ON LINEAR COMPLEMENTARY PAIR OF CODES

by
SELCEN SAYICI

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfilment of
the requirements for the degree of Doctor of Philosophy

Sabancı University
July 2020

ON LINEAR COMPLEMENTARY PAIR OF CODES

APPROVED BY:

Prof. Cem Güneri ....
(Thesis Supervisor)

Prof. Erkay Savaş ....

Assoc. Prof. Kağan Kurşungöz ....

Prof. Ferruh Özbudak ....

Assoc. Prof. Alp Bassa A. Bassa ....

DATE OF APPROVAL: 23/07/2020

ABSTRACT

ON LINEAR COMPLEMENTARY PAIR OF CODES

SELCEN SAYICI

MATHEMATICS Ph.D DISSERTATION, JULY 2020

Dissertation Supervisor: Prof. CEM GÜNERİ

Keywords: Linear complementary pair of codes, abelian codes, group codes, code equivalence, finite fields, finite chain rings

Linear complementary pair (C, D) of codes has drawn much attention recently due to their applications to cryptography, in the context of side channel and fault injection attacks. The security parameter of such a pair is defined to be the minimum of the minimum distances $d(C)$ and $d(D^{\perp})$. Carlet et al. showed that if C and D are both cyclic or both 2D cyclic over a finite field, then C and $D^{\perp}$ are equivalent codes. Hence $d(C) = d(D^{\perp})$. We extend this result to all nD cyclic, or abelian, codes over finite fields. Moreover, we prove the same result for all linear complementary pair of 2-sided group codes over finite chain rings.

ÖZET

DOĞRUSAL BÜTÜNLEYİCİ ÇİFT KODLARI ÜZERİNE

SELCEN SAYICI

MATEMATİK DOKTORA TEZİ, TEMMUZ 2020

Tez Danışmanı: Prof. Dr. CEM GÜNERİ

Anahtar Kelimeler: Doğrusal bütünleyici çift kodları, abelyen kodlar, grup kodları, kod denkliği, sonlu cisimler, sonlu zincir halkaları

Doğrusal bütünleyici çift (C, D) kodları son zamanlarda, kriptografide yan kanal ve sahte enjeksiyon atakları üzerine uygulamaları sebebiyle ilgi çekmişlerdir. Böyle bir çiftin güvenlik parametresi, $d(C)$ ve $d(D^{\perp})$ minimum uzaklıklarının minimumu olarak tanımlanır. C ve D her ikisi de devirsel, veya 2D devirsel, sonlu cisimler üzerinde tanımlı kodlar ise, Carlet vd. C'nin $D^{\perp}$'a denk olduğunu göstermişlerdir. Dolayısıyla $d(C) = d(D^{\perp})$ eşitliği doğrudur. Bu sonucu, sonlu cisimler üzerinde tanımlı tüm nD, veya abelyen, kodlara genişletiyoruz. Ayrıca, aynı sonucu sonlu zincir halkaları üzerinde tanımlı tüm 2-taraflı doğrusal bütünleyici çift kodları için de ispatlıyoruz.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Cem Güneri, for suggesting me this topic which I like so much and for being a part of this thesis. I learned a lot from him.

I thank my progress jury members Erkay Savaş and Kağan Kurşungöz for helpful comments they provided in our progress meetings and other professors Ferruh Özbudak and Alp Bassa for being jury members of this thesis. I also thank Edgar Martinez-Moro for his valuable contribution particularly to Section 3.2 of this thesis.

I would like to thank my teachers Alev Topuzoğlu and Henning Stichtenoth. I also learned a lot from them.

I should thank my dear family for being with me in every moment of my PhD period.

TABLE OF CONTENTS

1. INTRODUCTION

Linear Complementary Dual (LCD) codes and Linear Complementary Pair (LCP) of codes have been intensively studied in literature due to their cryptographic applications [1, 5, 6]. They are used in protection against side channel (SCA) and fault injection (FIA) attacks. A pair of linear codes (C, D) over $\mathbb{F}_q$ of length n is called LCP if $C \oplus D = \mathbb{F}_q^n$. When $D = C^\perp$, C is called an LCD code. In this context the security parameter for LCP of codes (C, D) is defined to be the minimum of the minimum distances of C and $D^\perp$, i.e. it is $\min\{d(C), d(D^\perp)\}$. For the LCD case, this parameter is simply $d(C)$ since $D^\perp = C$. The aim is to construct LCP of codes with big security parameter in order to strengthen the security of the system.

The notion of an LCD code was first introduced by James L. Massey in 1992 ([20]), long before their recent cryptographic applications. These codes provided an optimum linear coding solution for the two-user binary adder channel. Massey gave a characterization and some constructions of codes with complementary duals. He also showed that LCD codes are asymptotically good. In 2004, Nicolas Sendrier showed that LCD codes meet the Gilbert-Varshamov Bound as a corollary of the main result of his paper, which shows that linear codes with prescribed hull dimension meet the GV Bound ([25]). Here we note that LCD codes have hull dimension 0. In the same paper he proved that the proportion of $[n, k]$ LCD codes over $\mathbb{F}_q$ among all linear $[n, k]$ codes is approximately $1 - 1/q$. Recently in [9], Carlet et al. showed that when $q > 3$, any linear code over $\mathbb{F}_q$ is equivalent to an Euclidean LCD code. So when $q > 3$, q-ary Euclidean LCD codes are as good as q-ary linear codes. In 1994, X. Yang and James L. Massey gave a characterization for cyclic LCD codes ([26]) and recently Carlet et al. have characterized LCP of cyclic codes ([7]). Moreover, equivalence of C and $D^\perp$, for cyclic and 2D cyclic pairs, was also proved in the same paper. All of these results have been proven over a finite field. Although LCD and LCP of codes have been widely studied over finite fields, these code classes have not been as well understood over rings, particularly over chain rings. [18] and [19] study LCD codes over rings but there has not been any result on LCP of codes over rings.

In this thesis, we prove the following statement for abelian codes over a finite field and then more generally for group codes over a finite chain ring seperately.

Theorem 1.1. *Let (C, D) be an LCP of abelian (resp. 2-sided group) codes over a finite field (resp. a finite chain ring). Then C and $D^{\perp}$ are equivalent codes.*

This result enables us to say that there is an LCP of abelian codes, which has as good a security parameter as the abelian code with the best minumum distance. The same also holds for LCP of 2-sided group codes over finite chain rings. Along the way, we have also given some nice algebraic properties of abelian (resp. group codes) and LCP of abelian codes (resp. group codes). Chronologically, we generalized the result of Carlet et al. on LCP of cyclic and 2D cyclic codes to nD cyclic codes over finite fields, in the semsimple case, in [13]. Later, Borello et al. generalized this result to LCP of 2-sided group codes over finite fields for arbitrary length ([3]). Finally, the result for LCP of 2-sided group codes over chain rings, in arbitrary length, has been obtained in [11].

Let us note that we also provide a proof for LCP of abelian codes over finite fields in the non-semisimple case in this thesis. Although Borello et al.'s result holds more generally for group codes, the proof we give for non-semisimple abelian codes uses a different approach.

The organization of the chapters is as follows:

In Chapter 2, we start by giving definitions of and brief backround on cyclic codes, nD cyclic codes, LCD codes and LCP of codes. Then we introduce the cryptographic motivation of studying these codes.

In Chapter 3, we first prove the theorem over a finite field in the semisimple case. Theorem 1.1 is proven by Carlet et al. in [7] for cyclic codes under no restriction and for 2D cyclic codes when the code length and the characteristic of the field are relatively prime to each other (semisimple case). The proof of Carlet et al. for cyclic codes is based on polynomial arguments in one variable. Their proof for 2D cyclic case is based on the trace representation of the codes. Neither approach is feasible for nD cyclic codes. Our proof for the generalization is based on the zero sets of the ideals corresponding to nD cyclic codes in the semisimple case. Then we give a proof for the non-semisimple case using a Chinese Remainder Theorem type decomposition of the codes. In this chapter we also extend the results of Yang-Massey and Carlet et al. on the generator polynomials of cyclic LCD and LCP of codes to nD cyclic codes in the semisimple case.

In Chapter 4, we start with a brief backround on chain rings and give well-known facts on finite chain rings. Then we prove our theorem on LCP of 2-sided group codes over finite chain rings. For this we start with an LCP (C, D) over a chain ring, consider their projection to the residue field, where the images are shown to be LCP again. The pair over a finite field has the desired equivalence map, which we lift to codes C and $D^{\perp}$ over the chain ring.

2. BACKROUND AND MOTIVATION

2.1 LCD Codes and LCP of Codes

We begin this section with basic definitions and facts.

