

LINEAR COMPLEMENTARY PAIR OF GROUP CODES OVER FINITE CHAIN RINGS

CEM GÜNERİ, EDGAR MARTÍNEZ-MORO, SELCEN SAYICI

ABSTRACT. Linear complementary dual (LCD) codes and linear complementary pair (LCP) of codes over finite fields have been intensively studied recently due to their applications in cryptography, in the context of side channel and fault injection attacks. The security parameter for an LCP of codes (C, D) is defined as the minimum of the minimum distances $d(C)$ and $d(D^\perp)$. It has been recently shown that if C and D are both 2-sided group codes over a finite field, then C and D^\perp are permutation equivalent. Hence the security parameter for an LCP of 2-sided group codes (C, D) is simply $d(C)$. We extend this result to 2-sided group codes over finite chain rings.

Keywords: LCP of codes, group codes, finite chain rings, code equivalence.

1. INTRODUCTION

A pair of linear codes (C, D) of length n over a finite field \mathbb{F}_q is called a linear complementary pair (LCP) of codes if $C \cap D = \{0\}$ and $C + D = \mathbb{F}_q^n$ (i.e. $C \oplus D = \mathbb{F}_q^n$). In the case $D = C^\perp$, C is referred as a linear complementary dual (LCD) code.

LCD codes were introduced by Massey [10] in 1992. There has been a revived interest in LCD and LCP of codes due to their application in protection against side channel and fault injection attacks ([1, 4]). In this context, the security parameter of an LCP (C, D) is defined to be $\min\{d(C), d(D^\perp)\}$, where $d(C)$ stands for the minimum distance of the code C . In the LCD case, this parameter is simply $d(C)$, since $D^\perp = C$.

Carlet et al. ([5]) showed that if (C, D) is LCP, where C and D are both cyclic codes over a finite field \mathbb{F}_q , then C is equivalent to D^\perp . They showed that the same result holds if C and D are 2D cyclic codes, under the assumption that the length of the codes is relatively prime to the characteristic of the finite field (semisimple case). Cyclic and 2D cyclic codes are special abelian codes, which are defined as ideals of the group algebra $\mathbb{F}_q[G]$ for a finite abelian group G . In the case $\gcd(q, |G|) = 1$, Güneri et al. extended this result to LCP of abelian codes in $\mathbb{F}_q[G]$ ([6]). If G is any finite group (not necessarily abelian), a right ideal of $\mathbb{F}_q[G]$ is called a group code. In [3], 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 2-sided group codes (ideals) in $\mathbb{F}_q[G]$, then C and D^\perp are permutation equivalent. Note in particular that this implies $d(C) = d(D^\perp)$. Hence,

C. Güneri and S. Sayıcı are with Sabancı University, Faculty of Engineering and Natural Sciences, İstanbul, Turkey. Email: guneri@sabanciuniv.edu, selcensayici@sabanciuniv.edu.

E. Martinez-Moro is with University of Valladolid, Institute of Mathematics, Castilla, Spain. Email: edgar.martinez@uva.es.

there is an LCP of 2-sided group codes over finite fields which has as good a security parameter as the 2-sided group code with the best minimum distance.

Although LCD and LCP of codes have been extensively studied over finite fields, the literature on codes over rings in this context is very limited. LCD codes over rings, including chain rings, have been addressed recently in [2, 8, 9]. Here, we study LCP of codes over rings for the first time. Our main contribution is the extension of the result in [3] to finite chain rings. Namely, we prove that for an LCP of 2-sided group codes (C, D) in $R[G]$, where R is a finite chain ring and G is any finite group, C and D^\perp are equivalent codes (Theorem 3.9).

2. BACKGROUND

Unless otherwise stated R denotes a chain ring, which is a finite commutative ring with identity whose lattice of ideals forms a chain. Note that a finite field is a special chain ring. It is clear that R is a local ring and it is well-known that R is a principal ideal ring. Let γ be a generator of the maximal ideal and let the ideals of R be

$$R = R\gamma^0 \supset R\gamma \supset \cdots \supset R\gamma^{v-1} \supset R\gamma^v = \{0\}.$$

The number v with $\gamma^v = 0$ is called the nilpotency index of γ . Note that since R is a commutative ring, $R\gamma^i = \gamma^i R$ for all i .

