Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 3, pp. 891–905
DOI : 10.47974/JDMSC-2187

On LCP and checkable group codes over finite non-commutative Frobenius rings

Sanjit Bhowmick *
Department of Mathematics
Indraprastha Institute of Information Technology Delhi
New Delhi
India

Javier de la Cruz †
Departamento de Matemáticas
Universidad del Norte
Barranquilla
Colombia

Edgar Martınez-Moro §
Institute of Mathematics
University of Valladolid
Castilla
Spain

Anuradha Sharma #
Department of Mathematics
Indraprastha Institute of Information Technology Delhi
New Delhi
India

Abstract

We provide a simple proof for a complementary pair of group codes over a finite non-commutative Frobenius ring of the fact that one of them is equivalent to the other one. We also explore this fact for checkeable codes over the same type of alphabet.

Subject Classification (2010): *94B05, 20C05.*

Keywords: *Group codes, Non-commutative Frobenius ring.*

* *E-mail:* **sanjitbhowmick392@gmail.com (Corresponding Author)**
† *E-mail:* **jdelacruz@uninorte.edu.co**
§ *E-mail:* **edgar.martinez@uva.es**
§ *E-mail:* **anuradha@iiitd.ac.in**

1. Introduction

A linear code C of length n over a finite ring $\mathcal{R}$ is just a submodule of $\mathcal{R}^n$. A pair of linear codes (C,D) of the same length is called a *linear complementary pair* (LCP) if they meet trivially, i.e. $C \cap D = \{0\}$, and they cover all the space $C + D = \mathcal{R}^n$. LCP of codes over finite fields have been of interest and extensively explored because of their algebraic structure and wide applications in cryptography. Carlet et al. [4] showed that LCP of codes can be used to improve the security of data processed by sensitive devices, particularly against so-called side-channel assaults and fault injection attacks. In particular, the case one of the codes is the dual of the other one $C^{\perp} = D$, is *called linear complementary dual* (LCD) code that was introduced by Massey [14] and it has been extensively studied (see for example [1] and the references within). Recently, it has been shown that every linear code over a finite field of size greater than 3 is equivalent to an LCD code [6].

Group codes are an extension of the concept of cyclic codes and they can be seen as ideals in the group ring $\mathcal{R}G$, where $\mathcal{R}$ is a finite ring and G a finite group. From the very begining there were stated conditions for linear and cyclic codes over a field to be LCD [14, 17] and it was extended to group codes over finite fields in [7]. In [5], the authors proved that for linear complementary pairs (C,D), the codes C and $D^{\perp}$ (the dual od D) are equivalent if and are both cyclic or 2D-cyclic codes, and to n-cyclic in [10], both papers worked their results under the assumption that the characteristic of the field does not divide the length, i.e. they where semisimple. This result was extended to any LCP of group codes over a finite field (despite its characteristic) in [2]. The result was further generalized for finite chain rings in [9] and recently to commutative Frobenius rings in [12]. In this paper, we will cover the final gap till non-commutative Frobenius rings that constitute the more general type of alphabet for coding theory [16]. Despite we cover the same type of rings that [12] in the non-commutative case, our techniques differ from that ones and they mostly rely on the decomposition of modules and idempotents.

Finally we will pay attention to chekeable codes in $\mathcal{R}G$. If we are dealing with G an abelian code, one important feature of semisimple codes over fields or rings is that all of them can be generated by a single codeword, i.e., they can be regarded as principal ideals. This property is not generally true in the modular case, and it partly explains the reason why those codes are more difficult to describe. However, that of all the ideals in are principal

is not equivalent to the semisimple condition, see for example [13] and the references therein for a polynomial description of Abelian codes over finite chain rings and finite fields. In this paper we will deal with checkable codes in $\mathcal{R}G$, that is, ideals in $\mathcal{R}G$ whose anhihilator is a principal right ideal, see [3] for a study of checkable group codes over finite fields.

The outline of the paper will be as follows. Section 2 will show some preliminaries on non-commutative Frobenius rings and modules over them. For a given group ring $\mathcal{R}G$, where G is a finite group and $\mathcal{R}$ a non-commutative Frobenius ring, Section 3 will show its idempotents and the related decomposition of a $\mathcal{R}$-module in $\mathcal{R}G$. Sections 4 & 5 study when a group code is LCP in the case of the base ring being a a non-commutative finite local ring or a non-commutative finite Frobenius ring respectively. Finally, in Section 6, we deal with checkable codes in $\mathcal{R}G$.

2. Preliminaries

Throughout this paper, $\mathcal{R}$ will denote a finite Frobenius ring with identity $1_{\mathcal{R}}$. Furthermore, unless mentioned otherwise, we assume our rings to be non-commutative. In this section we will provide a brief overview to some results concerning modules over $\mathcal{R}$ (for a more detailed study see for example [8]) and some definitions and notations related to group codes.

A right $\mathcal{R}$-module A is called free $\mathcal{R}$-module if A is isomorphic to $\mathcal{R}^t$ as a $\mathcal{R}$-module, where $t \geq 1$.

Definition 2.1 (Projective & injective modules)

(1) A right $\mathcal{R}$-module P is called projective if there exists another right $\mathcal{R}$-module Q such that $P \oplus Q$ is free $\mathcal{R}$-module.

(2) A right $\mathcal{R}$-module I is said to be injective if for any monomorphism $g : A \to B$ of right $\mathcal{R}$-modules and any $\mathcal{R}$-homomorphism $h : A \to I$, there exists an $\mathcal{R}$-homomorphism $h' : B \to I$ such that $h = h' \circ g$.

The following results can be also found in [8].

