Designs, Codes and Cryptography (2019) 87:3077–3086
https://doi.org/10.1007/s10623-019-00664-3

Linear complementary dual codes over rings

Zihui Liu[1] · Jinliang Wang[2]

Received: 29 October 2018 / Revised: 25 April 2019 / Accepted: 16 July 2019 / Published online: 24 July 2019

Abstract
By using linear algebra over finite commutative rings, we will present some judging criterions for linear complementary dual (LCD) codes over rings, in particular, free LCD codes over finite commutative rings are described. By using free LCD codes over finite commutative rings and the Chinese Remainder Theorem, LCD codes over semi-simple rings are constructed and the equivalence of free codes and free LCD codes is given. In addition, all the possible LCD codes over chain rings are determined. We also generalize the judging criterion for cyclic LCD codes over finite fields to cyclic LCD codes over chain rings. Based on the above results and the Chinese Remainder Theorem, we also present results for LCD codes over principal ideal rings.

Keywords Principal ideal rings · Chain rings · LCD codes · Chinese Remainder Theorem · Generating polynomial

Mathematics Subject Classification 94B05

1 Introduction

A linear complementary dual code (LCD) is defined as a linear code $\mathcal{C}$ satisfying $\mathcal{C}\cap\mathcal{C}^{\perp}=\{0\}$, where $\mathcal{C}^{\perp}$ is the dual code of $\mathcal{C}$. LCD codes recently attracted much attention due to their wide applications in data storage communications systems, consumer electronics and cryptography [2,3]. Jin [6] showed that some Reed–Solomon codes are equivalent to LCD codes, and Li et al. [7] constructed several families of LCD cyclic codes. Two families of BCH codes which are LCD codes were constructed in [8]. Mesnager et al. [12] constructed algebraic geometry LCD codes which can be applied against side-channel attacks. More recent results related to LCD codes can be referred to [14–17].

Some research work on LCD codes over finite Frobenius rings are also carried out. In 2015, Liu et al. [9] studied LCD codes over chain rings, and as the main result, they presented a

Communicated by J.-L. Kim.

✉ Zihui Liu
lzhui@bit.edu.cn

[1] Department of Mathematics, Beijing Institute of Technology, Beijing 100081, China

[2] School of Computer Science, Liaocheng University, Liaocheng 252059, China

condition for a free code over chain rings to be an LCD code. In 2017, LCD λ-constacyclic codes over a finite commutative semi-simple ring which can be decomposed into direct sums of some finite fields were studied in [4], and necessary and sufficient conditions for the existence of LCD λ-constacyclic codes were given.

The aim of this paper proceeds to give contributions along the direction of LCD codes over rings. We will present some judging criterions on LCD codes over any finite commutative ring. In particular, we provide descriptions of free LCD codes over finite commutative rings. By using the Chinese Remainder Theorem, we also construct free LCD codes over finite semi-simple rings. Furthermore, we will present some results about the equivalence of free codes and free LCD codes over finite commutative rings. We next confine the study to chain rings, and will determine all LCD codes over chain rings, and this result substantially improves that obtained in [9]. Based the above result and by using the structure of cyclic codes over chain rings, i.e. generating set in standard form [13], we also provide the description of cyclic LCD codes over chain rings which generalizes that given by Massey [18]. Finally, we will present some results about general LCD codes and free cyclic LCD codes over principal ideal rings.

A finite local commutative ring with identity is defined as a one containing a unique maximal ideal. Denote K the residue finite field of any local commutative ring $\mathcal{R}$. There is a canonical homomorphism from $\mathcal{R}$ to K under which the image of $r \in \mathcal{R}$ is denoted by $\overline{r}$. A linear code $\mathcal{C}$ with length n over any commutative ring $\mathcal{R}$ (not confined to a local ring) is defined as a submodule of $\mathcal{R}^n$, and call $\mathcal{C}$ free if it is a free submodule of $\mathcal{R}^n$. If $\mathcal{R}$ is local, then for a codeword $c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$, define $\overline{c} = (\overline{c_1}, \overline{c_2}, \ldots, \overline{c_n})$ and define $\overline{\mathcal{C}} = \{\overline{c} \mid c \in \mathcal{C}\}$. Similarly, define $\overline{G} = (\overline{g_{ij}})$ for a matrix $G = (g_{ij})$ over $\mathcal{R}$. Also define $\overline{H}(x) = \overline{H_m}x^m + \overline{H_{m-1}}x^{m-1} + \cdots + \overline{H_0}$ for $H(x) = H_m x^m + H_{m-1}x^{m-1} + \cdots + H_0 \in \mathcal{R}[x]$.

For any square matrix A over a finite commutative ring, if the determinant of A, $det(A)$, is a unit, then call A *nonsingular*. According to linear algebra, if A is nonsingular, then the system of equations $AX = 0$ has only the zero solution.

A finite chain ring is a special family of local commutative rings whose maximum ideal is principal, and there have been many papers dedicated to such rings. Let $\mathcal{R}$ be a chain ring, and let γ be a fixed generator of the maximal ideal of $\mathcal{R}$ with the residue field $K = R/\gamma R$. Then γ is nilpotent, and assume ν is the smallest positive integer such that $\gamma^\nu = 0$. Then all the ideals of $\mathcal{R}$ are $\langle \gamma^i \rangle = \gamma^i \mathcal{R}$, $0 \leq i \leq \nu$. Any element $r \in \mathcal{R}$ can be written as $r = \gamma^j u$ with u a unit, and call the unique integer j the *order* of r, denoted by $\mathrm{ord}(r)$. Obviously $\mathrm{ord}(0) = \nu$.