It is clear that $R/R\gamma$ is a finite field, which we will denote by \mathbb{F}_q . The natural projection map $\varphi : R \rightarrow \mathbb{F}_q$ takes a ring element to its coset modulo $R\gamma$. This map is a surjective ring homomorphism and it extends to R^n and takes values in \mathbb{F}_q^n via

$$(2.1) \quad (r_i) \longmapsto \varphi(r_i),$$

where (r_i) denotes an n -tuple over R . We will denote the extended map by φ as well, which is a surjective R -module homomorphism. The kernel of this map is the set of all n tuples whose coordinates are multiples of γ (i.e. $(\gamma R)^n$). We will also denote this set with γR^n . Observe that φ maps an R -submodule of R^n to an \mathbb{F}_q -subspace of \mathbb{F}_q^n . An R -submodule of R^n is called a linear code over R . Hence, φ maps a linear code over R to a linear code over \mathbb{F}_q .

Now, let G be a finite group and denote by $R[G]$ the group ring of G over R . Hence the elements of $R[G]$ are of the form $\sum_{g \in G} \alpha_g g$, where $\alpha_g \in R$ and α_g is nonzero for finitely many $g \in G$. If G has order n , then it is clear that $R[G]$ and R^n are isomorphic as R -modules, where an element $\sum_{g \in G} \alpha_g g \in R[G]$ is identified with the n tuple (α_g) . We will use this identification throughout the text. The group rings will be specifically used when we have results which are valid for group codes over R . A right ideal of $R[G]$ is called a group code over R (see [3] for group codes over finite fields). Our main result (Theorem 3.9) holds for 2-sided ideals in $R[G]$. Therefore, unless otherwise stated, ideals will be 2-sided throughout and they will be referred to as group codes. If G is abelian, then a group code (ideal) in $R[G]$ is called an abelian code over R .

Remark 2.1. If G and G' are finite multiplicative groups which are isomorphic via a map ψ , and if R is any ring, then it is easy to see that ψ extends to a ring isomorphism

$$\begin{aligned} \psi : R[G] &\longrightarrow R[G'] \\ \sum_{g \in G} r_g g &\longmapsto \sum_{g \in G} r_g \psi(g) \end{aligned}$$

Hence such a map takes a group code in $R[G]$ to a group code in $R[G']$. If $G = G'$, we can consider an automorphism of G as a permutation on G . Note that an arbitrary permutation of G does not necessarily preserve the ideal structure in $R[G]$ but those which are automorphisms do.

A pair of linear codes (C, D) in R^n is called a linear complementary pair (LCP) of codes if $C \oplus D = R^n$. When $D = C^\perp$, C is said to be a linear complementary dual (LCD) code over R . The dual in this article will always be considered with respect to the Euclidean inner product on R^n . It is easy to see that the dual of a group code in $R[G]$ is also a group code.

For a finite field \mathbb{F} and an arbitrary finite group G , consider LCP of (2-sided) group codes (C, D) in $\mathbb{F}[G]$. Borello et al. showed in [3] that C is permutation equivalent to D^\perp . The permutation yielding the equivalence, which we will later denote by τ , is the inversion automorphism that takes g to g^{-1} , for all $g \in G$. We will extend this equivalence result to LCP of group codes over finite chain rings.

3. LCP OF GROUP CODES OVER CHAIN RINGS

We use the notation and notions introduced in Section 2. In particular, all codes over R are linear (i.e. R -module) and a group code in $R[G]$ is a 2-sided ideal.

Lemma 3.1. *If (C, D) is LCP of codes in R^n , then both C and D are free modules (codes).*

Proof. Note that by definition (being direct summands of the free module R^n), both C and D are projective modules over R . A chain ring is local and by [7, Theorem 2], a projective module over a local ring is free. \square

Proposition 3.2. (i) *If (C, D) is LCP of codes in R^n , then $(\varphi(C), \varphi(D))$ is LCP of codes in \mathbb{F}_q^n .*

(ii) *If (C, D) is LCP of group codes in $R[G]$, then $(\varphi(C), \varphi(D))$ is LCP of group codes in $\mathbb{F}_q[G]$.*

Proof. (i) Let $x \in \mathbb{F}_q^n$. Since R^n is the direct sum of C, D , and φ is surjective, there exist $c \in C, d \in D$ such that $x = \varphi(c) + \varphi(d)$. Hence, \mathbb{F}_q^n is the sum of $\varphi(C)$ and $\varphi(D)$.