Theorem 2.1

(1) *(Baer's criterion) A right $\mathcal{R}$-module I is injective if and only if, for any right ideal $\mathcal{I}$ of $\mathcal{R}$, any $\mathcal{R}$-homomorphism $\gamma : \mathcal{I} \to I$ extends to $\mathcal{R} \to I$, that is, $\gamma = c\cdot$ is the multiplication by an element $c \in I$.*

(2) $P = \bigoplus_{i=1}^{n} P_i$ *is projective* $\mathcal{R}$ *-module if and only if* P_i *is projective* $\mathcal{R}$ *module for each* $i \in \{1, 2, \ldots, n\}$.

(3) $I = \bigoplus_{i=1}^{n} I_i$ *is injective* $\mathcal{R}$ *-module if and only if each* I_i *is injective* $\mathcal{R}$ *module for each* $i \in \{1, 2, \ldots, n\}$.

A finite ring $\mathcal{R}$ is said to be Frobenius if $\mathcal{R}$ forms a self-injective right $\mathcal{R}$ -module (left $\mathcal{R}$ -module). Alternatively, for a given finite ring $\mathcal{R}$ is said to be Frobenius if right $\mathcal{R}$ -module $\frac{\mathcal{R}}{J(\mathcal{R})}$ is isomorphic to $\mathrm{Soc}(\mathcal{R})$ as a right $\mathcal{R}$ -module, where $J(\mathcal{R})$ denotes the intersection of all maximal ideals in $\mathcal{R}$ and $\mathrm{Soc}(\mathcal{R})$ the socle of $\mathcal{R}$, which is the sum of all irreducible ideals in $\mathcal{R}$ (for more details see [11]).

Theorem 2.2: *The following statements are equivalent:*

(1) $\mathcal{R}$ *is Frobenius,*

(2) *every ideal in* $\mathcal{R}$ *is projective if and only if it is injective in* $\mathcal{R}$.

A nonempty subset $C \subseteq \mathcal{R}^n$ is called a left (right) linear code of length n over $\mathcal{R}$ if it is an left (right) $\mathcal{R}$ -submodule of $\mathcal{R}^n$. In this paper all codes are assumed to be linear. We will denote by G a finite group and by $\mathcal{R}G$ the collection of formal sums $\{\sum_{g\in G} a_g g : g \in G, a_g \in \mathcal{R}\}$, with the componentwise addition and the product given by $a \cdot b = ab = \sum_{g\in G} (\sum_{h\in H} a_h b_{h^{-1}g} h)g$, for $a = \sum_{g\in G} a_g g$ and $b = \sum_{g\in G} b_g g$. Under this operations, $(\mathcal{R}G, +, \cdot)$ becomes an $\mathcal{R}$ -module with the elements of G as a basis and therefore we can think the ideals in $\mathcal{R}G$ as codes in $\mathcal{R}^{|G|}$. That is, a right (left) group code C in $\mathcal{R}G$ is a right (left) ideal in $\mathcal{R}G$, which is indeed an $\mathcal{R}$ -linear code if we see an element $a = \sum_{g\in G} a_g g$ as $(a_g)_{g\in G} \in \mathcal{R}^{|G|}$ for a given ordering on the elements in G. Throughout this paper, by a group code C, we will always mean a right ideal unless other thing is stated. For an element $a = \sum_{g\in G} \in \mathcal{R}G$, the adjoint of a is defined as $\hat{a} = \sum_{g\in G} a_g g^{-1}$, and it is called self-adjoint if $a = \hat{a}$. We will denote by $Z(\mathcal{R}G)$ the center of $\mathcal{R}G$.

The group ring $\mathcal{R}G$ has a symmetric non-degenerate G-invariant bilinear form $\langle\,,\rangle$ defined for the elemnets in G as

$$\langle g,h\rangle = \begin{cases} 1 & \text{if } g = h, \\ 0 & \text{otherwise} \end{cases},$$

that can be straightfoward extended to $\mathcal{R}G$. Note that the G-invariant means $\langle ag,bg\rangle = \langle a,b\rangle$ for all a,b in $\mathcal{R}G$ and g in G. The above form relates to the Euclidean inner product via the isomorphism $\mathcal{R}G$ and $\mathcal{R}^{|G|}$. With respect to this form, we can define the dual code $C^{\perp}$ of a group code C as usual $C^{\perp} = \{a \in \mathcal{R}G \mid \langle a,c\rangle = 0 \text{ for all } c \in C\}$.

As usual, if C_1 and C_2 are two codes in $\mathcal{R}G$, then $(C_1 + C_1)^{\perp} = C_1^{\perp} \cap C_2^{\perp}$ and $C_1^{\perp} + C_2^{\perp} = (C_1 \cap C_2)^{\perp}$. It is also well known that if C be a group code in $\mathcal{R}G$, then $|C|\,|C^{\perp}| = |\mathcal{R}G|$ (it follows from J. Wood's result in [16], since $\mathcal{R}G$ is a finite Frobenius ring).

Let C and D be two linear codes of length n over $\mathcal{R}$, we say that the pair (C,D) is a linear complementary pair (LCP) if $C \oplus D = \mathcal{R}^n$. Analogously, a pair of codes (C,D) in $\mathcal{R}G$, is called an LCP group code if $C \oplus D = \mathcal{R}G$.

3. Idempotents and the decomposition of $\mathcal{R}G$-modules

In this section we will review some results related to the relationship between the idempotents of the ring $\mathcal{R}G$ and the decomposition of right $\mathcal{R}G$-submodules. The results are in correspondence with those in [7] where the finite field case was studied.

Let M be a right $\mathcal{R}G$-submodule in $\mathcal{R}G$, then the dual module M is denoted by $M^{\star}$ and defined by $M^{\star} = \{f \mid f : M \to \mathcal{R} \text{ is an } \mathcal{R} \text{ module homomorphism}\}$. $M^{\star}$ is an $\mathcal{R}G$-right submodule under the action

$$(fg)(m) = f(mg^{-1})\; m \in M,\; f \in M^{\star},\; g \in G,$$

and clearly, $|M| = |M^{\star}|$.

