Group algebras and Coding Theory

César Polcino Milies *and Marinês Guerreiro †

July 4, 2017

Abstract

In the first part of this course, we present an introduction to the subject covering some of the important results that can be applied in this context, starting with the most basic facts. We begin with the famous theorem of Maschke and use Wedderburn's Theorem to describe the structure of group algebras in the semisimple case and its relation to primitive idempotents. We consider splitting fields and a Theorem of R. Brauer then study the theorem of Berman and Witt that gives the number of simple componentes in the semisimple case.

In the late sixties, S.D Berman [1] and F.J. MacWilliams [5], independently, introduced the idea of a group code, defined as an ideal of a finite group algebra. In the second part, we construct idempotents for abelian codes, always using the structure of subgroups of the underlying group. In some cases, it is possible to compute the parameters of the codes, and bases, using the group algebra structure. The construction of idempotents may also be extended to some non-abelian codes defined from dihedral and quaternion groups We finish mentioning some further developments on codes over rings.

Keywords: idempotents, group algebra, coding theory.

*C. Polcino Milies is with Instituto de Matemática e Estatística, Universidade de São Paulo, Rua do Matão, 1010 - CEP 05508-090 - São Paulo - SP

†M. Guerreiro is with Departamento de Matemática, Universidade Federal de Viçosa, Campus Universitário, CEP 36570-000 - Viçosa-MG (Brasil). E-mail: marines@ufv.br.

1 Introduction

The origins of Information Theory and Error Correcting Codes Theory are in the papers by Shannon [65] and Hamming [35], where they settled the theoretical foundations for such theories.

For a non empty finite set A, called **alphabet**, a **code** C of **length** n is simply a proper subset of A^n and an n-tuple $(a_0, a_1, \ldots, a_{n-1}) \in C$ is called a **word** of the code C.

If $A = \mathbb{F}_q$ is a finite field with q elements, then a **linear code** C of length n is a proper subspace of $\mathbb{F}_q^n$. If $\dim C = k$ $(k < n)$, then the number of words in C is q^k.

We shall call "cyclic shift" the linear map $\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ such that $\pi(a_0, a_1, \ldots, a_{n-1}) = (a_{n-1}, a_0, a_1, \ldots, a_{n-2})$.

A linear **cyclic code** is a linear code C that is invariant under the cyclic shift. This structure gives rise to fast-decoding algorithms, which is a considerable aspect regarding the conditions on communication.

Consider the quotient ring $R_n = \dfrac{\mathbb{F}_q[x]}{< x^n - 1 >}$ and denote by $[f(x)]$ the class of the polynomial $f(x)$ in R_n. There is a natural vector space isomorphism $\varphi : \mathbb{F}_q^n \longrightarrow R_n$ given by

$$\varphi(a_0, a_1, \ldots, a_{n-1}) = [a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}].$$

Linear cyclic codes are often realized as ideals in R_n and the cyclic shift is equivalent, via the isomorphism φ, to the multiplication by the class of x in R_n.

Group algebras may be defined in a more general setting, that is, for any group and over any field, as it was seen in the first part of this course. However, we restrict the definitions and results below to finite groups and finite fields because this is the context for coding theory. We recall some definitions.

Let G be a finite group written multiplicatively and $\mathbb{F}_q$ a finite field. The **group algebra of** G **over** $\mathbb{F}_q$ is the set of all formal linear combinations

$$\alpha = \sum_{g \in G} \alpha_g g, \quad \text{where} \quad \alpha_g \in \mathbb{F}_q.$$

Given $\alpha = \sum_{g \in G} \alpha_g g$ and $\beta = \sum_{g \in G} \beta_g g$ we have

$$\alpha = \beta \Longleftrightarrow \alpha_g = \beta_g, \quad \text{for all } g \in G.$$

The support of an element $\alpha \in \mathbb{F}_q G$ is the set of elements of G effectively appearing in α; i.e.,

$$\text{supp}(\alpha) = \{g \in G \mid a_g \neq 0\}.$$

We define

$$\left(\sum_{g\in G} \alpha_g g\right) + \left(\sum_{g\in G} \beta_g g\right) = \sum_{g\in G} (\alpha_g + \beta_g) g.$$

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) = \sum_{g,h\in G} (\alpha_g \beta_h) gh.$$

For λ in $\mathbb{F}_q$, we define

$$\lambda \left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} (\lambda \alpha_g) g.$$

It is easy to see that, with the operations above, $\mathbb{F}_q G$ is an algebra over the field $\mathbb{F}_q$.

The **weight** of an element $\alpha = \sum_{g\in G} a_g g \in \mathbb{F}_q G$ is the number of elements in its support; i.e.

$$w(\alpha) = |\{g \mid a_g \neq 0\}|.$$

For an ideal I of $\mathbb{F}_q G$, we define the **minimum weight** of I as:

$$w(I) = min\{w(\alpha) \mid \alpha \in I,\ \alpha \neq 0\}.$$

Let $C_n = \langle a \rangle$ denote a cyclic finite group of order n generated by an element a. MacWilliams [45] was the first one to consider cyclic codes as ideals of the group ring $\mathbb{F}_q C_n$ which is easily proved to be isomorphic to $\frac{\mathbb{F}_q[x]}{<x^n-1>}$. In $\mathbb{F}_q C_n$, the cyclic shift is equivalent to the multiplication of the elements of the code by a.

The following diagram helps us to understand the cyclic shift in these three different ways of considering a cyclic code.

$$\begin{array}{ccccc} C \subset \mathbb{F}_q^n & \xrightarrow{\varphi} & R_n = \frac{\mathbb{F}_q[x]}{<x^n-1>} & \xrightarrow{\cong} & \mathbb{F}_q C_n = \mathbb{F}_q < a > \\ \text{cyclic} & & & & \\ \downarrow & & \bar{x} \downarrow & & a \downarrow \\ \text{shift} & & & & \\ C \subset \mathbb{F}_q^n & \xrightarrow{\varphi} & R_n = \frac{\mathbb{F}_q[x]}{<x^n-1>} & \xrightarrow{\cong} & \mathbb{F}_q C_n = \mathbb{F}_q < a > \end{array}$$

Extending these ideas, Berman [9, 10] and, independently, MacWilliams [46] defined **abelian codes** as ideals in finite abelian group algebras and, more generally, a **group (left) code** was defined as an (left) ideal in a finite group algebra. Group codes were then studied using ring and character-theoretical results.

From now on, for a finite group G and a finite field $\mathbb{F}_q$, we treat ideals in a group algebra $\mathbb{F}_qG$ as codes. In this approach, the length of the code is the order of the group G and the dimension of a code I is its dimension as an $\mathbb{F}_q$-subspace in $\mathbb{F}_qG$. Length, dimension and minimum weight are the three parameters that define a linear code.

A group code is called **minimal** if the corresponding ideal is minimal in the set of ideals of the group algebra. Keralev and Solé in [40] showed that many important codes can be realized as ideals in a group algebra, for example, the generalized Reed-Muller codes and generalized quadratic residue codes. These results are included in Section 9.1 of [39]. There is also a good treatment on the subject in [22].

A word of warning is necessary here, because the expression "group code" may also have some other meanings. For example, in Computer Science, sometimes group codes consist of n linear block codes which are subgroups of G^n, where G is a finite abelian group, as in [12, 29].

Usually in the papers that present techniques to compute the idempotents that generate the codes, character theory is used in the context of polynomials, as it can be seen in [1, 2, 4, 5, 6, 51, 57, 58, 66]. Sometimes the expressions for the idempotents are not very "reader friendly". Moreover, the character theory and polynomial approaches in the computation of idempotents did not fully explore the structure of the group underneath the group algebra that defines the underlying set for the codes.

Here is the plan for this short course.

First Lecture: Introduction to the subject and construction of idempotents using subgroups of an abelian group.

Second Lecture: Discussion of some topics on dimension and minimum distance.

Third Lecture: Application of the previous topics to some specific cases.

Fourth Lecture: Approach of some equivalence questions.

Fifth Lecture: Some results on non-abelian codes.

In each lecture, some exercises or questions will be proposed.

FIRST LECTURE

2 Basic Facts

Let $\mathbb{F}_p$ be the Galois field with p elements. In this section we list some results on Finite Fields and Elementary Number Theory that will be needed in the sequel. Our first result is well-known.

Lemma 2.1. *[44, Theorem XVI.8] Let p be a positive prime number and r, $s \in \mathbb{N}^*$. Then*

$$\mathbb{F}_{p^r} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^s} \cong \gcd(r,s) \cdot \mathbb{F}_{p^{\mathrm{lcm}(r,s)}}.$$

Proof. Exercise. □

Remark 2.2. *Notice that any extension L of $\mathbb{F}_2$ of even degree contains a subfield K with four elements, hence there exists an element $1 \neq a \in L$ such that $a^3 = 1$.*

Lemma 2.3. *Let r, $s \in \mathbb{N}$ be non-zero elements such that $\gcd(r,s) = 2$. Let $u \in \mathbb{F}_{2^r}$ and $v \in \mathbb{F}_{2^s}$ be elements satisfying the equation $x^2 + x + 1 = 0$. Then*

$$\mathbb{F}_{2^r} \otimes_{\mathbb{F}_2} \mathbb{F}_{2^s} \cong \mathbb{F}_{2^{\frac{rs}{2}}} \oplus \mathbb{F}_{2^{\frac{rs}{2}}} \tag{1}$$

and $e_1 = (u \otimes v) + (u^2 \otimes v^2)$ and $e_2 = (u \otimes v^2) + (u^2 \otimes v)$ are the primitive idempotents generating to the simple components of (1).

Proof. The decomposition of $\mathbb{F}_{2^r} \otimes_{\mathbb{F}_2} \mathbb{F}_{2^s}$ as a direct sum follows from the previous lemma.

Since $u, u^2 \in \mathbb{F}_{2^r}$ (resp. $v, v^2 \in \mathbb{F}_{2^s}$) are linearly independent over $\mathbb{F}_2$, we have that $(u \otimes v)$, $(u^2 \otimes v^2)$, $(u \otimes v^2)$ and $(u^2 \otimes v)$ are linearly independent in $\mathbb{F}_{2^r} \otimes_{\mathbb{F}_2} \mathbb{F}_{2^s}$. Hence $e_1 \neq 0$ and $e_2 \neq 0$. As $1 + v + v^2 = 0$, $1 + u + u^2 = 0$, and hence also $u^3 = v^3 = 1$, we obtain:

$$e_1 \cdot e_2 = (u^2 \otimes 1) + (1 \otimes v^2) + (1 \otimes v) + (u \otimes 1) = (u^2 + u) \otimes 1 + 1 \otimes (v + v^2) = 0$$

and also

$$e_1 + e_2 = (u \otimes v) + (u^2 \otimes v^2) + (u \otimes v^2) + (u^2 \otimes v) = u \otimes (v + v^2) + u^2 \otimes (v + v^2) =$$

$$= 1 \otimes 1.$$

As $\mathbb{F}_{2^{\frac{rs}{2}}} \oplus \mathbb{F}_{2^{\frac{rs}{2}}}$ has two simple components, e_1 and e_2 are, in fact, the corresponding primitive idempotents. □

We shall also need the following result whose proof is elementary.

Lemma 2.4. *Let p and q be two distinct odd primes such that*

$$\gcd(p-1,\, q-1) = 2$$

and $\bar{2}$ generates both groups of units $U(\mathbb{Z}_p)$ and $U(\mathbb{Z}_q)$. Then the least positive integer k such that $2^k \equiv 1(\mod pq)$ is $\operatorname{lcm}(p-1, q-1) = \frac{(p-1)(q-1)}{2}$.

Proof. Exercise. □

3 Subgroups and idempotents

We recall that an element in the group algebra $\mathbb{F}_q G$ is called **central** if it commutes with every other element of the algebra. A non-zero central idempotent e is called **primitive** if it cannot be decomposed in the form $e = e' + e''$, where e' and e'' are both non-zero central idempotents such that $e'e'' = e''e' = 0$. For $\operatorname{char}(\mathbb{F}_q) \nmid |G|$, the group algebra $\mathbb{F}_q G$ is semisimple and the primitive central idempotents are the generators of the minimal two-sided ideals. Two idempotents e', e'' are **orthogonal** if $e'e'' = e''e' = 0$.

The primitive central idempotents of the rational group algebra $\mathbb{Q}G$ were computed in [34, Theorem VII.1.4] in the case G abelian; in [37, Theorem 2.1] when G is nilpotent; in [54, Theorem 4.4] in a more general context and in [13, Theorem 7] an algorithm to compute the primitive idempotents is given.

In what follows, we shall establish a correspondence between primitive idempotents of $\mathbb{F}_q G$ and certain subgroups of an abelian group G.

Let G be a finite (abelian) group and $\mathbb{F}_q$ a field such that $\operatorname{char}(\mathbb{F}_q) \nmid |G|$. Given a subgroup H of G, denote

$$\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h \tag{2}$$

which is an idempotent of $\mathbb{F}_q G$ and, for an element $x \in G$, set $\widehat{x} = \widehat{\langle x \rangle}$.

It is known that the idempotent $\widehat{G}$ is always primitive, as a consequence of [56, Proposition 3.6.7][1].

[1]

Definition 3.2. *Let G be an abelian group. A subgroup H of G is called a* ***co-cyclic subgroup*** *if the factor group $G/H \neq \{1\}$ is cyclic.*

We use the notation

$$\mathcal{S}_{\mathrm{cc}}(G) = \{H \mid H \text{ is a co-cyclic subgroup of } G\}.$$

For a finite group G, denote by $\exp(G)$ the **exponent** of G which is the smallest positive integer t such that $g^t = 1$, for all $g \in G$. A group G is called a p**-group** if its exponent is a power of a given prime p. In particular, this means that the order of every element of G is itself a power of p.

Let G be a finite abelian p-group and $\mathbb{F}_q$ a field such that $\mathrm{char}(\mathbb{F}_q) \nmid |G|$. For each co-cyclic subgroup H of G, we can construct an idempotent of $\mathbb{F}_q G$. In fact, we remark that, since G/H is a cyclic p-group, there exists a unique subgroup $H^\sharp$ of G containing H such that $|H^\sharp/H| = p$. Then $e_H = \widehat{H} - \widehat{H^\sharp}$ is an idempotent and we consider the set

$$\{\widehat{G}\} \cup \{e_H = \widehat{H} - \widehat{H^\sharp} \mid H \in \mathcal{S}_{\mathrm{cc}}(G)\}. \tag{3}$$

We recall the following results that are used throughout this paper.

