a code over R with generator matrix $G = \begin{pmatrix} 1 & 0 & 2 \end{pmatrix}$. Then the codes $(C : 3)$, $(C : 3^2)$, $C^\perp$, $(C^\perp : 3)$ and $(C^\perp : 3^2)$ are generated respectively by $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 9 & 0 \\ 0 & 0 & 9 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 13 \\ 0 & 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 13 \\ 0 & 1 & 0 \\ 0 & 0 & 9 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 13 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. The codes $\psi_2((C)) = \psi_2((C : 3^1))$ and $\psi_2((C^\perp)) = \psi_2((C^\perp : 3^1))$ are generated over $R/3^2R$ respectively by $\begin{pmatrix} 1 & 0 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 0 \end{pmatrix}$. Moreover, $\psi_2(C^\perp : 3^0) = (\psi_2((C : 3^1)))^\perp$, $\psi_2((C^\perp : 3)) = (\psi_2((C : 3^0)))^\perp$.

For the other characterizations of free codes over a finite chain ring, we refer the reader to [17, Corollary 3.12] and [18, Proposition 3.13].

4. LCD codes over R

In this section, we will examine LCD codes over a finite chain ring R. Using the results mentioned in the preceding section, we proceed with providing some necessary and sufficient conditions for an LCD code C over a finite chain ring. We will start with showing LCD codes over a finite chain ring are free codes. The following proposition will be used in the sequel.

Proposition 4.1. *LCD codes over a finite chain ring are free codes.*

Proof. First, let us point out that $(A^\perp)^\perp = A$ and $(A \cap B)^\perp = A^\perp + B^\perp$ for any linear codes A, B over R, see [9, Theorem 3.1]. Assume that C is an LCD code with length n over a chain ring R. It follows from our assumptions that $C + C^\perp = (C \cap C^\perp)^\perp = 0^\perp = R^n$. We obtain $C \oplus C^\perp = R^n$ using the property $C \cap C^\perp = 0$. Therefore, C is a direct summand of the free code R^n which yields the conclusion that C is a free code. □

In terms of the generator matrix, we now give a sufficient and necessary condition for a linear code C over R to be LCD code by Proposition 4.1 and [12, Theorem 3.5, Corollary 3.6].

Corollary 4.2. *Let C be a code over R with generator matrix G in standard form as in* (1)*. Then C is an LCD code if and only if the $k \times k$ matrix GG^{tr} is invertible, where k is the number of rows of G.*

Corollary 4.3. *A linear code C over R with generator matrix G in standard form as in* (1) *is free if the $k \times k$ matrix GG^{tr} is invertible, where k is the number of rows of G.*

The following example was given in [12] to show that the $k \times k$ matrix GG^{tr} is not invertible for some linear LCD code C with generator matrix G in standard form. However, the given code C is not an LCD code, hence the corresponding example is not correct.

Example 4.4. Let C be a code over Z_4 with generator matrix in standard form as follows

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 \end{pmatrix}.$$

This code is not LCD code, since $(2,0,0,0,2,0) \in C \cap C^{\perp} \neq 0$.

Using the results provided in the preceding section, we now give some necessary and sufficient conditions for an LCD code C over a finite chain ring, through Proposition 4.1.

Theorem 4.5. *Let C be a code over R for $1 \leq \nu < \infty$. The following assertions are equivalent*:

(1) *C is an LCD code over R;*
(2) *$\psi_t(C)$ is an LCD code and $\psi_t(C) = \psi_t((C : \gamma^{\nu-t}))$ over $R/\gamma^t R$ for all $1 \leq t < \nu$;*
(3) *$\psi_t(C)$ is an LCD code and $\psi_t(C) = \psi_t((C : \gamma^{\nu-t}))$ over $R/\gamma^t R$ for some $1 \leq t < \nu$.*

Proof. (1) $\Rightarrow$ (2) C is a free code by Proposition 4.1. Therefore, $\psi_t(C) = \psi_t((C : \gamma^{\nu-t}))$ over $R/\gamma^t R$ for all $1 \leq t < \nu < \infty$, through Corollary 3.5. The remaining part is an immediate consequence of [12, Theorem 3.9]. (2) $\Rightarrow$ (3) is obvious.