Lemma 3.1: *If e is an idempotent element in $\mathcal{R}G$, then $\hat{e}\mathcal{R}G \cong e\mathcal{R}G^{\star}$.*

Proof: Consider the mapping $\varphi : \hat{e}\mathcal{R}G \to eRG^{\star}$ by $\hat{e}r \mapsto \varphi_{\hat{e}r}$, with

$$\varphi_{er}(es) = \langle es, \hat{e}s\rangle, \text{ where } r,s \in \mathcal{R}G.$$

It is clear that φ is well define and that φ is group homomorphism under addition, as $\varphi(\hat{e}r+\hat{e}s) = \varphi(\hat{e}r) + \varphi(\hat{e}s)$, for all $r,s \in \mathcal{R}G$. Next, for any $\theta \in \mathcal{R}G$ and $\hat{e}r$ in $\mathcal{R}G$, we have to prove that $\varphi(\hat{e}r\theta) = \varphi(\hat{e}r)\theta$. Since

$$\varphi_{\hat{e}r\theta}(es) = \langle es, \hat{e}r\theta\rangle = \langle es\hat{\theta}, \hat{e}r\rangle = \varphi_{\hat{e}r}(es\hat{\theta}) = (\varphi_{\hat{e}r}\theta)(es).$$

we have that $\varphi(\hat{e}r\theta) = \varphi(\hat{e}r)\theta$, where $\theta \in \mathcal{R}G$. Thus, it follows that φ is a right $\mathcal{R}G$ -module homomorphism. Note that the kernel of φ is given by

$$\begin{aligned} ker(\varphi) &= \{\hat{e}r \mid \varphi(\hat{e}r) = 0\}, \\ &= \{\hat{e}r \mid \varphi_{\hat{e}r}(es) = 0, \text{for all } s \in \mathcal{R}G\}, \\ &= \{\hat{e}r \mid \langle es, \hat{e}r\rangle = 0, \text{for all } s \in \mathcal{R}G\} = \{0\}. \end{aligned}$$

Therefore, φ is a monomorphism. Since $|\hat{e}\mathcal{R}G| = |e\mathcal{R}G| = |eRG^{*}|$, it follows that φ is onto. Thus, φ is a left $\mathcal{R}G$ -module isomorphism.

Theorem 3.1: *Let $\mathcal{R}G$ be a finite group ring with $1_{\mathcal{R}G}$. Then there is a one-one correspondence between the following statements:*

(1) *There is a decomposition $\mathcal{R}G = I_1 \oplus \cdots \oplus I_s$ as a direct sum of right $\mathcal{R}G$ -submodules,*

(2) *there exist orthogonal idempotents $e_1, \ldots, e_s$ such that $e_1 + \cdots + e_s = 1_{\mathcal{R}G}$.*

Proof: Let us assume that $\mathcal{R}G = I_1 \oplus I_2 \oplus \cdots \oplus I_s$. Since $1_{\mathcal{R}G}$ in $\mathcal{R}G$, we have that $1_{\mathcal{R}G} = \sum_{i=1}^{s} x_i$, where $x_i \in I_i$ for all $1 \le i \le s$. Thus

$$x_i = 1 \cdot x_i = \sum_{j=1}^{s} x_j x_i$$

$$x_i - x_i^2 = \sum_{j(\neq i)=1}^{s} x_j x_i \in I_i \cap (I_1 + \ldots + I_{i-1} + I_{i+1} + \ldots + I_s),$$

and $x_i - x_i^2 = 0$ for all $1 \le i \le s$ and $x_i x_j = 0$ for all $i \neq j$ as required.

Conversely, given a set of orthogonal idempotents $\{e_i\}$, let us define $I_i = e_i\mathcal{R}G$ which is a right submodule of $\mathcal{R}G$. Since $\sum_{i=1}^{s} e_i = 1_{\mathcal{R}G}$, this implies $\mathcal{R}G = I_1 + I_2 + \cdots + I_s$. Therefore, $\mathcal{R}G = \bigoplus_{i=1}^{s} e_i\mathcal{R}G$, as e_i is an orthogonal idempotent element in $\mathcal{R}G$.

Theorem 3.2: *Let $\mathcal{R}G$ be a group ring with identity $1_{\mathcal{R}G}$ and e an idempotent in $\mathcal{R}G$. Then $e\mathcal{R}G$ is indecomposable if and only if e is primitive.*

Proof: Let us assume $e\mathcal{R}G$ is indecomposable, therefore , let $e = e_1 + e_2$, where the e_i are orthogonal idempotent elements. First, let $x \in e_1\,\mathcal{R}G \cap e_2\,\mathcal{R}G$, this implies

$$x = e_1^2 r_1 = e_1 e_2 r_2 = 0, \text{ for some } r_1, r_2 \in \mathcal{R}G.$$

It follows that $e_1\mathcal{R}G \cap \mathcal{R}G = \{0\}$, clearly $(e_1 + e_2)\,\mathcal{R}G \subset e_1\mathcal{R}G \oplus e_2\mathcal{R}G$.

Let $e_1 s_1 + e_2 s_2 \in e_1\mathcal{R}G \oplus e_2\mathcal{R}G$ for some $s_1, s_2 \in \mathcal{R}G$. Now,

$$(e_1 + e_2)(e_1 s_1 + e_2 s_2) \in (e_1 + e_2)\mathcal{R}G.$$

Hence, $e\mathcal{R}G = (e_1 + e_2)\mathcal{R}G = e_1\mathcal{R}G \oplus e_2\mathcal{R}G$.