Let $\mathbb{F}_q$ be a finite field with characteristic p. A q-ary *linear code* C of length n is a linear subspace of the vector space $\mathbb{F}_q^n$. If C has dimension k then C is called an $[n,k]$ code. The *minimum distance* of a nontrivial code C is $\min\{d(x,y)|x \in C, y \in C, x \neq y\}$, where $d(x,y)$ denotes the Hamming distance. An $[n,k,d]$ code C denotes a code of length n, dimension k with minimum distance d. A *generator matrix* G for an $[n,k]$ linear code C is a $k \times n$ matrix for which the rows are a basis of C. If C is an $[n,k]$ code we define the *dual code* $C^{\perp}$ by

$$C^{\perp} = \{y \in \mathbb{F}_q^n \mid <x,y>= 0 \ \ \forall x \in C\}.$$

The dual code $C^{\perp}$ is an $[n, n-k]$ code. Throughout this thesis, unless stated otherwise, the dual will be relative to the Euclidean inner product.

Definition 2.1. A linear code C of length n over $\mathbb{F}_q$ is called *cyclic* if $\left(c_{n-1}, c_0, \ldots, c_{n-2}\right) \in C$ whenever $\left(c_0, c_1, \ldots, c_{n-1}\right) \in C$.

There is an $\mathbb{F}_q$-linear isomorphism (considered only as an additive group) between $\mathbb{F}_q^n$ and $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. By using this fact it is well known that there is a one to one correspondence between cyclic codes in $\mathbb{F}_q^n$ and ideals in the quotient polynomial ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

Theorem 2.2. *A linear code C in $\mathbb{F}_q^n$ is cyclic if and only if C is an ideal in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.*

Consider cyclic codes of length n over $\mathbb{F}_q$ with $(n,q) = 1$. Since $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is a principal ideal ring, every cyclic code C consists of the multiples of a uniquely determined polynomial $g(x)$ which is the monic polynomial of lowest degree in the ideal. This polynomial $g(x)$ is called the *generator polynomial* of the cyclic code and this generator polynomial is a divisor of x^n-1.

The polynomial $g^*(x)=x^k g(x^{-1})$ is called the *reciprocal polynomial* of $g(x)$ where deg $g=k$. We have that the dual code of a cyclic code is also cyclic and moreover if $C=\langle g(x)\rangle$ is cyclic, then for $h(x)=(x^n-1)/g(x)$, the dual cyclic code $C^\perp$ has the generator polynomial $h^*(x)$.

From now on we focus on giving cryptographic motivation on LCD and LCP of codes. We also provide some important results on these codes accordingly for the rest of this section.

Definition 2.3. A pair of linear codes (C,D) over $\mathbb{F}_q$ of length n is called a *linear complementary pair (LCP) of codes* if $C\oplus D=\mathbb{F}_q^n$.

In the case $C=D^\perp$, C is referred to as a *linear complementary dual (LCD) code.*

Recent studies have shown that LCD and LCP of codes help to improve the security of the information (processed by sensitive devices), especially against side-channel attacks (SCA) and fault injection attacks (FIA). The aim is to produce an LCP of codes (C,D) which has a security parameter as high as possible. Let us explain how LCD codes are used in the FIA.

Let $x\in\mathbb{F}_2^k$ be our sensitive data. For a $k\times n$ matrix G of rank k, we code our information to $xG\in\mathbb{F}_2^n$. Then we add an $(n-k)$ bit "mask" y via encoding it with a $(n-k)\times n$ matrix H of rank $(n-k)$: yH - encoded mask. So, we work with $z=xG+yH$ and try not to reveal x at any point. Let C and D be length n codes with generating matrices G and H, respectively.

Assume that $D=C^\perp$ and the two codes satisfy $C\oplus C^\perp=\mathbb{F}_2^n$ (i.e. $C\cap C^\perp=\{0\}$). i.e a code C is an LCD code.

Here we need the following characterization by Massey in [20].

Theorem 2.4. *Let C be a linear code with a generator matrix G and a parity-check matrix H. Then C is an LCD code iff GG^T is non-singular iff HH^T is non-singular.*

Note that one can recover both the sensitive info x and the mask y from z as follows:

$$\begin{aligned} zG^t(GG^t)^{-1} &= (xG+yH)G^t(GG^t)^{-1} \\ &= xGG^t(GG^t)^{-1}+yHG^t(GG^t)^{-1}=x \end{aligned}$$

$$zH^t(HH^t)^{-1}=y \text{ similarly.}$$

Suppose one inserts an error ϵ into z to observe the system statistically, with the hope of reaching x. This is called FIA. Since $C \oplus C^{\perp}=\mathbb{F}_2^n$, we have $\epsilon=eG+fH$ for some e and f. So, the corrupted word is $z+\epsilon$. We want to detect if there is such an attack but we do not want to reveal x. Check y during the process:

$$(z+\epsilon)H^t(HH^t)^{-1}=y+f=y \iff f=0.$$

So the attack may be undetected if $f=0$ in ϵ. In this case $\epsilon=eG\in C$. Therefore, set $d(C)$ (security parameter) as high as possible so that FIA is only successful when a high weight codeword is inserted.

The definition of the security parameter for LCP of codes is as follows:

Definition 2.5. The *security parameter* of an LCP (C,D) is defined to be $\min\{d(C),d(D^{\perp})\}$. For the LCD case, this parameter is simply $d(C)$, since $D^{\perp}=C$.

The followings are the characterizations of cyclic LCD and cyclic LCP of codes by Yang-Massey and Carlet et al., respectively.

Theorem 2.6. *([26, Theorem]) If $g(x)$ is the generator polynomial of a q-ary (n,k) cyclic code C of length n, then C is an LCD code if and only if $g(x)$ is self-reciprocal and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ and in x^n-1.*

Theorem 2.7. *([7, Theorem 2.1]) Let C and D be q-ary cyclic codes of length n with the generating polynomials $g(x)$ and $u(x)$, respectively. Then (C,D) is LCP if and only if $u(x)=(x^n-1)/g(x)$ and $\gcd(u(x),g(x))=1$.*

Proof. $\{\overline{0}\}=C\cap D=$ lcm $\{g(x),u(x)\}$. This means that lcm $\{g(x),u(x)\}=x^n-1$. Since $C+D=\mathbb{F}_q^n=\mathbb{F}_q[x]/\langle x^n-1\rangle$, then $1\equiv a(x)g(x)+b(x)u(x) \mod (x^n-1)$ for some $a(x),b(x)\in\mathbb{F}_q[x]$. So gcd $(g(x),u(x))=1$. Conversely, since g and u are coprime then $C+D=\mathbb{F}_q[x]/\langle x^n-1\rangle$. By assumption $u(x)=(x^n-1)/g(x)$. Hence $C\cap D=\{\overline{0}\}$.

□

Corresponding scheme of cyclic codes in terms of generator polynomials when (C,D) is LCP of codes would be as follows :

$$\begin{array}{ccccccc} C^{\perp} & \longleftrightarrow & C & \longleftrightarrow & D & \longleftrightarrow & D^{\perp} \\ u^*(x) & \longleftrightarrow & g(x) & \longleftrightarrow & u(x) & \longleftrightarrow & g^*(x) \end{array} \tag{2.1}$$

where $u(x) = (x^n - 1)/g(x)$.

Remark 2.8. Theorem 2.7 generalizes Theorem 2.6 of Yang-Massey. A cyclic code C being LCD means $(C,C^{\perp})$ is LCP. Since $C = \langle g(x)\rangle$ then $C^{\perp} = \langle u^*(x)\rangle$ where $u(x) = (x^n-1)/g(x)$. Theorem 2.7 yields $\big((x^n-1)/g(x)\big)^* = (x^n-1)/g(x)$. This means that g is self-reciprocal which is what Theorem 2.6 says.

2.2 Cyclic Codes to nD Cyclic Codes

In this section, we give an overview on n dimensional cyclic codes and their zero sets.

A k-dimensional subspace C of $\mathbb{F}_q^{m_1\times m_2\times\cdots\times m_n}$ is called an nD linear code of area $m_1\times m_2\times\cdots\times m_n$ over $\mathbb{F}_q$ and denoted as an $[m_1\times m_2\times\cdots\times m_n$, k] code.

Definition 2.9. For an nD linear code $C\subset\mathbb{F}_q^{m_1\times m_2\times\cdots\times m_n}$ if $(a_{i_1,i_2,\ldots,i_n})$ is in C implies that $(a_{i_1+s_1,i_2+s_2,\ldots,i_n+s_n})$ is also in C for all s_k , where all i_k+s_k are taken in mod m_k, $1\le$ k $\le$ n, then C is called *an nD cyclic code* of area $m_1\times m_2\times\cdots\times m_n$. When $n=1$ they are cyclic codes. In other words as we recall, $C\subset\mathbb{F}_q^m$ is a cyclic code when $(a_0,\ldots,a_{m-1})\in C \implies (a_{m-1},a_0,\ldots,a_{m-2})\in C$.

