Do non-free LCD codes over finite commutative Frobenius rings exist?

Sanjit Bhowmick1 · Alexandre Fotue-Tabue2 · Edgar Martínez-Moro3 · Ramakrishna Bandi4 · Satya Bagchi1

Received: 4 February 2019 / Revised: 24 December 2019 / Accepted: 28 December 2019 / Published online: 20 January 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
In this paper, we clarify some aspects of LCD codes in the literature. We first prove that non-free LCD codes do not exist over finite commutative Frobenius local rings. We then obtain a necessary and sufficient condition for the existence of LCD codes over a finite commutative Frobenius ring. We later show that a free constacyclic code over a finite chain ring is an LCD code if and only if it is reversible, and also provide a necessary and sufficient condition for a constacyclic code to be reversible. We illustrate the minimum Lee distance of LCD codes over some finite commutative chain rings with examples. We found some new optimal cyclic codes over $\mathbb{Z}_4$ of different lengths which are LCD codes using computer algebra system MAGMA.

Keywords Frobenius ring · Linear complementary dual code · Constacyclic code · Chain ring

Mathematics Subject Classification 94B05 · 94B15 · 94B60 · 94B99

Communicated by C. Carlet.

Ramakrishna Bandi ramakrishna@iitmnr.edu.in
Sanjit Bhowmick sanjitbhowmick392@gmail.com
Alexandre Fotue-Tabue alexfotue@gmail.com
Edgar Martínez-Moro edgar.martinez@uva.es
Satya Bagchi satya.bagchi@maths.nitdgp.ac.in

1 Department of Mathematics, National Institute of Technology Durgapur, Durgapur, India
2 Department of Mathematics, HTTC of Bertoua, University of Ngaoundéré, Yaoundé, Cameroon
3 Institute of Mathematics, University of Valladolid, Valladolid, Spain
4 Department of Mathematics, Dr. SPM International Institute of Information Technology, Naya Raipur, India
1 Introduction

A linear code $C$ is called a Linear Complementary Dual (LCD) code if $C$ meets its dual $C^\perp$ trivially. LCD codes were first introduced by Massey in [22]. He gave a characterization of LCD codes and non-LCD codes over finite fields and showed that asymptotically good LCD codes exist [22]. LCD codes have been widely applied in data storage, communication systems, consumer electronics, and cryptography. Carlet and Guilley [3] showed an application of LCD codes against side-channel attacks and fault injection attacks and presented several constructions of LCD codes. In [31], Yang and Massey gave a necessary and sufficient condition for a cyclic code to have a complementary dual code and proved that reversible cyclic codes over finite fields are LCD codes. In [23], Massey showed that some cyclic LCD codes over finite fields are BCH codes, and also constructed reversible convolutional codes which are in fact LCD codes. Tzeng and Hartmann [27] proved that the minimum distance of a class of LCD codes is greater than that given by the BCH bound.

Using the hull dimension spectra of linear codes, Sendrier showed that LCD codes meet the asymptotic Gilbert–Varshamov bound [26]. Dougherty et al. developed linear programming bound on the largest size of an LCD code of given length and minimum distance [9]. Guneri et al. studied quasi-cyclic complementary dual codes using their concatenated structure in [15] and [14]. Ding et al. constructed several families of cyclic LCD codes over finite fields and analyzed their parameters [18]. In [19], Li et al. studied a class of LCD BCH codes. Jin showed that some Reed–Solomon codes are equivalent to LCD codes [16]. In [5], the authors proved that a Maximum Distance Separable (MDS) code is equivalent to an LCD code and constructed LCD MDS codes. Boonniyoma and Jitman studied complementary dual subfield linear codes over finite fields [2]. In [6], Carlet et al. gave a new characterization and parametrization of LCD codes. It is proved in [7] that some linear codes over $\mathbb{F}_q$ for $q > 3$ are equivalent to LCD codes.

Recently, in [20], Liu and Liu studied LCD codes over finite chain rings and provided a necessary and sufficient condition for a free linear code to be an LCD code over a finite chain ring. They also gave a sufficient condition [20, Theorem 3.5] for a linear code (not necessarily free) over a finite chain ring to have an LCD. They provided an example [20, Example 2] to state that the converse of [20, Theorem 3.5] is not in general true. However, there is a mistake in their example. In the first part of this paper, we prove the converse of [20, Theorem 3.5]. This result leads to the claim that there are no non-free LCD codes over finite commutative local Frobenius rings (see Theorem 2). Also, we show that a projection and a lift of an LCD code over a finite commutative local Frobenius ring are also LCD codes. Using these results, we answered the question which is posed in the title of this paper.

Constacyclic codes are well-known generalizations of cyclic and negacyclic codes. Constacyclic codes have a rich algebraic structure and can be easily encoded and decoded using linear shift registers. These codes are used in a wide variety of technological situations, including (quantum) error-correcting codes, modern high-density data storage systems, deterministic simulations of random processes, and digital tracking systems. Constacyclic LCD codes over finite fields have also been studied (see [30] and the references therein) in literature. In the later part of this paper, we consider constacyclic LCD codes over finite chain rings. We show that a free constacyclic code $C$ over a finite chain ring is an LCD code if and only if $C$ is reversible. We also prove a necessary and sufficient condition for a constacyclic code $C$ of length $n$ over a finite chain ring to be reversible when $n$ is relatively prime to the characteristic of the finite chain ring. Finally, we provide some new optimal LCD codes over $\mathbb{Z}_4$. 
The paper is organized as follows: In Sect. 2, we provide some essential tools which are required to understand the results of further sections. In Sect. 3, we discuss LCD codes over finite commutative Frobenius rings. Finally, Sect. 4 studies the constacyclic LCD codes over finite chain rings in a more general setting by a uniform method.

2 Codes over finite commutative Frobenius rings

Throughout the paper, we will consider finite commutative rings with multiplicative unity 1 different from 0. A finite commutative ring $R$ is Frobenius if the ring $R$ seen as an $R$-module is injective. Alternatively, we can say a finite ring is Frobenius if $R/\mathcal{J}(R)$ is isomorphic to $\text{soc}(R)$ (as $R$-modules), where $\mathcal{J}(R)$ is the Jacobson radical and $\text{soc}(R)$ is the socle of the ring $R$. Recall that the Jacobson radical of the ring $R$ is the intersection of all maximal ideals of the ring $R$, and the socle of the ring $R$ is the sum of the minimal $R$-submodules. A ring is called a local ring if it has a unique maximal ideal. A principal ideal ring is a ring in which every ideal is generated by one element. A local principal ideal ring is called a chain ring.

Let $R$ be a finite ring with maximal ideals $m_1, \ldots, m_u$ and $s_1, \ldots, s_u$ their indices of stability, respectively (Recall that the index of stability of a maximal ideal $m$ of a ring is the smallest positive integer $s$ such that $m^s = m^{s+1}$). For each index $j \in \{1, 2, \ldots, u\}$ we denote the ring $R/m_j^{s_j}$ as $R_j$ and it is clear that $R_j$ is a finite local ring with maximal ideal $m_j/m_j^{s_j}$.

