Designs, Codes and Cryptography (2023) 91:695–708
https://doi.org/10.1007/s10623-022-01120-5

LCP of group codes over finite Frobenius rings

Xiusheng Liu[1] · **Hualu Liu**[2]

Received: 14 November 2021 / Revised: 18 May 2022 / Accepted: 5 September 2022 /
Published online: 7 October 2022

Abstract
A pair (C, D) of group codes in $R[G]$ is called a linear complementary pair (abbreviated to LCP) if $C \oplus D = R[G]$, where R is a finite Frobenius ring, and G is a finite group. We provide a necessary and sufficient condition for a pair (C, D) of group codes in $R[G]$ to be LCP. Furthermore, we prove that if (C, D) is an LCP of group codes in $R[G]$, then C and $D^{\perp}$ are permutation equivalent.

Keywords Finite Frobenius rings · LCP of group codes · Code equivalence

Mathematics Subject Classification 94B15 · 94B60 · 11T71

1 Introduction

Linear complementary pairs of codes over finite fields which are a class of special properties have been of interest and extensively studied due to their rich algebraic structure and wide applications in cryptography. LCP of codes were introduced in [15], and then they were further studied in [3] and [4]. They showed that these pairs of codes can help improve the security of the information processed by sensitive devices, especially against so-called side-channel attacks (SCA) and fault injection attacks (FIA). The most generic and efficient known protection against SCA is achieved with masking: every sensitive data (that is, every data processed by the algorithm from which a part of the secret key can be deduced) is bitwise added with a uniformly distributed random vector of the same length or several ones, called globally a mask. If the sensitive data and the mask belong respectively to two supplementary subspaces C and D of a larger vector space, it is possible to deduce the sensitive data from the

Communicated by J.-L. Kim.

✉ Xiusheng Liu
lxs6682@163.com

Hualu Liu
hwlulu@aliyun.com

[1] School of Science and Technology, College of Arts and Science, Hubei Normal University, Huangshi 435109, Hubei, China

[2] School of Science, Hubei University of Technology, Wuhan 430068, Hubei, China

resulting masked data. And it is shown that the level of resistance against both SCA and FIA depends on $d_{LCP}(C, D) = \min\{d(C), d(D^{\perp})\}$ in which is called the security parameter, where $d(C)$ is the minimum distance of the code C and $d(D^{\perp})$ is the dual distance of the code D. This method is called Direct Sum Masking (DSM), and the pair (C, D) is called a complementary pair of codes. Note that the linear complementary dual (LCD) codes amount to the special case when $D = C^{\perp}$, in which case the security parameter is simply the minimum distance of C. We refer to [15] for further information on complementary pairs of codes over finite fields and their uses.

Let $\mathbb{F}_q$ be the finite field with $q = p^m$, where p is a prime and $m \geq 1$ is an integer. Carlet et al. [4] showed that if (C, D) is an LCP of codes, where C and D are both cyclic or $2D$ cyclic codes of length n over $\mathbb{F}_q$ and $\gcd(n, q) = 1$, then C and $D^{\perp}$ are permutation equivalent. In [9], Güneri et al. showed that the same result holds if C and D are mD cyclic codes for $m \in \mathbb{N}$. If G is any finite group, a right ideal of $\mathbb{F}_q[G]$ is called a group code. In [2], Borello et al. obtained the most general statement for any finite group (also without a restriction on the order of the group) by showing that if (C, D) is LCP of group codes (2-sided ideals) in $\mathbb{F}_q[G]$, then C and $D^{\perp}$ are permutation equivalent. Just recently, Gü̈neri et al. [8], this result has been extended to finite chain rings. Namely, they proved that for an LCP of group codes (C, D) in $\widetilde{R}[G]$, where $\widetilde{R}$ is a finite chain ring and G is any finite group, C and $D^{\perp}$ are permutation equivalent. Note in particular that this implies $d(C) = d(D^{\perp})$. Hence, there is an LCP of 2-sided group codes over finite chain rings which has as good a security parameter as the 2-sided group code with the best minimum distance.

The purpose of this paper is to examine LCP of group codes over finite Frobenius rings. In Sect. 2, we recall the necessary background materials on finite Frobenius rings R, linear codes, group codes and LCP of codes. Then we give a decomposition of $R[G]$ by using the Chinese Remainder Theorem. In Sect. 3, we first give two necessary and sufficient conditions for a pair of linear codes over finite local Frobenius rings to be LCP. Then we give a characterization of LCP of group codes in $\mathcal{R}[G]$, where $\mathcal{R}$ is a finite local Frobenius ring and G is any finite group. In addition, we show that if (C, D) is an LCP of group codes in $\mathcal{R}[G]$, then C and $D^{\perp}$ are permutation equivalent. By means of the results of the Sect. 3, in Sect. 4, we give a characterization of LCP of group codes in $R[G]$, where R is a finite Frobenius ring and G is any finite group. Our main contribution is the extension of the result in [8] to finite Frobenius rings. Namely, we shown that if (C, D) is an LCP of group codes in $R[G]$, then C and $D^{\perp}$ are permutation equivalent. Hence the security parameter for an LCP of group codes (C, D) in $R[G]$ is simply $d(C)$.

2 Preliminaries

Throughout the work we shall assume that all rings are commutative, finite and have a multiplicative unity.

2.1 Finite Frobenius rings

In this subsection, we first recall definitions and properties of finite Frobenius rings R, necessary for the development of this work. For more details, we refer to [5, 6, 13, 14, 16]. Then we will give a decomposition of $R[G]$ for a finite group G.

A finite commutative ring R is called a *Frobenius ring* if the R-module R is injective. Alternatively, we can say a finite commutative ring is Frobenius if $R/J(R)$ is isomorphic

to soc(R), where $J(R)$ is the Jacobson radical and soc(R) is the socle of the ring R. Recall that the Jacobson radical is the intersection of all maximal ideals in the ring and the socle of the ring is the sum of the minimal R-submodules. A ring is a local ring if it has a unique maximal ideal.

Throughout this paper, let R denote a Frobenius ring. Then there exist ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ are relatively prime in pairs and $\prod_{j=1}^{s} \mathfrak{m}_j = \{0\}$. By the ring version of the Chinese Remainder Theorem, the canonical ring homomorphism $\Lambda : R \to \bigcap_{j=1}^{s} R/\mathfrak{m}_j$, defined by $r \to (r + \mathfrak{m}_1, \ldots, r + \mathfrak{m}_s)$, is an isomorphism. Denote the rings $R/\mathfrak{m}_j$ by R_j for $1 \leq j \leq s$. Then

$$R = R_1 \times R_2 \times \cdots \times R_s.$$

By the Chinese Remainder Theorem the inverse map is an isomorphism. We denote the inverse of this map by CRT. For Frobenius rings we can say more. Namely, we have the following theorem which can be found in [5].

Theorem 2.1 *Let R be a Frobenius ring, then*

$$R \cong \mathrm{CRT}(R_1, R_2, \ldots, R_s),$$

where R_j is a local Frobenius ring for all $1 \leq j \leq s$.