Remark 2.10. Consider a 2D cyclic code $C\subset\mathbb{F}_q^{m_1\times m_2}$ of length $m_1\times m_2$ and a codeword $c=(c_{i_1,i_2})\in C$. One can see this codeword c as an $m_1\times m_2$ matrix where by Definition 2.9 this matrix is closed under row shift and column shift. So in polynomial space $\mathbb{F}_q[x_1,x_2]/\langle x_1^{m_1}-1, x_2^{m_2}-1\rangle$, this means that an $\mathbb{F}_q$-subspace corresponding to a code C is closed under multiplication by x_1 and x_2. So it is an ideal of this polynomial ring which is analogous result of Theorem 2.2. In general an nD cyclic code can be viewed as an ideal in the quotient ring of polynomials in n variables $\mathbb{F}_q[x_1,\ldots,x_n]/\langle x_1^{m_1}-1,\ldots,x_n^{m_n}-1\rangle$, which we denote by R_n.

Let $\mathcal{I}$ be an ideal of $\mathbb{F}_q[x]/\langle x^n-1\rangle$ corresponding a cyclic code $C\subset\mathbb{F}_q^n$ generated by $g(x)$. Then the set $\{$ zeros of $g(x)\} \subset \{n^{th}$ roots of unity $\}$ is the zero set of C.

Let $m_1, \ldots, m_n$ be positive integers all of which are relatively prime to q. Let us denote an $m_1 \times \cdots \times m_n$ array over $\mathbb{F}_q$ by $(a_{i_1,i_2,\ldots,i_n})$. Here, we understand that the index i_j runs over the set $\{0,1,\ldots,m_j-1\}$ for all $1 \le j \le n$. In other words, such an array is simply a vector over $\mathbb{F}_q$ of length $m_1 \cdots m_n$. One can identify the $\mathbb{F}_q$-space $\mathbb{F}_q^{m_1\times\cdots\times m_n}$ of all $m_1 \times \cdots \times m_n$ arrays with R_n via the map

$$\begin{array}{lrcl} & \mathbb{F}_q^{m_1\times\cdots\times m_n} & \longrightarrow & R_n \\ (2.2) & (a_{i_1,i_2,\ldots,i_n}) & \longmapsto & \displaystyle\sum_{j=1}^{n}\sum_{i_j=0}^{m_j-1} a_{i_1,i_2,\ldots,i_n} {x_1}^{i_1} {x_2}^{i_2} \ldots {x_n}^{i_n}. \end{array}$$

Note that, for simplicity, we denote the element of R_n not as a coset but just as a polynomial representing the coset in R_n. Under this identification, an nD cyclic code C becomes an $\mathbb{F}_q$-linear code of size (length) $m_1 \times \cdots \times m_n$ which satisfies the condition

$$(a_{i_1,i_2,\ldots,i_n}) \in C \implies (a_{i_1+s_1,i_2+s_2,\ldots,i_n+s_n}) \in C,$$

for all $s_1, \ldots, s_n$, where $i_j + s_j$ is computed modulo m_j for each j. Let us also note that the dual $C^{\perp}$ of an nD cyclic code of size $m_1 \times \cdots \times m_n$ is also an nD cyclic code of the same size.

Let α_j be a primitive m_j^{th} root of unity for $1 \le j \le n$. Note that all α_j's lie in a field $\mathbb{F}_{q^s}$ with the property that every m_j divides $q^s - 1$. Define the set

$$\Omega = \Big\{ ({\alpha_1}^{i_1}, \ldots, {\alpha_n}^{i_n}) : \ 0 \le i_j \le m_j - 1, \ 1 \le j \le n \Big\}.$$

The $\mathbb{F}_q$-conjugacy class containing $({\alpha_1}^{i_1}, \ldots, {\alpha_n}^{i_n})$ in Ω is defined as

$$\Big[({\alpha_1}^{i_1}, \ldots, {\alpha_n}^{i_n})\Big] = \Big\{ ({\alpha_1}^{i_1}, \ldots, {\alpha_n}^{i_n}), ({\alpha_1}^{i_1 q}, \ldots, {\alpha_n}^{i_n q}), \ldots, ({\alpha_1}^{i_1 q^{\delta-1}}, \ldots, {\alpha_n}^{i_n q^{\delta-1}}) \Big\},$$

where

$$\delta = \operatorname{lcm}\Big\{ \Big[\mathbb{F}_q({\alpha_j}^{i_j}) : \mathbb{F}_q\Big], 1 \le j \le n \Big\}.$$

Ω is a disjoint union of such $\mathbb{F}_q$-conjugacy classes.

Note that an ideal C of R_n (nD cyclic code) is of the form $\mathcal{J} + \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle$ for an ideal $\mathcal{J}$ of the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$ with $\mathcal{J} \supset \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle$. We define the zero set $Z(C)$ of an nD cyclic code C as the common zeros of all of the polynomials in $\mathcal{J}$ and observe that $Z(C) \subset \Omega$. In fact, $Z(C)$ is a union of $\mathbb{F}_q$-conjugacy classes.

Conversely for a subset $U \subset \Omega$, the nD cyclic code C_U in R_n corresponding to U is defined to be $\mathcal{I}_U + \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle$, where

$$\mathcal{I}_U = \{f(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n] : f(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in U\}.$$

If $\bar{U}$ denotes the smallest union of $\mathbb{F}_q$-conjugacy classes in Ω that contains U, then it can be seen that $C_U = C_{\bar{U}}$. Moreover, there is a one-to-one correspondence between subsets of Ω which are unions of $\mathbb{F}_q$-conjugacy classes and nD cyclic codes in R_n, given via the assignment $U \leftrightarrow C_U$. In other words, we have $Z(C_U) = U$ for any $U \subset \Omega$, which is a union of $\mathbb{F}_q$-conjugacy classes, and $C_{Z(C)} = C$ for any ideal (nD cyclic code) C of R_n.

Hence, the zero set $Z(C)$ uniquely determines an nD cyclic code C and working on $Z(C)$ is identical with working on C which will be effectively used in proof of the main result, Theorem 3.8, of Section 3.1.

3. LCP of Abelian Codes over Finite Fields

3.1 LCP of Abelian Codes over Finite Fields: Semisimple Case

Carlet et al. showed that if (C,D) is an LCP of codes where C and D are both cyclic or both 2D cyclic, then C and $D^{\perp}$ are equivalent ([7, Theorems 2.4 and 3.4]). We extend this result to nD cyclic codes (for any n) in this section. As in Section 2.2, we let $R_n = \mathbb{F}_q[x_1,\dots,x_n]/\langle x_1^{m_1}-1,\dots,x_n^{m_n}-1\rangle$ and assume that $\gcd(q,m_i)=1$ for all $1 \le i \le n$.

The following important facts will be used throughout, so we collect them in the next result. Let us note that these results are stated for 2D cyclic codes in [10, Theorem 3.4, Proposition 3.5] and for general nD cyclic codes in [12, Proposition 2.2].

Proposition 3.1. *Let $U = Z(C)$ be the zero set of the nD cyclic code $C \subset R_n$. Then,*

i. $\dim_{\mathbb{F}_q}(C) = |\Omega - U|$,

ii. $Z(C^{\perp}) = \Omega - U^{-1}$,

where $U^{-1} = \Big\{(a_1^{-1},\dots,a_n^{-1}) : (a_1,\dots,a_n) \in U\Big\}$.

Example 3.2. The class of nD cyclic codes contains some good code examples. We give an example of a good 2D cyclic code here. Consider the extension $\mathbb{F}_9$ over $\mathbb{F}_3$ and let α be a primitive element of $\mathbb{F}_9$ satisfying $\alpha^2+\alpha-1=0$. Let C be the 2D cyclic code over $\mathbb{F}_3$ of size 8×8 (i.e. length 64) whose dual $C^{\perp}$ has the zero set

$$Z(C^{\perp}) = [(\alpha,\alpha)] \cup [(\alpha,\alpha^2)].$$

In other words, C and $C^{\perp}$ are ideals of $\mathbb{F}_3[x_1,x_2]/\langle x_1^8-1, x_2^8-1\rangle$. It is easy to observe that the $\mathbb{F}_3$-conjugacy classes of (α,α) and (α,α^2) both have two elements. Hence, by Proposition 3.1, $\dim_{\mathbb{F}_3}(C^{\perp}) = 64-4 = 60$ and $\dim_{\mathbb{F}_3}(C) = 4$. It is shown in [10, Example 6.2] that the minimum distance of C is 42. This is the best minimum distance for a code of length 64 and dimension 4 over $\mathbb{F}_3$ according to [14].

We recall a basic ring theoretic fact. For the sake of completeness, a short proof is provided.

Proposition 3.3. *If I and J are ideals in a commutative ring R with identity such that $I+J=R$, then $I\cap J = IJ$.*

Proof. In general $IJ \subset I\cap J$, so we just need to show the opposite implication. Let a be an element of the intersection and write $1 = u+v$ for some $u \in I$ and $v \in J$. Then, $a = a(u+v) = au+av$. Since R is commutative, both au and av are elements of the ideal IJ. Hence $a \in IJ$. □

The next result collects important information on the zero sets of complementary nD cyclic codes and it will be essential in the proof of the main result.