Then we have the ring epimorphism

$$
\Phi_j : R \rightarrow R_j := R/m_j^{s_j}
$$

and $\ker(\Phi_j) = m_j^{s_j}$ ($1 \leq j \leq u$). The ring epimorphisms $\Phi_j$ ($1 \leq j \leq u$) induce the following ring homomorphism

$$
\Phi : R \rightarrow R_1 \times \cdots \times R_u
$$

Since the maximal ideals $m_1, \ldots, m_u$ of $R$ are coprime and $\bigcap_{j=1}^u m_j^{s_j} = \{0_R\}$, then (2.2) is a ring isomorphism by the Chinese remainder theorem (see [24, p. 224]). We denote the inverse of this map by CRT and we say that $R$ is the Chinese product of rings $\{R_j\}_{j=1}^u$.

**Theorem 1** [24, p. 224] If $R$ is a Frobenius ring, then $R = \text{CRT}(R_1, R_2, \ldots, R_u)$, where $R_j$ is a local Frobenius ring for each $j \in \{1, \ldots, u\}$.

The following example shows a finite commutative local Frobenius ring which is not a chain ring. We shall use this ring to exhibit several results of the paper.

**Example 1** [10] Let $\mathcal{A}_m = \mathbb{Z}_2[u_1, u_2, \ldots, u_m]/\langle u_1^2, u_2^2, \ldots, u_m^2 \rangle$, where $\langle u_1^2, u_2^2, \ldots, u_m^2 \rangle$ denotes the ideal generated by $u_1^2, u_2^2, \ldots, u_m^2$, and $m$ is a non-negative integer. Then

$$
\mathcal{J}(\mathcal{A}_m) = \langle u_1, u_2, \ldots, u_m \rangle \text{ and } \text{soc}(\mathcal{A}_m) = \left( \prod_{i=1}^k u_i \right).
$$

Thus $\mathcal{A}_m/\mathcal{J}(\mathcal{A}_m) \cong \text{soc}(\mathcal{A}_m)$ (as $\mathcal{A}_m$-modules), so $\mathcal{A}_m$ is a finite commutative local Frobenius ring. However $\mathcal{A}_m$ is non-chain if $m > 1$. 
A linear code $C$ of length $n$ over a finite ring $R$ is an $R$-submodule of $R^n$. For each index $j$ in the set $\{1, \ldots, u\}$ and a code $C_j$ of length $n$ over $R_j$, we extend the map $\Phi$ coordinatewise to $R^n$ as

$$
\Phi : R^n \rightarrow (R_1)^n \times \cdots \times (R_u)^n,
$$

where

$$
\Phi_j : R^n \rightarrow (R_j)^n,
$$

where $\Phi_j(a_1, a_2, \ldots, a_n) = (\Phi_j(a_1), \Phi_j(a_2), \ldots, \Phi_j(a_n))$.

Then we get a code $C = \text{CRT}(C_1, C_2, \ldots, C_u) = \Phi^{-1}(C_1 \times C_2 \times \cdots \times C_u)$ over $R$, where $\Phi_j(C) = C_j$ for $1 \leq j \leq u$. We say that $C$ is the Chinese product of the codes $C_1, C_2, \ldots, C_u$. The rank of a linear code $C$ of length $n$ over $R$ is defined as

$$
\text{rank}_R(C) = \min \left\{ i \in \mathbb{N} : \text{there exists a monomorphism } C \hookrightarrow R^i \text{ as } R\text{-modules} \right\}.
$$

A linear code $C$ over $R$ is free if $C$ is isomorphic (as an $R$-module) to $R^t$ for some positive integer $t$. It is immediate that if $C$ is free then $\text{rank}_R(C) = t$, where $C \cong R^t$. A code $C$ is a linear $[n, k]$-code over $R$ if $C$ is an $R$-submodule of $R^n$ of rank $k$.

**Lemma 1** [8, Theorem 2.4] Let $C_j$ be a linear code over $R_j$ for $i = 1, 2, \ldots, u$, and $C = \text{CRT}(C_1, C_2, \ldots, C_u)$. Then

1. $|C| = \prod_{j=1}^u |C_j|$;
2. $\text{rank}_R(C) = \max \left\{ \text{rank}_{R_j}(C_j) : 1 \leq j \leq u \right\}$;
3. $C$ is a free code if and only if each $C_j$ is a free code with the same rank $\text{rank}_R(C)$.

We define an inner-product on $R^n$ as

$$
\langle \mathbf{v}, \mathbf{w} \rangle = \sum_{j=1}^n v_j w_j,
$$

where $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ and $\mathbf{w} = (w_1, w_2, \ldots, w_n)$ are elements in $R^n$. Given a linear code $C$ of length $n$ over $R$ the (euclidean) dual code of $C$ is defined as

$$
C^\perp = \{ \mathbf{u} \in R^n : \langle \mathbf{u}, \mathbf{c} \rangle = 0, \text{ for all } \mathbf{c} \in C \}.
$$

It is well known that for any code $C$ over a Frobenius ring $R$, we have $|C||C^\perp| = |R|^n$, (see [29] for a proof).

**Lemma 2** [8, Theorem 2.7] With the above notation, if $C = \text{CRT}(C_1, C_2, \ldots, C_u)$ is a code over $R$, then $C^\perp = \text{CRT}(C_1^\perp, C_2^\perp, \ldots, C_u^\perp)$.

We denote by $M_{k \times n}(R)$, the set of all $k \times n$-matrices over the ring $R$. For a matrix $A \in M_{k \times n}(R)$, the transpose of $A$ is denoted by $A^T$. We also denote the zero matrix as $0$, where the size will either be obvious from the context or specified whenever necessary. Similarly, we denote the $k \times k$ identity matrix by $I_k$. The elements $e_1, e_2, \ldots, e_k$ in $R^n$ are said to be linearly independent over $R$ if for all $(x_1, x_2, \ldots, x_k) \in R^k$ such that $x_1 e_1 + x_2 e_2 + \cdots + x_k e_k = 0$, then $x_1 = x_2 = \cdots = x_k = 0$. If the rows of a $k \times n$-matrix $A$ over $R$ are linearly independent, then we say that $A$ is a full-row-rank matrix. If there is an $n \times k$-matrix $B$ over $R$ such that $AB = I_k$, then we say that $A$ is right-invertible and $B$ is a right inverse of $A$. When $k = n$, we say that $A$ is non-singular, if the determinant $\det(A)$ is a unit of the ring $R$. Otherwise, $A$ is
Do non-free LCD codes over finite commutative Frobenius rings exist? 829

said to be singular. Note that a matrix A is invertible over R, if and only if A is non-singular in R. The following two results about full-row-rank matrices over finite commutative Frobenius rings appeared in [11].

Lemma 3 Let R be a finite commutative Frobenius ring. A matrix \( A \in M_{k \times n}(R) \) is full-row-rank if and only if A is right-invertible.

Lemma 4 Let R be a finite commutative Frobenius ring and A a matrix over R. The following statements are equivalent:

1. A is invertible.
2. A is non-singular.
3. A is full-row-rank.

Therefore, the following result follows from a typical linear algebra argument.

Corollary 1 Let R be a finite commutative Frobenius ring. A matrix \( A \in M_{k \times n}(R) \) is not full-row-rank if and only if there is a non-zero element \( x \) in \( R^k \) such that \( Ax^T = 0 \).