Definition 1 Let $\mathcal{R}$ be a chain ring. The order of a vector $v = (v_1, \ldots, v_k) \in \mathcal{R}^k$, denoted by $\mathrm{ord}(v)$, is defined as $\min\{\mathrm{ord}(v_i) \mid i = 1, \ldots, k\}$.

2 LCD codes over finite commutative rings

The aim of this section is to present some results about LCD codes over any finite commutative ring. Any finite commutative ring is always assumed to have an identity element. The following facts are useful.

Lemma 2 [11] *The linear system of equations $AX = 0$ with A a square matrix over any commutative ring has a nontrivial solution if and only if $det(A)$ is a zero divisor in the ring.*

Since an element in a finite ring is either a zero divisor or a unit, Lemma 2 can also be stated as the following

Lemma 3 *The linear system of equations $AX = 0$ with A a square matrix over any finite commutative ring has only the zero solution if and only if A is nonsingular.*

Remark 4 Let $\mathcal{C} \in \mathcal{R}^n$ be a linear code over any finite commutative ring $\mathcal{R}$. Define a generator matrix of $\mathcal{C}$ as a matrix G with rows being a generating set of $\mathcal{C}$ with the smallest size. In particular, when $\mathcal{C}$ is a free code, then the rows of any generator matrix G are a group of basis elements of $\mathcal{C}$, and so the number of rows of any generator matrix of a free code $\mathcal{C}$ is uniquely determined. For a general linear code $\mathcal{C}$, there is no concept of basis elements, but we may fix any generating set W of $\mathcal{C}$ with the smallest size and then arrange the elements of W as rows to get a generator matrix G. Throughout the paper, we always suppose that a generator matrix of $\mathcal{C}$ be defined as the above. Assume $\mathcal{C}$ is a linear code with a $k \times n$ generator matrix G and $c \in \mathcal{C} \cap \mathcal{C}^{\perp}$, then one can write $c = X^T G$ for some column vector $X = (x_1, x_2, \ldots, x_k)^T$; on the other hand, since the fact $c \in \mathcal{C}^{\perp}$ also holds, which is equivalent to that the codeword $c = X^T G$ is perpendicular to each row of G, we should have $GG^T X = 0$ according to the definition of the usual inner product. Thus, $\mathcal{C}$ is an LCD code, i.e., $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$, if and only if $GG^T X = 0$ yields $c^T = G^T X = 0$. Since $G^T X = 0$ always leads to $GG^T X = 0$, we obtain the following theorem.

Theorem 5 *Let $\mathcal{C} \in \mathcal{R}^n$ be a linear code over any finite commutative ring $\mathcal{R}$ with a $k \times n$ generator matrix G. Then $\mathcal{C}$ is an LCD code if and only if the linear system of equations $G^T X = 0$ and $GG^T X = 0$ have the same set of solutions.*

Definition 6 Let $\mathcal{C}$ be a free code with a generator matrix G, then the number of basis elements, i.e., the number of rows of G, is called the *dimension* of $\mathcal{C}$ denoted by $\dim(\mathcal{C})$.

Obviously, the dimension of a free code is exactly the usual dimension of a code over a field.

Let notations be the same as in Remark 4. If $\mathcal{C}$ is free, then $G^T X = 0$ is equivalent to $X = 0$. Thus, for a free code $\mathcal{C}$, Theorem 5 can be restated as: $\mathcal{C}$ is an LCD code if and only if $GG^T X = 0$ has only the zero solution. This fact combined Lemma 3 yields the following theorem.

Theorem 7 *Assume $\mathcal{R}$ is any finite commutative ring, and assume $\mathcal{C}$ is a free code, then $\mathcal{C}$ is an LCD code if and only if GG^T is nonsingular.*

Lemma 8 [5] (Chinese Remainder Theorem) *Assume $\mathcal{R}$ is a finite commutative ring with a group of pairwise relatively prime ideals $\mathcal{P}_1, \ldots, \mathcal{P}_t$. Then there is an isomorphism denoted by CRT from $(\mathcal{R}/\mathcal{P}_1, \ldots, \mathcal{R}/\mathcal{P}_t)$ to $\mathcal{R}/(\mathcal{P}_1 \cap \mathcal{P}_2 \cap \cdots \cap \mathcal{P}_t)$, and $\mathcal{R}/(\mathcal{P}_1 \cap \mathcal{P}_2 \cap \cdots \cap \mathcal{P}_t)$ is call the* Chinese product *of the rings $\mathcal{R}/\mathcal{P}_1, \ldots, \mathcal{R}/\mathcal{P}_t$.*

Lemma 9 [10] *Any finite commutative ring $\mathcal{R}$ is the Chinese product of some local rings $\mathcal{R}_1, \ldots, \mathcal{R}_t$, that is, $\mathcal{R} = CRT(\mathcal{R}_1, \ldots, \mathcal{R}_t)$.*