Conversely, if $e\mathcal{R}G = I + J$, express $e = x + y$, where $x \in I$ and $y \in J$.

Since $I \subseteq e\mathcal{R}G$, then $x = er_1$, for some $r_1 \in \mathcal{R}G$. Therefore,

$$ex = e^2 r_1 = er_1 = x.$$

It follows that $x = ex = x^2 + yx$, i.e., $x - x^2 = yx \in I \cap J$, that means $x = x^2$ and $yx = 0$. Similarly, $y = y^2$ and $xy = 0$, which is a contradiction.

Theorem 3.3: *If $\mathcal{R}G$ is a finite module with identity $1_{\mathcal{R}G}$, then $\mathcal{R}G$ can be written as direct sum of indecomposable submodules.*

Proof: It follows directly from the contradiction between an ascending chain of decompositions and the fact that $\mathcal{R}G$ is finite.

4. LCP group codes over finite non-commutative local rings

In this section, we will assume that $\mathcal{R}$ is a finite non-commutative local ring, that is, whenever $x, y \in \mathcal{R}$ are non-unit, so is $x + y$. Let $\mathfrak{m} = J(\mathcal{R})$ the Jacobson radical of $\mathcal{R}$, it is well known that it is the set of non-units (since in an artinian local ring, every element is either unit or nilpotent). By Wedderburn's little theorem every finite domain is a field, thus we will denote by $\mathbb{F}_q = \mathcal{R}/\mathfrak{m}$ its residue field. There is a natural homomorphism from $\mathcal{R}$ onto $\mathbb{F}_q$, i.e., $\pi : \mathcal{R} \to \mathcal{R}/\mathfrak{m} = \mathbb{F}_q$, $r \mapsto \pi(r) = r + \mathfrak{m}$, for any r in $\mathcal{R}$.

This natural homomorphism from $\mathcal{R}$ onto $\mathbb{F}_q$ can be extended naturally to a homomorphism from $\mathcal{R}^n$ onto $\mathbb{F}_q^n$. It is clear that this map is a surjective ring homomorphism. Note that π maps a linear codes over $\mathcal{R}$ to a linear code over $\mathbb{F}_q$.

Theorem 4.1: *If C and D are two right ideal (or right $\mathcal{R}G$ -submodule) in $\mathcal{R}G$. Then the followings are equivalent*

(1) *the pair (C,D) is LCP in $\mathcal{R}G$;*

(2) *$C = e\mathcal{R}G$ and $D = (1-e)\mathcal{R}G$, where, $e = e^2 \in \mathcal{R}G$.*

Proof: First, suppose that (1) holds. Let $C + D = \mathcal{R}G$ with $C \cap D = \{0\}$ and write $1 = c + d$ with $c \in C$ and $d \in D$. It follows that $c = c^2 - dc = c^2 - cd$. Hence $c - c^2 = cd = dc \in C \cap D$, thus $c = c^2$ and $cd = dc = 0$. Furthermore, if we set $e = c$, then $e\mathcal{R}G \subset C$, $(1-e)\mathcal{R}G \subset D$ and, since $C \oplus D = \mathcal{R}G = e\mathcal{R}G \oplus (1-e)\mathcal{R}G$, we have that $C = e\mathcal{R}G$ and $D = (1-e)\mathcal{R}G$ with $e = e^2$.

Conversely, if we suppose that (2) holds, then $C = e\mathcal{R}G$ and $D = (1-e)\mathcal{R}G$ with $e = e^2 \in \mathcal{R}G$. Since e is an idempotent, we have $\mathcal{R}G = e\mathcal{R}G \oplus (1-e)\mathcal{R}G$. Therefore, we get the desired result.

Lemma 4.1: (See [15]). *If I is an two-sided ideal in the ring $\mathcal{R}$ and G is a finite group, then $\frac{\mathcal{R}G}{IG} \cong \frac{\mathcal{R}}{I}G$.*

Lemma 4.2: *If e is an idempotent element in $\mathbb{F}_q G$, then there exist an element e' in $\mathcal{R}G$ such that $\pi(e') = e$.*

Proof: Since $\mathfrak{m} = J(\mathcal{R})$ is a two-sided ideal in $\mathcal{R}$, then by Lemma 4.1, we get

$$\frac{\mathcal{R}G}{\mathfrak{m}G} \cong \frac{\mathcal{R}}{\mathfrak{m}}G \cong \mathbb{F}_q G$$

and $\frac{\mathcal{R}G}{\mathfrak{m}^i G} \cong \frac{\mathcal{R}}{\mathfrak{m}^i}G$, where $1 \le i \le f$, and $\mathfrak{m}^f = 0$ but $\mathfrak{m}^{f-1} \neq 0$ (note that in an artinian ring, the Jacoson radical is nilpotent).

We will prove the result by induction. Let us define idempotent $e_i \in \frac{\mathcal{R}G}{\mathfrak{m}^i G}$. as follows

(1) If $i = 1$, we set $e_1 = e$, then this lemma holds.

(2) If $i > 1$, let e_{i-1} is an idempotent element in $\frac{\mathcal{R}G}{\mathfrak{m}^{i-1}G}$. Let us consider h be an element in $\frac{\mathcal{R}G}{\mathfrak{m}^i G}$ with its image e_{i-1} in $\frac{\mathcal{R}G}{\mathfrak{m}^{i-1}G}$.

Then it is easy to verify that $h - h^2$ is in $\frac{\mathfrak{m}^{i-1}G}{\mathfrak{m}^i G}$. Hence, $(h-h^2)^2 = 0$.

Now, we set $e_i = (3h^2 - 2h^3)$. Thus $e_i^2 - e_i = (3h^2 - 2h^3)(3h^2 - 2h^3 - 1) = (2h-3)(1+2h)(h-h^2)^2 = 0$. and hhis lemma holds for all i. Since $\mathfrak{m}^f = 0$, so $e' = e_f$.