3 Characterization of LCD codes over finite commutative Frobenius rings

In [20, Theorem 3.5], it is proved that any linear code \( C \) over a chain ring \( R \) with a generator matrix \( G \) is an LCD code if \( GG^T \) is invertible, and on the other hand, it is also stated that the converse of [20, Theorem 3.5] is in general not true by citing the example [20, Example 2]. However, there is a mistake in that example (as \((2, 0, 0, 2, 0) \) is in \( C \cap C^\perp \)). From [20, Corollary 3.6], if \( C \) is free then the converse of [20, Theorem 3.5] is true. Therefore, in order to prove the converse of [20, Theorem 3.5], it is enough to prove that any LCD code over a finite commutative local Frobenius ring \( R \) is free.

Definition 1 Let \( R \) be a finite commutative local Frobenius ring. An \( R \)-module \( C \) of rank \( k \) is projective if there is an \( R \)-module \( M \) such that \( R^k \) and \( C \oplus M \) are isomorphic (as \( R \)-modules).

Remark 1 Note that, with the notation in the above definition, if \( A \) and \( B \) are two \( R \)-modules and \( A \oplus B \) is a free \( R \)-module, then both \( A \) and \( B \) are projective modules.

Lemma 5 [17, Theorem 2.] Any projective module over a local ring is free.

In the following result, we prove that there does not exist any non-free LCD code over a finite commutative local Frobenius ring.

Theorem 2 Over a finite commutative local Frobenius ring, any LCD code is a free code.

Proof Let \( C \) be an LCD code of length \( n \) over a commutative local Frobenius ring \( R \), then \( C \oplus C^\perp \) is a direct summand in \( R^n \). Since \( R \) is a Frobenius ring, the code \( C \) satisfies \( |C| \times |C^\perp| = |R|^n \) (see [29]), and hence \( C \oplus C^\perp = R^n \). Therefore \( C \oplus C^\perp \) is a free \( R \)-module. By Remark 1, it follows that \( C \) is a projective \( R \)-module. Now \( C \) is a finitely generated projective \( R \)-module and \( R \) is a local ring, thus by Lemma 5, \( C \) is free as an \( R \)-module. □

It follows from Theorem 2 and [20, Corollary 3.6] that there does not exist any non-free LCD code over a finite commutative local Frobenius ring. We now show that the converse of Theorem 2 does not hold in general. To illustrate this, we cite the following example.
Example 2 Let $C$ be a linear code over $\mathbb{Z}_4$ with generator matrix 

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 2 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 \\
\end{bmatrix}
$$

Clearly $C$ is free but $C$ is not an LCD code since as $(0, 0, 0, 2, 2, 0) \in C \cap C^\perp$.

Proposition 1 Let $R$ be a finite commutative local Frobenius ring. If $C$ is a linear code over $R$ with generator matrix $G$ such that $GG^T$ is non-singular, then $C$ is free.

Proof Suppose that $C$ is not a free $R$-module, then $G$ is not full-row-rank. From Lemma 3, it follows that $G$ is not right-invertible and therefore, $GG^T$ is a singular matrix. \(\square\)

Corollary 2 Let $R$ be a finite commutative local Frobenius ring. A linear code $C$ over $R$ with generator matrix $G$ is an LCD code, if and only if $GG^T$ is non-singular.

Proof Suppose that $C$ is an LCD code with generator matrix $G$ and $c \in C$. From Theorem 2, $C$ is a free $R$-module and $c$ can be written as $c = vG$ for some element $v$ in $R^k$. If $GG^T$ is singular, by Corollary 1, there is a non-zero element $u$ in $R^k$ such that $uGG^T = 0$. Now since $uG$ is a non-zero element in $C$ we have that $(uG)c^T = (uG)(vG)^T = uGG^Tv^T = 0v^T = 0$ and hence $uG$ is also an element in $C^\perp$. It follows that $C \cap C^\perp \neq \{0\}$, i.e., $C$ is not an LCD code, which is a contradiction. Therefore $GG^T$ is a non-singular matrix.

Suppose now that $GG^T$ is a non-singular matrix. Then from Proposition 1, $C$ is a free $R$-module. If we consider $c \in C \cap C^\perp$, then $c \in C$, which implies that there is a $u \in R^k$ such that $c = uG$. Therefore

$$
(cG)(GG^T)^{-1}G = uGG^T(GG^T)^{-1}G = uG = c. \quad (3.1)
$$

We also have that $c \in C^\perp$, hence it follows that $cG^T = 0$. Thus

$$
(cG^T)(GG^T)^{-1}G = 0(GG^T)^{-1}G = 0. \quad (3.2)
$$

From (3.1) and (3.2), it follows that $c = 0$, and hence $C$ is an LCD code. \(\square\)

Example 3 The linear code generated by 

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 2 & 1 \\
0 & 1 & 0 & 0 & 1 & 2 & 3 \\
0 & 0 & 1 & 0 & 0 & 3 & 2 \\
0 & 0 & 0 & 1 & 2 & 3 & 1 \\
\end{bmatrix}
$$

over $\mathbb{Z}_4$ is an LCD $[8, 4^4]$ code.

This code is a free code with rank 4.

Let $S$ and $R$ be two finite commutative local Frobenius rings and let $f : S \rightarrow R$ be a ring epimorphism. A linear $[n, k]$-code $C$ over $S$ is a lift of the linear $[n, k]$-code $C'$ over $R$ by $f$ if $C' = f(C)$, where

$$f(C) = \{ (f(c_1), f(c_2), \ldots, f(c_n)) : (c_1, c_2, \ldots, c_n) \in C \}.$$

We call the code $C'$ the projection of $C$ by $f$.

Lemma 6 Let $S$ and $R$ be two finite commutative local Frobenius rings with $S^\times$ and $R^\times$ the unit groups of $S$ and $R$, respectively. Then $f(S^\times) = R^\times$ for any ring epimorphism $f : S \rightarrow R$. \(\square\)
Proof If \( b \in f(S^x) \), then \( b = f(a) \), where \( a \in S^x \). Since \( a \in S^x \), there is an element \( a' \) in \( S^x \) such that \( aa' = 1_S \). Now, setting \( b' = f(a') \), we get that \( bb' = f(aa') = f(1_S) = 1_R \). Thus \( b \in R^x \) and so \( f(S^x) \subseteq R^x \).

On the other hand, for any \( b \in R^x \) there is an element \( a \in S \) such that \( b = f(a) \) as \( f \) is injective. If \( a \notin S^x \), then \( a \) is a nilpotent element in \( S \) because \( S \) is a finite commutative local Frobenius ring. Thus there is a positive integer \( n \) such that \( a^n = 0 \), so it follows that \( b^n = f(a^n) = 0_R \), a contradiction. Therefore, \( a \in S^x \). Hence \( b \in f(S^x) \) and so, \( R^x \subseteq f(S^x) \).

The following result is a generalization of [20, Theorem 3.9] to a finite commutative local Frobenius ring \( S \) and a ring epimorphism \( f : S \to R \).

Theorem 3 Let \( S \) and \( R \) be two finite commutative local Frobenius rings. The projection of an LCD \([n, k]\)-code over \( S \) by the ring epimorphism \( f : S \to R \) is also an LCD \([n, k]\)-code over \( R \).

Proof Let \( C \) be an LCD \([n, k]\)-code over \( S \) with generator matrix \( G \). From Theorem 2, \( C \) is a free code (as an \( S \)-module). Therefore, the projection \( f(C) \) of \( C \) is also a free \([n, k]\)-code over \( R \) with a generator matrix \( f(G) \). Now consider the element

\[
\det(f(GG^T)) = \det(f(G)f(G^T)).
\]

From Lemma 6 and Theorem 2, it follows that \( \det(f(G)f(G^T)) \) is a unit in \( R \), and hence \( f(C) \) is an LCD \([n, k]\)-code over \( R \). \( \square \)

The result revisits and extends [20, Theorem 3.10] as follows.