Denote by Φ: $\mathcal{R} \to (\mathcal{R}_1, \ldots, \mathcal{R}_t)$ the inverse map of CRT, and denote the composed map of Φ and the projection map $(\mathcal{R}_1, \ldots, \mathcal{R}_t) \to \mathcal{R}_i$, $1 \leq i \leq t$, by Φ_i, that is, Φ_i: $\mathcal{R} \to \mathcal{R}_i$, $1 \leq i \leq t$. These maps can be naturally extended to R^n coordinately and to $R[x]$. Thus, for a code $\mathcal{C} \subset \mathcal{R}^n$, we have $\mathcal{C} = CRT(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ with $\mathcal{C}_i \in \mathcal{R}_i^n$ being a code over $\mathcal{R}_i$, $1 \leq i \leq t$. In particular, a code $\mathcal{C} = CRT(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ over R is cyclic if and only if each $\mathcal{C}_i$ is cyclic over $\mathcal{R}_i$, $1 \leq i \leq t$. Furthermore, $\mathcal{C}^{\perp} = CRT(\mathcal{C}_1^{\perp}, \ldots, \mathcal{C}_t^{\perp})$, thus, $\mathcal{C}$ is an LCD code over $\mathcal{R}$ if and only if each $\mathcal{C}_i$ is an LCD code over $\mathcal{R}_i$, $1 \leq i \leq t$. The following result is also a direct consequence of the definition of the Chinese product.

Lemma 10 *Assume $\mathcal{C} = CRT(\mathcal{C}_1, \ldots, \mathcal{C}_t)$. Then the code $\mathcal{C}$ is free with* $\dim(\mathcal{C}) = k$ *if and only if each $\mathcal{C}_i$ is free with* $\dim(\mathcal{C}_i) = k$, $1 \leq i \leq t$.

Lemmas 9 and 10 transfer the problem of constructing free LCD codes over finite commutative rings to that of constructing free LCD codes over finite local commutative rings. To find the relationship of free LCD codes over finite local commutative rings and LCD codes over the residue fields, we present

Definition 11 [11] The *McCoy-rank* of a matrix $A_{m\times n}$ over commutative rings $\mathcal{R}$ is defined as the largest nonnegative integer s such that $\text{Anni}(F_s(A)) = 0$, where $\text{Anni}(F_s(A)) = \{r \in \mathcal{R} : rF_s(A) = 0\}$ and $F_s(A)$ is the ideal of $\mathcal{R}$ generated by all the determinants of the $s \times s$ submatrices of A with $F_0(A) = \mathcal{R}$ and $F_s(A) = 0$ for $s > \min\{m, n\}$.

Definition 12 A Noetherian ring is called a *full quotient ring* if every element is either a unit or a zero divisor.

It was shown in [11, p. 89] that a full quotient ring $\mathcal{R}$ satisfies

$$\langle a_1, \ldots, a_t\rangle = \mathcal{R} \text{ if and only if } \cap_{i=1}^{t} \text{Anni}(\langle a_i\rangle) = 0, \tag{1}$$

where $\langle a_1, \ldots, a_t\rangle$ stands for the ideal generated by $a_i \in \mathcal{R}$ for $1 \leq i \leq t$.

Since any finite commutative ring is a full quotient ring, we have

Lemma 13 *Any finite commutative ring $\mathcal{R}$ satisfies* (1)*, or equivalently, for any ideal $I \subsetneq \mathcal{R}$, we can find a non-zero element $a \in \mathcal{R}$ such that $aI = 0$.*

Lemma 14 *If $\mathcal{R}$ is a finite local commutative ring with the unique maximal ideal $\mathcal{M}$, then the McCoy-rank of any matrix A over $\mathcal{R}$ is the largest nonnegative integer s such that there exists an $s \times s$ submatrix of A whose determinant is a unit.*

Proof Assume the integer s_0 is the largest one such that there exists an $s_0 \times s_0$ submatrix of A whose determinant is a unit and assume $s_1 = \text{McCoy-rank}(A)$. Then $F_{s_0}(A) = \mathcal{R}$, thus, $\text{Anni}(F_{s_0}(A)) = 0$, and thus $s_0 \leq s_1$.

Since $s_1 = \text{McCoy-rank}(A)$, it follows that $\text{Anni}(F_{s_1}(A)) = 0$. Thus, $F_{s_1}(A) = \mathcal{R}$ by Lemma 13. If the determinants of all the $s_1 \times s_1$ submatrices of A are zero divisors, then $F_{s_1}(A) \subset \mathcal{M}$, and we get a contradiction to $F_{s_1}(A) = \mathcal{R}$, and this shows that there exists an $s_1 \times s_1$ submatrix of A whose determinant is a unit. We thus obtain $s_1 \leq s_0$. □

Lemma 15 *[11, p. 85] Let $A_{n\times k}$ be a matrix over any commutative ring, then the linear system of equations $AX = 0$ has a nontrivial solution $X = (x_1, \ldots, x_k)^T$ if and only if the McCoy-rank of A is less than k.*

Theorem 16 *Let $\mathcal{C} \subset \mathcal{R}^n$ be a free code over a finite local commutative ring $\mathcal{R}$ with $dim(\mathcal{C}) = k$, and let $G_{k\times n}$ be any generator matrix of $\mathcal{C}$. Then the matrix G contains a $k \times k$ submatrix whose determinant is a unit.*

Proof Since G is a generator matrix of the free code $\mathcal{C}$, the linear system of equations $G^T X = 0$ has only the zero solution, we thus get $\text{McCoy-rank}(G^T) = \text{McCoy-rank}(G) = k$ by Lemma 15, and thus G contains a $k \times k$ submatrix whose determinant is a unit due to Lemma 14. □

Corollary 17 *Assume $\mathcal{R}$ is any finite local commutative ring with residue field K, and assume $\mathcal{C}$ is a free code, then $\mathcal{C}$ is an LCD code over $\mathcal{R}$ with* $\dim(\mathcal{C}) = k$ *if and only if $\overline{\mathcal{C}}$ is an LCD code over K with* $\dim(\overline{\mathcal{C}}) = k$.