Let $G = \{g_1, \ldots, g_n\}$ be a finite group and denote by $R[G]$ (or $R_j[G]$) the group ring of G over R (or R_j). Hence the elements of $R[G]$ (or $R_j[G]$) are of the form $\sum_{i=1}^{n} a_{g_i} g_i$ where $a_{g_i} \in R$ (or $\sum_{i=1}^{n} a_{g_i}^{(j)} g_i$ where $a_{g_i}^{(j)} \in R_j$). It is clear that the map $\Psi : R[G] \to R^n$, defined by $\sum_{i=1}^{n} a_{g_i} g_i \to (a_{g_1}, a_{g_2}, \ldots, a_{g_n})$, is a R-module isomorphism.

We define two operations over $R_1[G] \times \cdots \times R_s[G]$ as follows:

$$\left(\sum_{i=1}^{n} a_{g_i}^{(1)} g_i, \ldots, \sum_{i=1}^{n} a_{g_i}^{(s)} g_i\right) + \left(\sum_{i=1}^{n} b_{g_i}^{(1)} g_i, \ldots, \sum_{i=1}^{n} b_{g_i}^{(s)} g_i\right)$$
$$= \left(\sum_{i=1}^{n} (a_{g_i}^{(1)} + b_{g_i}^{(1)}) g_i, \ldots, \sum_{i=1}^{n} (a_{g_i}^{(s)} + b_{g_i}^{(s)}) g_i\right),$$

and

$$\left(\sum_{i=1}^{n} a_{g_i}^{(1)} g_i, \ldots, \sum_{i=1}^{n} a_{g_i}^{(s)} g_i\right) \cdot \left(\sum_{i=1}^{n} b_{g_i}^{(1)} g_i, \ldots, \sum_{i=1}^{n} b_{g_i}^{(s)} g_i\right)$$
$$= \left(\sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{g_j}^{(1)} b_{g_j^{-1} g_i}^{(1)}\right) g_i, \ldots, \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{g_j}^{(s)} b_{g_j^{-1} g_i}^{(s)}\right) g_i\right),$$

where $a_{g_i}^{(j)}, b_{g_i}^{(j)} \in R_j$ for all $1 \leq j \leq s$.

It is easy to prove that the $R_1[G] \times \cdots \times R_s[G]$ is an algebra.

Theorem 2.2 *Let $R = R_1 \times R_2 \times \cdots \times R_s$ is a Frobenius ring where R_j is a local Frobenius ring for $1 \leq j \leq s$. If G is a finite group, then*

$$R[G] \cong R_1[G] \times \cdots \times R_s[G].$$

Proof Suppose that $G = \{g_1, \ldots, g_n\}$. Then we define a map Φ from $R[G]$ to $R_1[G] \times \cdots \times R_s[G]$ as follows:

$$\begin{aligned} \Phi : R[G] &\longrightarrow R_1[G] \times \cdots \times R_s[G] \\ \sum_{i=1}^{n} r_{g_i} g_i &\longrightarrow \left(\sum_{i=1}^{n} r_{g_i}^{(1)} g_i, \ldots, \sum_{i=1}^{n} r_{g_i}^{(s)} g_i \right), \end{aligned}$$

where $r_{g_j} = (r_{g_j}^{(1)}, \ldots, r_{g_j}^{(s)}) \in R$ and $r_{g_i}^{(j)} \in R_j$ for $1 \le i \le n$ and $1 \le j \le s$.

It is easy to check that Φ is an isomorphism from $R[G]$ to $R_1[G] \times \cdots \times R_s[G]$. □

From now on, we denote the inverse of the map Φ by CRT. The above theorem can be rewritten in the following form.

Theorem 2.3 *Let $R = R_1 \times R_2 \times \cdots \times R_s$ is a Frobenius ring where R_j is a local Frobenius ring for $1 \le j \le s$. If G is a finite group, then*

$$R[G] = \mathrm{CRT}(R_1[G], \ldots, R_s[G]).$$

2.2 Linear codes, group codes and LCP of codes

In this subsection, we recall the definitions and properties of linear codes, group codes, and LCP of codes (see [1, 2, 8, 17]).

A nonempty subset $C \subseteq R^n$ is called a *linear code* of length n over a finite Frobenius ring R if it is a R-submodule of R^n.

For two vectors $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ in R^n, we define the Euclidean inner product as $[\mathbf{a}, \mathbf{b}]$ to be $[\mathbf{a}, \mathbf{b}] = \sum_{i=1}^{n} a_i b_i$.

Let C be a linear code over R. We define the Euclidean dual code of C as

$$C^{\perp} = \{\mathbf{a} \in R^n \mid [\mathbf{a}, \mathbf{b}] = 0 \text{ for all } \mathbf{b} \in C\}.$$

Remark 2.4 In [17], it is proved that for any linear code C of length n over a finite Frobenius ring R,

$$|C| \cdot |C^{\perp}| = |R|^n.$$

Definition 2.5 Let C and D be two linear codes of length n over R. If $C \cap D = \{\mathbf{0}\}$ and $C + D = R^n$, or equivalently $C \oplus D = R^n$, then we call such (C, D) an linear complementary pair (LCP) of codes over R.

Note that the linear complementary dual (LCD) codes amount to the special case when $D = C^{\perp}$.

A right ideal of $R[G]$ (or $R_j[G]$) is called a group code in $R[G]$ (or $R_j[G]$) (see [8] for group codes over finite chain rings). Throughout this paper, ideals will be 2-sided and they will be referred to as group codes.

In addition, the group ring $R[G]$ (or $R_j[G]$) carries a symmetric non-degenerate G-invariant bilinear form $\langle \cdot, \cdot \rangle$ which is defined by

$$\langle a, b \rangle = \begin{cases} 1 & if\ a = b = 0, \\ 0 & otherwise. \end{cases}$$

Here G-invariance means that $\langle ug, vg \rangle = \langle u, v \rangle$, for all $u, v \in R[G]$ and all $g \in G$. Via the R-module isomorphism $R[G] \cong R^{|G|}$, the above form corresponds to the usual Euclidean

inner product. With respect to this form we may define the dual code $C^{\perp}$ of a group code C in $R[G]$ as usual. Obviously, the dual code $C^{\perp}$ of a group code C is also a group code in $R[G]$.

Definition 2.6 Let C and D be two group codes in $R[G]$. If $C \cap D = \{\mathbf{0}\}$ and $C + D = R[G]$, or equivalently $C \oplus D = R[G]$, then we call such (C, D) an linear complementary pair (LCP) of group codes in $R[G]$.

Two group codes C_1 and C_2 over $R[G]$ (or $R_j[G]$) are permutation equivalent provided there is a permutation of coordinates which sends C_1 to C_2. Then two group codes C_1 and C_2 are permutation equivalent if and only if there a permutation matrix P such that $C_2 = C_1 P$, where $C_1 P = \{\mathbf{y} | \mathbf{y} = \mathbf{x}P \text{ for } \mathbf{x} \in C_1\}$.