Let x be in the intersection $\varphi(C) \cap \varphi(D)$. Then $x = \varphi(c) = \varphi(d)$, for some $c \in C, d \in D$. This gives $\varphi(c - d) = 0$, and hence $(c - d) \in \gamma R^n$. Therefore, $\gamma^{v-1}(c - d) = 0$. Set

$$z := \gamma^{v-1}c = \gamma^{v-1}d.$$

Note that z is in $C \cap D$, which is by assumption trivial. So, $z = \gamma^{v-1}c = 0$, which yields $c \in \gamma R^n$. Hence, $x = \varphi(c) = 0$ and $\varphi(C) \cap \varphi(D) = \{0\}$.

(ii) We need to show that a left ideal $C \subset R[G]$ is mapped to a left ideal $\varphi(C) \subset \mathbb{F}_q[G]$, since the rest follows by part (i). For this, it suffices to show that $\varphi(C)$ is closed under left multiplication

by an arbitrary element $g' \in G$, since being closed under left multiplication by a general element in $\mathbb{F}_q[G]$ then follows by linearity. If $\sum_g c_g g \in C$, then

$$g' \varphi \left(\sum_g c_g g \right) = g' \sum_g \varphi(c_g) g = \sum_g \varphi(c_g) g' g = \varphi \left(g' \left(\sum_g c_g g \right) \right).$$

Since C is a left ideal, $g' \sum_g c_g g \in C$. Hence, $\varphi(C)$ is a left ideal in $\mathbb{F}_q[G]$. The proof for right ideal property is identical. \square

For an element $r \in R$ and $x \in R^n$, rx denotes the scalar multiplication, where each coordinate of x is multiplied by r . For a code C in $R[G]$, we set $rC := \{rc : c \in C\}$. We define

$$(C : r) := \{x \in R^n : rx \in C\},$$

which is a linear code in R^n . It is clear that

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

which implies

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

We collect some facts which will be needed. Let us note that the dual code of $C \subset R^n$ (with respect to the Euclidean product) is defined as in codes over finite fields, and it is denoted by C^\perp .

Proposition 3.3. ([11, Theorem 3.10]) *Let C be a code in R^n . Then,*

- (i) $|C^\perp| = |R^n|/|C|$.
- (ii) $\varphi((C : \gamma^{v-1-i}))^\perp = \varphi((C^\perp : \gamma^i))$, for all i .

Proposition 3.4. ([11, Proposition 3.13], [12, Proposition 3.11 and Corollary 3.12]) *The following holds for a free code C in R^n .*

- (i) C^\perp is free.
- (ii) $\varphi(C) = \varphi((C : \gamma)) = \cdots = \varphi((C : \gamma^{v-1}))$.
- (iii) $C \cap \gamma^i R^n = \gamma^i C$, for all i .
- (iv) For $\tilde{C} := C \setminus \gamma R^n = C \setminus \gamma C$, we have $C = \tilde{C} \cup \gamma \tilde{C} \cup \cdots \cup \gamma^{v-1} \tilde{C} \cup \{0\}$.

We are ready to proceed with the steps of our proof.

Proposition 3.5. *If (C, D) is LCP of codes in R^n , then (C^\perp, D^\perp) is also LCP.*

Proof. Let x be an element of $C^\perp \cap D^\perp$ and let $u = u_C + u_D$ be an arbitrary element in R^n , where $u_C \in C$ and $u_D \in D$. Then the Euclidean product of x and u is

$$x \cdot (u_C + u_D) = x \cdot u_C + x \cdot u_D = 0,$$

since x is orthogonal to both C and D . So, $x = 0$ since its inner product with any element in R^n is 0. Therefore $C^\perp \cap D^\perp = \{0\}$.