Let $\mathcal{R}$ be any finite commutative ring with prime ideals $\mathcal{P}_i$ for $1 \le i \le t$ which are also all the maximal ideals of $\mathcal{R}$. Then the radical $\mathrm{Rad}(\mathcal{R})$ of $\mathcal{R}$ is $\mathrm{Rad}(\mathcal{R}) = \cap_{i=1}^{t} \mathcal{P}_i$. Furthermore, according to Lemma 9 and its proof (see [10]), we obtain that $\mathcal{R} = CRT(\mathcal{R}_1, \ldots, \mathcal{R}_t)$ for some local rings $\mathcal{R}_i$, and the residue field of each local ring $\mathcal{R}_i$ is exactly $\mathcal{R}/\mathcal{P}_i$ for $1 \le i \le t$. Use the notations $\mathcal{R}_i \longrightarrow \overline{\mathcal{R}_i} = \mathcal{R}/\mathcal{P}_i$ for $1 \le i \le t$ and $\mathcal{R} \longrightarrow \mathcal{R}/\mathrm{Rad}(\mathcal{R})$ to stand for the standard maps, and these maps can be also extended to $\mathcal{R}_i^n$ and $\mathcal{R}^n$ coordinately. We can thus construct the following diagram

$$\begin{tikzcd}
(\mathcal{R}_1, \ldots, \mathcal{R}_t) \arrow[r] \arrow[d] & \mathcal{R} \arrow[d] \\
(\overline{\mathcal{R}_1}, \ldots, \overline{\mathcal{R}_t}) \arrow[r] & \mathcal{R}/\mathrm{Rad}(\mathcal{R}),
\end{tikzcd}$$

where the horizontal maps are the Chinese product CRT. It can be checked that this diagram is commutative, and the commutative diagram induces the following commutative diagram for codes with length n

$$\begin{tikzcd}
(\mathcal{C}_1, \ldots, \mathcal{C}_t) \arrow[r] \arrow[d] & \mathcal{C} \arrow[d] \\
(\overline{\mathcal{C}_1}, \ldots, \overline{\mathcal{C}_t}) \arrow[r] & (\mathcal{C} + (\mathrm{Rad}(\mathcal{R}))^n)/(\mathrm{Rad}(\mathcal{R}))^n.
\end{tikzcd} \tag{2}$$

By using this commutative diagram for codes, Lemma 10 and Corollary 17, we obtain

Theorem 18 *If $\mathcal{C} \subset \mathcal{R}^n$ is a free LCD code over any finite commutative ring $\mathcal{R}$ with $\dim(\mathcal{C}) = k$, then $\mathcal{C}/(Rad(\mathcal{R}))^n$ is also a free LCD code over $\mathcal{R}/Rad(\mathcal{R})$ with $\dim(\mathcal{C}/(Rad(\mathcal{R}))^n) = k$.*

Remark 19 For any finite commutative ring $\mathcal{R}$, $\mathcal{R}/\mathrm{Rad}(\mathcal{R})$ is a semi-simple ring over which LCD codes were studied in [4].

Recently, Carlet et al. [3] showed that any linear code over finite fields with q elements is equivalent to an LCD code only if $q \ge 4$, and their method to obtain the result is to use the system generator matrix of an equivalent code. By using Theorem 16 and transferring the method to free codes over rings, we can also present similar results for the equivalence of free codes and LCD codes over finite local commutative rings.

Definition 20 A code $\mathcal{C}'$ is called equivalent to $\mathcal{C}$ over finite commutative rings if the codewords of $\mathcal{C}'$ are obtained by permuting the coordinate positions and multiplying a unit in each coordinate position of all the codewords of $\mathcal{C}$.

Theorem 21 *Let $\mathcal{C} \subset \mathcal{R}^n$ be any free code over a finite commutative local ring $\mathcal{R}$. Assume the residue field of $\mathcal{R}$ contains at least 4 elements, then the code $\mathcal{C}$ is equivalent to an LCD code.*

Proof Assume $\dim(\mathcal{C}) = k$. Since any generator generator matrix of the free code $\mathcal{C}$ contains a nonsingular $k \times k$ submatrix by Theorem 16, $\mathcal{C}$ is equivalent to a free code generated by the matrix $(I_k, A_{k\times(n-k)})$, where I_k stands for the $k \times k$ identity matrix over $\mathcal{R}$. Consider a code $\mathcal{C}'$ generated by $(I_k, A_{k\times(n-k)})\mathrm{diag}(a_1, \ldots, a_k, 1, \ldots, 1)$, where $\mathrm{diag}(a_1, \ldots, a_k, 1, \ldots, 1)$ stands for the diagonal matrix with the first diagonal elements a_i $(1 \le i \le k)$ being units in $\mathcal{R}$ and other diagonal elements all being 1. By borrowing the proof of the main result in [3] and Theorem 7, we can show that $\mathcal{C}'$ is equivalent to an LCD code by choosing the units a_i for $1 \le i \le k$ properly, which is operated on condition that the residue field of $\mathcal{R}$ contains at least 4 elements. □