In the case of a rational abelian group algebra $\mathbb{Q}G$, the set (3) is the set of all primitive central idempotents [34, Theorem 1.4].

Theorem 3.3. [28, Lemma 5] *Let p be a prime integer and G a finite abelian group of exponent p^n and $\mathbb{F}_q$ a finite field with q elements such that $p \nmid q$. Then* (3) *is a set of pairwise orthogonal idempotents of $\mathbb{F}_q G$ whose sum is equal to* 1*, i.e.,*

$$1 = \widehat{G} + \sum_{H \in \mathcal{S}_{\mathrm{cc}}(G)} e_H, \tag{4}$$

where 1 *also denotes the identity element in $\mathbb{F}_q G$.*

Proposition 3.1. *Let R be a ring and H a normal subgroup of a group G. If $|H|$ is invertible in R, setting $e_H = \frac{1}{|H|}\widehat{H}$, we have a direct sum of rings*

$$RG = RGe_H \oplus RG(1 - e_H),$$

with $RGe_H \cong R(G/H)$, $RG(1 - e_H) = \triangle(G, H)$ and

$$\triangle(G, H) = \{\sum_{h \in H} \alpha_h (h - 1) \mid \alpha_h \in RG\}.$$

Proof. The fact that these elements are idempotents is straightforward. Let H and K be different subgroups of G such that both G/H and G/K are cyclic, not equal to $\{1\}$, H^* and K^* be subgroups containing H and K, respectively, such that H^*/H and K^*/K are cyclic of order p. We shall consider first the case when $H \subset K$. In this case, clearly $H^* \subset K^*$ and thus

$$e_H e_K = (\widehat{H} - \widehat{H^*}) \cdot (\widehat{K} - \widehat{K^*}) = \widehat{K} - \widehat{K^*} - \widehat{K} + \widehat{K^*} = 0.$$

If neither of these subgroups is contained in the other, then both H and K are properly contained in HK, so also H^* and K^* are contained in HK, hence $H^*K^* \subset HK$. Clearly, $HK \subset H^*K^*$. Therefore, $HK = H^*K^*$. Now, since $HK \subset HK^* \subset H^*K^*$, it follows also $HK^* = HK$ and, in a similar way, we have $H^*K = HK$. Thus

$$e_H e_K = (\widehat{H} - \widehat{H^*}) \cdot (\widehat{K} - \widehat{K^*}) = 0.$$

Also, if one of the idempotents is equal to e_G a similar result follows easily.

Finally, we wish to show that the sum of these idempotents is equal to 1. For each cyclic subgroup C of G, we denote by $\mathcal{G}(C)$ the set of all elements of C that generate this subgroup; i.e.,

$$\mathcal{G}(C) = \{c \in C \mid \gcd(o(c), |C|) = 1\}.$$

If $\mathcal{C}$ denotes the family of all cyclic subgroups of G, then clearly $|G| = \sum_{C \in \mathcal{C}} |\mathcal{G}(C)|$ and, since G is a p-group, $|G(C)| = |C| - |C|/p$.

Let $S = \{G\} \cup \mathcal{S}_{\mathrm{cc}}(G)$ and denote $e = \sum_{H \in S} e_H$. We claim that $e = 1$. To prove this fact, it is enough to show that $(\mathbb{F}G)e = \mathbb{F}G$. As we have shown that these idempotents are pairwise orthogonal, we have

$$(\mathbb{F}G)e = \bigoplus_{H \in S} (\mathbb{F}G)e_H,$$

so

$$\dim_F (\mathbb{F}G)e = \sum_{H \in S} \dim_F (\mathbb{F}G)e_H.$$

Notice that $\widehat{H} = \widehat{H^*} + e_H$ and that $\widehat{H^*}e_H = 0$, thus

$$(\mathbb{F}G)\widehat{H} = (\mathbb{F}G)\widehat{H^*} \oplus (\mathbb{F}G)e_H.$$

Hence

$$\dim_{\mathbb{F}} (\mathbb{F}G)e_H = \dim_{\mathbb{F}} (\mathbb{F}G)\widehat{H} - \dim_{\mathbb{F}} (\mathbb{F}G)\widehat{H^*}.$$

It follows from the proof of [56, Proposition 3.6.7] that

$$\dim_{\mathbb{F}}((\mathbb{F}G)e_H) = \dim_{\mathbb{F}} \mathbb{F}[G/H] - \dim_{\mathbb{F}} \mathbb{F}[G/H^*] \tag{5}$$

and, clearly, $\dim_{\mathbb{F}} \mathbb{F}[G/H] = |G/H|$ and $\dim_{\mathbb{F}} \mathbb{F}[G/H^*] = |G/H^*|$.

It is well known that there exists a bijection $\Phi : \mathcal{C} \longrightarrow S$ such that $|X| = |G/\Phi(X)|$, for all $X \in \mathcal{C}$. This is a consequence of character theory for finite abelian groups (see [61, Chapter 10]). If we denote by $C \in \mathcal{C}$ the subgroup such that $\Phi(C) = H$, we have

$$\dim_{\mathbb{F}} \mathbb{F}[G/H] = |C|,$$

$$\dim_{\mathbb{F}} \mathbb{F}[G/H^*] = |G/H^*| = |G/H|/|H^*/H| = |C|/p,$$

so

$$\dim_{\mathbb{F}}((\mathbb{F}G)e_H) = |C| - |C|/p = |\mathcal{G}(C)| \tag{6}$$

and thus

$$\sum_{H \in S} \dim_{\mathbb{F}}((\mathbb{F}G)e_H) = \sum_{C \in \mathcal{C}} |\mathcal{G}(C)| = |G|.$$

This finishes the proof.

□

In our next statement, we denote by $U(\mathbb{Z}_{p^n})$ the set of invertible elements of the ring $\mathbb{Z}_{p^n}$ of integers modulo p^n; $\bar{q}$ denotes the class of the integer q in $\mathbb{Z}_{p^n}$ and, when it is invertible, $o(\bar{q})$ denotes its multiplicative order; i.e., the least positive integer m such that $\bar{q}^m = \bar{1}$.

Theorem 3.4. [28, Theorem 4.1] *Under the same hypotheses of Theorem 3.3, the set* (3) *is the set of all primitive idempotents of* $\mathbb{F}_q G$ *if and only if* $o(\bar{q}) = \phi(p^n)$ *in* $U(\mathbb{Z}_{p^n})$*, with* ϕ *denoting the Euler's totient function.*

For positive integers r and m, we shall denote by $\bar{r} \in \mathbb{Z}_m$ the image of r in the ring of integers modulo m. Then, for an element g in a group G, define $\mathcal{G}_g = \{g^r \mid \gcd(r, o(g)) = 1\} = \{g^r \mid \bar{r} \in U(\mathbb{Z}_{o(g)})\}$. The following theorem gives us conditions on the exponent e of the group G and the size q of the finite field that satisfy Theorem 3.4.

Corollary 3.5. [47, Teorema 7.10] *Let* $\mathbb{F}_q$ *be a finite field with* q *elements and* G *a finite abelian group with exponent* e *such that* $\gcd(q, |G|) = 1$*. Then* $C_g = \mathcal{G}_g$*, for all* $g \in G$*, if only if one of following conditions holds, with* ϕ *denoting the Euler´s totient function:*

(a) $e = 2$ *and* q *is odd;*

(b) $e = 4$ *and* $q \equiv 3 (\text{mod } 4)$*;*

(c) $e = p^n$ *and* $o(q) = \phi(p^n)$ *in* $U(\mathbb{Z}_{p^n})$*;*

(d) $e = 2p^n$ *and* $o(q) = \phi(p^n)$ *in* $U(\mathbb{Z}_{2p^n})$.

Theorem 3.6. [28, Lemma 3] *Let* $G = \langle g \rangle$ *be a cyclic group with order* p^n *and* $\mathbb{F}_q$ *a finite field with* q *elements such that* $\overline{q}$ *generates* $U(\mathbb{Z}_{p^n})$*. Consider*

$$G = G_0 \supset G_1 \supset ... \supset G_n = \{1\}$$

the descending chain of all subgroups of G*. Then a complete set of primitive idempotents in* $\mathbb{F}_q G$ *is:*

$$e_0 = \widehat{G} = \frac{1}{p^n} \sum_{g \in G} g \quad \textit{and} \quad e_i = \widehat{G_i} - \widehat{G_{i-1}}, \ \textit{for } 1 \leq i \leq n, \tag{7}$$

with $G_i =< g^{p^i} >$*, for* $1 \leq i \leq n$.

As the authors comment in [28], a straightforward computation shows that these are the same idempotents given in [2, Theorem 3.5], though there they are expressed in terms of cyclotomic cosets.

The idempotent generators of minimal ideals in the case of cyclic groups of order $2p^n$ now follow easily from the previous results.

Theorem 3.7. [2, Theorem 2.6] *Let* $\mathbb{F}_q$ *be a finite field with* q *elements and* G *a cyclic group of order* $2p^n$*,* p *an odd prime, such that* $o(\bar{q}) = \phi(p^n)$ *in* $U(\mathbb{Z}_{2p^n})$*. Write* $G = C \times A$*, where* A *is the* p*-Sylow subgroup of* G *and* $C = \{1, t\}$ *is its* 2*-Sylow subgroup. If* e_i*, for* $0 \leq i \leq n$*, denote the primitive idempotents of* $\mathbb{F}_q A$*, then the primitive idempotents of* $\mathbb{F}_q G$ *are*

$$\frac{1+t}{2} e_i, \quad \frac{1-t}{2} e_i, \quad 0 \leq i \leq n. \tag{8}$$

Proof. (Sketch of the proof:) As C is a cyclic group of order 2, we have

$$\mathbb{F}_q C = \mathbb{F}_q C \left(\frac{1-t}{2} \right) \oplus \mathbb{F}_q C \left(\frac{1+t}{2} \right) \cong \mathbb{F}_q \oplus \mathbb{F}_q.$$

Now, since $\mathbb{F}_q G = \mathbb{F}_q (C \times A) \cong \mathbb{F}_q C \otimes \mathbb{F}_q A$ and $\mathbb{F}_q A = \sum_{i=0}^{n} (\mathbb{F}_q A) e_i$, with e_i as in (7), the result follows. □

More generally,

Theorem 3.8. [28, Theorem 4.2] *Let p be an odd prime, G be an abelian p-group of exponent $2p^r$ and $\mathbb{F}_q$ be a finite field with q elements such that $o(q) = \phi(p^r)$ in $U(\mathbb{Z}_{2p^r})$. Write $G = E \times A$, with E an elementary abelian 2-group and A a p-group. Then the primitive idempotents of $\mathbb{F}_q G$ are products of the form $f \cdot e$, where f is a primitive idempotent of $\mathbb{F}_q E$ and e a primitive idempotent of $\mathbb{F}_q A$.*

QUESTION FOR DISCUSSION: What are the difficulties (or challenges) to find the set of primitive idempotents if we drop the conditions on the size of the field?

SECOND LECTURE

3.1 Dimension and minimum distance

This section follows [28, Section 5] and is devoted to the computation of dimension and minimum weight of codes generated by the idempotents presented in previous theorems.

Let $|G| = 2^m p^n$, with p denoting an odd prime and $m \geq 0$. As before, we write $G = E \times A$, with E an elementary abelian 2-group of order 2^m (eventually trivial) and A a p-group.

First if we write $E = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \langle a_m \rangle$, then the primitive idempotents of $\mathbb{F}_q E$ are the products of the form $f = f_1 f_2 \cdots f_m$, with $f_i = \frac{1+a_i}{2}$ or $f_i = \frac{1-a_i}{2}$, for $1 \leq i \leq m$.

In view of Corollary 3.5, these are the only cases where primitive idempotents of finite abelian group algebras can be computed in this way.

As the primitive idempotents of $\mathbb{F}_q A$ are as in (7), then the products of the form $e_E \cdot e_B$, with e_E a primitive idempotent of $\mathbb{F}_q E$ and e_A a primitive idempotent of $\mathbb{F}_q A$.

For a fixed idempotent e_E of $\mathbb{F}_q E$ and an arbitrary element $y \in E$ such that $y = a_1^{\varepsilon_1} \cdots a_m^{\varepsilon_m}$, with each $\varepsilon_i = 0$ or 1, for $1 \leq i \leq m$, we have

$$y e_E = a_1^{\varepsilon_1} \left(\frac{1 \pm a_1}{2} \right) \cdot a_2^{\varepsilon_2} \left(\frac{1 \pm a_2}{2} \right) \cdots a_m^{\varepsilon_m} \left(\frac{1 \pm a_m}{2} \right) = \pm e_E = (-1)^{\varepsilon_y} e_E, \tag{9}$$

with $\varepsilon_y = 0$ or 1.

First let us consider the primitive idempotents of the form $e_E\,\widehat{A}$. An element of $(\mathbb{F}_qG)\cdot e_E\,\widehat{A}$ is of the form $\gamma\cdot e_E\widehat{A}$, with $\gamma=\sum_{y\in E,a\in A}\alpha_{ya}\,y\,a$. Hence

$$\gamma\cdot e_E\,\widehat{A}=\sum_{y\in E,a\in A}\alpha_{yb}\,y\,a\,e_E\,\widehat{A}=\left(\sum_{y\in E,a\in A}\alpha_{ya}(-1)^{\varepsilon_y}\right)e_E\,\widehat{A}$$

This computation shows both that the dimension of the ideal $I=(\mathbb{F}_qG)e_E\widehat{A}$ is 1 and that its minimum distance is $l(I)=|G|$.

Now, we consider idempotents of the form $e=e_E\,e_H$, with $e_E\in\mathbb{F}_qE$, as above, and $e_H=\widehat{H}-\widehat{H^*}$, with H a subgroup of A such that A/H is cyclic of order p^i, say, and H^* is the unique subgroup of A containing H such that $[H^*:H]=p$. Set $I_e=(\mathbb{F}_qG)e$. Let $b\in A$ be an element such that $A=\langle b,H\rangle$. Then we also have $H^*=\langle b^{p^{i-1}},H\rangle$.