3 LCP of group codes over finite local Frobenius rings

In this section, let $\mathcal{R}$ be a finite local Frobenius ring with unique maximal ideal $\mathfrak{m}$. We know that $\mathbb{F}_q = \mathcal{R}/\mathfrak{m}$ is a field. Assume that the characteristic of the field is p with $q = p^m$. Define

$$\mu : \mathcal{R} \longrightarrow \mathbb{F}_q = \mathcal{R}/\mathfrak{m}, \quad r \mapsto r + \mathfrak{m} = \mu(r), \quad \text{for any } r \in \mathcal{R}.$$

This homomorphism from $\mathcal{R}$ onto $\mathbb{F}_q = \mathcal{R}/\mathfrak{m}$ can be extended naturally to a homomorphism from $\mathcal{R}^n$ onto $\mathbb{F}_q^n$. For an element $\mathbf{c} \in \mathcal{R}^n$, let $\mu(\mathbf{c})$ be its image under this homomorphism. Let C be a code of length n over $\mathcal{R}$. We define $\mu(C) = \{\mu(\mathbf{c}) | \mathbf{c} \in C\}$.

We have the following chain of ideals:

$$\mathcal{R} = \mathfrak{m}^0 \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots \supset \mathfrak{m}^e = \{0\}.$$

The number e is the minimal such that $\mathfrak{m}^e = \{0\}$. This number is the nilpotency index of $\mathfrak{m}$. See [14, p. 84] for a proof of this fact. The following lemma will be used in the proof of Proposition 3.13.

Lemma 3.1 *Let $\mathcal{R}$ be a finite local Frobenius ring and let $\mathfrak{m}$ be the unique maximal ideal. Then there exists a $\delta \in \mathfrak{m}$ such that $\delta \neq 0$, and $\delta\alpha = 0$ for any $\alpha \in \mathfrak{m}$, where e is the nilpotency index of $\mathfrak{m}$.*

Proof By the definition of the nilpotency index of $\mathfrak{m}$, we have $\mathfrak{m}^{e-1} \neq \{0\}$. Thus, there exists a $\delta \in \mathfrak{m}^{e-1} \subset \mathfrak{m}$ such that $\delta \neq 0$. Again by $\mathfrak{m}^e = \{0\}$, i.e., $\mathfrak{m}^{e-1}\mathfrak{m} = \{0\}$, we have also $\delta\alpha = 0$ for any $\alpha \in \mathfrak{m}$. □

The following result has appeared in [14].

Lemma 3.2 *Let $\mathcal{R}$ be a finite local Frobenius ring and let $\mathfrak{m}$ be the unique maximal ideal. Then $\mathfrak{m}$ contains all non-units of $\mathcal{R}$.*

Consider the free $\mathcal{R}$-module $\mathcal{R}^n$ of rank n. Any element $\mathbf{u} = (u_1, \ldots, u_n)$ of $\mathcal{R}^n$ is also called a vector, and we let $\mathbf{0}$ denote the zero vector.

Definition 3.3 Let $\mathbf{u}_j = (u_{j1}, \ldots, u_{jn}) \in \mathcal{R}^n$, where $j = 1, \ldots, s$ and s is a positive integer. The vectors $\mathbf{u}_1, \ldots, \mathbf{u}_s$ are said to be linearly dependent if there exist $(t_1, \ldots, t_s)$ in the set difference $\mathcal{R}^s \setminus \{\mathbf{0}\}$ such that $t_1\mathbf{u}_1 + \cdots + t_s\mathbf{u}_s = \mathbf{0}$; otherwise, $\mathbf{u}_1, \ldots, \mathbf{u}_s$ are said to be linearly independent.

If an $\mathcal{R}$-submodule of $\mathcal{R}^n$ is generated by vectors $\mathbf{u}_1, \ldots, \mathbf{u}_s$ which are linearly independent, then it is a free $\mathcal{R}$-submodule of rank s and we say that $\mathbf{u}_1, \ldots, \mathbf{u}_s$ form a basis of the free $\mathcal{R}$-submodule.

Let $M_{m\times l}(\mathcal{R})$ be the set of all $m \times l$ matrices over $\mathcal{R}$. For $A \in M_{m\times l}(\mathcal{R})$, A^T denotes the transpose of the matrix A. We denote the $m \times m$ identity matrix by I_m, or simply I if the size is clear from the context.

Let $A = (a_{ij})_{m\times l}$ be a matrix over $\mathcal{R}$. If the rows of A are linearly independent, then we say that A is a full-row-rank (FRR) matrix. If there is an $l \times m$ matrix B over $\mathcal{R}$ such that $AB = I$, then we say that A is *right-invertible* and B is a right inverse of A. If $m = l$ and the determinant $\det A$ is a unit of $\mathcal{R}$, then we say that A is *nonsingular*.

The following two results about full-row-rank matrices over $\mathcal{R}$ appear in [7].

Lemma 3.4 *$A \in M_{m\times l}(\mathcal{R})$ is FRR if and only if A is right-invertible.*

Lemma 3.5 *Let A be in $M_{m\times m}(\mathcal{R})$. The following statements are equivalent:*

(1) A is invertible.
(2) A is nonsingular.
(3) A is FRR.

The next corollary follows from a typical linear algebra argument.

Corollary 3.6 *Let $A \in M_{m\times m}(R)$ and let $\mathbf{x} = (x_1, \ldots, x_m)$, where x_i's are variables. Then the linear system of equations $A\mathbf{x}^T = \mathbf{0}$ has only the zero solution if and only if A is nonsingular.*

Let C be a linear code of length n over $\mathcal{R}$. Define a generator matrix of C as a matrix G_C with rows being a generating set of C with the smallest size. In particular, when C is a free code, then the rows of any generator matrix G_C are a group of basis elements of C, and so the number of rows of any generator matrix of a free code C is uniquely determined.

Definition 3.7 We define the rank of a code C over $\mathcal{R}$, denoted by $\mathrm{rank}_{\mathcal{R}}(C)$, to be the minimum number of generators of C.

Let C be a linear code over $\mathcal{R}$ with a generator matrix G_C. We denote by $k(C)$ the number of rows of the generator matrix G_C. Clearly, $\mathrm{rank}_{\mathcal{R}}(C) = k(C)$.

The following definition and remark can be found in [1].

Definition 3.8 An $\mathcal{R}$-module A of rank l is projective if there is an $\mathcal{R}$-module B such that $\mathcal{R}^l$ and $A \oplus B$ are isomorphic (as $\mathcal{R}$-modules).

Remark 3.9 Let P and Q be two $\mathcal{R}$-modules. If $P \oplus Q$ is free, then P and Q are projective.

Lemma 3.10 [11, Theorem 2] *Any projective module over a local ring is free.*

Lemma 3.11 *Let C and D be linear codes of length n over $\mathcal{R}$. If (C, D) is an LCP of codes, then C and D are free.*

Proof Since (C, D) is an LCP of codes over $\mathcal{R}$, we have $C \oplus D = \mathcal{R}^n$ by Definition 2.5. Therefore, the $\mathcal{R}$-module $C \oplus D$ is free. By Remark 3.9, we know that C and D are projective. Since $\mathcal{R}$ is a finite local Frobenius ring, by Lemma 3.10, C and D are free. □

In the following, we first give characterization of LCP of codes over $\mathcal{R}$, and will play an important role in this section.