By checking the proof of Theorem 21, it is observed that the key to the theorem is that a generator matrix of a free code over finite commutative local rings contains a nonsingular submatrix. We may also demand a free code over any finite commutative ring satisfy this condition, and then get a similar result. To this end, note that if any generator matrix $G_{k\times n}$ of a free code over finite commutative rings contains a nonsingular $k \times k$ matrix, then so does any other generator matrix. By using Lemma 9 and Theorem 21, we obtain

Theorem 22 *Assume $\mathcal{R}$ is any finite commutative ring with prime ideals $\mathcal{P}_1, \ldots, \mathcal{P}_t$, and assume each field $\mathcal{R}/\mathcal{P}_i$ contains at least 4 elements. Then any free code $\mathcal{C} \subset \mathcal{R}^n$ with a generator matrix containing a nonsingular $k \times k$ submatrix is equivalent to an LCD code.*

3 LCD codes over chain rings

Theorem 7 holds particularly when $\mathcal{R}$ is a finite chain ring, and this is exactly the main result in [9], but what we are concerned is how to describe any LCD code over chain rings rather than only a free LCD code. Or equivalently, what we are concerned is whether all the possible LCD codes over chain rings can be determined. We will give a positive answer for the above question in this section, and our result is the following theorem.

Theorem 23 *Assume $\mathcal{C} \subset \mathcal{R}^n$ is a linear code with a $k \times n$ generator matrix G over a chain ring $\mathcal{R}$. Then, $\mathcal{C}$ is an LCD if and only if $\mathcal{C}$ is free and GG^T is nonsingular.*

Proof Sufficient conditions are assured by Theorem 7, and we only need to check the necessary conditions. Assume $\mathcal{C}$ is an LCD code, then from the results in [13], we may in general assume $G = D\widetilde{G}$, where $D = \mathrm{diag}(\gamma^{i_1}, \ldots, \gamma^{i_k})$ is a $k \times k$ diagonal matrix with $0 \le i_j \le \nu - 1$ for $1 \le j \le k$ and $\widetilde{G}$ is a generator matrix of a free code. Consider the linear system equations $GG^T X = D\widetilde{G}\widetilde{G}^T DX = 0$, where $X = (x_1, \ldots, x_k)^T$. Since $\mathcal{C}$ is an LCD code, it follows that $G^T X = 0$ for any solution X of $GG^T X = 0$. We state that $\widetilde{G}\widetilde{G}^T$ is nonsingular, otherwise, the linear system equations $\widetilde{G}\widetilde{G}^T X = 0$ will have a nonzero solution X_0 by Lemma 3, and we may further modify X_0 by multiplying it γ^j for suitable $j \ge 0$ such that $\gamma^j X_0 \ne 0$ and $\mathrm{ord}(\gamma^j X_0) = \nu - 1$. It follows that $\gamma^j X_0 = DY$ for some $Y \ne 0$. Thus, we get $GG^T Y = D\widetilde{G}\widetilde{G}^T DY = D\widetilde{G}\widetilde{G}^T(\gamma^j X_0) = \gamma^j D\widetilde{G}\widetilde{G}^T X_0 = 0$, and then $G^T Y = \widetilde{G}^T DY = 0$. It follows that $DY = \gamma^j X_0 = 0$ since $\widetilde{G}$ is a generator matrix of a free code, and this yields a contradiction to $DY = \gamma^j X_0 \ne 0$, and such a contradiction shows that $\widetilde{G}\widetilde{G}^T$ is nonsingular.

As a next step, we state that the matrix D is an identity matrix by showing $i_j = 0$ for any $1 \le j \le k$. Otherwise, find a $Z \in \mathcal{R}^k$ such that $\mathrm{ord}(Z) = \nu - 1$ with $DZ = 0$. The fact that $\widetilde{G}\widetilde{G}^T$ is nonsingular yields a $Y \in \mathcal{R}^k$ with $\mathrm{ord}(Y) = \mathrm{ord}(Z) = \nu - 1$ such that $Z = \widetilde{G}\widetilde{G}^T Y$. We can thus find a $X \in \mathcal{R}^k$ with $Y = DX$, then we get $0 = DZ = D\widetilde{G}\widetilde{G}^T Y = D\widetilde{G}\widetilde{G}^T DX = GG^T X$. It follows $G^T X = \widetilde{G}^T DX = 0$, and this yields $DX = Y = 0$, i.e. $\mathrm{ord}(Y) = \nu$, since $\widetilde{G}$ is a generator matrix of a free code. We then get a contradiction to $\mathrm{ord}(Y) = \nu - 1$. Thus, D is an identity matrix, and so $G = \widetilde{G}$ and $\mathcal{C}$ is free, furthermore, $GG^T = \widetilde{G}\widetilde{G}^T$ is nonsingular. □

3.1 Cyclic LCD codes over chain rings

Cyclic codes have more interesting structures than general linear codes, and Massey gave a judging criterion for a cyclic LCD code over finite fields [18] by using the generating polynomial of the code. For cyclic codes over chain rings, the detailed structure was given in [13], and in the section we will use this structure and Theorem 23 to generalize the result in [18].

Let $G(x) = G_m x^m + G_{m-1} x^{m-1} + \cdots + G_0$ with $G_m \not= 0$ and G_0 a unit be a polynomial over a ring, then define $\widetilde{G}(x) = {G_0}^{-1} x^m G(1/x)$ and call $\widetilde{G}(x)$ the *reciprocal polynomial* of $G(x)$.