Notice

$$\left(1-b^{p^{i-1}}\right)e_E\widehat{H}=\left(1-b^{p^{i-1}}\right)e_E(\widehat{H^*}+e_H)=\left(1-b^{p^{i-1}}\right)e_E\,e_H.$$

Since $b^{p^{i-1}}\notin H$, it is clear that $\operatorname{supp}\left(1-b^{p^{i-1}}\right)e_H$ is the disjoint union $H\cup b^{p^{i-1}}H$, hence the weight of this element is $\omega\left(\left(1-b^{p^{i-1}}\right)e_E\,e_H\right)=2|E||H|$. Now if we denote by $\ell(I_e)$ the minimum distance of I_e, we have $\ell(I_e)=2^{m+1}|H|$.

Since A is the disjoint union $A=H\cup bH\cup\cdots\cup b^{p^{i-1}}H$, then also $G=E\times A$ is the disjoint union $G=(E\times H)\cup b(E\times H)\cup\cdots\cup b^{p^{i-1}}(E\times H)$, so an arbitrary element $\mathbb{F}_qG$ can be written in the form $\alpha=\sum_{j=0}^{p^i-1}\alpha_jb^j$, with $\alpha_j\in\mathbb{F}_q[E\times H]$.

Taking into account formula (9) and the fact that $h\widehat{H}=\widehat{H}$, for all $h\in H$, then each product $\alpha_je_Ee_H=k_je_Ee_H$, with $k_j\in\mathbb{F}_q$, for all $0\le j\le p^{i-1}$.

Since $e_H\widehat{H}=e_H$, then $(\mathbb{F}_qG)e_Ee_H\subset(\mathbb{F}_qG)e_E\widehat{H}$ and an element $0\neq\gamma\in(\mathbb{F}_qG)e_Ee_H=I_e$ can be written in the form

$$\gamma=\alpha e_E\widehat{H}=(k_0+k_1b+\cdots+k_{p^{i-1}}b^{p^{i-1}})e_E\widehat{H}.$$

As $\gamma\neq0$, we have at least one coefficient $k_j\neq0$. If $\gamma=k_jb^je_E\widehat{H}$, we would have $e_E\widehat{H}\in(\mathbb{F}_qG)e_Ee_H$, a contradiction. So, at least two different coefficients $k_j,k_{j'}$ must be nonzero, for each $\gamma\in I_e$ and thus $\ell(I_e)\ge2^{m+1}|H|$. Hence $\ell(I_e)=2^{m+1}|H|$.

Finally, we shall compute the dimension of minimal abelian codes; i.e., the dimension of ideals of the form $(\mathbb{F}_q G)e$, with e is a primitive idempotent of $\mathbb{F}_q G$. Let $e = e_E e_H$ be one such primitive idempotent. We have

$$(\mathbb{F}_q G)e_E e_H = \mathbb{F}_q[E \times A]e_E e_H = ((\mathbb{F}_q E)A)e_E e_H = ((\mathbb{F}_q E)e_E)A \cdot e_H.$$

As $(\mathbb{F}_q E)e_E \cong \mathbb{F}_q$, for all primitive idempotents of $\mathbb{F}_q E$, we have

$$(\mathbb{F}_q G)e_E e_H \cong \mathbb{F}_A e_H,$$

so formula (6) gives

$$\dim_{\mathbb{F}_q}[(\mathbb{F}_q G)e_E e_H] = \phi(p^i).$$

By a similar argument, we have $\dim_{\mathbb{F}_q}[(\mathbb{F}_q G)e_E \widehat{A}] = \dim_{\mathbb{F}_q}[(\mathbb{F}_q A)\widehat{A}] = 1$.

For non-cyclic abelian groups, we may also apply the ideas above to construct idempotents. In [27], the following results are presented in details.

For a finite abelian group G, we write $G = G_{p_1} \times \cdots \times G_{p_t}$, where G_{p_i} denotes the p_i-Sylow subgroup of G, for the distinct prime numbers $p_1, \ldots, p_t$.

Lemma 3.9. [27, Lemma II.5] *Let $G = G_{p_1} \times \cdots \times G_{p_t}$ be a finite abelian group and $H \in \mathcal{S}_{\rm cc}(G)$. Write $H = H_{p_1} \times \cdots \times H_{p_t}$, where H_{p_i} is the p_i-Sylow subgroup of H. Then each subgroup H_{p_i} is co-cyclic in G_{p_i}, $1 \leq i \leq t$.*

Proof. For $H \in \mathcal{S}_{\rm cc}(G)$, the quotient

$$G/H \cong G_{p_1}/H_{p_1} \times \cdots \times G_{p_t}/H_{p_t}$$

is cyclic, hence each factor G_{p_i}/H_{p_i} must be cyclic. Therefore, $H_{p_i} = G_{p_i}$ or $H_{p_i} \in \mathcal{S}_{\rm cc}(G_{p_i})$, for $1 \leq i \leq t$. □

With the notation above, for each $H \in \mathcal{S}_{\rm cc}(G)$, define an idempotent $e_H \in \mathbb{F}_q G$ as follows. For each $1 \leq i \leq t$, either $H_{p_i} = G_{p_i}$ or there exists a unique subgroup $H^\sharp_{p_i}$ such that $[H^\sharp_{p_i} : H_{p_i}] = p_i$. Thus, let $e_{H_{p_i}} = \widehat{G_{p_i}}$ or $e_{H_{p_i}} = \widehat{H_{p_i}} - \widehat{H^\sharp_{p_i}}$, respectively, and define

$$e_H = e_{H_{p_1}} e_{H_{p_2}} \cdots e_{H_{p_t}}. \tag{10}$$

For any other $K \in \mathcal{S}_{\rm cc}(G)$, with $K \neq H$, we have $K_{p_i} \neq H_{p_i}$, for some $1 \leq i \leq t$, and, by Theorem 3.3, $e_{H_{p_i}} e_{K_{p_i}} = 0$, hence $e_H e_K = 0$. It is easy to see that $\widehat{G} e_H = 0$, for all $H \in \mathcal{S}_{\rm cc}(G)$.

Thus, we have the following.

Proposition 3.10. [27, Proposition II.6] *Let G be a finite abelian group and $\mathbb{F}_q$ a field such that* $\mathrm{char}(\mathbb{F}_q) \nmid |G|$. *Then*

$$\mathcal{B} = \{e_H \mid H \in \mathcal{S}_{\mathrm{cc}}(G)\} \cup \{\widehat{G}\} \tag{11}$$

is a set of orthogonal idempotents of $\mathbb{F}_q G$, where e_H is defined as in (10).

A similar construction of idempotents for rational group algebras of abelian groups is given in [34, Section VII.1]. For the rational case, these idempotents are primitive while for finite fields this is usually not true.

Now, we extend Theorem 3.3 to finite abelian groups.

Lemma 3.11. [27, Lemma II.7] *Let G be a finite abelian group and $\mathbb{F}_q$ a field such that* $\mathrm{char}(\mathbb{F}_q) \nmid |G|$. *Then, in the group algebra $\mathbb{F}_q G$, we have*

$$1 = \widehat{G} + \sum_{H \in \mathcal{S}_{\mathrm{cc}}(G)} e_H. \tag{12}$$

The following lemma starts the discussion about the relation between idempotents and certain subgroups of the abelian group, which we elaborate in more details in Section 5.

Lemma 3.12. [27, Lemma II.8] *Let G be a finite abelian group and $\mathbb{F}_q$ a field such that* $\mathrm{char}(\mathbb{F}_q) \nmid |G|$. *For each primitive idempotent $e \in \mathbb{F}_q G$, $e \neq \widehat{G}$, there exists a unique $H \in \mathcal{S}_{\mathrm{cc}}(G)$ such that $e \cdot e_H = e$. Also, $e \cdot e_K = 0$, for any other $K \in \mathcal{S}_{\mathrm{cc}}(G)$.*

QUESTION 1: How can we present a basis (as a vector space) for each code generated (as an ideal) by an idempotent?

QUESTION 2: How are the primitive idempotents in the general case?

THIRD LECTURE

4 Cyclic and abelian codes of length $p^n q^m$

4.1 Binary abelian codes

Primitive idempotents for $\mathbb{F}_r G$, together with the corresponding dimensions and weights of the ideals they generate, were determined in [28] under the

following hypotheses:

G is a finite abelian group of exponent p^m (or $2p^m$, with p odd)
$\mathbb{F}_r$ a field with r elements, r with multiplicative order $\varphi(p^m) \pmod{p^m}$.

In [15], we considered finite abelian groups of type $G = G_p \times G_q$, for distinct odd primes p and q such that G_p is a p-group, G_q is a q-group satisfying the following conditions which will allow us to use the results in [28]:

$$\begin{array}{ll} (i) & \gcd(p-1,\, q-1) = 2, \\ (ii) & \bar{2} \textit{ generates the groups of units } U(\mathbb{Z}_{p^2}) \textit{ and } U(\mathbb{Z}_{q^2}) \\ (iii) & \gcd(p-1, q) = \gcd(p, q-1) = 1. \end{array} \tag{13}$$

The hypothesis (i) above implies that at least one of the primes p and q is congruent to 3 (mod 4). In this section, to fix notations, we shall always assume that $q \equiv 3 \pmod 4$. As a code (ideal) generated by a primitive idempotent is always isomorphic to a field, condition (i) also helps us to have some control on the number of simple components that appear in the group algebra $\mathbb{F}_r(G_p \times G_q)$, because of the elementary facts of Number Theory which were presented in Section 2

Methods to determine idempotent generators for minimal cyclic codes were given in [5, 6, 71] using representation theory. We develop our results without appealing to representation theory, working inside the group algebra.

In this section, we shall take $r = 2$. For two co-cyclic subgroups H of G_p and K of G_q, consider the respective idempotents $e_H = \widehat{H} - \widehat{H^*}$ in $\mathbb{F}_2 G_p$ and $e_K = \widehat{K} - \widehat{K^*}$ in $\mathbb{F}_2 G_q$. Clearly $\widehat{G_p} \cdot \widehat{G_q} = \widehat{G_p \times G_q}$ is a primitive idempotent of $\mathbb{F}_2 G = \mathbb{F}_2(G_p \times G_q)$.

We claim that idempotents of the form $\widehat{G_p} \cdot e_K$ are primitive. In fact, we have $(\mathbb{F}_2 G)\widehat{G_p} \cdot e_K = (\mathbb{F}_2 G \cdot \widehat{G_p}) e_K \cong (\mathbb{F}_2 G_q) e_K$ which is a field. In a similar way, it follows that idempotents of the form $e_H \cdot \widehat{G_q}$ are primitive.

We prove that each idempotent of the form $e_H \cdot e_K$ decomposes as the sum of two primitive idempotents in $\mathbb{F}_2 G$, using the following argument. For $e_H = \widehat{H} - \widehat{H^*}$, set $a \in H^* \setminus H$ (hence aH is a generator of H^*/H). Set

$$u = \begin{cases} a^{2^0} + a^{2^2} + \cdots + a^{2^{p-3}}, & \text{if } p \equiv 1 (\mathrm{mod}\, 4) \text{ or} \\ 1 + a^{2^0} + a^{2^2} + \cdots + a^{2^{p-3}}, & \text{if } p \equiv 3 (\mathrm{mod}\, 4) \end{cases} \tag{14}$$

and

$$u' = \begin{cases} a^2 + a^{2^3} + \cdots + a^{2^{p-2}}, & \text{if } p \equiv 1 (\mathrm{mod}\, 4) \text{ or} \\ 1 + a^2 + a^{2^3} + \cdots + a^{2^{p-2}}, & \text{if } p \equiv 3 (\mathrm{mod}\, 4) \end{cases} \tag{15}$$

For $e_K = \widehat{K} - \widehat{K^*}$, set $b \in K^* \setminus K$ and define v and v' as in (14) and (15) replacing a by b. As $\gcd(p^{r-1}(p-1), q^{s-1}(q-1)) = 2$ we can apply Lemma 2.3 to see that

$$\begin{aligned} e_1(H,K) &= u\widehat{H} \cdot v\widehat{K} + u'\widehat{H} \cdot v'\widehat{K} \text{ and} \\ e_2(H,K) &= u\widehat{H} \cdot v'\widehat{K} + u'\widehat{H} \cdot v\widehat{K} \end{aligned}$$

are primitive orthogonal idempotents such that $e_1 + e_2 = e_H e_K$.

Hence, we have shown the following.

Theorem 4.1. [15, Theorem III.1] *Let G_p and G_q be abelian p and q-groups, respectively satisfying the conditions in* (13)*. For a group G, denote by $S(G)$ the set of subgroups N of G such that $G/N \neq 1$ is cyclic. Then the set of primitive idempotents in $\mathbb{F}_2[G_p \times G_q]$ is:*

$$\begin{array}{rl} \widehat{G_p} \cdot \widehat{G_q}, & \\ \widehat{G_p} \cdot e_K, & K \in S(G_q), \\ e_H \cdot \widehat{G_q}, & H \in S(G_p), \\ e_1(H,K),\ e_2(H,K), & H \in S(G_p), K \in S(G_q). \end{array}$$

Particularly, in [15, Section IV] we compute, for each minimal code of $\mathbb{F}_2(C_p \times C_q)$, the generating primitive idempotent, its dimension and give explicitly a basis for it over $\mathbb{F}_2$. We reproduce the results in the sequel.

Let $p \neq q$ be odd primes and consider the group $G = \langle g \mid g^{pq} = 1 \rangle$. Denote $a = g^q$, $b = g^p$ and write $G = C_p \times C_q$, with $C_p = \langle a \rangle$ and $C_q = \langle b \rangle$. Theorem 4.1, in this context, gives the following.

Theorem 4.2. *[15, Theorem 4.1] Let $G = \langle a \rangle \times \langle b \rangle$ be as above and assume that p and q satisfy* (13)*. Then the primitive idempotents of $\mathbb{F}G$ are:*

$$e_0 = \widehat{G},\ \ e_1 = \hat{a}(1-\hat{b}),\ \ e_2 = (1-\hat{a})\hat{b},\ \ e_3 = uv + u^2v^2 \text{ and } e_4 = uv^2 + u^2v,$$

where $u = u(a)$ and $v = v(b)$ are as in (14) *above.*

Proposition 4.3. *[15, Proposition 4.3] With the same hypothesis as in Theorem 4.2 we have:*

(*i*) $\{e_0\}$ *is a basis of* $(\mathbb{F}_2G)e_0$.