(3) $\Rightarrow$ (1) Assume that $\psi_t(C)$ is an LCD code and $\psi_t(C) = \psi_t((C : \gamma^{\nu-t}))$ over $R/\gamma^t R$ for fix t, $t \in \{1, \ldots, \nu-1\}$. Suppose, contrarily, that C is not an LCD code over R. Take $c \in C \cap C^{\perp}$ with $c \neq 0$. There exists $u \in R^n$ such that $c = \gamma^i u$, $\gamma \nmid u$ and $i \in \{0, 1, \ldots, \nu-1\}$. Then $u \in (C : \gamma^i) \cap (C^{\perp} : \gamma^i)$. Consider two cases for i, either $0 \leq i \leq \nu - t$ or $\nu - t < i \leq \nu - 1$.

In the former case, $\psi_t(u) \in \psi_t((C : \gamma^i)) \cap \psi_t((C^{\perp} : \gamma^i))$. Notice that $\psi_t(u) \neq 0$ in $R/\gamma^t R$, because otherwise, by Lemma 2.4, $\gamma^{\nu-t} u = 0$ in R implying $\gamma^t \mid u$ which contradicts with $\gamma \nmid u$. Now, since by our assumption $\psi_t(C) = \psi_t((C : \gamma^{\nu-t}))$, $\psi_t(C) = \psi_t((C : \gamma^i))$, hence $\psi_t(u) \in \psi_t(C)$. Notice that the assumption $\psi_t(C) = \psi_t((C : \gamma^{\nu-t}))$ for an arbitrary t, $t \in \{1, \ldots, \nu-1\}$ is necessary and sufficient for C to be free by Corollary 3.5. Then now, by [18, Proposition 3.13], $C^{\perp}$ is a free code, so that $\psi_t(C^{\perp}) = \psi_t((C^{\perp} : \gamma^i))$ for all $0 \leq i \leq \nu - t$ by Corollary 3.5, hence $\psi_t(u) \in \psi_t(C^{\perp})$. Since $\psi_t(C^{\perp}) = (\psi_t((C : \gamma^{\nu-t})))^{\perp}$ by Lemma 3.2, we have $\psi_t(C^{\perp}) = (\psi_t(C))^{\perp}$ by our assumption, whence $\psi_t(u) \in (\psi_t(C))^{\perp}$. However, $\psi_t(C)$ is an LCD code which contradicts with $0 \neq \psi_t(u) \in \psi_t(C) \cap (\psi_t(C))^{\perp}$. So, this case is not possible.

In the latter case, $i = (\nu - t) + k$ for some $1 \leq k \leq t-1$. Then now $c = \gamma^i u = \gamma^{\nu-t}(\gamma^k u)$, so that $\gamma^k u \in (C : \gamma^{\nu-t}) \cap (C^{\perp} : \gamma^{\nu-t})$, hence $\psi_t(\gamma^k u) \in \psi_t((C : \gamma^{\nu-t})) \cap \psi_t((C^{\perp} : \gamma^{\nu-t}))$. Before we proceed, let us note that $\psi_t(\gamma^k u) \neq 0$ in $R/\gamma^t R$, which otherwise yields, by Lemma 2.4, $\gamma^{\nu-t}(\gamma^k u) = \gamma^i u = 0$ in R. This contradicts with $c \neq 0$. In the same vein as the former case, one can obtain

$\psi_t(\gamma^k u) \in \psi_t(C) \cap (\psi_t(C))^{\perp}$. However, $\psi_t(C)$ is an LCD code which implies $\psi_t(\gamma^k u) = 0$, a contradiction. So, this case is also not possible.