Proposition 3.4. *Let (C,D) be an nD cyclic LCP of codes in R_n. Then,*

i. $Z(C)\cup Z(D) = Z(C\cap D) = \Omega$.

ii. $Z(C)\cap Z(D) = \emptyset$.

Proof. Since (C,D) is LCP, we have $C\cap D = CD$ in R_n by Proposition 3.3. So it suffices to show that $Z(C)\cup Z(D) = Z(CD)$.

i. Let a be in $\in Z(C)\cup Z(D)$ and assume without loss of generality that $a \in Z(C)$. So $f(a) = 0$ for all $f \in C$, and hence $f(a)g(a) = 0$ for any $g \in D$. Therefore, a is also a root of summation of such products, which implies that $a \in Z(CD)$.

Conversely, let a be an element of $Z(CD)$. If a does not belong to $Z(C)\cup Z(D)$, then there exist $f \in C$ and $g \in D$ such that $f(a) \neq 0$ and $g(a) \neq 0$. So $h(a) \neq 0$ for $h = fg \in CD$, which is a contradiction.

So we proved that $Z(C)\cup Z(D) = Z(CD) = Z(C\cap D)$. Since $C\cap D = \{0\}$, the corresponding zero set is Ω.

ii. Note that $|\Omega| = m_1\cdots m_n = \dim_{\mathbb{F}_q}(R_n)$. Since $C\oplus D = R_n$, we obtain

$$|\Omega| = \dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D).$$

Then by Proposition 3.1, we have

$$|\Omega| = (|\Omega| - |Z(C)|) + (|\Omega| - |Z(D)|),$$

and hence

$$|\Omega| = |Z(C)| + |Z(D)|. \tag{3.1}$$

By part i, we also have

$$|\Omega| = |Z(C) \cup Z(D)| = |Z(C)| + |Z(D)| - |Z(C) \cap Z(D)|. \tag{3.2}$$

Equations 3.1 and 3.2 imply that $|Z(C) \cap Z(D)| = 0$, which proves the result. □

Remark 3.5. Proposition 3.4 implies that Ω is a disjoint union of $Z(C)$ and $Z(D)$. Carlet et al. showed in [7, Theorem 2.1] that if C and D are complementary cyclic codes with the generating polynomials $g(x)$ and $u(x)$ (in $R_1 = \mathbb{F}_q[x]/\langle x^{m_1} - 1\rangle$), then $u(x) = (x^{m_1} - 1)/g(x)$ (this is their statement in the case $\gcd(q, m_1) = 1$). Hence, the zero sets (or the defining sets in the terminology of cyclic codes) of C and D partition $\{0, 1, \ldots, m_1 - 1\}$. Therefore, Proposition 3.1 extends their result to nD cyclic codes for all n.

The next observation is on the relation between $Z(C)$ and $Z(D^{\perp})$ for an LCP (C, D) of nD cyclic codes.

Proposition 3.6. *If (C, D) is an LCP of nD cyclic codes in R_n, then $Z(D^{\perp}) = Z(C)^{-1}$.*

Proof. Since Ω is a disjoint union of $Z(C)$ and $Z(D)$ (cf. Remark 3.5), and $\Omega^{-1} = \Omega$, the same is true for $Z(C)^{-1}$ and $Z(D)^{-1}$. We have $Z(D^{\perp}) = \Omega - Z(D)^{-1}$ by Proposition 3.1. By the preceding observation, this set is simply $Z(C)^{-1}$. □

Remark 3.7. Note that Proposition 3.6 also extends the analogous result for LCP of cyclic codes to LCP of nD cyclic codes.

We are ready to prove the main result.

Theorem 3.8. *Let (C, D) be an nD cyclic LCP of codes in R_n. Then C and $D^{\perp}$ are equivalent.*

Proof. Consider the following map:

$$\begin{array}{rcl}\psi : C & \longrightarrow & D^{\perp} \\ f(x_1,\dots,x_n) & \longmapsto & x_1^{m_1-1}...x_n^{m_n-1} f(x_1^{-1},\dots,x_n^{-1}).\end{array}$$

Note that $\psi(f)$ is a polynomial for any f whose degree in x_j is less than m_j (for all $j=1,\dots,n$). For $f \in C$, we have $f(a_1,\dots,a_n)=0$ for all $(a_1,\dots,a_n)\in Z(C)$. Therefore $\psi(f)(a_1^{-1},\dots,a_n^{-1})=0$ for any such n-tuple, meaning that $\psi(f)$ vanishes on $Z(C)^{-1}=Z(D^{\perp})$ (cf. Proposition 3.6). Hence, ψ indeed takes values in $D^{\perp}$.

The map is clearly one-to-one. Since the dimensions of C and $D^{\perp}$ are equal (by Propositions 3.1 and 3.6), ψ is a bijection between C and $D^{\perp}$.

More explicitly, if

$$f(x_1,\dots,x_n)=\sum_{j=1}^{n}\sum_{i_j=0}^{m_j-1} a_{i_1,\dots,i_n} x_1^{i_1}\dots x_n^{i_n},$$

then

$$\begin{array}{rcl}\psi(f) & = & \sum_{j=1}^{n}\sum_{i_j=0}^{m_j-1} a_{i_1,\dots,i_n} x_1^{m_1-1-i_1}\dots x_n^{m_n-1-i_n} \\ & = & \sum_{j=1}^{n}\sum_{i_j=0}^{m_j-1} a_{m_1-1-i_1,\dots,m_n-1-i_n} x_1^{i_1}\dots x_n^{i_n}.\end{array}$$

Under the correspondence (2.2) between $\mathbb{F}_q^{m_1\times\cdots\times m_n}$ and R_n, the map ψ sends the array (codeword) $(a_{i_1,\dots,i_n})$ to $(a_{m_1-1-i_1,\dots,m_n-1-i_n})$. In other words, if we set a permutation

$$\begin{array}{rcl}\sigma_j : \{0,1,\dots,m_j-1\} & \longrightarrow & \{0,1,\dots,m_j-1\} \\ i_j & \longrightarrow & m_j-1-i_j\end{array}$$

for each $j=1,\dots,n$, then

$$\begin{array}{rcl}\sigma : \{0,1,\dots,m_1-1\}\times\cdots\times\{0,1,\dots,m_n-1\} & \longrightarrow & \{0,1,\dots,m_1-1\}\times\cdots\times\{0,1,\dots,m_n-1\} \\ (i_1,\dots,i_n) & \longrightarrow & (\sigma_1(i_1),\dots,\sigma_n(i_n))\end{array}$$

yields the explicit equivalence between the codewords (as arrays or vectors) of C and $D^{\perp}$ via $(a_{\sigma(i_1,\dots,i_n)})=(a_{\sigma_1(i_1),\dots,\sigma_n(i_n)})$. □

3.2 LCP of Abelian Codes over Finite Fields: Non-Semisimple Case

The goal in this section is to extend the result, Theorem 3.8, to all abelian codes by proving it when the length and the characteristic are arbitrarily chosen.

Let R be a finite commutative ring with identity and G be a finite abelian group. We denote by $R[G]$ be the group ring of G over R thus the elements of $R[G]$ are of the form $\sum_{g\in G}\alpha_g g$, where $\alpha_g \in R$ and nonzero for finitely many $g \in G$. An *abelian code* over R is defined to be an ideal in $R[G]$.

The *Jacobson Radical* of R, *Jac(R)*, is defined to be the intersection of all maximal ideals of R. The ring R is *local* if it has a unique maximal ideal.

There is a characterization for a local group ring which is in the following:

Proposition 3.9 (Theorem, [22])**.** *Let R be a commutative ring with identity and let G be a finite abelian group. Then R[G] is local iff R is local, G is a p-group and* $p \in$ *Jac(R).*

Remark 3.10. Since $\mathbb{F}_q$ has characteristic p this yields $p \in Jac(\mathbb{F}_q) = \{0\}$. Also clearly $\mathbb{F}_q$ is local. So by using this characterization, we have that $\mathbb{F}_q[P]$ is a local group algebra for all p-groups P.

Denote the cyclic group of order m_i by C_{m_i} and consider the abelian group

$$G = C_{m_1} \times \cdots \times C_{m_n}.$$

Then there is a natural isomorphism between the group algebra $\mathbb{F}_q[G]$ and the quotient ring

$$R_n = \mathbb{F}_q[x_1,\ldots,x_n]/\langle x_1^{m_1}-1,\ldots,x_n^{m_n}-1\rangle.$$

We can extend the $\mathbb{F}_q$-linear isomorphism in (2.2) via the following mappings

(3.3)

$$\begin{array}{ccccc} \mathbb{F}_q^{m_1\times\cdots\times m_n} & \longleftrightarrow & R_n & \longleftrightarrow & \mathbb{F}_q[G] \\ \left(a_{i_1,i_2,\ldots,i_n}\right) & \longleftrightarrow & \displaystyle\sum_{j=1}^{n}\sum_{i_j=0}^{m_j-1} a_{i_1,i_2,\ldots,i_n} x_1^{i_1}\cdots x_n^{i_n} & \longleftrightarrow & \displaystyle\sum_{j=1}^{n}\sum_{i_j=0}^{m_j-1} a_{i_1,i_2,\ldots,i_n}(g_1^{i_1},\ldots,g_n^{i_n}) \end{array}$$

Moreover, R_n and $\mathbb{F}_q[G]$ are isomorphic as rings. Hence an abelian (nD cyclic) code C can be viewed as an ideal in $\mathbb{F}_q[G]$ or in R_n ([12, 15]). When viewed in $\mathbb{F}_q^{m_1\times\cdots\times m_n}$, C is a linear code with symmetries induced from the ideal structure.