Lemma 24 *[18] If $\mathcal{C} \in K^n$ is a cyclic code generated by a monic polynomial $g(x)$, i.e. $\mathcal{C} = \langle g(x) \rangle$, over a field K, then $\mathcal{C}$ is an LCD code if and only if $\widetilde{g}(x) = g(x)$ and each monic irreducible factor of $g(x)$ has the same multiplicity in $g(x)$ and in $x^n - 1$.*

Using Theorem 23 and Lemma 24, we can now describe cyclic LCD codes over chain rings.

Theorem 25 *A cyclic code $\mathcal{C} \in \mathcal{R}^n$ over a chain ring $\mathcal{R}$ with the residue field K is an LCD code if and only if $\mathcal{C} = \langle G(x) \rangle$, where $G(x)$ is monic with $G(x) | x^n - 1$, $\widetilde{G}(x) = G(x)$, and $G(x)$ and $(x^n - 1)/G(x)$ are coprime.*

Proof We first show the necessary conditions. Assume $\mathcal{C}$ is an LCD code. Then it follows that $\mathcal{C}$ is free and thus $\overline{\mathcal{C}}$ is an LCD code by Theorem 23 and Corollary 17. Thus, $\overline{\mathcal{C}} = \langle g(x) \rangle$ with $g(x)$ satisfying the conditions in Lemma 24. Assume $p = \text{char} K$ and $n = p^t n_1$ with $p \nmid n_1$ and $t \geq 0$. Write $x^n - 1 = g_1(x)^{p^t} \cdots g_i(x)^{p^t} \cdots g_r(x)^{p^t}$ with $g_i(x)$, $1 \leq i \leq r$, monic coprime irreducible polynomials in $K[x]$. Without loss of generality, we may assume $g(x) = g_1(x)^{p^t} \cdots g_i(x)^{p^t}$. By Hensel's lemma, we get $x^n - 1 = f_1(x) \cdots f_i(x) \cdots f_r(x)$ in $\mathcal{R}[x]$ such that $f_i(x)$, $1 \leq i \leq r$, are monic coprime polynomials and $\overline{f}_i(x) = g_i(x)^{p^t}$, and thus $x^n - 1 = f_1(x) \cdots f_i(x) \cdots f_r(x)$ is the unique primary factorization of $x^n - 1$ in $\mathcal{R}[x]$ [10]. Thus, $G(x) = f_1(x) \cdots f_i(x)$ is the unique monic Hensel lift of $g(x)$ such that $G(x) | x^n - 1$, $\overline{G}(x) = g(x)$ and $G(x)$ and $x^n - 1/G(x)$ being coprime. Since $x^n - 1 = \widetilde{G}(x)((x^n - 1)/\widetilde{G}(x))$ and $\overline{\widetilde{G}}(x) = \widetilde{\overline{G}}(x) = \widetilde{g}(x) = g(x)$, we get $\widetilde{G}(x)$ is also a monic Hensel lift of $g(x)$, and so $\widetilde{G}(x) = G(x)$. Finally, using the similar arguments as in the proof of [13, Theorem 4.4] and noting that $\mathcal{C}$ is free, we can obtain $\mathcal{C} = \langle G(x) \rangle$.

Conversely, assume $\mathcal{C} = \langle G(x) \rangle$ and $G(x)$ satisfies the conditions in the Theorem. Then, $\mathcal{C}$ and $\overline{\mathcal{C}} = \langle \overline{G}(x) \rangle$ have the same minimum number of generators, and thus $\mathcal{C}$ is free. To show $\mathcal{C}$ is an LCD code, it suffices to show that $\overline{\mathcal{C}}$ is an LCD code by Corollary 17. Thus, we check $\overline{G}(x)$ satisfies the conditions in Lemma 24. It is obvious that $\overline{G}(x) | x^n - 1$ and $\overline{G}(x)$ and $(x^n - 1)/\overline{G}(x)$ are coprime since $G(x)$ and $(x^n - 1)/G(x)$ are coprime. Thus, all the irreducible factors of $\overline{G}(x)$ have the same multiplicity in $\overline{G}(x)$ and in $x^n - 1$. Finally, the fact $\widetilde{G}(x) = G(x)$ yields that $\widetilde{\overline{G}}(x) = \overline{\widetilde{G}}(x) = \overline{G}(x)$. □

Example 26 As an example, we determine all the possible cyclic LCD codes $\mathcal{C} \subset \mathcal{R}^n$ over the chain ring $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{k-1}\mathbb{F}_q$, where $u^k = 0$ and $\mathbb{F}_q$ is a finite field with q elements satisfying $(n, q) = 1$, i.e, n and q are relatively prime. It was shown that any cyclic code over a chain ring has a unique *generating set in standard form* [13], and according to the proof of [1, Theorem 2.2], the generating set in standard form for a cyclic code over $\mathcal{R}$ should be $\{u^{a_0} g_{a_0}(x), u^{a_1} g_{a_1}(x), \ldots, u^{a_s} g_{a_s}(x)\}$, where $0 \leq a_0 < a_1 < \cdots < a_s \leq k - 1$, $g_{a_s}(x) | g_{a_{s-1}}(x) | \cdots | g_{a_0}(x) | x^n - 1$ and each $g_{a_i}(x) \in \mathbb{F}_q[x]$. We thus get each $g_{a_i}(x)$ is the Hensel lift of $\overline{g_{a_i}}(x) = g_{a_i}(x)$ according to the proof of [13, Theorem 4.4], i.e., each $g_{a_i}(x)$ is the Hensel lift of itself. Thus, the generating set in standard form for any free code $\mathcal{C} \subset \mathcal{R}^n$ is exactly the monic generating polynomial of $\overline{\mathcal{C}}$ over $\mathbb{F}_q$. Thus, according to the proof of Theorem 25, we obtain any cyclic LCD code $\mathcal{C}$ over $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{k-1}\mathbb{F}_q$ satisfies