Thus, either case leads to a contradiction, yielding the conclusion. □

In the following example, we show that the condition $\psi_t(C) = \psi_t((C : \gamma^{\nu-t}))$ over $R/\gamma^t R$ for some $1 \leq t < \nu$ in Theorem 4.5 is necessary.

Example 4.6. Let C be a linear code over the finite chain ring $R = Z_4$ with generator matrix in standard form as follows

$$G = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix}.$$

Obviously, C is not free, therefore it is not an LCD code by Proposition 4.1. $\psi_1^2(C)$ and $\psi_1^2(C : \gamma)$, by Corollary 4.2, are LCD codes over R_1 with generator matrix $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$ and $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. Clearly, $\psi_1^2(C) \neq \psi_1^2(C : \gamma)$.

Example 4.7. Let R be as in Example 3.3. Let C be a code over $R/9R$ with generator matrix $G = \begin{pmatrix} 1 & 0 & 8 \end{pmatrix}$. $GG^{tr} = (2)$ is invertible, and hence C is an LCD code. Note that $\psi_2(1) = \psi_2(1.3^0 + 0.3^1 + 0.3^2) = \psi_2(1.3^0 + 0.3^1 + (-1).3^2) = \psi_2(1.3^0 + 0.3^1 + 1.3^2) = 1$. Similarly, $\psi_2(18) = \psi_2(9) = \psi_2(0) = 0$ and $\psi_2(26) = \psi_2(17) = \psi_2(8) = 8$. There are 27 possible LCD code C' over R such that $\psi_2(C') = C$. For example, the codes which are generated by $\begin{pmatrix} 1 & 9 & 8 \end{pmatrix}$, $\begin{pmatrix} 1 & 18 & 17 \end{pmatrix}$, $\begin{pmatrix} 1 & 9 & 26 \end{pmatrix}$ are LCD codes over R, and whose projections on $R/9R$ are C.

Now, we will provide another necessary and sufficient condition for a linear code C to be an LCD code.

Theorem 4.8. *Let C be a code over R for $1 \leq \nu < \infty$. C is an LCD code if and only if $\gamma^{\nu-1} v$ does not belong to $C \cap C^{\perp}$ for any nonzero $v = (v_1, \ldots, v_n) \in F_q^n$.*

Proof. The necessity is obvious. For sufficiency, let us assume that $\gamma^{\nu-1} v$ does not belong to $C \cap C^{\perp}$ for any nonzero $v = (v_1, \ldots, v_n) \in F_q^n$. Also, let $u \in C \cap C^{\perp}$ with $u \neq 0$. There exists $v \in R^n$ such that $u = \gamma^i v$, $\gamma \nmid v$ and $i \in \{0, 1, \ldots, \nu - 1\}$. We have $v = (v_1, \ldots, v_n) = (v_{1,0} + v_{1,1}\gamma + \cdots + v_{1,\nu-1}\gamma^{\nu-1}, \ldots, v_{n,0} + v_{n,1}\gamma + \cdots + v_{n,\nu-1}\gamma^{\nu-1})$ where $v_{s,l} \in F_q$ for $1 \leq s \leq n$ and $0 \leq l \leq \nu - 1$. Since $\gamma \nmid v$, at least one of $v_{1,0}, \ldots, v_{n,0}$ should be nonzero. Now, consider the element $\gamma^{\nu-i-1} u$. Note that $\gamma^{\nu-i-1} u$ is not zero, which otherwise yields $0 = \gamma^{\nu-i-1} u = \gamma^{\nu-1} v$. This implies $\gamma \mid v$, which is a contradiction since $\gamma \nmid v$. $\gamma^{\nu-i-1} u \in C \cap C^{\perp}$ as $u \in C \cap C^{\perp}$. However, $\gamma^{\nu-i-1} u = \gamma^{\nu-1} v = \gamma^{\nu-1}(v_{1,0} + v_{1,1}\gamma + \cdots + v_{1,\nu-1}\gamma^{\nu-1}, \ldots, v_{n,0} + v_{n,1}\gamma + \cdots + v_{n,\nu-1}\gamma^{\nu-1}) = \gamma^{\nu-1}(v_{1,0}, \ldots, v_{n,0})$, where $(v_{1,0}, \ldots, v_{n,0}) \in F_q^n \setminus \{0\}$, contradicting our hypothesis. Therefore, we cannot have such a nonzero element as u above. □