One has that the abelian group G can be decomposed as

$$G = A \oplus P, \tag{3.4}$$

where $|G| = N = mp^t$ with $|A| = m$, $|P| = p^t$ and $\gcd(m,p) = 1$. In other words, P is the unique p-Sylow subgroup of G. Moreover, the group algebra $\mathbb{F}_q[A]$ can be decomposed using Discrete Fourier Transform as

$$\mathbb{F}_q[A] \simeq \prod_{i=1}^{a} \mathbb{F}_q \times \prod_{j=1}^{b} \mathbb{K}_j \times \prod_{\ell=1}^{c} \left(\mathbb{L}_\ell \times \mathbb{L}_\ell\right), \tag{3.5}$$

where $\mathbb{K}_j, \mathbb{L}_\ell$ are finite proper extensions of $\mathbb{F}_q$ for each $1 \leq j \leq b$ and $1 \leq \ell \leq c$, for some nonnegative integers a,b,c (see [16]). Hence, $\mathbb{F}_q[G] = \mathbb{F}_q[A][P]$ can be decomposed as

$$\mathbb{F}_q[G] = \mathbb{F}_q[A][P] \simeq \prod_{i=1}^{a} \mathbb{F}_q[P] \times \prod_{j=1}^{b} \mathbb{K}_j[P] \times \prod_{\ell=1}^{c} \left(\mathbb{L}_\ell[P] \times \mathbb{L}_\ell[P]\right).$$

Therefore abelian codes C, D in $\mathbb{F}_q[G]$ decompose as

$$\begin{aligned} C &= \prod_{i=1}^{a} C_{1,i} \times \prod_{j=1}^{b} C_{2,j} \times \prod_{\ell=1}^{c} \left(C_{3,\ell} \times C'_{3,\ell}\right), \\ D &= \prod_{i=1}^{a} D_{1,i} \times \prod_{j=1}^{b} D_{2,j} \times \prod_{\ell=1}^{c} \left(D_{3,\ell} \times D'_{3,\ell}\right), \end{aligned} \tag{3.6}$$

where $C_{1,i}, D_{1,i} \subseteq \mathbb{F}_q[P]$, $C_{2,j}, D_{2,j} \subseteq \mathbb{K}_j[P]$ and $C_{3,\ell}, C'_{3,\ell}, D_{3,\ell}, D'_{3,\ell} \subseteq \mathbb{L}_\ell[P]$ are abelian codes in respective group algebras, for all i, j, ℓ.

The following result is not difficult to prove using the fact that $\mathbb{F}[P]$ is a local group algebra for a finite field $\mathbb{F}$ of characteristic p and any finite abelian p-group P (see [22]).

Proposition 3.11. *([4, Theorem 2]) Let $\mathbb{F}$ be a finite field of characteristic p and P be a finite abelian p-group. Then the ideals $\{0\}$ and $\mathbb{F}[P]$ are the only direct summands of the group algebra $\mathbb{F}[P]$.*

Proof. It is clear that $\{0\}$ and $\mathbb{F}[P]$ are direct summands in $\mathbb{F}[P]$. Assume that an ideal (abelian code) C in $\mathbb{F}[P]$ is another direct summand. i.e. there exists an ideal D such that $C \cap D = \{0\}$ (and $C + D = \mathbb{F}[P]$) for $\{0\} \subsetneq C, D \subsetneq \mathbb{F}[P]$. Since $\mathbb{F}[P]$ is local, it has a unique maximal ideal M. So $C, D \subseteq M$ which yields $C \cap D \subseteq M$.

If we take the dual of both side we have $M^{\perp} \subseteq (C \cap D)^{\perp} \subseteq M$. It follows that $M^{\perp} \subseteq (C \cap D) \subseteq M$. But $M \neq \mathbb{F}[P]$ (So $M^{\perp} \neq \{0\}$). So (C,D) can not be a complementary pair of abelian codes.

□

A straightforward consequence of Proposition 3.11 is the following characterization:

Proposition 3.12. *For a finite abelian group G as in (3.4), let C and D be abelian codes in $\mathbb{F}_q[G]$ with the decompositions as in (3.6). Then, (C,D) is an LCP of abelian codes if and only if*

2.1 $(C_{1,i}, D_{1,i}) \in \Big\{(\{0\}, \mathbb{F}_q[P]), (\mathbb{F}_q[P], \{0\})\Big\}$ *for all* $i = 1, \ldots, a$,

2.2 $(C_{2,j}, D_{2,j}) \in \Big\{(\{0\}, \mathbb{K}_j[P]), (\mathbb{K}_j[P], \{0\})\Big\}$ *for all* $j = 1, \ldots, b$,

2.3 $(C_{3,\ell}, D_{3,\ell}), (C'_{3,\ell}, D'_{3,\ell}) \in \Big\{(\{0\}, \mathbb{L}_\ell[P]), (\mathbb{L}_\ell[P], \{0\})\Big\}$ *for all* $\ell = 1, \ldots, c$.

Hence, given an abelian code C in $\mathbb{F}_q[G]$, the complementary abelian code D is uniquely determined by C.

Proof. By (3.6) it is easy to see that a pair of abelian codes (C,D) is an LCP of codes in $\mathbb{F}_q[A \times P]$ iff $(C_{1,i}, D_{1,i})$ is LCP of abelian codes in $\mathbb{F}_q[P]$ for all $i = 1, 2, \ldots, a$ and $(C_{2,j}, D_{2,j})$ is LCP of abelian codes in $\mathbb{K}_j[P]$ for all $j = 1, 2, \ldots, b$ and $(C_{3,\ell}, D_{3,\ell}), (C'_{3,\ell}, D'_{3,\ell})$ are LCP of abelian codes in $\mathbb{L}_\ell[P]$ for all $\ell = 1, 2, \ldots, c$ iff $C_{1,i} \oplus D_{1,i} = \mathbb{F}_q[P]$, $C_{2,j} \oplus D_{2,j} = \mathbb{K}_j[P]$, $C_{3,\ell} \oplus D_{3,\ell} = \mathbb{L}_\ell[P]$ and $C'_{3,\ell} \oplus D'_{3,\ell} = \mathbb{L}_\ell[P]$ where $C_{1,i}, D_{1,i} \subseteq \mathbb{F}_q[P]$, $C_{2,j}, D_{2,j} \subseteq \mathbb{K}_j[P]$ and $C_{3,\ell}, C'_{3,\ell}, D_{3,\ell}, D'_{3,\ell} \subseteq \mathbb{L}_\ell[P]$ are abelian codes in respective group algebras, for all i, j, ℓ. Then the result follows from Proposition 3.11.

□

Remark 3.13. By Proposition 3.12, we have that any linear complementary pair of abelian codes (C,D) in $\mathbb{F}_q[A \times P]$ is independent of the sylow p-subgroup P. In other words, since in the decomposition of C and D, components are $\mathbb{K}_j[P]$, $\mathbb{L}_\ell[P]$, $\{0\}$ or $\mathbb{F}_q$, this allows us to write C and D as $\tilde{C}[P]$ and $\tilde{D}[P]$ respectively where $\tilde{C}$ and $\tilde{D}$ are linear complementary pair of abelian codes in $\mathbb{F}_q[A]$ (See also 3.5). Note that $p \nmid |A|$, so by using Theorem 3.8 we have that $\tilde{C}$ and $\tilde{D}^{\perp}$ are equivalent.