Theorem 4 Let \( S \) and \( R \) be two finite commutative local Frobenius rings. Then a lift of an LCD \([n, k]\)-code over \( R \) by ring epimorphism \( f : S \to R \) is also an LCD \([n, k]\)-code over \( S \).

Proof Let \( C' \) be an LCD \([n, k]\)-code over \( R \) with a generator matrix \( G \). Since \( f : S \to R \) is a ring-epimorphism, there is a full-row-rank matrix \( G \) over \( S \) such that \( G = f(G) \). Consider a free \([n, k]\)-code \( C \) over \( S \) with generator matrix \( G \),

\[
\det(f(GG^T)) = \det(f(G)f(G^T)).
\]

Thus by Lemma 6 and Theorem 2 it follows that \( GG^T \) is non-singular. Therefore \( C \) is an LCD code. \( \square \)

The map

\[
\pi_m : \sum_{A \subseteq \{1, 2, \ldots, m\}} c_A \prod_{i \in A} u_i \mapsto F_2^r,
\]

is a ring-epimorphism and \( A_m \) is a finite commutative local Frobenius ring (see Example 1).

From Theorems 3 and 4, a linear code \( C \) over \( A_m \) is an LCD code, if and only if \( \pi_m(C) \) is a binary LCD code. From [6, Theorem 1], if \((1, 1, \ldots, 1) \notin \pi_m(C)^\perp \) then \( C \) is an LCD code if and only if there exists a basis \( \{c_1, c_2, \ldots, c_k\} \) of \( C \) such that \( \{c_i, c_j\} = \delta_{i,j} \), for all \( 1 \leq i, j \leq k \).
Example 4 Consider the linear \([n, k]\)-code \(C\) over \(\mathcal{A}_m\) with generator matrix
\[
\begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & \lambda_{1,1} & \cdots & \lambda_{1,n-k} \\
0 & 1 & 0 & \cdots & 0 & \lambda_{2,1} & \cdots & \lambda_{2,n-k} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & \cdots & 0 & 1 & \lambda_{k-1,1} & \cdots & \lambda_{k-1,n-k} \\
0 & \cdots & 0 & 0 & \lambda_{k,1} & \cdots & \lambda_{k,n-k}
\end{pmatrix},
\]
where \(n-k\) is an even integer and \(\pi_m(\lambda_{i,j}) = 1\), for all \(1 \leq i \leq k, 1 \leq j \leq n - k\). From Theorem 4, \(C\) is an LCD code as \(\pi_m(C)\) is a binary LCD code by [6, Theorem 1].

Theorem 5 A linear code \(C = \text{CRT}(C_1, C_2, \ldots, C_u)\) over \(R = \text{CRT}(R_1, R_2, \ldots, R_u)\), where \(R_j\) is a finite commutative local Frobenius ring for all \(1 \leq j \leq u\), is an LCD code over \(R\) if and only if, \(C_j\) is an LCD code over \(R_j\) for all \(1 \leq j \leq u\).

Proof The map \(\Phi : R \rightarrow R_1 \times \cdots \times R_u\) is a ring-isomorphism, and by Lemma 2, it follows that
\[
C \cap C^\perp = \text{CRT}(C_1 \cap C_1^\perp, C_2 \cap C_2^\perp, \ldots, C_u \cap C_u^\perp).
\]
Thus \(C\) is an LCD code over \(R\) if and only if, \(C_j\) is an LCD code over \(R_j\) for all \(1 \leq j \leq u\).
\(\square\)

Remark 2 From Lemma 6 and Theorem 5, it is easy to see that an LCD code \(C = \text{CRT}(C_1, C_2, \ldots, C_u)\) over the ring \(R = \text{CRT}(R_1, R_2, \ldots, R_u)\) is non-free, if and only if there are \(1 \leq j_1 < j_2 \leq u\) such that \(\text{rank}_{R_{j_1}}(C_{j_1}) \neq \text{rank}_{R_{j_2}}(C_{j_2})\).

Example 5 Let \(C_1\) be an LCD code over \(\mathbb{Z}_3\) with generator matrix
\[
\begin{pmatrix}
1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1
\end{pmatrix},
\]
and \(C_2\) an LCD code over \(\mathbb{Z}_5\) with generator matrix
\[
\begin{pmatrix}
1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 4 & 2
\end{pmatrix}.\]
From Remark 2, the Chinese product of \(C_1\) and \(C_2\) is the non-free LCD code \(C\) over \(\mathbb{Z}_{15}\) with generator matrix
\[
\begin{pmatrix}
1 & 0 & 6 & 1 & 1 \\
0 & 1 & 0 & 4 & 7 \\
0 & 0 & 10 & 10 & 10
\end{pmatrix},
\]
as \(\text{rank}_{\mathbb{Z}_3}(C_1) = 3 \neq 2 = \text{rank}_{\mathbb{Z}_5}(C_2)\). But \(C\) is a projective module over \(\mathbb{Z}_{15}\).

We are now ready to answer the question on the title of our paper: “Do non-free LCD codes over a finite commutative Frobenius ring \(R\) exist?” It straightforward from Example 5 that “non-free LCD codes over a finite commutative Frobenius ring \(R\) exist, and they are projective modules over \(R\).”

4 Constacyclic LCD codes over finite chain rings

From now on \(R\) will denote a finite chain ring (and hence a Frobenius ring) with residue field \(\mathbb{F}_q\), \(\gamma\) a unit in \(R\), and \(n\) a positive integer relatively prime to \(q\). The projection \(\pi : R \rightarrow \mathbb{F}_q\) extends naturally to a projection \(R[X] \rightarrow \mathbb{F}_q[X]\) as follows: \(\pi(f) = \sum_i \pi(f_i)X^i\) for \(f =
\[ \sum_i f_i X^i; \text{ also to a projection } R^n \to (\mathbb{F}_q)^n \text{ as follows: } \pi(e) = (\pi(c_0), \pi(c_1), \ldots, \pi(c_{n-1})) \text{ for } e = (c_0, c_1, \ldots, c_{n-1}). \text{ Thus for any non-empty subset } C \text{ of } R^n, \pi(C) = \{ \pi(e) \mid e \in C \}. \]

Recall that a linear code \( C \) of length \( n \) over \( R \) is \( \gamma \)-constacyclic if \( (\gamma c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C \), whenever \( (c_0, c_1, \ldots, c_{n-1}) \in C \). \( C \) is called cyclic and negacyclic, respectively, when \( \gamma \) is 1 and \(-1\). A constacyclic code of length \( n \) over \( R \) is non-repeated root \( \gamma \)-constacyclic if each \( \gamma \)-constacyclic code over \( R \) are identified to ideals of \( R[X]/(X^n - \gamma) \) via the \( R \)-module isomorphism

\[ \mathcal{T} : R^n \to \mathcal{R}[X]/(X^n - \gamma) \]

\[ (c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}, \]

where \( x := X + (X^n - \gamma) \). In this section, we deal with non-repeated root \( \gamma \)-constacyclic LCD codes of length \( n \) over \( R \).