In [12, Theorem 3.10], Liu and Liu showed that a linear code C of length n over R_j for $1 \leq j < \infty$ is an LCD code if $\gamma^{j-1} v$ does not belong to $C \cap C^{\perp}$ for any nonzero $v = (v_1, \ldots, v_n) \in F_q^n$ and $\psi_k^j(C)$ is an LCD code over R_k for all

$1 \leq k < j$. In the previous theorem, we showed that the former condition itself in [12, Theorem 3.10] is sufficient and necessary for a linear code C to be LCD code over a chain ring. Therefore, the latter condition in [12, Theorem 3.10] is unnecessary.

Now, we will give a subclass of LCD codes over chain ring R. Every free code C over R is equivalent (up to a permutation of the coordinates of the codewords) to a code having a generator matrix in the standard form $G = (I_{k(C)}|M)$ for some M (Corollary 2.8). A square matrix B is called nilpotent if $B^k = 0$ for some positive integer k. Note that $I + B$ is an invertible matrix if B is a nillpotent matrix.

Proposition 4.9. *Let $G = (I_{k(C)}|M)$ be a generator matrix in standard form for a free code C over chain ring R. If MM^{tr} is nilpotent, then C is an LCD code.*

Proof. As we mentioned in the preceding paragraph, $I + MM^{tr}$ is invertible. Then, C is an LCD code by Corollary 4.2. □

Corollary 4.10. *Let $G = (I_{k(C)}|\gamma^i M)$ be a generator matrix in standard form for a code C over chain ring R. Then, C is an LCD code for each $i \geq 1$.*

The preceding result also appears in [12] for $i \geq \lceil \frac{\nu}{2} \rceil$, where $\lceil \rceil$ denotes the ceiling function.

Theorem 4.11. *Let C be a linear code of length n over R. There exists a corresponding LCD code C' of length $2n - k(C)$ over R with $d(C') > d(C)$.*

Proof. By [17, Corollary 4.7], there is a free code D of length n such that $k(C) = k(D)$ and $d(C) = d(D)$. Let $G = (I_{k(C)}|M)$ be an associated matrix in standard form for D. Then, since $\gamma^2 MM^{tr}$ is a nilpotent matrix, $G' = (I_{k(C)}|M|(\gamma - 1)M)$ is the generator matrix of an LCD code C' of length $2n - k(C)$ over R with $d(C') > d(C)$. □

The asymptotic goodness of LCD codes now follows trivially from that of general linear codes.

Acknowledgments. The author wishes to sincerely thank the anonymous referees for a very meticulous reading of this manuscript, and for valuable suggestions that help to create an improved version.

References

[1] A. R. Calderbank and N. J. A. Sloane, *Modular and p-adic cyclic codes*, Des. Codes Cryptogr. **6** (1995), no. 1, 21–35. https://doi.org/10.1007/BF01390768

[2] C. Carlet and S. Guilley, *Complementary dual codes for counter-measures to side-channel attacks*, Adv. Math. Commun. **10** (2016), no. 1, 131–150. https://doi.org/10.3934/amc.2016.10.131

[3] C. Carlet, S. Mesnager, C. M. Tang, Y. F. Qi, and R. Pellikaan, *Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$*, IEEE Trans. Inform. Theory **64** (2018), no. 4, part 2, 3010–3017. https://doi.org/10.1109/TIT.2018.2789347