For each i, j, ℓ, set

$$\tilde{C}_{1,i} \;:=\; \begin{cases} \{0\}, & \text{if } C_{1,i} = \{0\} \\ \mathbb{F}_q, & \text{if } C_{1,i} = \mathbb{F}_q[P] \end{cases},$$

$$\tilde{C}_{2,j} \;:=\; \begin{cases} \{0\}, & \text{if } C_{2,j} = \{0\} \\ \mathbb{K}_j, & \text{if } C_{2,j} = \mathbb{K}_j[P] \end{cases},$$

$$\tilde{C}_{3,\ell} \;\; (\tilde{C}'_{3,\ell}) \;:=\; \begin{cases} \{0\}, & \text{if } C_{3,\ell} = \{0\} \quad (\text{if } C'_{3,\ell} = \{0\}) \\ \mathbb{L}_\ell, & \text{if } C_{3,\ell} = \mathbb{L}_\ell[P] \quad (\text{if } C'_{3,\ell} = \mathbb{L}_\ell[P]) \end{cases}.$$

Define $\tilde{D}_{1,i}, \tilde{D}_{2,j}, \tilde{D}_{3,\ell}, \tilde{D}'_{3,\ell}$ analogously. Let

$$(3.7) \qquad \begin{aligned} \tilde{C} &= \prod_{i=1}^{a} \tilde{C}_{1,i} \times \prod_{j=1}^{b} \tilde{C}_{2,j} \times \prod_{\ell=1}^{c} \left(\tilde{C}_{3,\ell} \times \tilde{C}'_{3,\ell}\right), \\ \tilde{D} &= \prod_{i=1}^{a} \tilde{D}_{1,i} \times \prod_{j=1}^{b} \tilde{D}_{2,j} \times \prod_{\ell=1}^{c} \left(\tilde{D}_{3,\ell} \times \tilde{D}'_{3,\ell}\right). \end{aligned}$$

Then $(\tilde{C}, \tilde{D})$ is an LCP of abelian codes in $\mathbb{F}_q[A]$. Moreover, $C = \tilde{C}[P]$ and $D = \tilde{D}[P]$ in $\mathbb{F}_q[A][P] = \mathbb{F}_q[G]$.

Proposition 3.14. *With the above notation, let $(C, D) = (\tilde{C}[P], \tilde{D}[P])$ be LCP of abelian codes in $\mathbb{F}_q[G]$. Then $\tilde{C}[P]$ and $\tilde{D}^\perp[P]$ are equivalent codes.*

Proof. We observed that $(\tilde{C}, \tilde{D})$ is an LCP of codes in $\mathbb{F}_q[A]$. In the semisimple case, it was proved that there is an equivalence σ between $\tilde{C}$ and $\tilde{D}^\perp$ ([13, Theorem 8]). Then the following bijection is the equivalence desired:

$$\begin{array}{cccc} \pi \;: & \tilde{C}[P] & \longrightarrow & \tilde{D}^\perp[P] \\ & \displaystyle\sum_{h \in P} c_h h & \longmapsto & \displaystyle\sum_{h \in P} \sigma(c_h) h. \end{array}$$

□

Remark 3.15. The equivalence σ between $\tilde{C}$ and $\tilde{D}^\perp$ is explicitly given in the proof of Theorem 8 in [13]. Since the map π simply applies this permutation on each coefficient $c_h \in \tilde{C}$, we also have an explicit permutation equivalence established between $\tilde{C}[P]$ and $\tilde{D}^\perp[P]$. It is also helpful to visualize elements of the group algebra $\mathbb{F}_q[A][P]$ as $|P| = p^t$-tuple of elements of $\mathbb{F}_q[A]$ by ordering the elements in P as $(h_1, \ldots, h_{p^t})$. Then we can view elements of $C = \tilde{C}[P]$ as

$$\sum_{i=1}^{p^t} c_i h_i \longleftrightarrow (c_1, \ldots, c_{p^t}) \in \mathbb{F}_q[A]^{p^t},$$

where each c_i belongs to $\tilde{C}$.

We are ready to prove the main result of this section, which extends [13, Theorem 8] from abelian codes in $\mathbb{F}_q[A]$ to those in $\mathbb{F}_q[G]$ (i.e. all abelian codes over finite fields).

Theorem 3.16. *Let (C,D) be an LCP of abelian codes in $\mathbb{F}_q[G]$. Then C and $D^{\perp}$ are equivalent codes.*

Proof. We need to show that $\tilde{D}^{\perp}[P]$ and $(\tilde{D}[P])^{\perp}$ are equal. Note that if $\dim_{\mathbb{F}_q} \tilde{D} = k$, then $\dim_{\mathbb{F}_q} \tilde{D}^{\perp}[P] = \dim_{\mathbb{F}_q}(\tilde{D}[P])^{\perp} = (m-k)p^t$ (recall that $m = |A|$ and $p^t = |P|$). Hence it is enough to show that one of these codes is contained in the other. By Remark 3.15, an element of $\tilde{D}^{\perp}[P]$ can be viewed as a p^t-tuple $(d_1^{\perp}, \dots, d_{p^t}^{\perp})$ of elements of $\tilde{D}^{\perp}$. Same also holds for the elements of $\tilde{D}[P]$ for which the elements can be viewed as p^t-tuples of elements of $\tilde{D}$. Since the Euclidean inner product on $\mathbb{F}_q[A]$ is "coordinate-wise", $(d_1^{\perp}, \dots, d_{p^t}^{\perp})$ is orthogonal to all elements in $\tilde{D}[P]$. Hence $\tilde{D}^{\perp}[P] \subseteq (\tilde{D}[P])^{\perp}$ and the result follows. □

Remark 3.17. Recall that the *matrix product (MP) code* $C = [C_1, \dots, C_s]A$ is the set of all matrix products $[c_1, \dots, c_s]A$ where $C_1, \dots, C_s$ are linear codes of length m over $\mathbb{F}_q$, $c_i \in C_i$ is an $m \times 1$ column vector $c_i = (c_{1,i}, \dots, c_{m,i})^T$ for $i = 1, \dots, s$ and $A = (a_{ij})$ is an $s \times l$ matrix over $\mathbb{F}_q$ with $s \leq l$. It is known that if $(C_i)_{1 \leq i \leq s}$ are linear codes over $\mathbb{F}_q$ with parameters $[m, k_i]$ and A is an $s \times l$ full row rank matrix, then $C = [C_1, \dots, C_s]A$ is an $[ml, \sum_{i=1}^{s} k_i]$ code.

By using the following lemma, the equality $\tilde{D}^{\perp}[P] = (\tilde{D}[P])^{\perp}$ can also be proven via MP codes.

Lemma 3.18 (Proposition 6.2, [2]). *Let $(C_i)_{1 \leq i \leq s}$ be linear codes over $\mathbb{F}_q$ with parameters $[m, k_i]$ and A be a non-singular matrix. If $C = [C_1, \dots, C_s]A$, then $([C_1, \dots, C_s]A)^{\perp} = [C_1^{\perp}, \dots, C_s^{\perp}](A^{-1})^T$.*

Corollary 3.19. *Let $D = \tilde{D}[P]$ be as in Proposition 3.14. Then $\tilde{D}^{\perp}[P] = (\tilde{D}[P])^{\perp}$.*

Proof. We can see a linear code $D = \tilde{D}[P]$ as an MP code as follows. Let $A = (I)_{b \times b}$ be an identity matrix where $|P| = p^t = b$ for some t. Then,

$$\tilde{D}[P] = [\tilde{D}, \dots, \tilde{D}]A = [\tilde{D}, \dots, \tilde{D}] = \{(d_1, \dots, d_b), d_i \in \tilde{D})\}$$

is a matrix-product code. Since $(I)_{b \times b} = A = (A^{-1})^T$ by using Lemma 3.18,

$$(\tilde{D}[P])^{\perp} = [\tilde{D}^{\perp}, \dots, \tilde{D}^{\perp}] = \tilde{D}^{\perp}[P].$$

□

3.3 LCP of Abelian Codes: Generator Polynomials

Recall that, Yang and Massey characterized LCD cyclic codes in terms of the generator polynomial ([26]). This result was extended to LCP of cyclic codes by Carlet et al. ([7, Theorem 2.1]). Our goal in this section is to extend the same result to abelian codes.

Consider a finite abelian group $G = A \oplus P$ as in (3.4). It is noted in [16] that if P is a cyclic p-group, then $\mathbb{F}_q[G]$ is a principal ideal group algebra (PIGA). Clearly, $\mathbb{F}_q[G]$ is also a PIGA when P is trivial (i.e. when $\mathbb{F}_q[G]$ is semisimple). Hence an abelian code C in a PIGA $\mathbb{F}_q[G]$ can be generated by one element, though not uniquely, as in the case of cyclic codes. Let $u, v \in \mathbb{F}_q[G]$ such that

$$C = \mathbb{F}_q[G]u = \{x \in \mathbb{F}_q[G] : \; xv = 0\} =: Ann(v) \quad \text{(cf. [16, Proposition 3.1]).}$$

Here, $Ann(v)$ is the annihilator of v. Hence, one can define generator and check elements for an abelian code in a PIGA (u and v in this case). Moreover, for $v = \sum_{g\in G} v_g g \in \mathbb{F}_q[G]$, if we set

$$\bar{v} := \sum_{g\in G} v_{-g} g,$$

then $C^\perp = \mathbb{F}_q[G]\bar{v}$, see [16, Proposition 3.1]. We will also need the following fact.

Proposition 3.20. *([16, Corollary 5.8]) For $\mathbb{F}_q[G]u = Ann(v)$ in a semisimple algebra $\mathbb{F}_q[G]$, we have $\mathbb{F}_q[G]u \cap \mathbb{F}_q[G]v = \{0\}$.*

With generator and check elements defined as above for an abelian code in a PIGA, we can now extend the relation between the generator polynomials of an LCP of cyclic codes ([7, Theorem 2.1]) to the abelian codes in a semisimple PIGA.