Let \( k \in \{0, 1, 2, \ldots, n\} \) and \( f := f_0 + f_1 X + \cdots + f_k X^k \) be a polynomial of degree \( \deg(f) := k \) over \( R \). We denote by \( M_k(f) \), an \( (n-k) \times n \)-matrix defined by:

\[
M_k(f) = \begin{pmatrix}
0 & f_0 & f_1 & \cdots & f_k & 0 & 0 & \cdots & 0 \\
0 & f_0 & f_1 & \cdots & f_k & 0 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & \cdots & 0 & f_0 & f_1 & \cdots & f_k & 0 \\
0 & \cdots & 0 & 0 & f_0 & f_1 & \cdots & f_k
\end{pmatrix}.
\]

(4.1)

Obviously, if \( f_0 \) is a unit in \( R \), then the rank of \( M_k(f) \) is \( n-k \). Note that for any free \( \gamma \)-constacyclic code \( C \) over \( R \) of rank \( n-k \), there is only one monic polynomial \( g \) of degree \( k \) dividing \( X^n - \gamma \) in \( \mathcal{R}[X] \) whose \( M_k(g) \) is a generator matrix for \( C \). This polynomial \( g \) is called the generator polynomial of \( C \). A free \( \gamma \)-constacyclic code of length \( n \) over \( R \) with generator polynomial \( g \) is denoted by \( \mathcal{P}(R ; n ; g) \). Conventionally, \( \mathcal{P}(R; n; g) = \{0\} \), if \( \deg(g) \geq n \). Thus \( X^n - \gamma \) is the generator polynomial of \( \{0\} \).

From now on, \( g \) denotes a monic polynomial over \( R \) with \( g(0) \) a unit in \( R \), and the non-zero element \( \gamma \) in \( \mathcal{F}(R) \) is the remainder of the Euclidean division of \( X^n \) by \( g \).

From [21, Theorem 5.2.], the quotient ring \( \mathcal{R}[X]/(X^n - \gamma) \) is a principal ideal ring, if either \( R \) is a field, or \( X^n - \pi(\gamma) \) is free-square. Recall that a polynomial over the finite field \( \mathbb{F}_q \) is called square-free, if it has no multiple irreducible factors in its decomposition. Of course, \( X^n - \pi(\gamma) \) is free-square as \( \gcd(n, q) = 1 \). From [25, Theorem 2.7], if \( g \in \mathcal{R}[X] \) is monic and \( \pi(g) \) is square-free, then \( g \) factors uniquely into monic, coprime basic-irreducible polynomials. For any polynomial \( f \) in \( \mathbb{F}_q[X] \) dividing \( X^n - \pi(\gamma) \) [24, Theorem XIII.4], there exists a unique polynomial \( g \in \mathcal{R}[X] \) such that \( \pi(g) = f \) and \( g \) divides \( X^n - \gamma \). The polynomial \( g \) is called the Hensel lift of \( f \).

**Lemma 7** [12, Lemma 3.1 (3)] Let \( g_1 \) and \( g_2 \) be monic polynomials over \( R \) dividing \( X^n - \gamma \). Then

\[
\mathcal{P}(R; n ; g_1) \cap \mathcal{P}(R; n ; g_2) = \mathcal{P}(R; n ; \mu(g_1, g_2)),
\]

where \( \mu(g_1, g_2) \) denotes the Hensel lift of \( \text{lcm}(\pi(g_1), \pi(g_2)) \) to \( \mathcal{R}[X] \).

For a polynomial \( f(X) \) of degree \( r \), \( f^*(X) \) denotes its reciprocal polynomial and is given by \( f^*(X) = X^r f\left(\frac{1}{X}\right) \). A polynomial \( f(X) \) is self-reciprocal, if \( f^*(X) = f(X) \). Consider

\[^1\text{lcm}(\pi(g_1), \pi(g_2)): \text{the least common multiple of } \pi(g_1), \pi(g_2).\]
the permutation $\Phi : R^n \to R^n$ defined as $\Phi((a_0, a_1, \ldots, a_{n-1})) = (a_{n-1}, a_{n-2}, \ldots, a_0)$. Recall that a linear code $C$ of length $n$ over $R$ is reversible if $\Phi(C) = C$. Obviously,

$$\Phi(\mathcal{P}(R; n; g)) = \mathcal{P}(R; n; \hat{g}^*) \tag{4.3}$$

On the other hand, for any $\gamma$-constacyclic code $C = \mathcal{P}(R; n; g)$, it is well-know that

$$C^\perp = \Phi(\mathcal{P}(R; n; \hat{g}^*)) \tag{4.4}$$

where $\hat{g}(X)g(X) = X^n - \gamma$. This leads to the following result.

**Proposition 2** Let $g(X)$ be a monic polynomial of degree $k$ and $g(x)$ divides $X^n - \gamma$. If $C = \mathcal{P}(R; n; g)$, then $C^\perp = \mathcal{P}(R; n; \hat{g}^*)$, where $\hat{g}(X)g(X) = X^n - \gamma$.

From the precedent result, we have $C^\perp = \mathcal{P}(R; n; \hat{g}^*)$ and $\hat{g}^*(X)$ divides $X^n - \gamma^{-1}$. For this, we have the following result.

**Proposition 3** The dual code of a $\gamma$-constacyclic code over $R$ is $\gamma^{-1}$-constacyclic.

Obviously, both $\{0\}$ and $R^n$ are $\gamma$-constacyclic codes for any unit $\gamma$ in $R$. Inversely, we have the following result.

**Lemma 8** Let $C$ be a free code of length $n$ over $R$. If $C$ is both $\alpha$-constacyclic and $\beta$-constacyclic for $\alpha, \beta$ units in $R$ with $\pi(\alpha) \neq \pi(\beta)$, then either $C = \{0\}$ or $C = R^n$.

**Proof** Assume that $C \neq \{0\}$. There exists a polynomial $g := g_0 + g_1X + \cdots + g_{k-1}X^{k-1} + X^k$ with $k < n$ such that $C = \mathcal{P}(R; n; g)$. Then the word $c := (0, \ldots, 0, g_0, g_1, \ldots, g_{k-1}, 1)$ belongs to $C$. Since $C$ is both $\alpha$-constacyclic and $\beta$-constacyclic, $c_\alpha := (\alpha, 0, \ldots, 0, g_0, g_1, \ldots, g_{k-1}) \in C$ and $c_\beta := (\beta, 0, \ldots, 0, g_0, g_1, \ldots, g_{k-1}) \in C$. Thus $\alpha c_\beta - \beta c_\alpha = (\alpha - \beta)(0, 0, \ldots, 0, g_0, g_1, \ldots, g_{k-1})$. Now $\pi(\alpha) \neq \pi(\beta)$ and $C$ is linear over $R$, therefore $c' := (0, 0, \ldots, 0, g_0, g_1, \ldots, g_{k-1}) \in C$. By continuing this, we get $(0, \ldots, 0, 1) \in C$ as $g_0$ is a unit in $R$. By constacyclicity of $C$, it follows that $C = R^n$. \qed

**Corollary 3** If $\pi(\gamma^2) \neq 1$, then any free $\gamma$-constacyclic code of length $n$ over $R$ is an LCD code.