(*ii*) $\mathcal{B}_1 = \{\hat{a}(b^j - 1) \mid 1 \leq j \leq q-1\}$ *and* $\mathcal{B}_1' = \{b^j e_1 \mid 1 \leq j \leq q-1\}$ *are bases of* $(\mathbb{F}_2G)e_1$.

(*iii*) $\mathcal{B}_2 = \{(a^j - 1)\hat{b} \mid 1 \leq j \leq p-1\}$ *and* $\mathcal{B}_2' = \{a^j e_2 \mid 1 \leq j \leq p-1\}$ *are bases of* $(\mathbb{F}_2G)e_2$.

Let $s, t \in \mathbb{Z}$ *be such that* $sq \equiv 1(\mod p)$ *and* $tp \equiv 1(\mod q)$*, then:*

(*iv*) $\{y, gy, g^2y, \ldots, g^{\frac{(p-1)(q-1)}{2}-1}y\}$*, with* $y = (1+a^s)(1+b^t)e_3$*, is a basis of* $(\mathbb{F}_2G)e_3$.

(*v*) $\{y, gy, g^2y, \ldots, g^{\frac{(p-1)(q-1)}{2}-1}y\}$*, with* $y = (1+a^s)(1+b^t)e_4$*, is a basis of* $(\mathbb{F}_2G)e_4$.

Proof. The validity of (i) is obvious. To prove (ii), notice that

$$(\mathbb{F}_2G)e_1 = (\mathbb{F}_2G)\hat{a}(1-\hat{b}) \cong (\mathbb{F}_2C_q)(1-\hat{b})$$

and this isomorphism maps the element $x \in (\mathbb{F}_2C_q)(1-\hat{b})$ to $x\hat{a} \in (\mathbb{F}_2G)e_1$. As the set $\{b^j - 1 \mid 0 < j \leq q-1\}$ is a basis of $(\mathbb{F}_2C_q)(1-\hat{b})$ (see [56, Proposition 3.2.10, p.133]), it follows that $\mathcal{B}_1'$ is a basis of $(\mathbb{F}_2G)e_1$.

To prove that $\mathcal{B}_1$ is also a basis of $(\mathbb{F}_2G)e_1$, we prove first that the set $\{b^j - \hat{b} \mid 1 \leq j \leq q-1\}$ is a basis of $(\mathbb{F}_2C_q)(1-\hat{b})$. To do so, it suffices to show that it is linearly independent, as it contains precisely $q-1$ elements.

Assume that there exist coefficients $x_j \in \mathbb{F}_2$, $1 \leq j \leq q-1$, such that $\sum_{j=1}^{q-1} x_j(b^j - \hat{b}) = 0$. If $\sum_{j=1}^{q-1} x_j = 0$, then $\sum_{j=1}^{q-1} x_j b^j = 0$ so $x_j = 0$ for all j, $1 \leq j \leq q-1$. If $\sum_{j=1}^{q-1} x_j = 1$ then $\sum_{j=1}^{q-1} x_j b^j + \hat{b} = 0$ so we must have $x_j = 1$, for all $1 \leq j \leq q-1$, which implies $\sum_{j=1}^{q-1} x_j = 0$, a contradiction.

Because of the isomorphism above, it follows that also $\mathcal{B}_1$ is a basis of $(\mathbb{F}_2G)e_1$.

The proof of (iii) is similar.

To prove (iv), notice that, by Lemma (2.1), $\dim_{\mathbb{F}_2}[(\mathbb{F}_2G)e_3] = \frac{(p-1)(q-1)}{2}$. Also, $(\mathbb{F}_2G)e_3 = \mathbb{F}_2(ge_3)$ is a finite field and ge_3 is a root of an irreducible polynomial of degree $\frac{(p-1)(q-1)}{2}$. Hence, the set

$$\{e_3, ge_3, g^2e_3, \ldots, g^{\frac{(p-1)(q-1)}{2}-1}e_3\}$$

is a basis of $(\mathbb{F}_2G)e_3$.

We shall prove independently in Lemma 4.5 that the element

$$y = (1 + a^s)(1 + b^t)e_3 \in (\mathbb{F}_2G)e_3$$

is nonzero. Then $\{y, gy, g^2y, \ldots, g^{\frac{(p-1)(q-1)}{2}-1}y\}$ is also a basis of $(\mathbb{F}_2G)e_3$.

The proof of (v) is a consequence of the isomorphism $(\mathbb{F}_2G)e_3 \cong (\mathbb{F}_2G)e_4$. □

Corollary 4.4. *[15, Corollary 4.4] Let G be as above. The dimensions of the minimal ideals of $\mathbb{F}_2G$ are:*

(i) $\dim_{\mathbb{F}_2}[(\mathbb{F}_2G)e_0] = 1.$

(ii) $\dim_{\mathbb{F}_2}[(\mathbb{F}_2G)e_1] = q - 1.$

(iii) $\dim_{\mathbb{F}_2}[(\mathbb{F}_2G)e_2] = p - 1.$

(iv) $\dim_{\mathbb{F}_2}[(\mathbb{F}_2G)e_3] = (p-1)(q-1)/2.$

(v) $\dim_{\mathbb{F}_2}[(\mathbb{F}_2G)e_4] = (p-1)(q-1)/2.$

In [15, Theorem 4.7] we presented the results on minimum weight for these codes.

We now compute the weight of a particular element of $\mathbb{F}_2G$.

Lemma 4.5. *With the same hypothesis of the Theorem 4.2 and notation above, the element $y = (1 + g^{sq})(1 + g^{tp})e_3 = (1 + a^s)(1 + b^t)e_3 \in (\mathbb{F}_2G)e_3$, with $s, t \in \mathbb{Z}$ such that $sq \equiv 1(\mod p)$ and $tp \equiv 1(\mod q)$, has weight $p + q$.*

Remark 4.6. *Lemma 4.5, shows that the elements in the bases defined in parts (iv) and (v) of Proposition 4.3 have all the same weight $p + q$.*

Theorem 4.7. *Let $G =< g >$ be an abelian group of order pq as in Theorem 4.2. Then:*
(i) $\omega((\mathbb{F}_2G)e_0) = p\,q.$
(ii) $\omega((\mathbb{F}_2G)e_1) = 2\,p.$
(iii) $\omega((\mathbb{F}_2G)e_2) = 2\,q.$
(iv) $4 \leq \omega((\mathbb{F}_2G)e_3) \leq p + q.$
(v) $4 \leq \omega((\mathbb{F}_2G)e_4) \leq p + q.$

Proof. (i) follows immediately as $(\mathbb{F}_2G)e_0 \cong \mathbb{F}_2$.

(ii) Recall that $e_1 = \hat{a}(1-\hat{b})$. Since $(b+b^2)e_1 = (b+b^2)\hat{a} \in (\mathbb{F}_2G)e_1$ and $supp(b\hat{a}) \cap supp(b^2\hat{a}) = \emptyset$ then $\omega((b+b^2)e_1) = 2p$. Hence $\omega((\mathbb{F}_2G)e_1) \leq 2p$.

An arbitrary element $\alpha \in (\mathbb{F}_2G)e_1$ is of the form

$$\alpha = \sum_{i,j} k_{ij}a^ib^j\hat{a}(1-\hat{b}) = \left[\sum_{j=0}^{q-1}(\sum_{i=0}^{p-1} k_{ij})b^j(1-\hat{b})\right]\hat{a}, \quad \text{with} \quad k_{i,j} \in \mathbb{F}_2,$$

hence is also an element of $(\mathbb{F}_2G)\hat{a}$. An element $\beta \in (\mathbb{F}_2G)\hat{a}$ is of the form

$$\beta = \sum_{i,j} \ell_{ij}a^ib^j\hat{a} = \sum_{j=0}^{q-1}(\sum_{i=0}^{p-1} \ell_{ij})b^j\hat{a}, \quad \text{with} \quad \ell_{i,j} \in \mathbb{F}_2.$$

Thus a nonzero element $\beta \in (\mathbb{F}_2G)\hat{a}$ has weight $\omega(\beta) = np$, with $n \geq 1$, as the elements $b^j\hat{a}$, for different values of j have disjoint supports.

Now as $b^j\hat{a}e_1 = b^je_1 \neq b^j\hat{a}$, the element $b^j\hat{a} \notin (\mathbb{F}_2G)e_1$. Hence, for an element $\alpha \in (\mathbb{F}_2G)e_1$ to have weight p, we must have $\alpha = b^j\hat{a}$, for some j, a contradiction. Therefore, $2p$ is the minimum weight of the code $(\mathbb{F}_2G)e_1$.

(iii) follows as (ii) interchanging a with b and p with q.

For (iv) and (v) it is enough to compute the weight of one of these codes, since there exists an automorphism of $\mathbb{F}_2G$ induced by a group automorphism of G that maps one code into the other, hence they are equivalent.

As $(1+a)(1+b)(e_3+e_4) = (1+a)(1+b)(1+\hat{a})(1+\hat{b}) = (1+a)(1+b)$, then $(1+a)(1+b) \in (\mathbb{F}_2G)(e_3+e_4)$. Besides, it is easy to prove that there is no element of weight 2 in $(\mathbb{F}_2G)(e_3+e_4)$ and, as $e_3, e_4 \in (\mathbb{F}_2G)(e_3+e_4)$, then $4 \leq \omega[(\mathbb{F}_2G)(e_3+e_4)] \leq \omega[(\mathbb{F}_2G)e_j]$, for $j = 3, 4$. By Lemma 4.5, we have $\omega[(\mathbb{F}_2G)e_3] \leq p+q$.

□

4.2 Examples

Example 4.8. *The upper bound for the weights of the codes in parts (iv) and (v) of Theorem 4.7 is sharp, as it is attained by the code generated by the primitive idempotent* $e = g + g^2 + g^3 + g^4 + g^6 + g^8 + g^9 + g^{12} \in \mathbb{F}_2C_{15}$. *Indeed, the group code* $I = (\mathbb{F}_2C_{15})e$ *has dimension* 4 *over* $\mathbb{F}_2$ *and it is easy to see that* $I = \{g^j\ e \,|\, j = 0, \ldots, 14\} \cup \{0\}$. *Hence all non zero elements in* I *have weight equal to* $\omega(e) = 8$.

However, this is not always the case as we can see below.

Example 4.9. *Let $C_{33} = \langle g \mid g^{33} = 1\rangle$ be the cyclic group with 33 elements and $(\mathbb{F}_2C_{33})e$ the abelian code generated by the primitive idempotent $e = g + g^2 + g^3 + g^4 + g^6 + g^8 + g^9 + g^{11} + g^{12} + g^{15} + g^{16} + g^{17} + g^{18} + g^{21} + g^{22} + g^{24} + g^{25} + g^{27} + g^{29} + g^{30} + g^{31} + g^{32}$. Then the weight distribution of $(\mathbb{F}_2C_{33})e_3$ is as follows:*

Vector Weight	12	14	16	18	20	22
Number of Vectors	165	165	165	330	165	33

In fact, notice first that the ideal $(\mathbb{F}_2C_{33})e$ is a field and Corollary 4.4 shows that its dimension over $\mathbb{F}_2$ is 10, so its group of units, $U((\mathbb{F}_2C_{33})e)$, has order $\mathbb{F}_2^{10} - 1 = 1023 = 33 \cdot 31$.

Notice that $C_{33} \cong C_{33} \cdot e \subset U((\mathbb{F}_2C_{33})e)$. Also $((g+g^{-1})e)^{32} = (g^{-1}+g)e$ thus $x = (g + g^{-1})e$ is an element of order equal to either 1 or 31 inside $U((\mathbb{F}_2C_{33})e)$. But, $x \neq e$, as $\omega(x) = 18$ and $\omega(e) = 22$. Hence $U((\mathbb{F}_2C_{33})e) = C_{33} \cdot e \times \langle x\rangle$.

Computing the 2-cyclotomic classes of x in $\langle x\rangle$, we have $U_0^* = \{0\}$,
$U_1^* = \{x, x^2, x^4, x^8, x^{16}\}$, $U_2^* = \{x^3, x^6, x^{12}, x^{24}, x^{17}\}$,
$U_3^* = \{x^5, x^{10}, x^{20}, x^9, x^{18}\}$, $U_4^* = \{x^7, x^{14}, x^{28}, x^{25}, x^{19}\}$,
$U_5^* = \{x^{11}, x^{22}, x^{13}, x^{26}, x^{21}\}$ and $U_6^* = \{x^{15}, x^{30}, x^{29}, x^{27}, x^{23}\}$.

Now for a fixed $0 \leq k \leq 31$, we have $\omega(g^j x^k) = \omega(x^k)$, for all $0 \leq j \leq 32$ and for each $0 \leq t \leq 6$, all $y \in U_t^*$ have the same weight.

Using these facts to compute the weights, we have that:

- There are 33 distinct elements of weight 22 in $(\mathbb{F}_2C_{33})e_3$, since $\omega(e_3) = 22$.
- There are 330 distinct elements in $(\mathbb{F}_2C_{33})e_3$ with weight 18, as $\omega(x) = 18$, $\omega(x^5) = 18$ and $U_1^* \cap U_3^* = \emptyset$.
- There are 165 distinct elements in $(\mathbb{F}_2C_{33})e_3$ with weight 16, since $\omega(x^3) = 16$.
- There are 165 distinct elements in $(\mathbb{F}_2C_{33})e_3$ with weight 20, since $\omega(x^7) = 20$.
- There are 165 distinct elements in $(\mathbb{F}_2C_{33})e_3$ with weight 12, since $\omega(x^{11}) = 12$.

- There are 165 distinct elements in $(\mathbb{F}_2 C_{33})e_3$ with weight 14, since $\omega(x^{15}) = 14$.

4.3 Ideals in $\mathbb{F}_2(C_{p^m} \times C_{q^n})$, $m \geq 2, n \geq 2$

The results in Section 4.1 allow us to obtain the following.