Before stating our result about LCP of codes over $\mathcal{R}$, we need the following lemma to appear in [10].

Lemma 3.12 [10, Theorem 2.10] *Let C be a free code of length n over $\mathcal{R}$ with generator matrix G_C, and let D be a free code of length n over $\mathcal{R}$ with parity-check matrix H_D. Then (C, D) is LCP if and only if* $\text{rank}_R(C)+\text{rank}_R(D) = n$ *and the matrix $G_C H_D^T$ is nonsingular.*

Proposition 3.13

(1) *Let C and D be free codes of length n over $\mathcal{R}$. Then (C, D) is an LCP of codes over $\mathcal{R}$ if and only if $(\mu(C), \mu(D))$ is an LCP of codes over $\mathbb{F}_q$.*
(2) *(C, D) is an LCP of group codes in $\mathcal{R}[G]$ if and only if $(\mu(C), \mu(D))$ is an LCP of group codes in $\mathbb{F}_q[G]$.*

Proof (1) Let $\mathbf{a} \in \mu(C)\cap\mu(D)$. Then there are $\mathbf{c} \in C$ and $\mathbf{d} \in D$ such that $\mathbf{a} = \mu(\mathbf{c}) = \mu(\mathbf{d})$. This means that $\mu(\mathbf{c} - \mathbf{d}) = \mathbf{0}$. Thus $(\mathbf{c} - \mathbf{d}) \in \mathfrak{m} \times \cdots \times \mathfrak{m}$. Therefore, there exists a $\mathbf{u} = (u_1, \ldots, u_n) \in \mathfrak{m} \times \cdots \times \mathfrak{m}$ such that $\mathbf{c} - \mathbf{d} = \mathbf{u}$. By Lemma 3.1, there exists a $\delta \in \mathfrak{m}$ such that $\delta \neq 0$ and $\delta\alpha = 0$ for any $\alpha \in \mathfrak{m}$. Thus, we have

$$\delta\mathbf{c} - \delta\mathbf{d} = \mathbf{0},$$

which implies that $\delta\mathbf{c} = \delta\mathbf{d} \in C\cap D$. Since (C, D) is an LCP of codes over $\mathcal{R}$, we have $\delta\mathbf{c} = \mathbf{0}$. Thus, $\mathbf{c} \in \mathfrak{m} \times \cdots \times \mathfrak{m}$. Otherwise, let $\mathbf{c} = (c_1, c_2, \ldots, c_n)$. Without loss of generality, we assume that $c_1 \notin \mathfrak{m}$. Then, by Lemma 3.2, there exists a $v \in \mathcal{R}$ such that $c_1 v = 1$. It follows that $v\delta\mathbf{c} = (\delta, v\delta c_2, \ldots, v\delta c_n) \neq \mathbf{0}$, which leads a contradiction. Therefore, $\mathbf{a} = \mu(\mathbf{c}) = \mathbf{0}$, i.e., $\mu(C) \cap \mu(D) = \{\mathbf{0}\}$.

Next, for any $\mathbf{a} \in \mathbb{F}_q^n$, by $C + D = \mathcal{R}^n$, and μ is surjective, there are $\mathbf{c} \in C$ and $\mathbf{d} \in D$ such that $\mathbf{a} = \mu(\mathbf{c}) + \mu(\mathbf{d})$. Hence, $\mu(C) + \mu(D) = \mathbb{F}_q^n$.

Summarizing, we have shown that $(\mu(C), \mu(D))$ is an LCP of codes over $\mathbb{F}_q$.

Conversely, assume that the G_C is a generator matrix of C and the H_D is a parity-check matrix of D, it is easy to see that $\mu(G_C H_D^T) = \mu(G_C) \cdot \mu(H_D)^T$. Since $(\mu(C), \mu(D))$ is an LCP of codes over $\mathbb{F}_q$, $\dim_{\mathbb{F}_q}(\mu(C)) + \dim_{\mathbb{F}_q}(\mu(D)) = n$, and $\mu(G_C) \cdot \mu(H_D)^T$ is nonsingular by [12, Theorem 2.6]. Thus, $\text{rank}_R(C) + \text{rank}_R(D) = n$, and $G_C H_D^T$ is nonsingular. According to Lemma 3.12, (C, D) is an LCP of codes over $\mathcal{R}$.

(2) Similar to the proof of Proposition 3.2 (ii) in [8], we can easily prove that a ideal $C \subset R[G]$ is mapped to a ideal $\mu(C) \subset \mathbb{F}_q[G]$. The rest follows by part (1). □

Remark 3.14 Güneri et al. [8, Proposition 3.2 (i) and (ii)], proved $(\mu(C), \mu(D))$ is an LCP of codes (or LCP of group codes) over $\mathbb{F}_q$ (or $\mathbb{F}_q[G]$) if (C, D) is an LCP of codes (or LCP of group codes) over chain ring $\widetilde{R}$ (or $\widetilde{R}[G]$). In the above Proposition 3.13, we prove that the former conditions themselves in [8, Proposition 3.2 (i) and (ii)], are sufficient and necessary for a pairs of linear codes (or group codes) (C, D) to be LCP of codes (or LCP of group codes) over a finite local Frobenius ring $\mathcal{R}$ (or $\mathcal{R}[G]$). Therefore, Proposition 3.13 generalizes and improves their results of [8].

Lemma 3.15 *If C and D are two linear codes over $\mathcal{R}$, then*

(1) $(C + D)^\perp = C^\perp \cap D^\perp$.
(2) $(C \cap D)^\perp = C^\perp + D^\perp$.

Proof Let $\mathbf{a} \in (C + D)^\perp$. Then, for any $\mathbf{b} \in C + D$, we have $[\mathbf{a}, \mathbf{b}] = 0$.

Case 1. When $\mathbf{b} \in C \subset C + D$, we obtain $[\mathbf{a}, \mathbf{b}] = 0$, which implies that $\mathbf{a} \in C^\perp$.

Case 2. When $\mathbf{b} \in D \subset C + D$, we obtain $[\mathbf{a}, \mathbf{b}] = 0$, which implies that $\mathbf{a} \in D^\perp$.

Combining cases 1 and 2, we have $(C + D)^\perp \subset C^\perp \cap D^\perp$.

On the other hand, if $\mathbf{a} \in C^{\perp} \cap D^{\perp}$, then for any $\mathbf{b} = \mathbf{c} + \mathbf{d} \in C + D$ with $\mathbf{c} \in C$ and $\mathbf{d} \in D$, we have $[\mathbf{a}, \mathbf{b}] = [\mathbf{a}, \mathbf{c}] + [\mathbf{a}, \mathbf{d}] = 0$. This means that $(C + D)^{\perp} \supset C^{\perp} \cap D^{\perp}$.

Summarizing, we have shown that $(C + D)^{\perp} = C^{\perp} \cap D^{\perp}$.

(2) The proof is similar to (1), so it is omitted here. □

By means of the above lemma, we obtain the following corollary.