For $c, c' \in C^\perp$ and $d, d' \in D^\perp$, if $c + d = c' + d'$ then $c - c' = d' - d \in C^\perp \cap D^\perp$. But this intersection is shown to be trivial, hence $c = c'$ and $d = d'$. Therefore the number of elements in $C^\perp + D^\perp = \{c' + d' : c' \in C^\perp, d' \in D^\perp\}$ is $|C^\perp||D^\perp|$. By Proposition 3.3,

$$|C^\perp||D^\perp| = \frac{|R^n|^2}{|C||D|} = |R^n|.$$

Hence, $C^\perp + D^\perp = R^n$. The result follows since the two dual codes intersect only at 0. \square

Proposition 3.6. (i) For a free code $C \subset R^n$, we have $\varphi(C)^\perp = \varphi(C^\perp)$.

(ii) If (C, D) is LCP of group codes in $R[G]$, then $\varphi(C)$ and $\varphi(D^\perp)$ are equivalent codes.

Proof. (i) We have $\varphi(C)^\perp = \varphi((C^\perp : \gamma^{v-1}))$ by Proposition 3.3. By Proposition 3.4 ((i) and (ii)), $\varphi((C^\perp : \gamma^{v-1})) = \varphi(C^\perp)$ for the free code C^\perp . Hence the result follows.

(ii) By Proposition 3.2, $(\varphi(C), \varphi(D))$ is LCP of group codes in $\mathbb{F}_q[G]$. Then by [3] (cf. Section 2), $\varphi(C)$ and $\varphi(D)^\perp$ are equivalent group codes. The result follows since D is a free code and we have $\varphi(D)^\perp = \varphi(D^\perp)$ by part (i). \square

Remark 3.7. Note that for an LCP of group codes (C, D) in $R[G]$, we have

$$\begin{aligned} |D^\perp| &= \frac{|R[G]|}{|D|} \quad (\text{by Proposition 3.3(i)}) \\ &= \frac{|C||D|}{|D|} \quad (\text{since } C \oplus D = R[G]) \\ &= |C|. \end{aligned}$$

Let τ denote the permutation between $\varphi(C)$ and $\varphi(D^\perp)$ ([3]). Then,

$$\varphi(\tau(C)) = \tau(\varphi(C)) = \varphi(D^\perp).$$

For a free code over R , the minimum distance is equal to the minimum distance of its image under φ ([12, Corollary 4.3]). A permutation clearly preserves the minimum distance. Hence, we have

$$d(C) = d(\tau(C)) = d(\varphi(\tau(C))) = d(\varphi(D^\perp)) = d(D^\perp).$$

Our aim is to lift the equivalence τ between $\varphi(C)$ and $\varphi(D^\perp)$ to an equivalence between C and D^\perp , whose cardinalities and minimum distances have been shown to be equal.

From this point on, we consider an LCP of group codes (C, D) in $R[G]$, since we will build up a proof for the main result (Theorem 3.9) from the permutation equivalence between $\varphi(C)$ and $\varphi(D^\perp)$ (cf. Proposition 3.6, Remark 3.7). However, note that Proposition 3.8 is true more generally (for free codes in R^n).

If we restrict the map $\varphi : R[G] \rightarrow \mathbb{F}_q[G]$ to the (free) group codes C and D^\perp , and use Proposition 3.4(iii), we obtain the isomorphisms

$$(3.1) \quad C/(C \cap \gamma R[G]) = C/\gamma C \simeq \varphi(C) \quad \text{and} \quad D^\perp/(D^\perp \cap \gamma R[G]) = D^\perp/\gamma D^\perp \simeq \varphi(D^\perp).$$

Let $t := |\varphi(C)| = |\varphi(D^\perp)|$ and set the elements of the cosets $C/\gamma C$ and $D^\perp/\gamma D^\perp$ as follows:

$$\begin{aligned} C/\gamma C &:= \{c_1 + \gamma C = \gamma C, c_2 + \gamma C, \dots, c_t + \gamma C\}, \\ D^\perp/\gamma D^\perp &:= \{d_1 + \gamma D^\perp = \gamma D^\perp, d_2 + \gamma D^\perp, \dots, d_t + \gamma D^\perp\}. \end{aligned}$$