$\mathcal{C} = \langle g(x) \rangle$, where $g(x) \in \mathbb{F}_q[x]$ generates a cyclic LCD code over $\mathbb{F}_q$. Or equivalently, all cyclic LCD codes over $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{k-1}\mathbb{F}_q$ have the same generating polynomials as the ones over $\mathbb{F}_q$.

4 LCD codes over principal ideal rings

A ring $\mathcal{R}$ is called a principal ideal ring if each ideal of $\mathcal{R}$ is generated by one element. Any finite principal ideal ring $\mathcal{R}$ is a Chinese product of some, say t, chain rings [5]. That is, $\mathcal{R} = CRT(\mathcal{R}_1, \ldots, \mathcal{R}_t)$ for some local rings $\mathcal{R}_i$, $1 \le i \le t$. By using this fact and Theorems 23 and 25, we can judge whether a code over a principal ideal ring is an LCD code. Note however the necessary conditions of Theorems 23 and 25 may not be right for a code over a principal ideal ring since an LCD code may not be free. See the following

Example 27 Consider a code $\mathcal{C}$ over Z_6 with a generator matrix

$$G = \begin{pmatrix} 1 & 3 & 3 \\ 0 & 4 & 4 \end{pmatrix}.$$

Then $\mathcal{C} = CRT(\mathcal{C}_1, \mathcal{C}_2)$ with $\mathcal{C}_1$ being a code over Z_2 and $\mathcal{C}_2$ being a code over Z_3, and $\mathcal{C}_1$ and $\mathcal{C}_2$ are generated by

$$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

over Z_2 and Z_3, respectively.

It can be checked that both $\mathcal{C}_1$ and $\mathcal{C}_2$ are LCD codes, and thus $\mathcal{C}$ is an LCD code over Z_6. However, It can be seen that $\mathcal{C}$ is not free and

$$GG^T = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

is not nonsingular.

For any LCD code over principal ideal rings, we can give a description as follows.

Theorem 28 *If $\mathcal{C} \subset \mathcal{R}^n$ is any LCD code over principal ideal rings $\mathcal{R}$, then $\mathcal{C}/(Rad(\mathcal{R}))^n$ is also an LCD code over $\mathcal{R}/Rad(\mathcal{R})$.*

Proof Since $\mathcal{R} = CRT(\mathcal{R}_1, \ldots, \mathcal{R}_t)$ for chain rings $\mathcal{R}_i$ and $\mathcal{C}$ is an LCD code, it follows that $\mathcal{C} = CRT(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ for LCD codes $\mathcal{C}_i$ over chain rings $\mathcal{R}_i$, $1 \le i \le t$. Thus, Theorem 23 yields that each $\mathcal{C}_i$ is a free LCD code over the chain ring $\mathcal{R}_i$ for $1 \le i \le t$, and thus each $\overline{\mathcal{C}_i}$ is an LCD code over the residue field of $\mathcal{R}_i$ for $1 \le i \le t$ by Corollary 17. It thus follows by commutative diagram (2) that $\mathcal{C}/(\mathrm{Rad}(\mathcal{R}))^n$ is an LCD code over $\mathcal{R}/\mathrm{Rad}(\mathcal{R})$. □

Based on Theorem 23, for free cyclic codes over principal ideal rings we may similarly present a judging criterion by using polynomials.

Theorem 29 *A free cyclic code $\mathcal{C} = CRT(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ over a principal ideal ring R is an LCD code if and only if $\mathcal{C} = \langle \xi(x) \rangle$ with $\xi(x)$ monic satisfying $\xi(x) | x^n - 1$ and $\xi(x)$ and $(x^n - 1)/\xi(x)$ are coprime, furthermore, $\widetilde{\xi}(x) = \xi(x)$.*

Proof Assume the free cyclic code $\mathcal{C}$ is an LCD code. Then, since $\mathcal{C} = CRT(\mathcal{C}_1, \ldots, \mathcal{C}_t)$, each $\mathcal{C}_i$, $1 \leq i \leq t$ is free and with the same minimum number of generators as $\mathcal{C}$, and also each $\mathcal{C}_i$ is a cyclic LCD code over the finite chain ring $\mathcal{R}_i$. It follows from Theorem 25 that $\mathcal{C}_i = \langle G_i(x)\rangle$, where $G_i(x) \in \mathcal{R}_i[x]$ satisfies the conditions in Theorem 25 and all the $G_i(x)$, $1 \leq i \leq t$, have the same degree. Let $\xi(x) = CRT(G_1(x), \ldots, G_t(x))$, then $\xi(x)$ is monic and has the same degree as each $G_i(x)$. It follows that $\widetilde{\xi}(x) = CRT(\widetilde{G}_1(x), \ldots, \widetilde{G}_t(x)) = CRT(G_1(x), \ldots, G_t(x)) = \xi(x)$ and $\mathcal{C} = CRT(\mathcal{C}_1, \ldots, \mathcal{C}_t) = CRT(\langle G_1(x)\rangle, \ldots, \langle G_t(x)\rangle) = \langle \xi(x)\rangle$. Since $x^n - 1 = CRT(x^n - 1, \ldots, x^n - 1)$ and each $G_i(x)|x^n - 1$, it follows that $\xi(x)|x^n - 1$. Since $G_i(x)$ and $x^n - 1/G_i(x)$ are coprime for each $1 \leq i \leq t$, it follows that $\xi(x)$ and $(x^n - 1)/\xi(x) = CRT((x^n - 1)/G_1(x), \ldots, (x^n - 1)/G_t(x))$ are coprime.