Corollary 3.16 *(C, D) is an LCP of codes over $\mathcal{R}$ if and only if $(C^{\perp}, D^{\perp})$ is also an LCP of codes.*

Proof (C, D) is an LCP of codes over $\mathcal{R}$ if and only if $C + D = \mathcal{R}^n$ and $C \cap D = \{\mathbf{0}\}$. Thus, $(C + D)^{\perp} = (\mathcal{R}^n)^{\perp}$ and $(C \cap D)^{\perp} = \{\mathbf{0}\}^{\perp}$. According to the Lemma 3.15, we obtain that $C + D = \mathcal{R}^n$ and $C \cap D = \{\mathbf{0}\}$ if and only if $C^{\perp} \cap D^{\perp} = \{\mathbf{0}\}$ and $C^{\perp} + D^{\perp} = \mathcal{R}^n$.

This means that (C, D) is an LCP of codes over $\mathcal{R}$ if and only if $(C^{\perp}, D^{\perp})$ is also an LCP of codes over $\mathcal{R}$. □

Now, we give the second characterization of LCP of codes over $\mathcal{R}$ by using the bases of codes C and D.

Theorem 3.17 *Let $\{\mathbf{a}_i\}_{i=1}^{k}$ be a basis of the free code C of length n over $\mathcal{R}$, and let $\{\mathbf{b}_j\}_{j=1}^{n-k}$ be a basis of the free code D of length n over $\mathcal{R}$. Then (C, D) is an LCP of codes over $\mathcal{R}$ if and only if $\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{b}_1, \ldots, \mathbf{b}_{n-k}$ are linearly independent.*

Proof We first prove the sufficiency.

Since $\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{b}_1, \ldots, \mathbf{b}_{n-k}$ are linearly independent, $\{\mathbf{a}_i\}_{i=1}^{k} \cup \{\mathbf{b}_j\}_{j=1}^{n-k}$ is a basis of the code $C + D$. Then, we obtain $\mathrm{rank}_{\mathcal{R}}(C + D) = n$, which implies that $C + D = \mathcal{R}^n$.

On the other hand, let $\mathbf{u} \in C \cap D$. Then, by $\mathbf{u} \in C$, there are $\lambda_1, \ldots, \lambda_k \in \mathcal{R}$ such that

$$\mathbf{u} = \lambda_1 \mathbf{a}_1 + \cdots + \lambda_k \mathbf{a}_k.$$

Again by $\mathbf{u} \in D$, there are $\mu_1, \ldots, \mu_{n-k} \in \mathcal{R}$ such that

$$\mathbf{u} = \mu_1 \mathbf{b}_1 + \cdots + \mu_{n-k} \mathbf{b}_{n-k}.$$

Thus, we have

$$\lambda_1 \mathbf{a}_1 + \cdots + \lambda_k \mathbf{a}_k - \mu_1 \mathbf{b}_1 - \cdots - \mu_{n-k} \mathbf{b}_{n-k} = \mathbf{0},$$

which implies that $\lambda_1 = \cdots = \lambda_k = 0$, i.e., $\mathbf{u} = \mathbf{0}$. So, $C \cap D = \{\mathbf{0}\}$. According to Definition 2.5, (C, D) is an LCP of codes over $\mathcal{R}$.

Next, we prove the necessary by contradiction. Suppose that $\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{b}_1, \ldots, \mathbf{b}_{n-k}$ are linearly dependent. Let $G = \begin{pmatrix} G_C \\ G_D \end{pmatrix}$ where

$$G_C = \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_k \end{pmatrix}, \text{ and } G_D = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_{n-k} \end{pmatrix}.$$

Then, by Corollary 3.6, there exists a nonzero vector $\mathbf{x} \in \mathcal{R}^n$ such that $G\mathbf{x}^T = \mathbf{0}$, i.e., $\begin{pmatrix} G_C \\ G_D \end{pmatrix} \mathbf{x}^T = \mathbf{0}$. Thus, $G_C \mathbf{x}^T = \mathbf{0}$ and $G_D \mathbf{x}^T = \mathbf{0}$. This means that $\mathbf{0} \neq \mathbf{x} \in C^{\perp} \cap D^{\perp}$. Since (C, D) is LCP, $(C^{\perp}, D^{\perp})$ is also LCP by Corollary 3.16, which is a contradiction as $C^{\perp} \cap D^{\perp} = \mathbf{0}$. It follows that $\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{b}_1, \ldots, \mathbf{b}_{n-k}$ are linearly independent. □

Proposition 3.18 (1) *If (C, D) is an LCP of codes over $\mathcal{R}$, then $\mu(D^\perp) = \mu(D)^\perp$.*
(2) *If (C, D) is an LCP of group codes in $\mathcal{R}[G]$, then $\mu(C)$ and $\mu(D^\perp)$ are equivalent.*

Proof (1) Since (C, D) is an LCP of codes over $\mathcal{R}$, we know that $(C^\perp, D^\perp)$ is also an LCP of codes by Corollary 3.16. According to the Lemma 3.11, D and $D^\perp$ are free.

Let $D \cong \mathcal{R}^t$. Then $|\mu(D)| = |\mathbb{F}_q|^t$. By Remark 2.4, we have $|D||D^\perp| = |\mathcal{R}|^n$. Thus, $D^\perp \cong \mathcal{R}^{n-t}$, which implies that $|\mu(D^\perp)| = |\mathbb{F}_q|^{n-t}$.

On the other hand, if $\mathbf{a} \in \mu(D^\perp)$, then there is a $\mathbf{b} \in D^\perp$ such that $\mathbf{a} = \mu(\mathbf{b})$.

Let $\mu(\mathbf{d})$ be any element in $\mu(D)$ with $\mathbf{d} \in D$. Then

$$[\mathbf{a}, \mu(\mathbf{d})] = [\mu(\mathbf{b}), \mu(\mathbf{d})] = \mu([\mathbf{b}, \mathbf{d}]) = 0.$$

Thus, $\mathbf{a} \in \mu(D)^\perp$, and hence $\mu(D^\perp) \subset \mu(D)^\perp$.

Since $|\mu(D)||\mu(D)^\perp| = |\mathbb{F}_q|^n$, we have $|\mu(D)^\perp| = |\mathbb{F}_q|^{n-t}$.

Summarizing, we have shown that $\mu(D^\perp) = \mu(D)^\perp$.

(2) We omit the proof of (2) because it is similar with the proof of Proposition 3.6 (ii) in [8]. □

If we restrict the map $\mu : \mathcal{R}[G] \to \mathbb{F}_q[G]$ to the (free) group codes C and $D^\perp$, then we obtain the isomorphisms

$$\frac{C}{\delta C} \cong \mu(C) \text{ and } \frac{D^\perp}{\delta D^\perp} \cong \mu(D^\perp),$$

where $0 \neq \delta \in \mathfrak{m}$ and $\delta m = 0$ for any $m \in \mathfrak{m}$.