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

$$(3.2) \quad C = \dot{\bigcup}_{1 \leq i \leq t} (c_i + \gamma C) \quad \text{and} \quad D^\perp = \dot{\bigcup}_{1 \leq i \leq t} (d_i + \gamma D^\perp)$$

Note that φ is constant on cosets, since a multiple of γ is mapped to 0. Namely for all $i = 1, \dots, t$, we have

$$\begin{aligned} \varphi(c_i + \gamma c) &= \varphi(c_i) + \varphi(\gamma c) = \varphi(c_i) \quad \text{for all } c \in C, \\ \varphi(d_i + \gamma d) &= \varphi(d_i) + \varphi(\gamma d) = \varphi(d_i) \quad \text{for all } d \in D^\perp. \end{aligned}$$

Moreover $\varphi(c_i) \neq \varphi(c_j)$ (for $i \neq j$), since otherwise c_i and c_j would be in the same coset modulo γC . The same holds for representatives of cosets of D^\perp modulo γD^\perp . Hence, we have

$$\begin{aligned} \varphi(C) &= \{\varphi(c_1) = 0, \varphi(c_2), \dots, \varphi(c_t)\}, \\ \varphi(D^\perp) &= \{\varphi(d_1) = 0, \varphi(d_2), \dots, \varphi(d_t)\}. \end{aligned}$$

Without loss of generality, we assume that the coset representatives are indexed so that the permutation τ between the equivalent codes $\varphi(C)$ and $\varphi(D^\perp)$ (cf. Remark 3.7) satisfies

$$(3.3) \quad \tau(\varphi(c_i)) = \varphi(\tau(c_i)) = \varphi(d_i), \quad \text{for all } i = 1, \dots, t.$$

Note that this implies

$$(3.4) \quad \tau(c_i) - d_i \in \gamma R[G] \quad \text{for all } i = 1, \dots, t.$$

Before the proof of the main result, let us state the following which gives a generating set as an R -module for a free code C in $R[G]$.

Proposition 3.8. *Let C be a free code in $R[G]$ with the following representation (cf. (3.2)):*

$$C = \dot{\bigcup}_{1 \leq i \leq t} (c_i + \gamma C).$$

Let $S := \{c_2, \dots, c_t\}$. Then any element of C can be represented as sum of the elements in

$$S \cup \gamma S \cup \dots \cup \gamma^{v-1} S.$$

Proof. By Proposition 3.4, we have

$$C = \tilde{C} \cup \gamma \tilde{C} \cup \dots \cup \gamma^{v-1} \tilde{C} \cup \{0\},$$

where $\tilde{C} = C \setminus \gamma C$. Since cosets modulo γC partition C , and recalling that $c_1 = 0$, we have

$$\begin{aligned} \tilde{C} &= (c_2 + \gamma C) \dot{\cup} \dots \dot{\cup} (c_t + \gamma C), \\ \gamma C &= \gamma \tilde{C} \cup \dots \cup \gamma^{v-1} \tilde{C} \cup \{0\}. \end{aligned}$$

Hence,

$$\tilde{C} = \bigcup_{2 \leq i \leq t} (c_i + \gamma C) = \bigcup_{2 \leq i \leq t} \left(c_i + (\gamma \tilde{C} \cup \dots \cup \gamma^{v-1} \tilde{C} \cup \{0\}) \right).$$

Since $\gamma^v = 0$, we have

$$\begin{aligned} \gamma^{v-1} \tilde{C} &= \bigcup_{i=2}^t \{ \gamma^{v-1} c_i \}, \\ \gamma^{v-2} \tilde{C} &= \bigcup_{i=2}^t \left(\gamma^{v-2} c_i + (\gamma^{v-1} \tilde{C}) \right) \\ &= \bigcup_{i=2}^t \left(\gamma^{v-2} c_i + \left(\bigcup_{i=2}^t \{ \gamma^{v-1} c_i \} \right) \right). \end{aligned}$$

Continuing in the same manner until $\gamma \tilde{C}$, we obtain the desired result. \square

We are ready to prove the main result for LCP of group codes (2-sided ideals) over a chain ring.