Theorem 4.2: *If C and D are two group codes in $\mathcal{R}G$ and $\pi(C) = e\mathbb{F}_q G$, $D = (1-e)\mathbb{F}_q G$ with $e = e^2$, then there exist an element e' such that $C = e'\mathcal{R}G$, $D = (1-e')\mathcal{R}G$ with $e'^2 = e'$ and $\pi(e') = e$.*

Proof: Since e is an idempotent element in $\mathbb{F}_q G$ with $\pi(C) = e\mathbb{F}_q G$, $\pi(D) = (1-e)\mathbb{F}_q G$, the pair $(\pi(C), \pi(D))$ is an LCP in $\mathbb{F}_q G$. Now from Lemma 4.2, we there exists e' such that $\pi(e') = e$. In particular, take $C = e'\mathcal{R}G$ and $D = (1-e')\mathcal{R}G$.

Theorem 4.3: *If C and D are two group codes over $\mathcal{R}G$, then the pair (C, D) is a LCP in $\mathcal{R}G$ if and only if $(\pi(C), \pi(D))$ is a LCP in $\mathbb{F}_q G$.*

Proof: Let us assume that the pair (C, D) is LCP in $\mathcal{R}G$, by the Theorem 4.1, there exist a idempotent e in $\mathcal{R}G$ such that $C = e\mathcal{R}G$, $D = (1-e)\mathcal{R}G$. Since π is a surjective homomorphism from $\mathcal{R}G$ to $\mathbb{F}_q G$, then we obtain that

$$\pi(C) = \pi(e)\mathbb{F}_q G,\ \pi(D) = (1-\pi(e))\mathbb{F}_q G.$$

Whence, the pair $(\pi(C), \pi(D))$ is a LCP in $\mathbb{F}_q G$.

Conversely, let us suppose that $(\pi(C), \pi(D))$ is a LCP in $\mathbb{F}_q G$. Then there exists an idempotent e in $\mathbb{F}_q G$ such that $\pi(C) = e\mathbb{F}_q G$ and $\pi(D) = (1-e)\mathbb{F}_q G$. Then by Theorem 4.2, there is e' in $\mathcal{R}G$ such that $C = e'\mathcal{R}G$ and $D = (1-e')\mathcal{R}G$ with $e'^2 = e'$. Hence the pair (C, D) is a LCP in $\mathcal{R}G$.

Lemma 4.3: *If $C = e\mathcal{R}G$ with $e = e^2$, then the dual of C is given by $C^{\perp} = (1-\hat{e})\mathcal{R}G$.*

Proof: It is easily seen that $\hat{e}^2 = \hat{e}$ and also $\langle ab, c\rangle = \langle b, \hat{e}c\rangle$, for all a, b, c in $\mathcal{R}G$. For any x in $(1-\hat{e})\mathcal{R}G$, then $x = (1-\hat{e})f$, for some f in $\mathcal{R}G$. Therefore, $\langle ea, x\rangle = \langle ea, (1-\hat{e})\ f\rangle = \langle a, \hat{e}\ (1-\hat{e})\ f\rangle = 0$, for all ea in C. Hence $(1-\hat{e})\ \mathcal{R}G \subseteq C^{\perp}$. Taking into account that $C = e\mathcal{R}G$ and $e\mathcal{R}G \cong \hat{e}\mathcal{R}G$ we have

$$|C^{\perp}| = \frac{|\mathcal{R}G|}{|C|} = \frac{|e\mathcal{R}G|\ |(1-e)\mathcal{R}G|}{|C|} = |(1-e)\mathcal{R}G| = |(1-\hat{e})\mathcal{R}G|$$

Thus, we obtain the desired result.

Theorem 4.4: *If $e \in Z(\mathcal{R}G)$ with $e = e^2$, then $C = e\mathcal{R}G$ and $D^{\perp} = \hat{e}\mathcal{R}G$ are permutation equivalent.*

Proof: Note that (C,D) is an LCP group code in $\mathcal{R}G$ with $C = e\mathcal{R}G$ and $D = (1-e)\mathcal{R}G$, as e is idempotent. By Lemma 4.3 we know that $D^{\perp} = \hat{e}\mathcal{R}G$. Thus for the group code C, $\hat{C}$ is given by

$$\begin{aligned}\hat{C} &= \{\hat{a} \in \mathcal{R}G : \forall\, a \in C = e\mathcal{R}G\} = \{\widehat{e\theta} \in \mathcal{R}G : \forall\, e\theta \in C = e\mathcal{R}G\} \\ &= \{\hat{\theta}\hat{e} \in \mathcal{R}G : \forall\, e\theta \in C = e\mathcal{R}G\} \overset{(*)}{=} \{\theta\hat{e} \in \mathcal{R}G : \forall\, \theta \in \mathcal{R}G\} \\ &\overset{(**)}{=} \{\hat{e}\theta \in \mathcal{R}G : \forall\, \theta \in \mathcal{R}G\} = D^{\perp},\end{aligned}$$

where (*) holds because $RG \cong \widehat{RG}$ and (**) holds because $e \in Z(\mathcal{R}G)$. This completes the proof.

5. LCP group codes over finite non-commutative Frobenius rings

In this section, we will denote $\mathcal{R}$ as a finite non-commutative ring with identity $1_{\mathcal{R}}$.