By Proposition 3.18 (2), we have $|\mu(C)| = |\mu(D^\perp)|$. Let $s := |\mu(C)|$ and set the elements of the cosets $\frac{C}{\delta C}$ and $\frac{D^\perp}{\delta D^\perp}$ as follows:

$$\frac{C}{\delta C} := \{c_1 + \delta C = \delta C, c_2 + \delta C, \ldots, c_s + \delta C\},$$

and

$$\frac{D^\perp}{\delta D^\perp} := \{d_1 + \delta D^\perp = \delta D^\perp, d_2 + \delta D^\perp, \ldots, d_s + \delta D^\perp\}.$$

(i.e. $c_1 = 0 = d_1$ in $\mathcal{R}[G]$). Clearly, cosets partition the codes C and $D^\perp$:

$$C = \cup_{i=1}^s (c_i + \delta C) \text{ and } D^\perp = \cup_{i=1}^s (d_i + \delta D^\perp).$$

By definition of the map μ, we have

$$\mu(C) = \{\mu(c_1) = 0, \mu(c_2), \ldots, \mu(c_s)\},$$
$$\mu(D^\perp) = \{\mu(d_1) = 0, \mu(d_2), \ldots, \mu(d_s)\},$$

and

$$\mu(C) = \cup_{i=1}^s (\tau(c_i) + \delta\tau(C)).$$

Without loss of generality, we assume that the coset representatives are indexed so that the permutation τ between the equivalent codes $\mu(C)$ and $\mu(D^\perp)$ satisfies

$$\tau(\mu(C)) = \mu(\tau(c_i)) = \mu(d_i), \quad \text{for all } i = 1, 2, \ldots, s.$$

Lemma 3.19 *If (C, D) be an LCP of group codes in $\mathcal{R}[G]$, then $C^\perp \cap \tau(C) = \{0\}$.*

Proof We first prove that $C^{\perp} \cap \tau(C) \subset \delta C^{\perp}$. Otherwise, there exists a $a \in C^{\perp} \cap \tau(C)$ such that $a \in \mathbf{c}'_j + \delta C^{\perp}$ for some $2 \leq j \leq l$, where we assume that $C^{\perp} = \cup_{i=1}^{l}(c'_i + \delta C^{\perp})$ with $c'_1 = 0$. Then $\mu(a) = \mu(c'_j) \in \mu(C^{\perp})$ and $\mu(a) \neq 0$. By Corollary 3.16, $(C^{\perp}, D^{\perp})$ is also an LCP of group codes in $\mathcal{R}[G]$. Further, $(\mu(C^{\perp}), \mu(D^{\perp}))$ is an LCP of group codes in $\mathbb{F}_q[G]$. Thus, $\mu(a) \notin \mu(D^{\perp}) = \mu(\tau(C))$. This is a contradiction.

Next, we prove that $C^{\perp} \cap \tau(C) \subset \delta\tau(C)$. Otherwise, there exists a $b \in C^{\perp} \cap \tau(C)$ such that $b \in \tau(c_j) + \delta\tau(C)$, where $\tau(c_j) \neq 0$. Then $\mu(b) = \mu(\tau(c_i)) = \mu(d_i) \in \mu(D^{\perp})$ and $\mu(b) \neq 0$. Note that $\mu(b) \in \mu(C^{\perp})$ since $b \in C^{\perp}$. Thus, $\mu(b) \in \mu(C^{\perp}) \cap \mu(D^{\perp}) = \{0\}$ since $(\mu(C^{\perp}, \mu(D^{\perp}))$ is an LCP of group codes in $\mathbb{F}_q[G]$. This is a contradiction.

According to the above facts, we can assume that $x = \delta\tau(c) = \delta c_1^{\perp}$ for any $x \in C^{\perp} \cap \tau(C)$, where $c \in C$ and $c_1^{\perp} \in C^{\perp}$. Then $\delta(\tau(c) - c_1^{\perp}) = 0$. Let $\tau(c) - c_1^{\perp} = \sum_{g \in G} r_g g$ where $r_g \in \mathcal{R}$. Then $r_g \in \mathfrak{m}$ for all $g \in G$. Otherwise, if there exists a $r_{g'} \notin \mathfrak{m}$ for some $g' \in G$, then $r_{g'}^{-1}\delta(\tau(c) - c_1^{\perp}) \neq 0$. This is a contradiction. Thus, $\tau(c) = c_1^{\perp} + \sum_{g \in G} r_g g$. By Lemma 3.1,

$$x = \delta\tau(c) = \delta c_1^{\perp} + \sum_{g \in G} \delta r_g g = \delta c_1^{\perp}.$$

If $c_1^{\perp} \in C^{\perp} \backslash \delta C^{\perp}$, then $0 \neq \mu(\tau(c)) = \mu(c_1^{\perp}) \notin \mu(D^{\perp}) = \mu(\tau(C))$, which is a contradiction. Hence, there exists a $c_2^{\perp} \in C^{\perp}$ such that $c_1^{\perp} = \delta c_2^{\perp}$. It follows that

$$x = \delta^2\tau(c) = \delta^2 c_2^{\perp}.$$

Continuing in this manner, by $\delta^e = 0$, we have $x = 0$, i.e., $C^{\perp} \cap \tau(C) = \{0\}$. □

Combining The Propositions 3.13 and 3.18 with Lemma 3.19, we obtain the following theorem, whose proof is similar to the Theorem 3.9 in [8], so we omit it here for simplification.

Theorem 3.20 *Let (C, D) be an LCP of group codes in $\mathcal{R}[G]$, where G is a finite group. Then C and $D^{\perp}$ are equivalent.*

Remark 3.21 Güneri et al. [8, Theorem 3.9], proved C and $D^{\perp}$ are equivalent if (C, D) is an LCP of group codes in $\widetilde{R}[G]$ where $\widetilde{R}$ is a finite chain ring and G is a finite group. It is well known that a finite chain ring is a finite local Frobenius ring. Therefore, Theorem 3.20 generalizes their results of [8].

4 LCP of group codes over finite Frobenius rings

In this section, let the symbols be the same as in the Sect. 1.

Let C_j be a group code in $R_j[G]$ for all $1 \leq j \leq s$, and let

$$\begin{aligned} C &= \mathrm{CRT}(C_1, C_2, \ldots, C_s) = \Phi^{-1}(C_1 \times C_2 \times \cdots \times C_s) \\ &= \{\Phi^{-1}(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_s) | \mathbf{c}_j \in C_j\}. \end{aligned}$$

We call C the Chinese product of group codes $C_1, C_2, \ldots, C_s$.

Theorem 4.1 *Let C_j be a group code in $R_j[G]$ for all $1 \leq j \leq s$. Then $C = \mathrm{CRT}(C_1, C_2, \ldots, C_s)$ is a group code over the $R[G]$.*

Proof For any $\mathbf{a} \in C$, there is an $\mathbf{a}_j \in C_j$ such that

$$\mathbf{a} = \Phi^{-1}(\mathbf{a}_1, \ldots, \mathbf{a}_s),$$

where $\mathbf{a}_j = \sum_{i=1}^{n} a_{g_i}^{(j)} g_i$ with $a_{g_i}^{(j)} \in R_j$ for all $1 \le j \le s$.