Theorem 3.9. *Let (C, D) be an LCP of group codes in $R[G]$, where R is a finite chain ring and G is a finite group. Then C and D^\perp are equivalent codes.*

Proof. By Proposition 3.6, $\varphi(C)$ and $\varphi(D^\perp)$ are equivalent codes. Let τ be the permutation between them (i.e. $\varphi(\tau(C)) = \varphi(D^\perp)$). Note that (C^\perp, D^\perp) is also an LCP of codes in $R[G]$ by Proposition 3.5, and hence $(\varphi(C^\perp), \varphi(D^\perp))$ is LCP in $\mathbb{F}_q[G]$ (Proposition 3.2). If $\{c'_1 = 0, c'_2, \dots, c'_s\}$ denotes the coset representatives of C^\perp modulo γC^\perp and $\{d_1 = 0, d_2, \dots, d_t\}$, as before, denotes the coset representatives of D^\perp modulo γD^\perp , we have

$$(3.5) \quad \mathbb{F}_q[G] = \varphi(C^\perp) \oplus \varphi(D^\perp) = \{\varphi(c'_i) + \varphi(d_j) : 1 \leq i \leq s, 1 \leq j \leq t\}.$$

Since C is free, $\tau(C)$ is also a free code in $R[G]$ and partitions as

$$\tau(C) = \bigcup_{1 \leq i \leq t} (\tau(c_i) + \gamma \tau(C)) \quad (\text{cf. (3.2)}),$$

where $\{c_1 = 0, c_2, \dots, c_t\}$ is the set of coset representatives of C modulo γC .

If $\tau(C) \cap C^\perp$ contains an element x in a coset $c'_i + \gamma C^\perp$ for some $i \in \{2, \dots, s\}$, then

$$\varphi(x) = \varphi(c'_i) \notin \varphi(\tau(C)) = \varphi(D^\perp) = \{\varphi(d_1) = 0, \varphi(d_2), \dots, \varphi(d_t)\} \quad (\text{cf. (3.5)}).$$

Therefore $\tau(C) \cap C^\perp$ is contained in γC^\perp , hence in $\gamma \tau(C)$ (cf. Proposition 3.4 (iii)). Let $x \in \tau(C) \cap C^\perp$ be $x = \gamma \tau(c(1)) = \gamma c'(1)$, where $c(1) \in C$ and $c'(1) \in C^\perp$. Then $\gamma(\tau(c(1)) - c'(1)) = 0$ and hence the difference $\tau(c(1)) - c'(1)$ is a multiple of γ^{v-1} :

$$\text{i.e. } \tau(c(1)) = c'(1) + \gamma^{v-1} y_1, \text{ for some } y_1 \in R[G].$$

If $c'(1) \in C^\perp \setminus \gamma C^\perp$, then $\varphi(\tau(c(1))) = \varphi(c'(1)) \notin \varphi(\tau(C))$ again. Hence, $c'(1) = \gamma c'(2)$ for some $c'(2) \in C^\perp$ and

$$x = \gamma^2 c'(2) = \gamma^2 \tau(c(2)),$$

where $c(2) \in C$. This yields $\gamma^2(\tau(c(2)) - c'(2)) = 0$ and hence the difference $\tau(c(2)) - c'(2)$ is a multiple of γ^{v-2} . In other words, $\tau(c(2)) = c'(2) + \gamma^{v-2}y_2$ for some $y_2 \in R[G]$. By the same reasoning, $c'(2) \in \gamma C^\perp$ and hence

$$x = \gamma^3 \tau(c(3)) = \gamma^3 c'(3) \text{ for some } c(3) \in C \text{ and } c'(3) \in C^\perp.$$

Continuing in this manner, we conclude that the element x in $\tau(C) \cap C^\perp$ must be $\{0\}$.