Theorem 5.1: *Let C and D be two group codes in $\mathcal{R}G$. Then the pair (C,D) forms an LCP of group codes in $\mathcal{R}G$ if and only if $C = \oplus_{i=1}^{u} e_i\mathcal{R}G$ and $D = \oplus_{i=u+1}^{u+v} e_i\mathcal{R}G$ with $\sum_{i=1}^{u+v} e_i = 1$, $e_i^2 = e_i$ for all $1 \le i \le u+v$ and $e_ie_j = 0$ for all $i \ne j$.*

Proof: Let us assume that the pair (C,D) is an LCP group code in $\mathcal{R}G$. Hence $C \oplus D = \mathcal{R}G$, so C and D both are projective. By Theorem 3.3, C can be written as the direct sum of indecomposable ideals, i.e., $C = \bigoplus_{i=1}^{u} I_i$, where $I_i = a_i\mathcal{R}G$ for all $1 \le i \le u$. Since C is projective and $\mathcal{R}G$ is Frobenius, then by Theorem 2.2 we obtain that $I_i = a_i\mathcal{R}G$ is injective. Now, consider $\gamma : a_i\mathcal{R}G \to I_i$ given by $\gamma(a_ir) = a_ir$. By Baer's criterion in Theorem 2.1 we have that $\gamma = m\cdot$, where $m \in I_i$, that is $m = a_ib$ with $b \in \mathcal{R}G$, and henceforth $a_i = \gamma(a_i) = ma_i = a_iba_i$, and $a_i\mathcal{R}G = e_i\mathcal{R}G$ where $e_i^2 = e_i = a_ib$. Hence a_i is idempotent element. Therefore, it follows from the Theorem 3.2 that a_i is primitive. Whence, $C = \bigoplus_{i=1}^{u} a_i\mathcal{R}G$, where a_i is primitive idempotent for all $1 \le i \le u$.

Similarly, $D = \bigoplus_{j=1}^{v} b_j\mathcal{R}G$, where b_i is primitive idempotent for all $1 \le i \le u$. Since $C \oplus D = \mathcal{R}G$, then

$$\left(\bigoplus_{i=1}^{u} a_i\mathcal{R}G\right) \oplus \left(\bigoplus_{j=1}^{v} b_j\mathcal{R}G\right) = \mathcal{R}G.$$

Then by Theorem 3.1, we get set of idempotents $e_1, \ldots, e_u, e_{u+1}, \ldots, e_{u+v}$ such that $C = \overset{u}{\underset{i=1}{\oplus}} e_i \mathcal{R}G$ and $D = \overset{u+v}{\underset{i=u+1}{\oplus}} e_i \mathcal{R}G$ with $\sum_{i=1}^{u+v} e_i = 1$ with $e_i^2 = e_i$ for all $1 \le i \le u+v$ and $e_i e_j = 0$ for all $i \ne j$.

Conversely, let $C = \overset{u}{\underset{i=1}{\oplus}} e_i \mathcal{R}G$ and $D = \overset{u+v}{\underset{i=u+1}{\oplus}} e_i \mathcal{R}G$ with $\sum_{i=1}^{u+v} e_i = 1$ with $e_i^2 = e_i$ for all $1 \le i \le u+v$ and $e_i e_j = 0$ for all $i \ne j$. Therefore, $C + D = \mathcal{R}G$, as $\sum_{i=1}^{u+v} e_i = 1$ and $C \cap D = \mathcal{R}G$ as $e_i e_j = 0$ and $e_i^2 = e_i$. Whence, the pair (C, D) forms an LCP group code in $\mathcal{R}G$.

Theorem 5.2: *Let C and D be two group codes in $\mathcal{R}G$. Then the pair (C, D) forms an LCP group code in $\mathcal{R}G$ if and only if $C = e\mathcal{R}G$ and $D = (1-e)\mathcal{R}G$ with $e^2 = e \in \mathcal{R}G$.*

Proof: In Theorem 5.1, we set $e = \sum_{i=1}^{u} e_i$. It is easily verified that $e^2 = e$ and we get our required result.

Theorem 5.3: *If $C = \overset{u}{\underset{i=1}{\oplus}} e_i \mathcal{R}G$ with $\sum_{i=1}^{u+v} e_i = 1$, $e_i^2 = e_i$ for all $1 \le i \le u+v$ and $e_i e_j = 0$ for all $i \ne j$, then the dual of C, i.e., $C^{\perp} = \overset{v}{\underset{i=u+1}{\oplus}} \hat{e}_i \mathcal{R}G$.*

Proof: The dual of C, i.e.,

$$C^{\perp} = \left(\overset{u}{\underset{i=1}{\oplus}} e_i \mathcal{R}G \right)^{\perp} = \bigcap_{i=1}^{u} (e_i \mathcal{R}G)^{\perp} \overset{(*)}{=} \bigcap_{i=1}^{u} (1 - \hat{e}_i)\mathcal{R}G$$
$$\overset{(**)}{=} (1 - \sum_{i=1}^{u} \hat{e}_i)\mathcal{R}G \overset{(***)}{=} \overset{v}{\underset{i=u+1}{\oplus}} \hat{e}_i \mathcal{R}G$$

where $(*)$ follows from Lemma 4.3, $(**)$ holds because $e_i e_j = 0$ and $(***)$ because $\sum_{i=1}^{u+v} e_i = 1$. Thus, we get $C^{\perp} = \overset{v}{\underset{i=u+1}{\oplus}} \hat{e}_i \mathcal{R}G$.