Theorem 4.10. *Let p and q satisfy (13). Let $G = \langle a \rangle \times \langle b \rangle$, with $C_{p^m} = \langle a \rangle$ and $C_{q^n} = \langle b \rangle$. Then the minimal ideals of $\mathbb{F}_2(C_{p^m} \times C_{q^n})$ are described in the following table.*

Ideal	Primitive Idempotent	Dimension	Code Weight
I_0	$\widehat{a}\widehat{b}$	1	$p^m q^n$
I_{0j}	$\widehat{a}(\widehat{b^{q^j}} + \widehat{b^{q^{j-1}}})$	$q^{j-1}(q-1)$	$2p^m q^{n-j}$
I_{i0}	$(\widehat{a^{p^i}} + \widehat{a^{p^{i-1}}})\widehat{b}$	$p^{i-1}(p-1)$	$2p^{m-i} q^n$
I_{ij}^*	$uv + u^2v^2$	$\frac{(p^i - p^{i-1})q^{j-1}(q-1)}{2}$	
I_{ij}^{**}	$uv^2 + u^2 v$	$\frac{p^{i-1}(p-1)q^{j-1}(q-1)}{2}$	

where $0 \leq i \leq m$, $0 \leq j \leq n$,

$$\begin{aligned} u &= \widehat{a^{p^i}}(a^{2^0 p^{i-1}} + a^{2^2 p^{i-1}} + \cdots + a^{2^{p-3} p^{i-1}}), \text{ if } p \equiv 1(\mod 4) \text{ or} \\ u &= \widehat{a^{p^i}}(1 + a^{2^0 p^{i-1}} + a^{2^2 p^{i-1}} + \cdots + a^{2^{p-3} p^{i-1}}), \text{ if } p \equiv 3(\mod 4) \end{aligned}$$

and

$$\begin{aligned} v &= \widehat{b^{q^j}}(b^{2^0 q^{j-1}} + b^{2^2 q^{j-1}} + \cdots + b^{2^{q-3} q^{j-1}}), \text{ if } q \equiv 1(\mod 4) \text{ or} \\ v &= \widehat{b^{q^j}}(1 + b^{2^0 q^{j-1}} + b^{2^2 q^{j-1}} + \cdots + b^{2^{q-3} q^{j-1}}), \text{ if } q \equiv 3(\mod 4) \end{aligned}$$

Proof. EXERCISE.

□

Example 4.11. *For $p = 3$ and $q = 5$, let $G = C_{3^m} \times C_{5^n} = \langle a \rangle \times \langle b \rangle$, with $o(a) = 3^m$ and $o(b) = 5^n$. According to Theorem 4.10, in $\mathbb{F}_2(C_{3^m} \times C_{5^n})$ with*

$1 \leq i \leq m-1$ *and* $1 \leq j \leq n-1$, *the code* $I_{ij}^* = \langle uv + u^2v^2 \rangle$ *is generated by the element*

$$\begin{aligned} e_{ij}^{(1)} &= uv + u^2v^2 = \widehat{a^{3^{i+1}}}\widehat{b^{5^{j+1}}}(b^{5^j} + b^{2\cdot 5^j} + b^{2^2\cdot 5^j} + b^{2^3\cdot 5^j}) \\ &+ \widehat{a^{3^{i+1}}}\widehat{b^{5^{j+1}}}[a^{3^i}(b^{5^j} + b^{2^2\cdot 5^j}) + a^{2\cdot 3^i}(b^{2\cdot 5^j} + b^{2^3\cdot 5^j})]. \end{aligned}$$

Using Example 4.8 and the computations above, we see that $\omega(e_{ij}^{(1)}) = \omega(I_{ij}^*) = 3^{m-(i+1)} \cdot 5^{n-(j+1)} \cdot 8$.

4.4 The case of three primes

The methods of the previous sections can be extended to the general case, but computations become much more envolved. As an illustration, we show below how to obtain the primitive idempotents when $|G|$ envolves three distinct primes.

Theorem 4.12. *Let* p_1, p_2 *and* p_3 *be three distinct positive odd prime numbers such that* $\gcd(p_i - 1, p_j - 1) = 2$, *for* $1 \leq i \neq j \leq 3$, *and* $\bar{2}$ *generates the groups of units* $U(\mathbb{Z}_{p_i})$. *Then the primitive idempotents of the group algebra* $\mathbb{F}_2G$ *for the finite abelian group* $G = C_{p_1} \times C_{p_2} \times C_{p_3}$, *with* $C_{p_1} =< a >$, $C_{p_2} =< b >$ *and* $C_{p_2} =< c >$, *are*

$e_0 = \hat{a}\hat{b}\hat{c}$, $e_1 = \hat{a}\hat{b}(1-\hat{c})$, $e_2 = \hat{a}(1-\hat{b})\hat{c}$, $e_3 = (1-\hat{a})\hat{b}\hat{c}$,
$e_4 = (uv + u^2v^2)\hat{c}$, $e_5 = (u^2v + uv^2)\hat{c}$ $e_6 = (uw + u^2w^2)\hat{b}$,
$e_7 = (u^2w + uw^2)\hat{b}$ $e_8 = (vw + v^2w^2)\hat{a}$, $e_9 = (v^2w + vw^2)\hat{a}$
$e_{10} = (1-\hat{a})(1-\hat{b})(1-\hat{c}) + u^2v^2w + uvw^2$
$e_{11} = (1-\hat{a})(1-\hat{b})(1-\hat{c}) + u^2v^2w^2 + uvw$
$e_{12} = (1-\hat{a})(1-\hat{b})(1-\hat{c}) + u^2vw + uv^2w^2$ *and*
$e_{13} = (1-\hat{a})(1-\hat{b})(1-\hat{c}) + uv^2w + u^2vw^2$,

where $u = u(a)$, $v = v(b)$, $w = w(c)$ *are defined as in* (14).

Proof. EXERCISE.

□

Comparing and using both the group algebra techniques of [15, 28] with the polynomial techniques of [5], Bastos and Guerreiro [7, 8] improved the presentation of minimal idempotents of length p^nq given in [41], correcting some coefficients in their expressions.

4.5 Cyclic codes of length 2^m

Codes are usually considered over the binary field $\mathbb{F}_2$. For cyclic codes of length 2^m, with a natural $m \geq 1$, over a field of odd size, the results obtained using a polynomial approach by Bakshi and Raka [4], Pruthi [60], Sharma et al. [68], Sharma et al. [67] and using the group algebra approach, by Prado [59] in her Ph.D. thesis, are essentially the same. In Chapter 2, Prado states the general facts:

Theorem 4.13. [59, Lema 2.1.1] *Let $G = \langle a \rangle$ be a finite cyclic group of order $2^m, m \geq 1$ and $\mathbb{F}_q$ a finite field of odd characteristic. Let*

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$$

be the descending chain of all subgroups of G, with $G_i = \langle a^{2^i} \rangle$ and $|G_i| = 2^{m-i}$. Then the elements $e_0 = \widehat{G}$ and $e_i = \widehat{G_i} - \widehat{G_{i-1}}$, with $1 \leq i \leq m$, form a set of orthogonal idempotents of $\mathbb{F}_q G$ such that $e_0 + e_1 + \cdots + e_m = 1$.

Theorem 4.14. [59, Lema 2.2.1] *Under the same hypothesis of Theorem 4.13, let $I_i = \mathbb{F}_q G e_i$, with $1 \leq i \leq m$, be the ideals of $\mathbb{F}_q G$ generated by the idempotents e_i of Theorem 4.13. Then*

$$\begin{aligned} \dim(I_0) &= 1, \qquad d(I_0) = |G| = 2^m \\ \dim(I_i) &= 2^{i-1}, \quad d(I_i) = |G| = 2^{m-i+1}, \text{ for } 1 \leq i \leq m. \end{aligned}$$

The notion of a visible code was given by Ward [75], where he defines a **visible basis** for a code as a basis where all its elements have the same weight. Prado also proved the following for codes of length 2^m.

Theorem 4.15. [59, Proposição 2.3.1] *Under the same hypothesis of Theorem 4.13, for $1 \leq i \leq m$, the set*

$$B_i = \{e_i, ae_i, a^2 e_i, \ldots, a^{2^{i-1}-1} e_i\}$$

is a visible basis for the code $I_i = \mathbb{F}_q G e_i$.

In her thesis [59], Prado studied in details the minimal codes generated by primitive idempotents in $\mathbb{F}_q C_{2^m}$, with q odd. She considered four cases: $q \equiv 1 (\mathrm{mod}\, 8)$, $q \equiv 3 (\mathrm{mod}\, 8)$, $q \equiv 5 (\mathrm{mod}\, 8)$ and $q \equiv 7 (\mathrm{mod}\, 8)$. The order of $q (\mathrm{mod}\, 2^m)$, the number of simple components of $\mathbb{F}_q C_{2^m}$ and the computation of idempotents are different for each one of these cases. For $q \equiv 3 (\mathrm{mod}\, 8)$ and $q \equiv 5 (\mathrm{mod}\, 8)$ a complete discussion is presented in the thesis and the other cases are exemplified with particular examples. Here is the case $q \equiv 3 (\mathrm{mod}\, 8)$.

Theorem 4.16. [59, Proposição 3.1.1] *Let $\mathbb{F}_q$ be a field with q elements such that $q \equiv 3 (\mathrm{mod}\, 8)$ and $G = \langle a \,|\, a^{2^m} = 1 \rangle$ be a cyclic group of order 2^m. The following elements of the group algebra $\mathbb{F}_q G$*

$$
\begin{aligned}
e_0 &= \frac{1 + a + a^2 + \cdots + a^{2^m - 1}}{2^m} \\
e_1 &= \frac{1 - a + a^2 - \cdots - a^{2^m - 1}}{2^m} \\
e_2 &= \frac{1 - a^2 + a^4 - \cdots - a^{2^m - 2}}{2^{m-1}} \\
e_3 &= (1 - a^4)\frac{(1 + a^{2^3} + \cdots + a^{2^m - 2^3})(2 + \alpha a + \alpha a^3)}{2^m} \\
e_3' &= (1 - a^4)\frac{(1 + a^{2^3} + \cdots + a^{2^m - 2^3})(2 - \alpha a - \alpha a^3)}{2^m} \\
e_4 &= (1 - a^8)\frac{(1 + a^{2^4} + \cdots + a^{2^m - 2^4})(2 + \alpha a^2 + \alpha a^{3\cdot 2})}{2^{m-1}} \\
e_4' &= (1 - a^8)\frac{(1 + a^{2^4} + \cdots + a^{2^m - 2^4})(2 - \alpha a^2 - \alpha a^{3\cdot 2})}{2^{m-1}} \\
&\cdots, \\
e_{m-1} &= (1 - a^{2^{m-2}})\frac{(1 + a^{2^m - 1})(2 + \alpha a^{2^{m-4}} + \alpha a^{3\cdot 2^{m-4}})}{2^4} \\
e_{m-1}' &= (1 - a^{2^{m-2}})\frac{(1 + a^{2^m - 1})(2 - \alpha a^{2^{m-4}} - \alpha a^{3\cdot 2^{m-4}})}{2^4} \\
e_m &= (1 - a^{2^{m-1}})\frac{(2 + \alpha a^{2^{m-3}} + \alpha a^{3\cdot 2^{m-3}})}{2^3} \\
e_m' &= (1 - a^{2^{m-1}})\frac{(2 - \alpha a^{2^{m-3}} - \alpha a^{3\cdot 2^{m-3}})}{2^3}
\end{aligned}
$$

form a complete set of primitive idempotents of $\mathbb{F}_q G$, with $\alpha^2 = -2$ in $\mathbb{F}_q$.

In Chapter 4 of her thesis, Prado simplifies results of Poli [57] in order to obtain a clearer description of the principal nilpotent ideals of a group algebra of finite abelian groups in a modular case (i.e., when $\mathrm{char}(\mathbb{F}_q)$ divides the order of the group G). She also exemplifies the process of lifting idempotents modulo a nilpotent ideal.

FOURTH LECTURE

5 On equivalence of abelian codes

The question of equivalence in Coding Theory has many approaches. In Section 6.2, we have define combinatorial equivalence and mention some other definitions. In [51], we found the following for abelian codes. Here G stands for a finite abelian group and $\mathbb{F}_q$ is a finite field with q elements.

Definition 5.1. *Two abelian codes $\mathcal{I}_1$ and $\mathcal{I}_2$ are* G-equivalent *if there exists an automorphism θ of G whose linear extension to $\mathbb{F}_q G$ maps $\mathcal{I}_1$ on $\mathcal{I}_2$.*

The following statements also appeared in [51].

Theorem A [51, Theorem 3.6] *Let G be a finite abelian group of odd order and exponent n and denote by $\tau(n)$ the number of divisors of n. Then there exist precisely $\tau(n)$ non G-equivalent minimal abelian codes in $\mathbb{F}_2 G$.*

Theorem B [51, Theorem 3.9] *Let G be a finite abelian group of odd order. Then two minimal abelian codes in $\mathbb{F}_2 G$ are G-equivalent if and only if they have the same weight distribution.*

Unfortunately both statements are not correct. The errors arise from the assumption, implicit in the last paragraph of [51, p. 167], that if e and f are primitive idempotents of $\mathbb{F}_2 C_m$ and $\mathbb{F}_2 C_n$, respectively, then ef is a primitive idempotent of $\mathbb{F}_2[C_m \times C_n]$. To the best of our knowledge, these results have not been used in a wrong way in the literature.

We first communicated the following counterexamples to both Theorems A and B in [26]. The ommited proofs of this section may be found in [27].

Proposition 5.2. [26, Proposition 3.1] *Let p be an odd prime such that $\bar{2}$ generates $U(\mathbb{Z}_{p^2})$ and $G = \langle a \rangle \times \langle b \rangle$ an abelian group, with $o(a) = p^2$ and $o(b) = p$. Then $\mathbb{F}_2 G$ has four inequivalent minimal codes, namely, the ones generated by the idempotents $e_0 = \widehat{G}$, $e_1 = \widehat{b} - \widehat{\langle a^p \rangle \times \langle b \rangle}$, $e_2 = \widehat{a} - \widehat{G}$ and $e_3 = \widehat{\langle a^p \rangle \times \langle b \rangle} - \widehat{G}$.*

Also all minimal codes of $\mathbb{F}_2 G$ are described in Table 1 with their dimension and weight. Moreover, the minimal inequivalent codes I_2 and I_3 have the same weight distribution.