[4] S. T. Dougherty, J.-L. Kim, B. Özkaya, L. Sok, and P. Solé, *The combinatorics of LCD codes: linear programming bound and orthogonal matrices*, Int. J. Inf. Coding Theory **4** (2017), no. 2-3, 116–128. https://doi.org/10.1504/IJICOT.2017.083827
[5] M. Esmaeili and S. Yari, *On complementary-dual quasi-cyclic codes*, Finite Fields Appl. **15** (2009), no. 3, 375–386. https://doi.org/10.1016/j.ffa.2009.01.002
[6] Y. Fan, S. Ling, and H. Liu, *Matrix product codes over finite commutative Frobenius rings*, Des. Codes Cryptogr. **71** (2014), no. 2, 201–227. https://doi.org/10.1007/s10623-012-9726-y
[7] C. Güneri, B. Özkaya, and P. Solé, *Quasi-cyclic complementary dual codes*, Finite Fields Appl. **42** (2016), 67–80. https://doi.org/10.1016/j.ffa.2016.07.005
[8] M. Hazewinkel, *Handbook of Algebra. Vol. 5*, Handbook of Algebra, **5**, Elsevier/North-Holland, Amsterdam, 2008.
[9] T. Honold and I. Landjev, *Linear codes over finite chain rings*, Electron. J. Combin. **7** (2000), Research Paper 11, 22 pp.
[10] L. Jin, *Construction of MDS codes with complementary duals*, IEEE Trans. Inform. Theory **63** (2017), no. 5, 2843–2847. https://doi.org/10.1109/TIT.2016.2644660
[11] C. Li, *Hermitian LCD codes from cyclic codes*, Des. Codes Cryptogr. **86** (2018), no. 10, 2261–2278. https://doi.org/10.1007/s10623-017-0447-0
[12] X. Liu and H. Liu, *LCD codes over finite chain rings*, Finite Fields Appl. **34** (2015), 1–19. https://doi.org/10.1016/j.ffa.2015.01.004
[13] J. L. Massey, *Reversible codes*, Information and Control **7** (1964), 369–380.
[14] ———, *Linear codes with complementary duals*, Discrete Math. **106/107** (1992), 337–342. https://doi.org/10.1016/0012-365X(92)90563-U
[15] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, Inc., New York, 1974.
[16] S. Mesnager, C. Tang, and Y. Qi, *Complementary dual algebraic geometry codes*, IEEE Trans. Inform. Theory **64** (2018), no. 4, part 1, 2390–2397. https://doi.org/10.1109/TIT.2017.2766075
[17] G. H. Norton and A. Sălăgean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory **46** (2000), no. 3, 1060–1067. https://doi.org/10.1109/18.841186
[18] ———, *On the structure of linear and cyclic codes over a finite chain ring*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), no. 6, 489–506. https://doi.org/10.1007/PL00012382
[19] N. Sendrier, *Linear codes with complementary duals meet the Gilbert-Varshamov bound*, Discrete Math. **285** (2004), no. 1-3, 345–347. https://doi.org/10.1016/j.disc.2004.05.005
[20] L. Sok, M. Shi, and P. Solé, *Constructions of optimal LCD codes over large finite fields*, Finite Fields Appl. **50** (2018), 138–153. https://doi.org/10.1016/j.ffa.2017.11.007
[21] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575. https://doi.org/10.1353/ajm.1999.0024
[22] X. Yang and J. L. Massey, *The condition for a cyclic code to have a complementary dual*, Discrete Math. **126** (1994), no. 1-3, 391–393. https://doi.org/10.1016/0012-365X(94)90283-6
[23] H. Zhu and M. Shi, *On linear complementary dual four circulant codes*, Bull. Aust. Math. Soc. **98** (2018), no. 1, 159–166. https://doi.org/10.1017/S0004972718000175

Yilmaz Durğun
Department of Mathematics
Cukurova University
Adana, Turkey
Email address: ydurgun@cu.edu.tr