**Proof** Assume that $\pi(\gamma^2) \neq 1$, and let $C$ be a free $\gamma$-constacyclic code of length $n$ over $R$. Then by Proposition 3, $C^\perp$ is a $\gamma^{-1}$-constacyclic code. Thus, $C \cap C^\perp$ is both $\gamma$-constacyclic and $\gamma^{-1}$-constacyclic. Therefore, by Lemma 8, $C \cap C^\perp = \{0\}$, i.e., $C$ is an LCD code, as $C \cap C^\perp$ can not be $R^n$, when $\pi(\gamma^2) \neq 1$. \qed

Thus, in order to obtain all $\gamma$-constacyclic LCD codes, we need to consider only the case when $\pi(\gamma^2) = 1$. Moreover, when $\pi(\gamma^2) = 1$, the dual code of a $\pi(\gamma)$-constacyclic code over $\mathbb{F}_q$ is $\pi(\gamma)$-constacyclic.

**Lemma 9** Let $C$ be an $\alpha$-constacyclic code of length $n$ generated by $f$ over $\mathbb{F}_q$ with $\alpha^2 = 1$. Then the following assertions are equivalent.

1. $C$ is an LCD code;
2. $f$ is self-reciprocal;
3. $C$ is reversible.
Theorem 6 Let $C$ be a $\gamma$-constacyclic code of length $n$ over $R$ and $g$ its generator polynomial. Then $C$ is an LCD code if and only if $\pi(C)$ is both $\pi(\gamma)$-constacyclic and an LCD code.

The following result generalizes a particular case of [4, Theorem 2.1].

**Theorem 6** Let $C$ be a $\gamma$-constacyclic code of length $n$ over $R$ and $g$ its generator polynomial. Then $C$ is an LCD code if and only if $C$ is reversible.

**Proof** Let $C = \mathcal{P}(\mathbb{F}_q; n; g)$. Then from Proposition 2, $C^\perp = \mathcal{P}(\mathbb{F}_q; n; \hat{g}^*)$. Since $\gamma^2 = 1$, $g^*$ divides $X^n - \gamma$. We have from Lemma 7 that $C \cap C^\perp = \mathcal{P}(\mathbb{F}_q; n; \gamma g^*)$. Therefore, $g^*$ divides $X^n - \gamma$. We have from Lemma 7 that $C \cap C^\perp = \mathcal{P}(\mathbb{F}_q; n; \gamma g^*)$. Then $C$ is an LCD code and $\gamma^2 = 1$ if and only if $\mu(g, \hat{g}^*) = X^n - \gamma$. This implies that $\mu(g, \hat{g}^*) = g g^*$. Since $g g^* = X^n - \gamma$, it follows that $\gamma^2 = 1$. By Equation (4.3), $C$ is reversible.

Conversely, if $C$ is reversible, then $\pi(C)$ is also reversible. From Lemmas 9 and 10, $C$ is an LCD code. Since $C$ is reversible, we have $g^* = g$. But $g \hat{g} = X^n - \gamma$ and $g g^* \hat{g}^* = X^n - \gamma^{-1}$. So $X^n - \gamma = X^n - \gamma^{-1}$. Hence $\gamma^2 = 1$. 

**Remark 4** Let $n$ be an odd positive integer, $k$ an integer, and $p$ a prime such that $p$ does not divide $n$. In [13], the factorization of $X^n - 1$ in $\mathbb{Z}_{p^k+1}[X]$ is deduced from the factorization of $X^n - 1$ in $\mathbb{Z}_{p}[X]$ by the Hensel Lemma. Inversely, the factorization of $X^n - 1$ in $\mathbb{Z}_{p^k}[X]$ is deduced from the factorization of $X^n - 1$ in $\mathbb{Z}_{p^k+1}[X]$ modulo $p^k$. Moreover, if $\gamma$ is a unit in $\mathbb{Z}_{p^k+1}$ such that $\gamma^2 = 1$, $g$ is a factor of $X^n - 1$ in $\mathbb{Z}_{p^k+1}[X]$. Then $\gamma g(\gamma X) = (\gamma X)^n - 1 = \gamma(X^n - \gamma)$, hence by Theorem 6, $\mathcal{P}(\mathbb{Z}_{p^k+1}; n; g\gamma)$ is a $\gamma$-constacyclic LCD code, and from Theorem 3, it follows that $\mathcal{P}(\mathbb{Z}_{p^k}; n; \pi_k(g\gamma))$ is a $\pi_k(\gamma)$-constacyclic LCD code, since $\pi_k(\mathcal{P}(\mathbb{Z}_{p^k+1}; n; g\gamma)) = \mathcal{P}(\mathbb{Z}_{p^k}; n; \pi_k(g\gamma))$, where $\pi_k : \mathbb{Z}_{p^k+1} \rightarrow \mathbb{Z}_{p^k}$ is the reduction modulo $p^k$.

We will now provide some examples to illustrate our results. We used the Magma Computer Algebra System [28] in our computations. We have got some good codes, some optimal known codes, and some new optimal codes over $\mathbb{Z}_4$ [1]. In the following examples, $d_H$ and $d_L$ represent the Hamming and Lee distances, respectively.
Example 6  The factorization of $X^7 - 1$ over $\mathbb{Z}_4$ into a product of basic irreducible polynomials over $\mathbb{Z}_4$ is given by

$$X^7 - 1 = (X - 1)(X^3 + 2X^2 + X + 3)(X^3 + 3X^2 + 2X + 3).$$

Let $f(X) = X^3 + 2X^2 + X + 3$ and $g(X) = X^3 + 3X^2 + 2X + 3$. From Theorem 6, we have

- The cyclic code $P(\mathbb{Z}_4; 7; (X - 1))$ is an LCD code and it is reversible. This is a $[7, 46, 2]$ optimal code.
- The cyclic code $P(\mathbb{Z}_4; 7; f(X))$ is not an LCD code, since $f(X)$ is not self-reciprocal.
- The cyclic code $P(\mathbb{Z}_4; 7; f(X)g(X))$ is an LCD code, since $f(X)g(X)$ is self-reciprocal.

This code has minimum Lee distance 7 but has only 4 codewords.

Note that if $C$ is a $\gamma$-constacyclic of an odd length over $\mathbb{Z}_4$, then $C$ is an LCD code if and only if $C$ is reversible.

Example 7  The factorization of $X^{15} - 1$ over $\mathbb{Z}_4$ into a product of basic irreducible polynomials over $\mathbb{Z}_4$ is given by

$$X^{15} - 1 = (X - 1)(X^2 + X + 1)(X^4 + X^3 + X^2 + X + 1)(X^4 + 2X^2 + 3X + 1) (X^4 + 3X^3 + 2X^2 + 1).$$

The self-reciprocal polynomials and the LCD cyclic codes generated by those self-reciprocal polynomials are shown in the following table:

| Generators (self-reciprocal) of LCD cyclic code C | $[n, d_L, d_L']$ | Remarks |
|-------------------------------------------------|-----------------|---------|
| $g_1 = X - 1$                                    | [15, 4^{15}, 2] |         |
| $g_2 = X^4 + X + 1$                              | [15, 4^{14}, 2] |         |
| $g_3 = (X - 1)(X^2 + X + 1)$                     | [15, 4^{14}, 2] |         |
| $g_5 = X^4 + X^2 + X + 1$                        | [15, 4^{13}, 2] |         |
| $g_6 = (X^2 + X + 1)(X^4 + X^3 + X^2 + X + 1)$   | [15, 4^{12}, 4] | Good    |
| $g_7 = (X - 1)(X^2 + X + 1)(X^4 + X^3 + X^2 + X + 1)$ | [15, 4^{12}, 4] |         |
| $g_8 = (X^4 + 2X^2 + 3X + 1)(X^4 + 3X^2 + 2X + 1)$ | [15, 4^{11}, 3] |         |
| $g_9 = (X - 1)(X^2 + 2X^2 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$ | [15, 4^{10}, 6] | Good    |
| $g_{10} = (X^2 + X + 1)(X^4 + 2X^3 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$ | [15, 4^{9}, 3] |         |
| $g_{11} = (X - 1)(X^2 + X + 1)(X^4 + 2X^3 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$ | [15, 4^{8}, 6] |         |
| $g_{12} = (X^4 + 2X^2 + 3X + 1)(X^4 + X^3 + 2X^2 + 1)(X^4 + X^2 + X^3 + X + 1)$ | [15, 4^{7}, 5] |         |
| $g_{13} = (X - 1)(X^2 + 2X^3 + 3X + 1)(X^4 + 3X^2 + 2X + 1)(X^4 + X^2 + X^3 + X + 1)$ | [15, 4^{6}, 10] | Good    |
| $g_{14} = (X^2 + X + 1)(X^4 + 2X^3 + 3X + 1)(X^4 + 3X^2 + 2X^2 + 1)(X^4 + X^3 + X^2 + X + 1)$ | [15, 4^{5}, 15] |         |

Example 8  The factorization of $X^9 - 1$, $X^{17} - 1$, $X^{31} - 1$ and $X^{63} - 1$ over $\mathbb{Z}_4$ into a product of basic irreducible polynomials are given by

$$X^9 - 1 = (X - 1)(X^2 + X + 1)(X^6 + X^3 + 1),$$

$$X^{17} - 1 = (X - 1)(X^8 + 2X^6 + 3X^5 + X^4 + 3X^2 + 2X^2 + 1) (X^8 + X^7 + 3X^6 + 3X^4 + 3X^2 + X + 1),$$

$$X^{31} - 1 = h_1h_2h_3h_4h_5h_6h_7,$$ and

$$X^{63} - 1 = g_1g_2 \cdots g_{13},$$

where

$$h_1 = (X - 1),$$

$$h_2 = (X^5 + 3X^2 + 2X + 3),$$

$$h_3 = (X^5 + 2X^4 + X^3 + 3),$$
\[ h_4 = (X^5 + 2X^4 + 3X^3 + X^2 + 3X + 3), \]
\[ h_5 = (X^5 + 3X^4 + X^2 + 3X + 3), \]
\[ h_6 = X^5 + X^4 + 3X^3 + X + 3), \]
\[ h_7 = (X^5 + X^4 + 3X^3 + 2X^2 + 2X + 3), \]
\[ g_1 = (X - 1), \]
\[ g_2 = (X^2 + X + 1), \]
\[ g_3 = (X^3 + 2X^2 + X + 3), \]
\[ g_4 = (X^3 + 3X^2 + 2X + 3), \]
\[ g_5 = (X^6 + 2X^3 + 3X + 1), \]
\[ g_6 = (X^6 + X^3 + 1), \]
\[ g_7 = (X^6 + 2X^5 + 3X^4 + X^2 + X + 1), \]
\[ g_8 = (X^6 + 2X^5 + X^4 + 3X + 1), \]
\[ g_9 = (X^6 + 3X^5 + 2X^3 + 1), \]
\[ g_{10} = (X^6 + 3X^5 + 2X^4 + X^2 + X + 1), \]
\[ g_{11} = (X^6 + 3X^5 + X^3 + 2X^2 + 2X + 1), \]
\[ g_{12} = (X^6 + X^5 + X^4 + 2X^2 + 3X + 1), \]
\[ g_{13} = (X^6 + X^5 + 3X^4 + 3X^2 + 2X + 1). \]

In the following table, we list cyclic LCD codes over \( \mathbb{Z}_4 \) of different lengths and their generators. It is noted that some of the codes (which are LCD codes) are good known codes, and some are new optimal codes over \( \mathbb{Z}_4 \) [1].

| Generators of C | \([n, 4^6, d_L]\) | Remarks |
|-----------------|-------------------|---------|
| \((X - 1)(X^6 + X^3 + 1)\) | \([9, 4^6, 6]\) | Good |
| \((X^6 + X^3 + 1)\) | \([9, 4^6, 3]\) | Good |
| \((X - 1)(X^2 + X + 1)\) | \([9, 4^6, 2]\) | Good |
| \((X^8 + X^7 + 3X^6 + 3X^4 + 3X^2 + X + 1)\) | \([17, 4^7, 7]\) | Optimal |
| \((X - 1)(X^8 + X^7 + 3X^6 + 3X^4 + 3X^2 + X + 1)\) | \([17, 4^8, 8]\) | Optimal |
| \(h_{1h_{2h_{3h_{4h_{h_{7}}}}}h_{7}}\) | \([31, 4^{10}, 16]\) | Optimal |
| \(h_{2h_{3h_{h_{6}}}h_{6}}\) | \([31, 4^{11}, 12]\) | Optimal |
| \(h_{1h_{h_{6}}}h_{6}\) | \([31, 4^{20}, 8]\) | Optimal |
| \(h_{2h_{3}}\) | \([31, 4^{21}, 6]\) | Optimal |
| \(g_{2g_{3g_{4g_{5g_{6g_{7g_{9g_{10g_{12g_{13}}}}}}}}}}\) | \([63, 4^{13}, 36]\) | Optimal |
| \(g_{1g_{3g_{4g_{5g_{6g_{7g_{9g_{10g_{12g_{13}}}}}}}}}}\) | \([63, 4^{14}, 34]\) | Optimal |
| \(g_{3g_{4g_{5g_{6g_{7g_{8g_{10g_{11g_{12g_{13}}}}}}}}}}\) | \([63, 4^{15}, 21]\) | Optimal |
| \(g_{1g_{8g_{10g_{11g_{12g_{13}}}}}}\) | \([63, 4^{20}, 18]\) | Optimal |
| \(g_{18g_{5g_{6g_{7g_{8g_{9g_{13}}}}}}}\) | \([63, 4^{32}, 16]\) | Optimal |
| \(g_{1g_{18g_{2g_{3g_{4g_{5g_{6g_{10g_{13}}}}}}}}}\) | \([63, 4^{24}, 14]\) | Optimal |
| \(g_{1g_{2g_{3g_{4g_{5g_{6g_{12}}}}}}}\) | \([63, 4^{37}, 12]\) | Optimal |
| \(g_{1g_{2g_{3g_{4g_{10g_{12}}}}}}\) | \([63, 4^{42}, 10]\) | Optimal |
| \(g_{2g_{2g_{3g_{4g_{5g_{12}}}}}}\) | \([63, 4^{37}, 9]\) | Optimal |
| \(g_{3g_{3g_{4g_{5g_{6g_{11g_{13}}}}}}}\) | \([63, 4^{43}, 7]\) | Optimal |
Example 9 The factorization of $X^9 - 1$ over $\mathbb{Z}_8$ into a product of basic irreducible polynomials over $\mathbb{Z}_8$ is given by

$$X^9 - 1 = (X - 1)(X^2 + X + 1)(X^6 + X^3 + 1).$$

All three factors of $X^9 - 1$ over $\mathbb{Z}_8$ are self-reciprocal polynomials in $\mathbb{Z}_8[X]$ and hence all cyclic codes of length 9 over $\mathbb{Z}_8$ are LCD codes and so reversible.