Code	Primitive Idempotent	Dimension	Minimum Weight
I_0	$e_0 = \widehat{a}\widehat{b} = \widehat{G}$	1	p^3
I_1	$e_1 = \widehat{b} - \widehat{\langle a^p \rangle \times \langle b \rangle}$	$p^2 - p$	$2p$
I_{1j}	$e_{1j} = \widehat{a^{jp}b} - \widehat{\langle a^p \rangle \times \langle b \rangle}$ $j = 1, \ldots, p-1$	$p^2 - p$	$2p$
I_2	$e_2 = \widehat{a} - \widehat{G}$	$p - 1$	$2p^2$
I_{2i}	$e_{2i} = \widehat{ab^i} - \widehat{G}$ $i = 1, \ldots, p-1$	$p - 1$	$2p^2$
I_3	$e_3 = \widehat{\langle a^p \rangle \times \langle b \rangle} - \widehat{G}$	$p - 1$	$2p^2$

Table 1: Minimal codes in $\mathbb{F}_2(C_{p^2} \times C_p)$

In [26, Proposition 4.2] we showed that Theorem A holds in the special case of minimal codes in $\mathbb{F}_2(C_{p^n} \times C_{p^n})$ and, in [27, Theorem V.3], we generalize these result for G a direct product of $m \geq 2$ copies of a cyclic group C_{p^n}, as follows.

Proposition 5.3. [27, Proposition V.3] *Let m and r be positive integers and p a prime number. If $G = (C_{p^r})^m$ is a finite abelian p-group and $\mathbb{F}_q$ is a field of $\mathrm{char}(\mathbb{F}_q) \neq p$. Then a primitive idempotent of $\mathbb{F}_q G$, different from $\widehat{G}$, is of the form $\widehat{K} \cdot e_h$, where K is a subgroup of G isomorphic to $(C_{p^r})^{m-1}$ and e_h is a primitive idempotent of $\mathbb{F}_q\langle h \rangle$, where $h \in G$ is such that $G = \langle h \rangle \times K$ and $\langle h \rangle \cong C_{p^r}$.*

PROOF: Exercise.

This result can be applied as follows.

Corollary 5.4. [27, Corollary V.4] *Let m and r be positive integers, p a prime number, a finite abelian p-group $G = (C_{p^r})^m$ and $\mathbb{F}_q$ a finite field with q elements such that $o(\bar{q}) = \phi(p^r)$ in $U(\mathbb{Z}_{p^r})$. Then the minimal abelian codes*

in $\mathbb{F}_q G$ are as follows, where h and K are as in Proposition 5.3.

Primitive Idempotent	Dimension	Weight
$\widehat{G}$	1	p^{rm}
$\widehat{K}(\widehat{h^p} - \widehat{h})$	$p-1$	$2p^{r(m-1)+(r-1)}$
$\widehat{K}(\widehat{h^{p^2}} - \widehat{h^p})$	$p(p-1)$	$2p^{r(m-1)+(r-2)}$
$\widehat{K}(\widehat{h^{p^3}} - \widehat{h^{p^2}})$	$p^2(p-1)$	$2p^{r(m-1)-(r-3)}$
$\cdots$	$\cdots$	
$\widehat{K}(\widehat{h^{p^i}} - \widehat{h^{p^{i-1}}})$	$p^{i-1}(p-1)$	$2p^{r(m-1)-(r-i)}$
$\cdots$	$\cdots$	
$\widehat{K}(1 - \widehat{h^{p^{r-1}}})$	$p^{r-1}(p-1)$	$2p^{r(m-1)}$

Consequently, the number of non G-equivalent minimal abelian codes is $r+1 = \tau(p^r)$.

PROOF: Exercise.

Corollary 5.5. [27, Corollary V.5] *Let $n, m \geq 2$ be integers, $G = (C_n)^m$ an abelian group and $\mathbb{F}_q$ a finite field such that $\gcd(q,n) = 1$. Then the primitive idempotents of $\mathbb{F}_q G$ are of the form $\widehat{K} \cdot e_h$, where K is a subgroup of G isomorphic to $(C_n)^{m-1}$, $h \in G$ is such that $G = K \times \langle h \rangle$ and e_h is a primitive idempotent of $\mathbb{F}_q\langle h \rangle$.*

PROOF: Exercise.

Theorem 5.6. [27, Theorem V.6] *Let $G = C^n$ be a direct product of cyclic groups isomorphic to one another, of exponent n, and $\mathbb{F}_q$ a finite field such that $char(\mathbb{F}_q) \nmid |G|$. Then, the number of non G-equivalent minimal abelian codes is precisely $\tau(n)$.*

PROOF: Exercise.

We fully discussed the G-equivalence of abelian codes and established in [27, Section III] a relation between the classes of equivalence of G-equivalent codes and some classes of isomorphisms of subgroups of G, as follows.

We say that two subgroups H and K of a group G are ***G-isomorphic*** if there exists an automorphism $\psi \in \mathrm{Aut}(G)$ such that $\psi(H) = K$.

Notice that isomorphic subgroups are not necessarily G-isomorphic. For example, for a prime p, if $G = \langle a \rangle \times \langle b \rangle$ with $o(a) = p^2$ and $o(b) = p$, then $\langle a^p \rangle$ and $\langle b \rangle$ are isomorphic, as they are both cyclic groups of order p. However, they are not G-isomorphic, since $\langle b \rangle$ is contained, as a subgroup of index p, only in $\langle a^p \rangle \times \langle b \rangle$ while $\langle a^p \rangle$ is contained in $\langle a \rangle$ and in $\langle a^i b \rangle$, for all $1 \leq i \leq p-1$. An automorphism of G carrying one to the other would preserve also inclusions.

We shall denote by $\mathcal{P}(\mathbb{F}_q G)$ the set of all primitive idempotents of $\mathbb{F}_q G$. Recall the notion of co-cyclic subgroup (Definition 3.2). Then, under the same hypotheses of Lemma 3.12, the following map is well-defined

$$\begin{array}{rccc} \Phi \ : & \mathcal{P}(\mathbb{F}_q G) & \longrightarrow & \mathcal{S}_{\mathrm{cc}}(G) \cup \{G\} \\ & e \neq \widehat{G} & \longmapsto & \Phi(e) = H_e, \\ & \widehat{G} & \longmapsto & G \end{array} \tag{16}$$

where H_e is the unique co-cyclic subgroup of G such that $e \cdot e_{H_e} = e$.

Theorem 5.7. [27, Theorem II.9] *Let G be a finite abelian group, $\mathbb{F}_q$ a field such that $\mathrm{char}(\mathbb{F}_q) \nmid |G|$ and $H \in \mathcal{S}_{\mathrm{cc}}(G)$. Then e_H is the sum of all primitive idempotents $e \in \mathcal{P}(\mathbb{F}_q G)$ such that $\Phi(e) = H$.*

The study of the G-equivalence of ideals involves to know how the group of automorphisms $\mathrm{Aut}(G)$ acts on the lattice of the subgroups of G and hence on the idempotents in the group algebra which arise from these subgroups. From now on, we use the same notation for an automorphism of the group G and its linear extension to the group algebra $\mathbb{F}_q G$. The following results from [27] relate subgroups in G and idempotents in $\mathbb{F}_q G$.

Lemma 5.8. [27, Lemma III.1] *Let G be a finite abelian group, $H \in \mathcal{S}_{\mathrm{cc}}(G)$ and e_H its corresponding idempotent defined as in* (10)*. Then, for any $\psi \in \mathrm{Aut}(G)$, we have $\psi(e_H) = e_{\psi(H)}$ and $\psi(\widehat{G}) = \widehat{G}$.*

Proof. By Lemma 3.9, $H = H_{p_1} \times H_{p_2} \times \cdots \times H_{p_t}$, where H_{p_i} is the p_i-Sylow subgroup of H which is either equal to G_{p_i} (the p_i-Sylow subgroup of G) or co-cyclic in G_{p_i} , for each $1 \leq i \leq t$. Since $\psi \in \mathrm{Aut}(G)$, $\psi(H) = \psi(H_{p_1}) \times \psi(H_{p_2}) \times \cdots \times \psi(H_{p_t})$. Then each $\psi(H_{p_i})$ is either equal to G_{p_i}, the p_i-Sylow subgroup of $\psi(H)$, or is also co-cyclic in G_{p_i}. Hence $\psi(H_{p_i}^{\sharp}) = \psi(H)_{p_i}^{\sharp}$. Clearly, $\psi(\widehat{G}) = \widehat{G}$, for all $\psi \in \mathrm{Aut}(G)$. $\square$

For finite abelian groups, Propositions 5.9, 5.10 and 5.11 below establish a correspondence between G-equivalent minimal ideals in $\mathbb{F}_qG$ and G-isomorphic subgroups of G.

Proposition 5.9. [27, Proposition III.2] *Let G be a finite abelian group and $\mathbb{F}_q$ a field such that $\mathrm{char}(\mathbb{F}_q) \nmid |G|$. If $e, e' \in \mathcal{P}(\mathbb{F}_qG)$ are such that $\psi(e) = e'$, for some automorphism $\psi \in \mathrm{Aut}(G)$ linearly extended to $\mathbb{F}_qG$, then*

$$\psi(H_e) = H_{\psi(e)} = H_{e'},$$

i.e., H_e and $H_{e'}$ are G-isomorphic.

We set $\mathcal{L}\mathrm{Aut}(G) = \{\psi \in \mathrm{Aut}(G) \,|\, \psi(H) = H, \text{ for all } H \leq G\}$.

Proposition 5.10. [27, Proposition III.7] *Let G be a finite abelian group and $\mathbb{F}_q$ a field such that $\mathrm{char}(\mathbb{F}_q) \nmid |G|$. If $e', e'' \in \mathcal{P}(\mathbb{F}_qG)$ are both different from $\widehat{G}$ and $H_{e'} = H_{e''}$, then there exists an automorphism $\psi \in \mathcal{L}\mathrm{Aut}(G)$ whose linear extension to $\mathbb{F}_qG$ maps e' to e''.*

The following is the converse of Proposition 5.9.

Proposition 5.11. [27, Proposition III.8] *Let G be a finite abelian group and $\mathbb{F}_q$ a field such that $\mathrm{char}(\mathbb{F}_q) \nmid |G|$. If $e', e'' \in \mathcal{P}(\mathbb{F}_qG)$, both different from $\widehat{G}$, are such that $\psi(H_{e'}) = H_{e''}$, for some $\psi \in \mathrm{Aut}(G)$, then there exists an automorphism $\theta \in \mathrm{Aut}(G)$ whose linear extension to $\mathbb{F}_qG$ maps e' to e'', i.e., the ideals of $\mathbb{F}_qG$ generated by e' and e'' are G-equivalent.*

Proof. Since $\psi(H_{e'}) = H_{e''}$, for $\psi \in \mathrm{Aut}(G)$, by Lemma 5.8, we have

$$\psi(e')\, e_{H_{e''}} \;=\; \psi(e')\, \psi(e_{H_{e'}}) \;=\; \psi(e'\, e_{H_{e'}}) \;=\; \psi(e').$$

Hence, by uniqueness, we have $H_{\psi(e')} = H_{e''}$. Now, by Proposition 5.10, there exists an automorphism $\delta \in \mathcal{L}\mathrm{Aut}(G)$ such that $\delta(\psi(e')) = e''$. Therefore, taking $\theta = \delta\psi \in \mathrm{Aut}(G)$, the result follows. □

As an application of Propositions 5.9 and 5.11, in [27, Section IV] we consider the minimal codes in $\mathbb{F}_2(C_{p^n} \times C_p)$, for an odd prime p and $n \geq 3$. Its proof is similar to the proof of Proposition 5.2. This gives a whole family of counterexamples to Theorem A.

Code	Dimension	Weight
$I_0 = \langle\widehat{a}\widehat{b}\rangle = \langle\widehat{G}\rangle$	1	p^{n+1}
$I_1 = \langle\widehat{\langle a^p\rangle \times \langle b\rangle} - \widehat{G}\rangle$	$p-1$	$2p^n$
$I_{1i} = \langle\widehat{ab^i} - \widehat{G}\rangle$ $i = 0, \ldots, p-1$	$p-1$	$2p^n$
$I_2 = \langle\widehat{\langle a^{p^2}\rangle \times \langle b\rangle} - \widehat{\langle a^p\rangle \times \langle b\rangle}\rangle$	$p(p-1)$	$2p^{n-1}$
$I_{2i} = \langle\widehat{a^pb^i} - \widehat{\langle a^p\rangle \times \langle b\rangle}\rangle$ $i = 1, \ldots, p-1$	$p(p-1)$	$2p^{n-1}$
$\ldots$	$\ldots$	
$I_k = \langle\widehat{\left\langle a^{p^k}\right\rangle \times \langle b\rangle} - \widehat{\left\langle a^{p^{k-1}}\right\rangle \times \langle b\rangle}\rangle$	$p^{k-1}(p-1)$	$2p^{n-k+1}$
$I_{ki} = \langle\widehat{a^{p^{k-1}}b^i} - \widehat{\left\langle a^{p^{k-1}}\right\rangle \times \langle b\rangle}\rangle$ $i = 1, \ldots, p-1$	$p^{k-1}(p-1)$	$2p^{n-k+1}$
$\ldots$	$\ldots$	
$I_{n-1} = \langle\widehat{\langle b\rangle} - \widehat{\langle a^{p^{n-2}}\rangle \times \langle b\rangle}\rangle$	$p^{(n-1)}(p-1)$	$2p$
$I_{n-1,i} = \langle\widehat{a^{p^{n-1}}b^i} - \widehat{\langle a^{p^{n-2}}\rangle \times \langle b\rangle}\rangle$ $i = 1, \ldots, p-1$	$p^{(n-1)}(p-1)$	$2p$

Table 2: Minimal codes in $\mathbb{F}_2(C_{p^n} \times C_p)$

Proposition 5.12. [27, Theorem IV.3] *Let $n \geq 3$ be a positive integer and p an odd prime such that $\bar{2}$ generates $U(\mathbb{Z}_{p^n})$ and $G = \langle a\rangle \times \langle b\rangle$ be an abelian group, with $o(a) = p^n$ and $o(b) = p$. Then the minimal codes of $\mathbb{F}_2G$ are described in Table 2. Moreover, there are $2n$ inequivalent minimal codes in $\mathbb{F}_2(C_{p^n} \times C_p)$.*

In the first column of Table 3 we give a complete list of representatives of classes of G-isomorphisms of subgroups of $C_{p^n} \times C_p$ and, in the second column, we list the corresponding representatives of G-equivalent classes of minimal codes of $\mathbb{F}_2(C_{p^n} \times C_p)$.