Note that any permutation does not necessarily take an ideal of $R[G]$ to an ideal of $R[G]$. However τ does, as noted in Remark 2.1, since it is induced from an automorphism of G . So, $\tau(C)$ is an ideal of $R[G]$. By (3.4), we have (for all $1 \leq i \leq t$)

$$\tau(c_i) = d_i + \gamma x + \gamma y,$$

for uniquely determined $x \in D^\perp$ and $y \in C^\perp$, since $R[G] = C^\perp \oplus D^\perp$. Let $1 = a + b$ for $a \in C^\perp, b \in D^\perp$. Then, $\tau(c_i) = \tau(c_i)a + \tau(c_i)b$. Since $\tau(C)$ is an ideal, $\tau(c_i)a$ belongs to both $\tau(C)$ and C^\perp , whose intersection is $\{0\}$ (observe that we use the fact that $\tau(C)$ and C^\perp are 2-sided ideals). Hence,

$$\tau(c_i) = (d_i + \gamma x + \gamma y)b = (d_i + \gamma x)b + \gamma yb.$$

Note that $yb = 0$ since it belongs to $C^\perp \cap D^\perp = \{0\}$ (again, both codes are 2-sided ideals). Hence, $\tau(c_i) \in D^\perp$ for each i . This implies, by Proposition 3.8, that $\tau(C) \subset D^\perp$. Since $\tau(C)$ and D^\perp have the same cardinalities (cf. Remark 3.7), we have $\tau(C) = D^\perp$. This concludes the proof. \square

Remark 3.10. Note that Theorem 3.9 does not hold for LCP of one-sided group codes (C, D) in $R[G]$. The proof of Theorem 3.9 utilizes the permutation τ between $\varphi(C)$ and $\varphi(D^\perp)$, whose existence is due to the result of Borello et al. and requires the codes in $\mathbb{F}_q[G]$ to be 2-sided group codes. Aside from this, 2-sided ideal structure of C, C^\perp and D^\perp are used, and pointed out, in several steps of the proof.

4. ACKNOWLEDGMENT

We would like to thank the reviewers for their valuable comments, which drastically improved the manuscript. The first author is supported by the TÜBİTAK project 215E200, which is associated with the SECODE project in the scope of the CHIST-ERA Program. The second author is partially funded by the Spanish Research Agency (AEI) under grant PGC2018-096446-B-C21. The third author visited the Institute of Mathematics of University of Valladolid during February-March 2019. She thanks the Institute for their kind hospitality.

REFERENCES

- [1] S. Bhasin, J.-L. Danger, S. Guilley, Z. Najm and X. T. Ngo, “Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses”, *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 5-7, 2015.
- [2] Sanjit Bhowmick and Alexandre Fotue-Tabue and Edgar Martínez-Moro and Ramakrishna Bandi and Satya Bagchi. “Do non-free LCD codes over finite commutative Frobenius rings exist?”, *Des. Codes Cryptogr.* 88, 825840 (2020).

- [3] M. Borello, J. de la Cruz, W. Willems, “A note on linear complementary pairs of group codes”, *Discrete Math.*, vol. 343, 111905.
- [4] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, and H. Maghrebi, “Orthogonal direct sum masking - a smartcard friendly computation paradigm in a code, with builtin protection against side-channel and fault attacks”, in WISTP, Springer, Heraklion, 2014, 40-56.
- [5] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya and P. Solé, “On linear complementary pairs of codes”, *IEEE Trans. Inform. Theory*, vol. 64, 6583-6589, 2018.
- [6] C. Güneri, B. Özkaya and S. Sayıcı, “On linear complementary pair of n D cyclic codes”, *IEEE Commun. Lett.*, vol. 22, 2404-2406, 2018.
- [7] I. Kaplansky, “Projective modules”, *Ann. of Math (2)*, vol. 68, 372-377, 1958.
- [8] X. Liu and H. Liu, “LCD codes over finite chain rings”, *Finite Fields Appl.*, vol. 34, 1-19, 2015.
- [9] Z. Liu and J. Wang, “Linear complementary dual codes over rings”, *Des. Codes Cryptogr.*, vol. 87, 3077-3086, 2019.
- [10] J.L. Massey, “Linear codes with complementary duals”, *Discrete Math.*, vol. 106/107, 337-342, 1992.
- [11] G.H. Norton and A. Salagean, “On the structure of linear and cyclic codes over a finite chain ring”, *Appl. Algebra Engrg. Comm. Comput.*, vol. 10, 489-506, 2000.
- [12] G.H. Norton and A. Salagean, “On the Hamming distance of linear codes over a finite chain ring”, *IEEE Trans. Inform. Theory*, vol. 46, 1060-1067, 2000.