| Generators of $C$ | $[n, 4^k, d_H]$ |
|-------------------|------------------|
| $(X - 1)$         | $[9, 8^0, 2]$    |
| $(X^6 + X^3 + 1)$ | $[9, 8^1, 3]$    |
| $(X^2 + X + 1)$   | $[9, 4^1, 2]$    |
| $(X - 1)(X^6 + X^3 + 1)$ | $[9, 8^2, 6]$ |
| $(X - 1)(X^2 + X + 1)$ | $[9, 8^0, 3]$ |
| $(X^2 + X + 1)(X^6 + X^3 + 1)$ | $[9, 8^1, 9]$ |

Example 10 The factorization of $X^{15} - 1$ over $\mathbb{Z}_8$ into a product of basic irreducible polynomials over $\mathbb{Z}_8$ is given by $X^{15} - 1 = (X - 1)(X^2 + X + 1)(X^4 + X^3 + X^2 + X + 1)(X^4 + 4X^3 + 6X^2 + 3X + 1)(X^4 + 3X^3 + 6X^2 + 4X + 1)$. Out of 1 and $X^{15} - 1$, there are 14 self-reciprocal polynomials dividing $X^{15} - 1$ in $\mathbb{Z}_8[X]$ and they are:

$g_1 = X^2 + X + 1$,

$g_2 = (X - 1)(X^2 + X + 1)$,

$g_3 = X^4 + 3X^3 + 6X^2 + 4X + 1$,

$g_5 = (X - 1)(X^4 + 3X^3 + 6X^2 + 4X + 1)$,

$g_6 = (X^2 + X + 1)(X^4 + 3X^3 + 6X^2 + 4X + 1)$,

$g_7 = (X - 1)(X^2 + X + 1)(X^4 + 3X^3 + 6X^2 + 4X + 1)$,

$g_8 = (X^4 + 4X^3 + 6X^2 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$,

$g_9 = (X - 1)(X^4 + 4X^3 + 6X^2 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$,

$g_{10} = (X^2 + X + 1)(X^4 + 4X^3 + 6X^2 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$,

$g_{11} = (X - 1)(X^2 + X + 1)(X^4 + 4X^3 + 6X^2 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$,

$g_{12} = (X^4 + 4X^3 + 6X^2 + 4X + 1)(X^4 + 4X^3 + 6X^2 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$,

$g_{13} = (X - 1)(X^4 + 4X^3 + 6X^2 + 4X + 1)(X^4 + 4X^3 + 6X^2 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$,

$g_{14} = (X^2 + X + 1)(X^4 + 4X^3 + 6X^2 + 4X + 1)(X^4 + 4X^3 + 6X^2 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1)$.

From Remark 4, for all $\gamma \in \{1; 3; 5; 7\}$ the nontrivial $\gamma$-constacyclic code $\mathcal{P}(\mathbb{Z}_8; 15; g_{i, \gamma})$, is an LCD code, for all $1 \leq i \leq 14$, where $g_{i, \gamma}(X) = \begin{cases} \gamma g_i(\gamma X), & \text{if } i \text{ is odd;} \\ g_i(\gamma X), & \text{otherwise.} \end{cases}$

Hence there are exactly 56 nontrivial constacyclic LCD codes of length 15 over $\mathbb{Z}_8$.

5 Conclusion

In this paper, we have done an extensive study of LCD codes over finite commutative Frobenius rings. We have first corrected a wrong result given in [20], which led to the claim that “there do not exist non-free LCD codes over finite commutative local Frobenius rings.” We then answered the question posed in the title of this paper. We have also obtained a necessary and sufficient condition for any linear code over a finite commutative Frobenius ring to be an LCD code. We also characterized non-repeated root constacyclic LCD codes over finite chain rings. We computed some new optimal codes over $\mathbb{Z}_4$, which are cyclic LCD codes over $\mathbb{Z}_4$. 
Do non-free LCD codes over finite commutative Frobenius rings exist? 839

Acknowledgements The first author of the paper would like to thank the Ministry of Human Resource and Development India for financial support to carry out this work. The third author is partially funded by the Spanish State Research Agency (AEI) under Grant PGC2018-096446-B-C21.

References
1. Aydin N., Asamov T.: http://www.asamov.com/Z4Codes/CODES/ShowCODESTablePage.aspx.
2. Boonniyoma K., Jitman S.: Complementary dual subfield linear codes over finite fields. ArXiv:1605.06827 [cs.IT] (2016).
3. Carlet C., Güneri C., Özbudak F., Ozkaya B., Solé P.: On linear complementary pairs of codes. IEEE Trans. Inf. Theory 64(10), 6583–6589 (2018).
4. Carlet C., Mesnager S., Tang C.: Euclidean and Hermitian LCD MDS codes. Des. Codes Cryptogr. 86(11), 2606–2618 (2018).
5. Dougherty S.T., Liu H.: Independence of vectors in codes over rings. Des. Codes Cryptogr. 71, 201–227 (2014).
6. Dougherty S.T., Yildiz B., Karadeniz S.: Codes over $\mathbb{F}_q$, Gray maps and their binary images. Finite Fields Appl. 17, 205–219 (2011).
7. Fan Y., Ling S., Liu H.: Matrix product codes over finite commutative Frobenius rings. Des. Codes Cryptogr. 71, 201–227 (2014).
8. Fotue-Tabue A., Martínez-Moro E., Blackford T.: On polycyclic codes over a finite chain ring. Adv. Math. Commun. https://doi.org/10.3934/amc.2020028 (2019).
9. Gary M.G.: An approach to Hensel’s lemma. Ir. Math. Soc. Bull. 47, 15–21 (2001).
10. Kaplansky I.: Projective modules. Ann. Math. 68(107), 337–342 (1958).
11. Li C., Ding C., Li S.: LCD cyclic codes over finite fields. IEEE Trans. Inf. Theory 63(9), 5699–5717 (2017).
12. Löffler N.: Linear codes with complementary duals meet the Gilbert-Varshamov bound. Discret. Math. 285(1), 345–357 (2004).
13. Massey J.L.: Linear codes with complementary duals. Discret. Math. 106(107), 337–342 (1992).
14. Massey J.L.: Reversible codes. Inf. Control 7(3), 369–380 (1964).
15. McDonald B.R.: Finite Rings with Identity. Marcel Dekker, New York (1974).
16. Norton G.H., Salagean A.: On the structure of linear and cyclic codes over finite chain rings. Appl. Algebra Eng. Commun. Comput. 10, 489–506 (2000).
17. Sendrier N.: Linear codes with complementary duals. IEEE Trans. Inf. Theory 63(9), 5699–5717 (2017).
18. Tzeng K., Hartmann C.: On the minimum distance of certain reversible cyclic codes. IEEE Trans. Inf. Theory 16(5), 644–646 (1970).
19. Wieb J., John C., Catherine P.: The Magma algebra system I. The user language, computational algebra and number theory (London, 1993). J. Symb. Comput. 24(3–4), 235–265 (1997).
20. Wood J.: Duality for modules over finite rings and applications to coding theory. Am. J. Math. 121, 555–575 (1999).
30. Wu Y., Yue Q.: Factorizations of binomial polynomials and enumerations of LCD and self-dual constacyclic codes. IEEE Trans. Inf. Theory 65(3), 1740–1751 (2019).

31. 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.