5.1 Codes of length p^n also for non-cyclic abelian groups

Let $\mathbb{F}_q$ be a finite field with q elements and G a cyclic group of order p^n generated by a such that $\gcd(q, p) = 1$. Then the group algebra $\mathbb{F}_qG$ is semisimple and each of its ideals is a direct sum of minimal ones. Under

Subgroups	Codes
G	$I_0 = \langle \widehat{G} \rangle$
$\langle a \rangle$	$I_{11} = \langle \widehat{a} - \widehat{G} \rangle$
$\langle a^p \rangle \times \langle b \rangle$	$I_1 = \langle \widehat{\langle a^p \rangle \times \langle b \rangle} - \widehat{G} \rangle$
$\langle a^p b \rangle$	$I_{21} = \langle \widehat{a^p b} - \widehat{\langle a^p \rangle \times \langle b \rangle} \rangle$
$\left\langle a^{p^2} \right\rangle \times \langle b \rangle$	$I_2 = \langle \widehat{\langle a^{p^2} \rangle \times \langle b \rangle} - \widehat{\langle a^p \rangle \times \langle b \rangle} \rangle$
$\ldots$	$\ldots$
$\left\langle a^{p^k} b \right\rangle$	$I_{k+1,1} = \langle \widehat{a^{p^k} b} - \widehat{\left\langle a^{p^k} \right\rangle \times \langle b \rangle} \rangle$
$\left\langle a^{p^{k+1}} \right\rangle \times \langle b \rangle$	$I_{k+1} = \langle \widehat{\langle a^{p^{k+1}} \rangle \times \langle b \rangle} - \widehat{\left\langle a^{p^k} \right\rangle \times \langle b \rangle} \rangle$
$\ldots$	$\ldots$
$\langle b \rangle$	$I_{n-1} = \langle \widehat{b} - \widehat{\langle a^{p^n - 1} \rangle \times \langle b \rangle} \rangle$

Table 3:

the conditions (b) and (c) of Corollary 3.5, the minimal ideals (codes) are generated by the primitive idempotents given by Theorem 3.6.

In her thesis [49], Melo first considered **all** cyclic codes of $\mathbb{F}_q G$, that is, not only the minimals and computed dimension and minimum weights of these codes, using the following result.

Lemma 5.13. [25, Proposição 2.1] *Under the hypothesis above and considering I_i the minimal ideal of $\mathbb{F}_q G$ generated by the primitive idempotent e_i, as in (7), for $1 \leq i \leq n$, we have*

$$d(I_i) = 2|G_i| = 2p^{n-i} \quad \text{and} \quad \dim_{\mathbb{F}_q} I_i = \phi(p^i) = p^i - p^{i-1},$$

and a basis for I_i is

$$\mathcal{B}_i = \{a(1-b)\widehat{G_i} \,|\, a \in A, 1 \neq b \in B\},$$

with A a transversal of G_i in G_{i-1} and B a transversal of G_i in G. For the minimal code $I_0 = (\mathbb{F}_q G)e_0$, we have

$$w(I_0) = p^n \quad \text{and} \quad \dim_{\mathbb{F}_q} I_0 = 1.$$

Considering that the dimension of a direct sum of ideals is the sum of their dimensions, Melo [49, 50] focused her attention on computing minimum weight of the direct sum of minimal ideals as follows.

Theorem 5.14. *Under the hypothesis of this section and of Lemma 5.13, we have:*

(i) [49, Lema 2.3] *if* $0 < i < j$, *then* $w(I_i \oplus I_j) = 2|G_j| = 2p^{n-j}$.

(ii) [49, Lema 2.4] *If* $1 < j$, *then* $w(I_0 \oplus I_j) = 2|G_j| = 2p^{n-j}$.

(iii) [49, Lema 2.5] *If* $I = I_0 \oplus I_1$, *then* $w(I) = |G_1| = p^{n-1}$.

(iv) [49, Lema 2.6] *If* $I = \bigoplus_{i=0}^{t}(\mathbb{F}_q G)e_i$, *then* $I = (\mathbb{F}_q G)\widehat{G_t}$ *and* $w(I) = |G_t| = p^{n-t}$.

(v) [49, Lema 2.7] *If* $I = \bigoplus_{k=0}^{t}(\mathbb{F}_q G)e_{i_k}$, *with* $0 \leq i_1 < i_2 < \cdots < i_t$ *and* $e_{i_1} + e_{i_2} + \cdots + e_{i_t} \neq e_0 + e_1 + \cdots + e_t$, *then* $w(I) = 2|G_{i_t}| = 2p^{n-i_t}$.

Melo [49, Section 2.3] also considered the distribution of weights for these cyclic codes. Furthermore, in [49, Chapter 3], she briefly compared cyclic and non-cyclic abelian codes of length p^2, fully exploring some examples using GAP Wedderga package.

For the group $G = C_p \times C_p = \langle a \rangle \times \langle b \rangle$ and $\mathbb{F}_q$ a finite field of q elements such that $\bar{q}$ generates $U(\mathbb{Z}_p)$, the idempotents of $\mathbb{F}_q G$ are

$$e_0 = \widehat{G}, e_1 = \widehat{a} - \widehat{G}, e_2 = \widehat{b} - \widehat{G}, f_i = \widehat{ab^i} - \widehat{G}, \text{ with } 1 \leq i \leq p-1.$$

Note that if H and K are any among the subgroups $\langle a \rangle$, $\langle b \rangle$,$\langle ab^i \rangle$, with $1 \leq i \leq p-1$, then $G = H \times K$. For the idempotents $e = \widehat{H} - \widehat{G}$ and $e = \widehat{K} - \widehat{G}$ associated to H and K, respectively, and considering the ideal $I = (\mathbb{F}_q G)e \oplus (\mathbb{F}_q G)f$, Melo proved:

Theorem 5.15. [49, Teorema 3.2.1] *The minimum weight of the ideal* I *is* $d(I) = 2p - 2$ *and its dimension is* $\dim_{\mathbb{F}_q} I = 2p - 2$.

5.2 Essential idempotents an one weight cyclic codes

In [16], a special type of idempotent elements in the semisimple group algebra of a finite abelian group is considered, the so called *essencial* idempotents. These idempotents were previously considered by Bakshi, Raka and Sharma in [6], where they were called *non-degenerate*, in the special case of group algebras of cyclic groups over finite fields.

Definition 5.16. *In a semisimple group algebra* $\mathbb{F}_q G$ *of a finite group* G, *a primitive idempotent* e *is an* **essential idempotent** *if* $e\widehat{H} = 0$, *for every subgroup* $H \neq \{1\}$ *in* G. *A minimal ideal of* $\mathbb{F}_q G$ *is called an* **essential ideal** *if it is generated by an essential idempotent.*

The following is a characterization of essential idempotents.

Proposition 5.17. [16, Proposition 2.3] *Let $e \in \mathbb{F}_q G$ be a primitive central idempotent. Then e is essential if and only if the map $\pi : G \longrightarrow Ge$ is a group isomorphism.*

Corollary 5.18. [16, Corollary 2.4] *If G is an abelian group and $\mathbb{F}_q G$ contains an essential idempotent, then G is cyclic.*

For cyclic groups, Chalom, Ferraz and Polcino Milies [16] proved the existence of a non-zero central idempotent which is the sum of all essential idempotents. They also give a criteria to determine essential idempotents using the well-known Galois descent method and, as a consequence, compute the number of these idempotents in $\mathbb{F}_q C_n$, for C_n a cyclic group of order n.

In [16, Section 3] they show that the coeficients of the primitive idempotents of a semisimple group algebra $\mathbb{F}_q A$, for A is a finite abelian group, can be easily computed as a concatenation of the coeficients of an essential idempotent in the group algebras of a cyclic factor of A. In terms of coding theory, this will imply that every minimal abelian code generated by a non essential idempotent is a repetition code: their elements can be written as repetitions of the coeficients of elements in a cyclic code generated by an essential idempotent. In particular, one application of this is to determine the weight distribution of all codes when the weight distributions of codes generated by essential idempotents are known.

Nascimento, in her Ph.D. Thesis [52], uses this notion of essential idempotents to state conditions for a cyclic code in $\mathbb{F}_q C_n$ to be a one-weight code. Besides, she describes precisely the form of the elements on such a code and determines the number of one-weight codes in $\mathbb{F}_q C_n$. She also constructs examples of two weight codes in $\mathbb{F}_q(C_n \times C_n)$ and gives conditions to ensure that a code is of constant weight in $\mathbb{F}_q A$, for A an abelian group. Her work simplifies many of the proofs given by Vega [73] for the same facts. In the literature there is also an interesting paper by Wood [79] on linear codes of constant weight.

FIFTH LECTURE

6 Non Abelian Codes

6.1 Dihedral and Quaternion Codes

As a natural way to proceed, Theorem 3.3 is used by Dutra [23, 25] in her Ph.D. thesis to compute idempotents for non abelian group codes, particularly, for dihedral and quaternion groups. For the proofs of the results presented in this section, the thesis can be fully accessed in http://www.mat.ufmg.br/site/pos-principa/mestrado-e-doutorado/teses/

For $n \geq 1$, Dutra considered the semisimple group algebras $\mathbb{F}_q D_n$ of the dihedral groups $D_n = \langle a, b \,|\, a^n = b^2 = 1, bab = a^{-1} \rangle$ over a finite field $\mathbb{F}_q$ and gave conditions under which the number of its simple components is minimum, that is, the same as for the rational group algebra $\mathbb{Q}D_n$. These conditions are stated in the following theorem.

Theorem 6.1. [23, Teorema 2.2] *Let $\mathbb{F}_q$ be a field with q elements and D_n the dihedral group with $2n$ elements such that $\gcd(q, 2n) = 1$. Let p, p_1 and p_2 be distinct odd primes and m, m_1 and m_2 be positive integers. Then $\mathbb{F}_q D_n$ and $\mathbb{Q}D_n$ have the same number of simple components if and only if one of the following conditions occurs:*

(i) $n = 2$ or 4 and q is odd.

(ii) $n = 2^m$, with $m \geq 3$ and congruent to 3 or 5 modulo 8.

(iii) $n = p^m$ and the class $\bar{q}$ generates the group of units $U(\mathbb{Z}_{p^m})$.

(iv) $n = p^m$, the class $\bar{q}$ generates the group $U^2(\mathbb{Z}_{p^m}) = \{x^2 \,|\, x \in U(\mathbb{Z}_{p^m})\}$ and -1 is not a square modulo p^m.

(v) $n = 2p^m$ and the class $\bar{q}$ generates the group of units $U(\mathbb{Z}_{p^m})$.

(vi) $n = 2p^m$, $\bar{q}$ generates the group $U^2(\mathbb{Z}_{p^m}) = \{x^2 \,|\, x \in U(\mathbb{Z}_{p^m})\}$ and -1 is not a square modulo p^m.

(vii) $n = 4p^m$, 4 divides $\phi(p^m)$ and the class $\bar{q}$ generates the group $U(\mathbb{Z}_{p^m})$.

(viii) $n = 4p^m$, 4 does not divide $\phi(p^m)$, $q \equiv 1 (\mathrm{mod}\, 4)$ and the class $\bar{q}$ generates the group $U(\mathbb{Z}_{p^m})$.

(ix) $n = 4p^m$, 4 does not divide $\phi(p^m)$, $q \equiv -1 (\mathrm{mod}\, 4)$ and the class $\bar{q}$ has order $\phi(p^m)/2$.

(x) $n = p_1^{m_1} p_2^{m_2}$, with $\gcd(\phi(p_1^{m_1}), \phi(p_2^{m_2})) = 2$ and q or $-q$ has order $\phi(p_1^{m_1} p_2^{m_2})/2$ modulo $p_1^{m_1} p_2^{m_2}$.

(xi) $n = 2p_1^{m_1} p_2^{m_2}$, with $\gcd(\phi(p_1^{m_1}), \phi(p_2^{m_2})) = 2$ and q or $-q$ has order $\phi(p_1^{m_1} p_2^{m_2})/2$ modulo $p_1^{m_1} p_2^{m_2}$.

Under such conditions, Dutra computed the set of minimal codes of $\mathbb{F}_q D_n$, their dimensions, minimum weights and bases for these codes as follows.

Theorem 6.2. [23, Proposição 3.1] *Let q and n be integers related as in conditions (i) and (ii) of Theorem 6.1. If $\mathcal{C}$ is a dihedral code of length $2n$ generated by the idempotent e, then $\mathcal{C}$ has dimension and minimum weight described in the table below.*

e	$\dim_{\mathbb{F}_q}\mathcal{C}$	$w(\mathcal{C})$
$\widehat{b}\widehat{a}$	1	2^{m+1}
$(1-\widehat{b})\widehat{a}$	1	2^{m+1}
$\widehat{b}(\widehat{a^2}-\widehat{a})$	1	2^{m+1}
$(1-\widehat{b})(\widehat{a^2}-\widehat{a})$	1	2^{m+1}
$(\widehat{a^{2^i}}-\widehat{a^{2^{i-1}}})$	2^i	2^{m-i+1}

Theorem 6.3. [23, Proposição 3.2] *Let q and n be integers related as in conditions (iii) and (iv) of Theorem 6.1. If $\mathcal{C}$ is a dihedral code of length $2n$ generated by the idempotent e, then $\mathcal{C}$ has dimension and minimum weight described in the table below.*

e	$\dim_{\mathbb{F}_q}\mathcal{C}$	$w(\mathcal{C})$
$\widehat{b}\widehat{a}$	1	$2p^m$
$(1-\widehat{b})\widehat{a}$	1	$2p^m$
$(\widehat{a^{p^i}}-\widehat{a^{p^{i-1}}})$	$2\phi(p^i)$	$2p^{m-i}$

Theorem 6.4. [23, Proposição 3.3] *Let q and n be integers related as in conditions (v) to (ix) of Theorem 6.1. For $n = p_1^{m_1}p_2^{m_2}$ with $p_1 = 2, m_1 = 1$ or 2 and p_2 an odd prime, if $\mathcal{C}$ is a dihedral code of length $2n$ generated by the idempotent e_1e_2, then $\mathcal{C}$ has dimension and minimum weight described in*

the table below.