Theorem 5.4: *If $e_i \in Z(\mathcal{R}G)$ with $\sum_{i=1}^{u+v} e_i = 1$, $e_i^2 = e_i$ for all $1 \le i \le u+v$ and $e_i e_j = 0$ for all $i \ne j$, then $C = \overset{u}{\underset{i=1}{\oplus}} e_i \mathcal{R}G$ and $D^{\perp} = \overset{u}{\underset{i=1}{\oplus}} \hat{e}_i \mathcal{R}G$ are permutation equivalent.*

Proof: For given group code C, $\hat{C}$ is defined as follows (note that $\widehat{\ }$ is homomorphism under addition and an antisomorphism and that $e_i \in Z(\mathcal{R}G)$)

$$\begin{aligned}\hat{C} &= \left\{\hat{c} : c \in C = \bigoplus_{i=1}^{u} e_i \mathcal{R}G\right\} = \left\{\widehat{\sum_{i=1}^{u} e_i f_i} : \sum_{i=1}^{u} e_i f_i \in \mathcal{R}G\right\} \\ &= \left\{\sum_{i=1}^{u} \widehat{e_i f_i} : f_i \in \mathcal{R}G\right\} = \left\{\sum_{i=1}^{u} \hat{f}_i \hat{e}_i : f_i \in \mathcal{R}G\right\} = \left\{\sum_{i=1}^{u} \hat{e}_i \hat{f}_i : f_i \in \mathcal{R}G\right\} \\ &= D^{\perp},\end{aligned}$$

which completes the proof.

6. Checkable codes

In this section, we will characterize checkable codes in $\mathcal{R}G$ for a finite group G over a finite Frobenius ring $\mathcal{R}$. Let I be a right ideal in $\mathcal{R}G$, the left annihilator of I is defined by $\mathrm{Ann}_l(I) = \{r \in \mathcal{R}G \mid r \cdot a = 0 \ \forall\, a \in I\}$. Let J be a left ideal in $\mathcal{R}G$, the right annihilator of J is defined by $\mathrm{Ann}_r(J) = \{s \in \mathcal{R}G \mid a \cdot s = 0 \ \forall\, a \in J\}$. The following result follows from [11, 16].

Proposition 6.1: For a group ring $\mathcal{R}G$ over Frobenius ring $\mathcal{R}$, then

(a) $\mathrm{Ann}_r(a) = \mathrm{Ann}_r(\mathcal{R}Ga)$ for any a in $\mathcal{R}G$.

(b) $\mathrm{Ann}_l(a) = \mathrm{Ann}_l(a\mathcal{R}G)$ for any a in $\mathcal{R}G$.

(c) $I = \mathrm{Ann}_l(\mathrm{Ann}_r(I))$ for any left ideal I in $\mathcal{R}G$.

(d) $J = \mathrm{Ann}_r(\mathrm{Ann}_l(J))$ for any right ideal J in $\mathcal{R}G$.

(e) $|I|\,|\mathrm{Ann}_r(I)| = \mathcal{R}G$, for a left ideal I in $\mathcal{R}G$.

(f) $|J|\,|\mathrm{Ann}_l(J)| = \mathcal{R}G$, for a right ideal J in $\mathcal{R}G$.

Definition 6.1 (Checkable codes):

(a) A right ideal I in $\mathcal{R}G$ is called checkable if there exists an element u in $\mathcal{R}G$ such that $I = \{a \mid a \in \mathcal{R}G,\ ua = 0\} = \mathrm{Ann}_r(u) = \mathrm{Ann}_r(\mathcal{R}Gu)$.

(b) A group algebra $\mathcal{R}G$ is called code-checkable if all right ideals of $\mathcal{R}G$ are checkable.

Theorem 6.1: *In $\mathcal{R}G$ a right (resp. left) ideal I is checkable if and only if* $\mathrm{Ann}_l(I)$ (*resp.* $\mathrm{Ann}_r(I)$) *is a principal left (resp. right) ideal.*

Lemma 6.1: *If C is a right (resp. left) ideal in $\mathcal{R}G$, then $C^{\perp} = \widehat{\mathrm{Ann}_l(C)}$ $(resp.\, C^{\perp} = \widehat{\mathrm{Ann}_r(C)})$.*

Proof: Let us assume C is a right ideal in $\mathcal{R}G$. For any element $a \in \widehat{\mathrm{Ann}_l(C)}$, this implies $\hat{a} \in \mathrm{Ann}_l(C)$, and $\hat{a}cg = 0$ for all $c \in C$ and $g \in G$. Then we obtain that $\langle a, c \rangle = 0$ for all $c \in C$, hence $a \in C^{\perp}$. Therefore, $\widehat{\mathrm{Ann}_r(C)} \subseteq C^{\perp}$.

$$|C^{\perp}| = \frac{|\mathcal{R}G|}{|C|} = |\widehat{\mathrm{Ann}_l(C)}|,$$

which completes the proof.

Theorem 6.2: *If C is a right ideal (or right $\mathcal{R}G$-submodule) in $\mathcal{R}G$. Then the following statements are equivalent*

(1) *C is checkable;*

(2) *$C^{\perp}$ is a principal right ideal.*

Proof: Let us assume C is checkable, thus by Theorem 6.1, $\mathrm{Ann}_l(C)$ is a principal left ideal in $\mathcal{R}G$, i.e., $\mathrm{Ann}_l(C) = \mathcal{R}Gu$, for some $u \in \mathcal{R}G$. Then, applying Lemma 6.1, we have that $C^{\perp} = \widehat{\mathrm{Ann}_l(C)} = \widehat{\mathcal{R}Gu} = \hat{u}\mathcal{R}G$, hence we get the desired result.

Note that for checkable code C, we have $C^{*} \cong \mathcal{R}G / v\mathcal{R}G$, for some $u \in \mathcal{R}G$. Since, by applying consequence of Theorem 6.2, i.e., $C^{*} \cong \mathcal{R}G / C^{\perp}$.

For a finite group G and a finite Frobenius ring $\mathcal{R}$, we recall that the group ring $\mathcal{R}G$ can be written as $\mathcal{R}G = \bigoplus_{i=1}^{s} e_i \mathcal{R}G$, where $e_i\mathcal{R}G$ is a indecomposable submodule in $\mathcal{R}G$, $\sum_{i=1}^{s} e_i = 1$, $e_i^2 = e_i$, for all $i = 1, \ldots, s$ and $e_i e_j = 0$ for all $i \neq j$. Further, if e_i are primitive idempotents in the centre of $\mathcal{R}G$, then $e_i\mathcal{R}G$ are both side indecomposable submodule of $\mathcal{R}G$.