Conversely, we show that $\mathcal{C}$ is an LCD code on condition that $\mathcal{C} = \langle \xi(x)\rangle$ with $\xi(x)$ satisfying the conditions of the theorem. Since $\mathcal{C} = CRT(\mathcal{C}_1, \ldots, \mathcal{C}_t)$, it suffices to show each $\mathcal{C}_i$, $1 \leq i \leq t$, is an LCD code. Let $G_i(x) = \Phi_i(\xi(x))$, $1 \leq i \leq t$. Then, $\mathcal{C}_i = \langle G_i(x)\rangle$, and the conditions satisfied by $\xi(x)$ yield $G_i(x)$ monic, $G_i(x)|x^n - 1$ and $G_i(x)$ and $(x^n - 1)/G_i(x)$ are coprime. Further, for each $1 \leq i \leq t$, $\widetilde{G}_i(x) = \Phi_i(\widetilde{\xi}(x)) = \Phi_i(\xi(x)) = G_i(x)$. It follows that each $\mathcal{C}_i$, $1 \leq i \leq t$, is an LCD code by Theorem 25. □

5 Conclusion

We gave judging criterions on LCD codes over finite commutative rings. Particularly, free LCD codes were described by using their generator matrices over rings. Using Chinese Remainder Theorem, we gave a construction of LCD codes over semi-simple rings and presented results about the equivalence of free codes and LCD codes over finite commutative rings. In addition, all the possible LCD codes over chain rings were determined, and the judging criterion on cyclic LCD codes over finite fields was generalized to cyclic LCD codes over chain rings. Based on above results and the Chinese Remainder Theorem, we also presented results about LCD codes over principal ideal rings.

References

1. Cao Y., Cao Y.L., Fu F.W.: Matrix-product structure of constacyclic codes over finite chain rings $\mathbb{F}_{p^m}[u]/\langle u^e\rangle$. Appl. Algebra Eng. Commun. Comput. **29**(6), 455–478 (2018).
2. Carlet C., Guilley S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. **10**(1), 131–150 (2016).
3. Carlet C., Mesnager S., Tang C.M., Qi Y.F., Pellikaam R.: Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q{>}3$. IEEE Trans. Inf. Theory **64**(4), 3010–3017 (2018).
4. Dinh H.Q., Nguyen B.T., Sriboonchitta S.: Constacyclic codes over finite commutative semi-simple rings. Finite Fields Appl. **45**, 1–18 (2017).
5. Dougherty S.T., Kim J.L., Kulosman H.: MDS codes over finite principal ideal rings. Des. Codes Cryptogr. **50**, 77–92 (2009).
6. Jin L.F.: Construction of MDS codes with complementary duals. IEEE Trans. Inf. Theory **63**(5), 2843–2847 (2017).
7. Li C., Ding C., Li S.: LCD cyclic codes over finite fields. IEEE Trans. Inf. Theory **63**(7), 4344–4356 (2017).
8. Li S., Li C., Ding C., Liu H.: Two families of LCD BCH codes. IEEE Trans. Inf. Theory **63**(9), 5699–5717 (2017).
9. Liu X.S., Liu H.L.: LCD codes over finite chain rings. Finite Fields Appl. **34**, 1–19 (2015).
10. McDonald B.R.: Finite Rings with Identity. Marcel Dekker, New York (1974).
11. McDonald B.R.: Linear Algebta Over Commutative Rings. Marcel Dekker Inc., New York (1984).

12. Mesnager S., Tang C., Qi Y.: Complementary dual algebraic geometry codes. IEEE Trans. Inf. Theory **64**(4), 2390–2397 (2018).
13. Norton G.H., Salagean A.: On the structure of linear and cyclic codes over a finite chain ring. Appl. Algebra Eng. Commun. Comput. **10**, 489–506 (2000).
14. Shi M.J., Zhang Y.P.: Quasi-twisted codes with constacyclic constituent codes. Finite Fields Appl. **39**, 159–178 (2016).
15. Shi M.J., Qian L.Q., Solé P.: On self-dual negacirculant codes of index two and four. Des. Codes Cryptogr. **86**(11), 2485–2494 (2018).
16. Shi M.J., Sok L., Solé P., Calkavur S.: Self-dual codes and orthogonal matrices over large finite fields. Finite Fields Appl. **54**, 297–314 (2018).
17. Sok L., Shi M.J., Solé P.: Construction of optimal LCD codes over large finite fields. Finite Fields Appl. **50**, 138–153 (2018).
18. Yang X., Massey J.L.: The condition for a cyclic code to have a complementary dual. Discret. Math. **126**, 391–393 (1994).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.