Suppose that $a_{g_i} = (a_{g_i}^{(1)}, a_{g_i}^{(2)}, \ldots, a_{g_i}^{(s)})$ for $1 \le i \le n$. Then $\mathbf{a} = \sum_{i=1}^{n} a_{g_i} g_i$. Therefore, for any $g \in G$, we have $g\mathbf{a} = \sum_{i=1}^{n} a_{g_i} g g_i = \sum_{i=1}^{n} a_{g^{-1}g_i} g_i$.

On the other hand, $g\mathbf{a}_j = \sum_{i=1}^{n} a_{g_i}^{(j)} g g_i = \sum_{i=1}^{n} a_{g^{-1}g_i}^{(j)} g_i$ for all $1 \le j \le s$.

Thus, we have $g\mathbf{a} = \Phi^{-1}(g\mathbf{a}_1, \ldots, g\mathbf{a}_s)$. Since C_j is a group code over $R_j[G]$, $g\mathbf{a}_j \in C_j$. Thus, $g\mathbf{a} \in C$.

By using a similar technique we can show that $\mathbf{a}g \in C$.

Summarizing, we have proved that C is an ideal in $R[G]$, i.e., C is a group code over $R[G]$. □

Now, we give a useful lemma that will be used in later characterization of LCP of group codes in $R[G]$.

Lemma 4.2 *Let C_j and D_j be two group codes over the $R_j[G]$ for all $1 \le j \le s$. If $C = \mathrm{CRT}(C_1, C_2, \ldots, C_s)$ and $D = \mathrm{CRT}(D_1, D_2, \ldots, D_s)$, then*

(1) $C \cap D = \mathrm{CRT}(C_1 \cap D_1, C_2 \cap D_2, \ldots, C_s \cap D_s)$.
(2) $C + D = \mathrm{CRT}(C_1 + D_1, C_2 + D_2, \ldots, C_s + D_s)$.

Proof Suppose that $\mathbf{a} = \sum_{i=1}^{n} a_{g_i} g_i$ where $a_{g_i} = (a_{g_i}^{(1)}, \ldots, a_{g_i}^{(s)})$ and $a_{g_i}^{(j)} \in R_j$ for $1 \le j \le s$. Then $\mathbf{a} \in R[G]$.

(1) $\mathbf{a} \in C \cap D$ if and only if

$$\mathbf{a} = \Phi^{-1}\left(\sum_{i=1}^{n} a_{g_i}^{(1)} g_i, \sum_{i=1}^{n} a_{g_i}^{(2)} g_i, \ldots, \sum_{i=1}^{n} a_{g_i}^{(s)} g_i\right) \in \mathrm{CRT}(C_1, C_2, \ldots, C_s).$$

and

$$\mathbf{a} = \Phi^{-1}\left(\sum_{i=1}^{n} a_{g_i}^{(1)} g_i, \sum_{i=1}^{n} a_{g_i}^{(2)} g_i, \ldots, \sum_{i=1}^{n} a_{g_i}^{(s)} g_i\right) \in \mathrm{CRT}(D_1, D_2, \ldots, D_s).$$

Then, $\mathbf{a} \in C \cap D$ if and only if $\mathbf{a} \in \mathrm{CRT}(C_1 \cap D_1, C_2 \cap D_2, \ldots, C_s \cap D_s)$.

Therefore, we have

$$C \cap D = \mathrm{CRT}(C_1 \cap D_1, C_2 \cap D_2, \ldots, C_s \cap D_s).$$

(2) $\mathbf{a} \in C + D$ if and only if

$$\begin{aligned}\mathbf{a} &= \Phi^{-1}\left(\sum_{i=1}^{n} a_{g_i}^{(1)} g_i, \sum_{i=1}^{n} a_{g_i}^{(2)} g_i, \ldots, \sum_{i=1}^{n} a_{g_i}^{(s)} g_i\right) + \Phi^{-1}\left(\sum_{i=1}^{n} b_{g_i}^{(1)} g_i, \sum_{i=1}^{n} b_{g_i}^{(2)} g_i, \ldots, \sum_{i=1}^{n} b_{g_i}^{(s)} g_i\right) \\ &= \Phi^{-1}\left(\sum_{i=1}^{n} a_{g_i}^{(1)} g_i + \sum_{i=1}^{n} b_{g_i}^{(1)} g_i, \sum_{i=1}^{n} a_{g_i}^{(2)} g_i + \sum_{i=1}^{n} b_{g_i}^{(2)} g_i, \ldots, \sum_{i=1}^{n} a_{g_i}^{(s)} g_i + \sum_{i=1}^{n} b_{g_i}^{(s)} g_i\right),\end{aligned}$$

where

$$\Phi^{-1}\left(\sum_{i=1}^{n} a_{g_i}^{(1)} g_i, \sum_{i=1}^{n} a_{g_i}^{(2)} g_i, \ldots, \sum_{i=1}^{n} a_{g_i}^{(s)} g_i\right) \in C,$$

and

$$\Phi^{-1}\left(\sum_{i=1}^{n} b_{g_i}^{(1)} g_i, \sum_{i=1}^{n} b_{g_i}^{(2)} g_i, \ldots, \sum_{i=1}^{n} b_{g_i}^{(s)} g_i\right) \in D.$$

Then, $\mathbf{a} \in C + D$ if and only if $\mathbf{a} \in \mathrm{CRT}(C_1 + D_1, C_2 + D_2, \ldots, C_s + D_s)$.

Therefore, we have

$$C + D = \mathrm{CRT}(C_1 + D_1, C_2 + D_2, \ldots, C_s + D_s).$$

□

The proof of the following lemma is similar with the proofs of Theorems 2.4, 2.7 and Lemma 2.5 in [5], so we omit it here.

Lemma 4.3 *Let $C = \mathrm{CRT}(C_1, C_2, \ldots, C_s)$ be a group code over $R[G]$, where C_j is a group code over the $R_j[G]$ for all $1 \leq j \leq s$. Then*

(1) $|C| = \prod_{j=1}^{s} |C_j|$.
(2) $C^{\perp} = \mathrm{CRT}(C_1^{\perp}, C_2^{\perp}, \ldots, C_s^{\perp})$

The following result gives a necessary and sufficient condition for a pair (C, D) of group codes over $R[G]$ to be LCP.

Theorem 4.4 *Let C_j and D_j be group codes in $R_j[G]$ for all $1 \leq j \leq s$, and let $C = \mathrm{CRT}(C_1, C_2, \ldots, C_s)$ and $D = \mathrm{CRT}(D_1, D_2, \ldots, D_s)$. Then (C, D) is an LCP of group codes in $R[G]$ if and only if (C_j, D_j) is an LCP of group codes in $R_j[G]$ for all $1 \leq j \leq s$.*

Proof Since (C_j, D_j) is an LCP of group codes in $R_j[G]$ for all $1 \leq j \leq s$, we have $C_j \cap D_j = \{\mathbf{0}\}$ and $C_j + D_j = R_j[G]$ or $|C_j||D_j| = |R_j[G]|$ for all $1 \leq j \leq s$. By Lemma 4.2,

$$C \cap D = \mathrm{CRT}(C_1 \cap D_1, C_2 \cap D_2, \ldots, C_s \cap D_s) = \mathrm{CRT}(\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}) = \{\mathbf{0}\}.$$

Then, according to the Lemma 4.3 (1),

$$|C + D| = |C| \cdot |D| = \prod_{j=1}^{s} |C_j| \cdot \prod_{j=1}^{s} |D_j| = \prod_{j=1}^{s} |C_j||D_j| = \prod_{j=1}^{s} |R_j[G]| = |R[G]|.$$

Therefore, (C, D) is an LCP of group codes in $R[G]$.