Proposition 3.21. *Assume that $\gcd(q, |G|) = 1$ and let $C = \mathbb{F}_q[G]u = Ann(v)$ and $D = \mathbb{F}_q[G]w$ be abelian codes, where $u, v, w \in \mathbb{F}_q[G]$. Then, (C, D) is an LCP of abelian codes if and only if $D = \mathbb{F}_q[G]v$.*

Proof. Assume that $\mathbb{F}_q[G]u \oplus \mathbb{F}_q[G]w = \mathbb{F}_q[G]$ (i.e. (C,D) is LCP). Then,

$$\begin{aligned}\mathbb{F}_q[G]v &= (\mathbb{F}_q[G]u \oplus \mathbb{F}_q[G]w) \cap \mathbb{F}_q[G]v \\ &= (\mathbb{F}_q[G]u \cap \mathbb{F}_q[G]v) \oplus (\mathbb{F}_q[G]w \cap \mathbb{F}_q[G]v) \\ &= \mathbb{F}_q[G]w \cap \mathbb{F}_q[G]v \ \ \text{(Proposition 3.20)}.\end{aligned}$$

Hence, $\mathbb{F}_q[G]v \subseteq \mathbb{F}_q[G]w$.

Note that $|\mathbb{F}_q[G]u||\mathbb{F}_q[G]\bar{v}| = |\mathbb{F}_q[G]| = |\mathbb{F}_q[G]u||\mathbb{F}_q[G]w|$. The first equality follows since $C^{\perp} = \mathbb{F}_q[G]\bar{v}$, and the second follows since (C,D) is LCP. Hence, $|\mathbb{F}_q[G]\bar{v}| = |\mathbb{F}_q[G]w|$. It is easy to see that $|\mathbb{F}_q[G]\bar{v}| = |\mathbb{F}_q[G]v|$ (cf. [16, Corollary 3.2]). Therefore $|\mathbb{F}_q[G]v| = |\mathbb{F}_q[G]w|$. Thus we obtain $\mathbb{F}_q[G]v = \mathbb{F}_q[G]w$.

For the converse statement, let us assume that $\mathbb{F}_q[G]w = \mathbb{F}_q[G]v$. Then $\mathbb{F}_q[G]u \cap \mathbb{F}_q[G]w = \{0\}$ by Proposition 3.20. The fact that $|\mathbb{F}_q[G]| = |\mathbb{F}_q[G]u||\mathbb{F}_q[G]w|$ follows using the same argument above. Hence, $\mathbb{F}_q[G]$ is the direct sum of $\mathbb{F}_q[G]u$ and $\mathbb{F}_q[G]w$. □

Remark 3.22. Theorem 2.1 in [7] states in the semisimple case that a pair of cyclic codes (C,D) of length n with generator polynomials $g(x), h(x)$, respectively, is LCP if and only if $h(x) = (x^n - 1)/g(x)$. Note that these are codes in $\mathbb{F}_q[C_n]$, or in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Hence, $g(x)h(x) = 0$ in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ and $C = Ann(h(x))$. Hence, Proposition 3.21 indeed extends the result of Carlet et al. Let us also note that [7, Theorem 2.1] extends the Yang-Massey characterization of cyclic LCD codes (i.e. $(C, C^{\perp})$ is LCP), which states that C is LCD if and only if $g(x)$ is a self-reciprocal polynomial. In the general semisimple abelian code case, since $C^{\perp} = \mathbb{F}_q[G]\bar{v}$, Proposition 3.21 concludes that C is LCD if and only if $C^{\perp} = \mathbb{F}_q[G]\bar{v} = \mathbb{F}_q[G]v$. This is analogous to the Yang-Massey result, since $\bar{v}$ amounts to “reciprocal" of v. Moreover, $\mathbb{F}_q[G]\bar{v} = \mathbb{F}_q[G]v$ and $\mathbb{F}_q[G]\bar{u} = \mathbb{F}_q[G]u$ are equivalent statements, as shown in [16, Theorems 5.4 and 5.9], for LCD abelian codes in the semisimple case.

4. LCP of Group Codes over Finite Chain Rings

4.1 Finite Chain Rings

We start with brief background on chain rings. Let us note that unless otherwise specified, R will denote a finite chain ring in this section.

A finite commutative ring R with identity is called a *chain ring* if its lattice of ideals is a chain under set-theoretic inclusion. For the class of finite commutative chain rings, we have the following equivalent conditions:

Proposition 4.1. *Let R be a finite commutative chain ring. The following are equivalent:*

i. R is a local ring and the maximal ideal M of R is principal.

ii. R is a local principal ideal ring.

iii. R is a chain ring.

So R is a local ring and 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 $\varphi : R \to \mathbb{F}_q$ 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

$$(r_i) \longmapsto \varphi(r_i), \tag{4.1}$$

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 $\mathbb{F}_q$.

A well-known example of a finite chain ring is in the following (see [21], Theorem XIV.8, Corollary XV.4):

Example 4.2. The Galois ring of characteristic p^a and dimension m, denoted by $\mathrm{GR}(p^a,m)$, is the Galois extension of degree m of the ring $\mathbb{Z}_{p^a}$. Equivalently,

$$\mathrm{GR}(p^a,m) = \mathbb{Z}_{p^a}[x]/\langle h(x)\rangle,$$

where $h(x)$ is basic irreducible polynomial of degree m in $\mathbb{Z}_{p^a}[x]$. Each ideal of $\mathrm{GR}(p^a,m)$ is of the form $\langle p^k\rangle = p^k\mathrm{GR}(p^a,m)$ for $0 \le k \le a$. In particular, $\mathrm{GR}(p^a,m)$ is a chain ring with maximal ideal $\langle p\rangle = p\mathrm{GR}(p^a,m)$ and residue field $\mathrm{GF}(p^m) = \mathbb{F}_{p^m}$ via considering a natural projection map

$$\begin{aligned} \varphi : \mathrm{GR}(p^a,m) &\longrightarrow \mathrm{GR}(p,m) \\ f(x) + \langle h(x)\rangle &\longmapsto f(x)(\text{mod p}) + \langle h(x)\rangle. \end{aligned}$$

Note that if $a = 1$, then $\mathrm{GR}(p,m) = \mathrm{GF}(p^m) = \mathbb{F}_{p^m}$ and if $m = 1$, then $\mathrm{GR}(p^a,1) = \mathbb{Z}_{p^a}$.

Now, let G be a finite group. 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 Chapter. 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 4.13) 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 an abelian code over R.

Remark 4.3. 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

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

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. 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.

4.2 LCP of Group Codes over Chain Rings

In [3], Borello et al. obtained the most general statement of Theorem 3.16 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 (ideals) in $\mathbb{F}_q[G]$, then C and $D^\perp$ are permutation equivalent. Our goal in this section is to generalize this result to all group codes over finite chain rings. We start with a simple observation on LCP of codes over a chain ring.

Lemma 4.4. *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 [17, Theorem 2], a projective module over a local ring is free. □

Proposition 4.5. *(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. □

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 the *submodule quotient* of C by r as

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

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 4.6. *([23, 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 4.7. *([23, Proposition 3.13], [24, 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 4.8. *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 4.6,

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

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

Proposition 4.9. *(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 4.6. By Proposition 4.7 ((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 4.5, $(\varphi(C), \varphi(D))$ is LCP of group codes in $\mathbb{F}_q[G]$. Then by [3] (cf. Section 4.1), $\varphi(C)$ 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). □

Remark 4.10. When we take an LCP of group codes (C,D) over R, by using φ projection map we go below over $\mathbb{F}_q$ where we showed in Proposition 4.9 that $\varphi(C)$ and $\varphi(D^{\perp})$ are equivalent group codes. Therefore $\tau(\varphi(C)) = \varphi(D^{\perp})$ for some permutation τ.

Consider an isomorphism f via

$$\begin{aligned} R[G]/\mathrm{Ker}(\varphi) &\longrightarrow \mathbb{F}_q[G], \\ x + \mathrm{Ker}(\varphi) &\longmapsto \varphi(x). \end{aligned}$$

Then, $f(C + \mathrm{Ker}(\varphi)) = \varphi(C)$ and $f(D^{\perp} + \mathrm{Ker}(\varphi)) = \varphi(D^{\perp})$.
So $C + \mathrm{Ker}(\varphi) = f^{-1}(\varphi(C))$ and $D^{\perp} + \mathrm{Ker}(\varphi) = f^{-1}(\varphi(D^{\perp}))$.

Hence we get,

$$D^{\perp} + \mathrm{Ker}(\varphi) = f^{-1}(\varphi(D^{\perp})) = f^{-1}(\tau(\varphi(C))) = \tau(f^{-1}(\varphi(C))).$$

So, $D^{\perp} + \mathrm{Ker}(\varphi) = \tau(C + \mathrm{Ker}(\varphi))$ which gives that $\tau(C) - D^{\perp} \in \mathrm{Ker}(\varphi)$ (over R).