If C is a group code in $\mathcal{R}G$, then

$$C = \sum_{i_j=0}^{t} e_{i_j} \mathcal{R}G, \tag{6.1}$$

where $0 \leq t \leq s$. Therefore, $C = \sum_{i_j=0}^{t} e_{i_j} \mathcal{R}G$, if and only if $C = \mathrm{Ann}_r\,(\mathcal{R}G(1 - \sum_{i_j=0}^{t} e_{i_j})) = \mathrm{Ann}_r\,(\mathcal{R}G \sum_{i_k=0}^{r} e_{i_k})$, where $\sum_{i_j=0}^{t} e_{i_j} + \sum_{i_k=0}^{r} e_{i_k} = 1$, and from Proposition 6.1(a) it follows that $C = \mathrm{Ann}_r(\sum_{i_k=0}^{r} e_{i_k})$.

Proposition 6.2: Let C is a group code in $\mathcal{R}G$, and $C = \sum_{i_j=0}^{t} e_{i_j}\mathcal{R}G$ its decomposition as in Equation 6.1 where $\sum_{i_j=0}^{t} e_{i_j} + \sum_{i_k=0}^{r} e_{i_k} = 1$. Then C is a checkable code if and only if $C = \bigcap_{i_k=0}^{r} \mathrm{Ann}_r(\mathcal{R}Ge_{i_k})$.

Proof: It follows from the above reasonig and the well known fact that

$$\mathrm{Ann}_r(\sum_{i_k=0}^{r} e_{i_k}) = \bigcap_{i_k=0}^{r} \mathrm{Ann}_r(e_{i_k}) = \bigcap_{i_k=0}^{r} \mathrm{Ann}_r(\mathcal{R}Ge_{i_k}).$$

Acknowledgements

First and fourth authors were supported from the IHUB-ANUBHUTI-IIITD FOUNDATION set up under the NM-ICPS scheme of the Department of Science and Technology, India, under Grant no. IHUB Anubhuti/Project Grant/12. Third author was partially supported by Grant TED2021-130358B-I00 funded by MCIN/AEI/10.13039/501100011033 and by the "European Union NextGenerationEU/PRTR"

References

[1] S. Bhowmick, A. Fotue-Tabue, E. Martínez-Moro, R. Bandi, and S. Bagchi, "Do non-free LCD codes over finite commutative Frobenius rings exist?" *Des. Codes Cryptogr.,* vol. 88, no. 5, pp. 825–840 (2020).

[2] M. Borello, J. de la Cruz, and W. Willems, "A note on linear complementary pairs of group codes," *Discrete Math.,* vol. 343, no. 8, 111905 (2020).

[3] M. Borello, J. de la Cruz, and W. Willems, "On checkable codes in group algebras," *J. Algebra Appl.,* vol. 21, no. 6, Paper No. 2250125, 11 (2022).

[4] C. Carlet and S. Guilley, "Complementary dual codes for counter-measures to side-channel attacks," *Adv. Math. Commun.,* vol. 10, no. 1, pp. 131–150 (2016).

[5] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya, and P. Solé, "On linear complementary pairs of codes," *IEEE Trans. Inform. Theory,* vol. 64, no. 10, pp. 6583–6589 (2018).

[6] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, "Linear codes over Fq are equivalent to LCD codes for q>3," *IEEE Trans. Inform. Theory,* vol. 64, no. 4, part 2, pp. 3010–3017 (2018).

[7] J. de la Cruz and W. Willems, "On group codes with complementary duals," *Des. Codes Cryptogr.,* vol. 86, no. 9, pp. 2065–2073 (2018).

[8] D. S. Dummit and R. M. Foote, Abstract Algebra, 3rd ed., Hoboken, NJ: John Wiley & Sons, Inc. (2004).

[9] C. Güneri, E. Martínez-Moro, and S. Sayıcı, "Linear complementary pair of group codes over finite chain rings," *Des. Codes Cryptogr.,* vol. 88, no. 11, pp. 2397–2405 (2020).

[10] C. Güneri, B. Özkaya, and S. Sayıcı, "On linear complementary pair of n-dimensional cyclic codes," *IEEE Commun. Lett.,* vol. 22, no. 12, pp. 2404–2406 (2018).

[11] T. Y. Lam, Lectures on Modules and Rings, vol. 189, Graduate Texts in Mathematics, New York: Springer-Verlag (1999).

[12] X. Liu and H. Liu, "LCP of group codes over finite Frobenius rings," *Des. Codes Cryptogr.,* vol. 91, no. 3, pp. 695–708 (2023).

[13] E. Martínez-Moro, A. Piñera Nicolás, and I. F. Rúa, "Multivariable codes in principal ideal polynomial quotient rings with applications to additive modular bivariate codes over F4," *J. Pure Appl. Algebra,* vol. 222, no. 2, pp. 359–367 (2018).

[14] J. L. Massey, "Linear codes with complementary duals," vol. 106/107, pp. 337–342, A collection of contributions in honour of Jack van Lint (1992).

[15] C. Polcino Milies and S. K. Sehgal, An Introduction to Group Rings, vol. 1, Algebra and Applications, Dordrecht: Kluwer Academic Publishers (2002).

[16] J. A. Wood, "Duality for modules over finite rings and applications to coding theory," *Amer. J. Math.,* vol. 121, no. 3, pp. 555–575 (1999).

[17] X. Yang and J. L. Massey, "The condition for a cyclic code to have a complementary dual," *Discrete Math.,* vol. 126, no. 1–3, pp. 391–393 (1994).

Received April, 2024