Conversely, suppose that (C, D) is an LCP of group codes in $R[G]$. Then $C + D = R[G]$ and $C \cap D = \{\mathbf{0}\}$. By Theorem 2.3 and Lemma 4.2, we have

$$C \cap D = \mathrm{CRT}(C_1 \cap D_1, C_2 \cap D_2, \ldots, C_s \cap D_s) = \{\mathbf{0}\},$$

and

$$C + D = \mathrm{CRT}(C_1 + D_1, C_2 + D_2, \ldots, C_s + D_s) = \mathrm{CRT}(R_1[G], R_2[G], \ldots, R_s[G]).$$

Thus,

$$C_1 \cap D_1 = \{\mathbf{0}\}, C_2 \cap D_2 = \{\mathbf{0}\}, \ldots, C_s \cap D_s = \{\mathbf{0}\},$$
$$C_1 + D_1 = R_1[G], C_2 + D_2 = R_2[G], \ldots, C_s + D_s = R_s[G].$$

This proves that (C_j, D_j) is an LCP of group codes in $R_j[G]$ for all $1 \leq j \leq s$. □

Theorem 4.5 *Let $R = \mathrm{CRT}(R_1, R_2, \ldots, R_s)$ be a finite Frobenius ring, where R_j is a finite local Frobenius ring for all $1 \leq j \leq s$, and let G be a finite group. If (C, D) is an LCP of group codes in $R[G]$, Then C and $D^{\perp}$ are equivalent. In particular $d(D^{\perp}) = d(C)$.*

Proof Let $C = \mathrm{CRT}(C_1, C_2, \ldots, C_s)$ and $D = \mathrm{CRT}(D_1, D_2, \ldots, D_s)$, where C_j and D_j are group codes in $R_j[G]$ for all $1 \le j \le s$. Since (C, D) is an LCP of group codes in $R[G]$, (C_j, D_j) is an LCP group codes in $R_j[G]$ for all $1 \le j \le s$ by Theorem 4.4.

According to the Theorem 3.20, C_j and $D_j^{\perp}$ are equivalent codes for all $1 \le j \le s$. Then there is a permutation matrix P_j such that $C_j = D_j^{\perp} P_j$ for all $1 \le j \le s$.

Set

$$P = \begin{pmatrix} P_1 & 0 & \cdots & 0 \\ 0 & P_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & P_s \end{pmatrix}.$$

Then $C_1 \times C_2 \times \cdots \times C_s = (D_1^{\perp} \times D_2^{\perp} \times \cdots \times D_s^{\perp})P$.

Since $C = \mathrm{CRT}(C_1, C_2, \ldots, C_s) \cong C_1 \times C_2 \times \cdots \times C_s$ and $D^{\perp} = \mathrm{CRT}(D_1^{\perp}, D_2^{\perp}, \ldots, D_s^{\perp})$, we have

$$C = \mathrm{CRT}(C_1, C_2, \ldots, C_s) = \mathrm{CRT}(D_1^{\perp}, D_2^{\perp}, \ldots, D_s^{\perp})P.$$

Thus, C and $D^{\perp}$ are equivalent. □

Remark 4.6 When R is a finite Frobenius ring, we know that $(C^{\perp})^{\perp} = C$ for any submodule C of any free R-module R^n. According to Remark 2.4, we have $|C| \cdot |C^{\perp}| = |R|^n$. This is one of the reasons why only finite Frobenius rings are suitable for coding alphabets. In this sense, we believe that Theorem 4.5 solves the equivalence problem of C and $D^{\perp}$ if (C, D) is an LCP of group codes.

Acknowledgements This work was supported by Research Funds of Hubei Province, Grant No. D20144401.

References

1. Bhowmick S., Fotue-Tabue A., Martínez-Moro E., Bandi R., Bagchi S.: Do non-free LCD codes over finite commutative Frobenius rings exist? Des. Codes Cryptogr. **88**(5), 825–840 (2020).
2. Borello M., de Cruz J., Willems W.: A note on linear complementary pairs of group codes. Discret. Math. **343**, 111905 (2020).
3. Carlet C., Güneri C., Mesnager S., Özbudak F.: Construction of some codes suitable for both side channel and fault injection attacks. In: Proceedings of International Workshop on the Arithmetic of Finite Fields (WAIFI 2018), Bergen (2018).
4. Carlet C., Güneri C., Özbudak F., Özkaya B., Solè P.: On linear complementary pairs of codes. IEEE Trans. Inf. Theory **64**(1), 6583–6588 (2018).
5. Dougherty S.T., Liu H.: Independence of vectors in codes over rings. Des. Codes Cryptogr. **51**, 55–68 (2009).
6. Dougherty S.T., Kim J.L., Kulosman H.: MDS codes over finite principal ideal rings. Des. Codes Cryptogr. **50**, 77–92 (2009).
7. Fan Y., Ling S., Liu H.: Matrix product codes over finite commutative Frobenius rings. Des. Codes Cryptogr. **71**, 201–227 (2014).
8. Güneri C., Martınez-Moro E., Sayıcı S.: Linear complementary pair of group codes over finite chain rings. Des. Codes Cryptogr. https://doi.org/10.1007/s10623-020-00792-1
9. Güneri C., Özkaya B., Sayıcı S.: On linear complementary pair of $n D$ cyclic codes. IEEE Commun. Lett. **22**, 2404–2406 (2018).
10. Hu P., Liu X.S.: Linear complementary pairs of codes over rings. Des. Codes Cryptogr. **89**, 2495–2509 (2021).
11. Kaplansky I.: Projective modules. Ann. Math. **68**, 372–377 (1958).
12. Liu H., Liu X.S.: LCP of matrix product codes. Linear Multilinear Algebra. https://doi.org/10.1080/03081087.2021.1999889

13. Liu X.S., Liu H.: LCD codes over finite chain rings. Finite Field Appl. **15**, 1–19 (2015).
14. McDonald D.: Finite Rings with Identity. Marcel Dekker, New York (1974).
15. Ngo X.T., Bhasin S., Danger J.-L., Guilley S., Najm Z.: Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses. In: Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST), pp. 82–87 (2015).
16. Norton G.H., Sălăgean A.S.: On the structure of linear and cyclic codes over a finite chain ring. Appl. Algebra Eng. Commun. Comput. **10**, 489–506 (2000).
17. Wood J.: Duality for modules over finite rings and applications to coding theory. Am. J. Math. **121**, 555–575 (1999).