In order to prove that C and $D^{\perp}$ are equivalent codes in $R[G]$, we will prove $\tau(C) = D^{\perp}$ where we have that $\tau(C) - D^{\perp} \in \mathrm{Ker}(\varphi)$. This says that when we take two codewords of C and $D^{\perp}$ above, which are τ-equivalent below, their difference may not be 0 but they will be in the same coset of $\mathrm{Ker}(\varphi) = \gamma R[G]$ with respect to $R[G]$. At this point related results of Norton and Salagean will be important in order to prove the equivalence between C and $D^{\perp}$.

Remark 4.11. Note that for an LCP of group codes (C,D) in $R[G]$, we have

$$\begin{aligned} |D^{\perp}| &= \frac{|R[G]|}{|D|} \quad \text{(by Proposition 4.6(i))} \\ &= \frac{|C||D|}{|D|} \quad \text{(since } C \oplus D = R[G]) \\ &= |C|. \end{aligned}$$

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 ([24, 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 4.13) from the permutation equivalence between $\varphi(C)$ and $\varphi(D^\perp)$ (cf. Proposition 4.9, Remark 4.11). However, note that Proposition 4.12 is true more generally (for free codes in R^n).

If we restrict the map $\varphi : R[G] \to \mathbb{F}_q[G]$ to the (free) group codes C and $D^\perp$, and use Proposition 4.7(iii), we obtain the isomorphisms

(4.2)
$$C/(C \cap \gamma R[G]) = C/\gamma C \simeq \varphi(C) \ \text{ and } \ D^\perp/(D^\perp \cap \gamma R[G]) = D^\perp/\gamma D^\perp \simeq \varphi(D^\perp).$$

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:

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

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

$$C = \dot{\bigcup_{1\le i\le t}} (c_i + \gamma C) \ \text{ and } \ D^\perp = \dot{\bigcup_{1\le i\le t}} (d_i + \gamma D^\perp) \tag{4.3}$$

Note that φ is constant on cosets, since a multiple of γ is mapped to 0. Namely for all $i = 1, \ldots, t$, 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 $\gamma D^\perp$. 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 4.11) satisfies

$$\tau(\varphi(c_i)) = \varphi(\tau(c_i)) = \varphi(d_i), \quad \text{for all } i = 1, \dots, t. \tag{4.4}$$

Note that this implies

$$\tau(c_i) - d_i \in \gamma R[G] \quad \text{for all } i = 1, \dots, t. \tag{4.5}$$

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 4.12. *Let C be a free code in $R[G]$ with the following representation (cf. (4.3)):*

$$C = \dot{\bigcup_{1 \le i \le t}} (c_i + \gamma C).$$

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 4.7, 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

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

Hence,

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

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

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

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

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

Theorem 4.13. *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 4.9, $\varphi(C)$ 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 4.8, and hence $(\varphi(C^{\perp}), \varphi(D^{\perp}))$ is LCP in $\mathbb{F}_q[G]$ (Proposition 4.5). If $\{c'_1 = 0, c'_2, \ldots, c'_s\}$ denotes the coset representatives of $C^{\perp}$ modulo $\gamma C^{\perp}$ and $\{d_1 = 0, d_2, \ldots, d_t\}$, as before, denotes the coset representatives of $D^{\perp}$ modulo $\gamma D^{\perp}$, we have

$$\mathbb{F}_q[G] = \varphi(C^{\perp}) \oplus \varphi(D^{\perp}) = \{\varphi(c'_i) + \varphi(d_j) : \ 1 \le i \le s, \ 1 \le j \le t\}. \tag{4.6}$$

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

$$\tau(C) = \dot{\bigcup_{1 \le i \le t}} (\tau(c_i) + \gamma\tau(C)) \ \ \text{(cf. (4.3))},$$

where $\{c_1 = 0, c_2, \ldots, c_t\}$ 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 $i \in \{2, \ldots, s\}$, then

$$\varphi(x) = \varphi(c'_i) \notin \varphi(\tau(C)) = \varphi(D^{\perp}) = \{\varphi(d_1) = 0, \varphi(d_2), \ldots, \varphi(d_t)\} \ \ \text{(cf. (4.6))}.$$

Therefore $\tau(C) \cap C^{\perp}$ is contained in $\gamma C^{\perp}$, hence in $\gamma\tau(C)$ (cf. Proposition 4.7 (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 4.3, since it is induced from an automporhism of G. So, $\tau(C)$ is an ideal of $R[G]$. By (4.5), 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 4.12, that $\tau(C) \subset D^{\perp}$. Since $\tau(C)$ and $D^{\perp}$ have the same cardinalities (cf. Remark 4.11), we have $\tau(C) = D^{\perp}$. This concludes the proof. □

Remark 4.14. Since $\tau(C)$, $C^{\perp}$ and $D^{\perp}$ are 2-sided ideals in $R[G]$, one can also observe that

$$\begin{aligned} \tau(C) &= \tau(C)R[G] \\ &= \tau(C)\Big(C^{\perp} \oplus D^{\perp}\Big) \\ &= \Big(\tau(C)C^{\perp}\Big) \oplus \Big(\tau(C)D^{\perp}\Big) \end{aligned}$$

where we have $\tau(C)C^{\perp} \subset \tau(C) \cap C^{\perp} = \{0\}$. So $\tau(C)C^{\perp} = \{0\}$, which gives that $\tau(C) = \tau(C)D^{\perp}$. Hence $\tau(C) \subset D^{\perp}$.

BIBLIOGRAPHY

[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] T. Blackmore and G.H. Norton, "Matrix-product codes over $\mathbb{F}_q$", *Appl. Algebra Engrg. Comm. Comput.*, vol. 12, 477-500, 2001.

[3] M. Borello, J. de la Cruz, W. Willems, "A note on linear complementary pairs of group codes", *Discrete Math.*, vol. 343, 111905.

[4] A. Boripan, S. Jitman and P. Udomkavanich, "Characterization and enumeration of complementary dual abelian codes", *J. Appl. Math. Comput.*, vol. 58, 527-544, 2018.

[5] 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.

[6] C. Carlet and S. Guilley, " Complementary dual codes for counter-measures to side-channel attacks", *Advances in Mathematics of Communications*, vol. 10, 131-150, 2016.

[7] 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.

[8] C. Carlet, S. Mesnager, C. Tang and Y. Qi, "Euclidean and Hermitian LCD MDS codes", *Des. Codes Cryptogr.*, vol. 86, 2605–2618, 2018 .

[9] C. Carlet, S. Mesnager, C. Tang, Y. Qi and R. Pellikaan, "Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$", *IEEE Trans. Inform. Theory*, vol.64, 3010-3017, 2018.

[10] C. Güneri, "Artin-Schreier curves and weights of two-dimensional cyclic codes", *Finite Fields Appl.*, vol. 10, 481-505, 2004.

[11] C. Güneri, E. Martinez-Moro and S. Sayıcı, "Linear complementary pair of group codes over finite chain rings", to appear in *Des. Codes Cryptogr.*

[12] C. Güneri and F. Özbudak, "Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields", *Finite Fields Appl.*, vol. 14, 44-58, 2008.

[13] C. Güneri, B. Özkaya and S. Sayıcı, "On linear complementary pair of nD cyclic codes", *IEEE Commun. Lett.*, vol. 22, 2404-2406, 2018.

[14] M. Grassl, “Bounds on the minimum distance of linear codes and quantum codes”, online available at http://www.codetables.de.

[15] J. Jensen, “The concatenated structure of cyclic and Abelian codes”, *IEEE Trans. Inform. Theory*, vol. 31, 788-793, 1985.

[16] S. Jitman, S. Ling, H. Liu and X. Xie “Abelian codes in principal ideal group algebras”, *IEEE Trans. Inform. Theory*, vol. 59, 3046-3058, 2013.

[17] I. Kaplansky, “Projective modules”, *Ann. of Math (2)*, vol. 68, 372-377, 1958.

[18] X. Liu and H. Liu, “LCD codes over finite chain rings”, *Finite Fields Appl.*, vol. 34, 1-19, 2015.

[19] Z. Liu and J. Wang, “Linear complementary dual codes over rings”, *Des. Codes Cryptogr.*, vol. 87, 3077-3086, 2019.

[20] J.L. Massey, “Linear codes with complementary duals”, *Discrete Math.*, vol. 106/107, 337-342, 1992.

[21] B.R. McDonald, “Finite rings with identity”, *Pure and Applied Mathematics*, Marcel Dekker, New York, vol. 28, 1974.

[22] W. K. Nicholson, “Local group rings”, *Canad. Math. Bull.*, vol. 15, 137-138, 1972.

[23] 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.

[24] 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.

[25] N. Sendrier, “Linear codes with complementary duals meet the Gilbert-Varshamov bound”, *Discrete Mathematics*, vol. 285, 345-347, 2004.

[26] X. Yang and J.L. Massey, “The condition for a cyclic code to have a complementary dual”, *Discrete Math.*, vol. 126, 391-393, 1994.