e_1	e_2	$\dim_{\mathbb{F}_q}\mathcal{C}$	$w(\mathcal{C})$
$\widehat{b\overline{C_{p_1^{m_1}}}}$	$\widehat{C_{p_2^{m_2}}}$	1	$2p_1^{m_1}p_2^{m_2}$
$(1-\widehat{b})\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2}}}$	1	$2p_1^{m_1}p_2^{m_2}$
$\widehat{b}(\widehat{C_{p_1^{m_1-1}}}-\widehat{C_{p_1^{m_1}}})$	$\widehat{C_{p_2^{m_2}}}$	1	$2p_1^{m_1}p_2^{m_2}$
$(1-\widehat{b})(\widehat{C_{p_1^{m_1-1}}}-\widehat{C_{p_1^{m_1}}})$	$\widehat{C_{p_2^{m_2}}}$	1	$2p_1^{m_1}p_2^{m_2}$
$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2-j}}}-\widehat{C_{p_2^{m_2-j+1}}}$	$2\phi(p_2^j)$	$2p_1^{m_1}p_2^{m_2-j}$
$\widehat{C_{p_1^{m_1-i}}}-\widehat{C_{p_1^{m_1-i+1}}}$	$\widehat{C_{p_2^{m_2}}}$	$2\phi(p_1^j)$	$2p_1^{m_1-i}p_2^{m_2}$
$\widehat{C_{p_1^{m_1-i}}}-\widehat{C_{p_1^{m_1-i+1}}}$	$\widehat{C_{p_2^{m_2-j}}}-\widehat{C_{p_2^{m_2-j+1}}}$	$2\phi(p_1^j)2\phi(p_2^j)$	$4p_1^{m_1-i}p_2^{m_2-j}$

Theorem 6.5. [23, Proposição 3.4] *Let q and $n=p_1^{m_1}p_2^{m_2}$, with p_1 and p_2 odd distinct prime numbers, integers related as in condition (x) of Theorem 6.1. If $\mathcal{C}$ is a dihedral code of length $2n$ generated by the idempotent e_1e_2, then $\mathcal{C}$ has dimension and minimum weight described in the table below.*

e_1	e_2	$\dim_{\mathbb{F}_q}\mathcal{C}$	$w(\mathcal{C})$
$\widehat{b\overline{C_{p_1^{m_1}}}}$	$\widehat{C_{p_2^{m_2}}}$	1	$2p_1^{m_1}p_2^{m_2}$
$(1-\widehat{b})\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2}}}$	1	$2p_1^{m_1}p_2^{m_2}$
$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2-j}}}-\widehat{C_{p_2^{m_2-j+1}}}$	$2\phi(p_2^j)$	$2p_1^{m_1}p_2^{m_2-j}$
$\widehat{C_{p_1^{m_1-i}}}-\widehat{C_{p_1^{m_1-i+1}}}$	$\widehat{C_{p_2^{m_2}}}$	$2\phi(p_1^j)$	$2p_1^{m_1-i}p_2^{m_2}$
$\widehat{C_{p_1^{m_1-i}}}-\widehat{C_{p_1^{m_1-i+1}}}$	$\widehat{C_{p_2^{m_2-j}}}-\widehat{C_{p_2^{m_2-j+1}}}$	$2\phi(p_1^j)2\phi(p_2^j)$	$4p_1^{m_1-i}p_2^{m_2-j}$

Theorem 6.6. [23, Proposição 3.5] *Let q and $n=2p_1^{m_1}p_2^{m_2}$, with p_1 and p_2 odd distinct prime numbers, integers related as in condition (xi) of Theorem 6.1. If $\mathcal{C}$ is a dihedral code of length $2n$ generated by the idempotent $e_0e_1e_2$, then $\mathcal{C}$ has dimension and minimum weight described in the table*

below.

e_0	e_1	e_2	$\dim_{\mathbb{F}_q}\mathcal{C}$	$w(\mathcal{C})$
$\widehat{b}\widehat{C_2}$	$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2}}}$	1	$4p_1^{m_1}p_2^{m_2}$
$(1-\widehat{b})\widehat{C_2}$	$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2}}}$	1	$4p_1^{m_1}p_2^{m_2}$
$\widehat{b}(1-\widehat{C_2})$	$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2}}}$	1	$4p_1^{m_1}p_2^{m_2}$
$(1-\widehat{b})(1-\widehat{C_2})$	$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2}}}$	1	$4p_1^{m_1}p_2^{m_2}$
$\widehat{C_2}$	$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2-j}}} - \widehat{C_{p_2^{m_2-j+1}}}$	$2\phi(p_2^j)$	$4p_1^{m_1}p_2^{m_2-j}$
$\widehat{C_2}$	$\widehat{C_{p_1^{m_1-i}}} - \widehat{C_{p_1^{m_1-i+1}}}$	$\widehat{C_{p_2^{m_2}}}$	$2\phi(p_1^j)$	$4p_1^{m_1-i}p_2^{m_2}$
$(1-\widehat{C_2})$	$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^{m_2-j}}} - \widehat{C_{p_2^{m_2-j+1}}}$	$2\phi(p_2^j)$	$4p_1^{m_1}p_2^{m_2-j}$
$(1-\widehat{C_2})$	$\widehat{C_{p_1^{m_1-i}}} - \widehat{C_{p_1^{m_1-i+1}}}$	$\widehat{C_{p_2^{m_2}}}$	$2\phi(p_1^j)$	$4p_1^{m_1-i}p_2^{m_2}$
$\widehat{C_2}$	$\widehat{C_{p_1^{m_1-i}}} - \widehat{C_{p_1^{m_1-i+1}}}$	$\widehat{C_{p_2^{m_2-j}}} - \widehat{C_{p_2^{m_2-j+1}}}$	$2\phi(p_1^j)2\phi(p_2^j)$	$8p_1^{m_1-i}p_2^{m_2-j}$
$(1-\widehat{C_2})$	$\widehat{C_{p_1^{m_1-i}}} - \widehat{C_{p_1^{m_1-i+1}}}$	$\widehat{C_{p_2^{m_2-j}}} - \widehat{C_{p_2^{m_2-j+1}}}$	$2\phi(p_1^j)2\phi(p_2^j)$	$8p_1^{m_1-i}p_2^{m_2-j}$

Similar results were obtained by Dutra [23, Capítulos 4 e 5] for group codes over the quaternion groups.

6.2 Metacyclic Codes and Equivalence Questions

A group G is **metacyclic** if it contains a normal cyclic subgroup H such that G/H is also cyclic. It is easy to prove that a finite metacyclic group has the following presentation

$$G = \left\langle a,\, b \,|\, a^m = 1,\, b^n = a^s,\, bab^{-1} = a^i \right\rangle, \tag{17}$$

with a and b such that $H = \langle a \rangle$ and $G/H = \langle bH \rangle$, for $m, n \in \mathbb{N}$ and $1 \leq s, i \leq m$ such that $s|m$, $m|s(i-1)$, $i < m$, $\gcd(i,m) = 1$. For $s = m$, we say that G is a **split metacyclic group** and, in this case, G is the semi-direct product $G = \langle a \rangle \rtimes \langle b \rangle$.

Earlier approaches on non-abelian metacyclic codes include results obtained by Sabin [62] and Sabin and Lomonaco [63], where we also find the following definition of equivalence of codes.

Definition 6.7. *Let G and H be two finite groups of the same order and $\mathbb{F}_q$ a field. A* **combinatorial equivalence** *is a vector space isomorphism $\psi : \mathbb{F}_q G \longrightarrow \mathbb{F}_q H$ induced by a bijection $\psi : G \longrightarrow H$.*

Two codes $C \subset \mathbb{F}_q G$ and $\tilde{C} \subset \mathbb{F}_q H$ are said to be **combinatorially equivalent** *if there exists a combinatorial equivalence $\psi : \mathbb{F}_q G \longrightarrow \mathbb{F}_q H$ such that $\psi(C) = \tilde{C}$.*

For G a metacyclic finite group such that $\gcd(q, |G|) = 1$, Sabin and Lomonaco [63], by using group representation theory, proved that codes generated by central idempotents in $\mathbb{F}_q G$ are combinatorially equivalent to abelian codes. This motivated the search for left minimal codes in $\mathbb{F}_q G$.

Considering the group algebra of a non-abelian split metacyclic group G over a finite field $\mathbb{F}_q$, Assuena [3] in his Ph.D. thesis, found a necessary condition under which $\mathbb{F}_q G$ has the minimum number of simple components.

Theorem 6.8. [3, Teorema 2.1.16] *Let G be a metacyclic group and $\mathbb{F}_q$ a finite field with q elements such that $\gcd(q, |G|) = 1$. If the number of simple components of the group algebra $\mathbb{F}_q G$ is minimal, then $U(\mathbb{Z}_n) = \langle \bar{q} \rangle$ and $U(\mathbb{Z}_m) = \langle \bar{i} \rangle \langle \bar{q} \rangle$.*

In his thesis, Assuena used the structure of the group to determine the minimal metacyclic codes for a non abelian split metacyclic group of order $p^m \ell^n$, with p and ℓ odd prime numbers, under the conditions that $\mathbb{F}_q G$ is semisimple and the number of simple components of $\mathbb{F}_q G$ is minimum.

For D_{p^m}, the dihedral group of order $2p^m$, and $\mathbb{F}_q$ a finite field such that $\gcd(q, 2p^m) = 1$, he constructs left minimal codes that **are not** combinatorially equivalent to abelian codes and also exhibits one case where a left minimal code is more efficient then the abelian ones of the same length, giving a positive answer to a conjecture of Sabin and Lomonaco [63].

Further studies on group codes are given in [11], where it is defined a **(left) G-code** as any linear (left) code of length n over a field $\mathbb{F}_q$ which is the image of a (left) ideal of a group algebra via an isomorphism $\mathbb{F}_q G \longrightarrow \mathbb{F}_q^n$ which maps the finite group G of order n to the standard basis of $\mathbb{F}_q^n$. Their ideas are used in [64] to study two-sided and abelian group ring codes and in [30], where García Pillado et al. first communicated an example of a non-abelian S_4-code over $\mathbb{F}_5$. The full proof of this computacional construction was given later in [31]. New examples of non-abelian G-codes are given in [32] and, particularly, using the group $SL(2; \mathbb{F}_3)$ instead of the symmetric group, they prove, without using a computer for it, that there is a code over $\mathbb{F}_2$ of length 24, dimension 6 and minimal weight 10. This code has greater minimum distance than any abelian group code having the same length and dimension over $\mathbb{F}_2$, and, moreover, it has the greatest minimum weight among all binary linear codes with the same length and dimension.

In [24] Elia and García Pillado give an overview of the properties of ideal group codes defined as principal ideals in the group algebra of a finite group

G over a finite field $\mathbb{F}_q$ and present their encoding and syndrome decoding. They also describe in detail a correction of a single error, using syndromes.

7 Codes over rings

In the 1990's many papers on cyclic codes over rings started to appear, motivated by the fact that good non linear binary codes were related to linear codes over $\mathbb{Z}_4$ (see, for example, [17, 38, 55]). The paper [36] by Hammons et al. was even the best paper award for Information Theory of the IEEE-IT Society in the 1996 Symposium of IT - Whistler (Canadá). Wood [77] addressed the problem of duality for modules over finite chain rings and applied it to equivalence of codes and to the extension theorem of MacWilliams.

In [14] Carlderbank e Sloane determine the structure of cyclic codes over $\mathbb{Z}_{p^m}$. Later on, in [38] Kanwar and López-Permouth did the same, but with different proofs. With the same techniques, Wan [74] extended the results from [38] to cyclic codes over Galois rings. Em 1999, Norton and Sălăgean-Mandache in [53] extended results of [14, 38] to cyclic codes over finite chain rings and later on, in 2004, Dinh and López-Permouth in [19] prove the same results in a different way.

Codes over rings developed even more in the beginning of the 21st century that they deserved a CIMPA Summer School in 2008 [72]. Further works can be found in [18], [42], [48]. A small survey on the subject is [33].

In his thesis [69, 70], Silva used group ring approach to characterize cyclic codes over chain rings, their duals and some conditions on self-dual codes, simplifying the proofs and improving results given in [19].

Let R be a finite commutative chain ring with unity such that $\mid R \mid = q^k$, for a prime q. For M the maximal ideal of R, the quotient $\overline{R} = \frac{R}{M}$ is a field and we work under the hypotesis that $q \nmid \mid G \mid$, for a finite cyclic group G. Under these conditions, the group ring RG is a principal ideal ring, as Silva proves in [69, Teorema 2.1.9], after characterizing all the ideals in RG. The following general fact is a basis for all this work.

Theorem 7.1. [69, Teorema 2.1.2] *Let R be a local ring, with maximal ideal $M =< a >$ and $\mid R \mid = q^k$, and G a cyclic group of order n such that $q \nmid n$. If $\{\overline{e}_0, ..., \overline{e}_m\}$ is a full set of primitive orthogonal idempotents in $\overline{R}G$, then $\{e_0, ..., e_m\}$ is a full set of primitive orthogonal idempotents in RG.*

The next theorem characterizes all cyclic codes of length n over the local ring RGe_i (see [69, Corollary 11.31]), for R a chain ring and e_i a primitive orthogonal idempotent, translating results of [19] to the group ring setting. To simplify the notation we write $(RG)a^j e_i$ as $\langle a^j e_i \rangle$.

Theorem 7.2. [69, Teorema 2.1.3] *Let R be a commutative finite chain ring with unity, $\mid R \mid = q^k$, $M = \langle a \rangle$ the maximal ideal of R and t the nilpotency index o índice de nilpotência of a in R. Let $G = C_n$ such that $q \nmid n$. If I is an ideal of RGe_i, then I is of the form $I = \left\langle a^{k_i} e_i \right\rangle$, with $0 \leq k_i \leq t$.*

Corollary 7.3. [69, Corollary 2.1.4] *Under the same hypothesis of Theorem 7.2, the ideal RGe_i is indecomposable in RG and the code $\langle a^{t-1} e_i \rangle$ is minimal.*

From this we have a characterization of all cyclic codes of length n over chain rings.

Theorem 7.4. *Let R be a commutative finite chain ring with unity, $\mid R \mid = q^k$, $M = \langle a \rangle$ the maximal ideal of R and t the nilpotency index of a in R. Let $G = \langle g_0 \,/\, g_0^n = 1 \rangle$ be such that $q \nmid n$ and $\{e_0, ..., e_m\}$ be a full set of primitive orthogonal idempotents of RG. Then:*

(i) [69, Teorema 2.1.5] *If I is an ideal of RG, then I is of the form $I = I_0 \oplus ... \oplus I_m$, with $I_i = \left\langle a^{k_i} e_i \right\rangle$, for $0 \leq k_i \leq t$.*

(ii) [69, Teorema 2.1.8] *The number of such codes of length n over R is $(t+1)^{m+1}$.*

One important data in a code is its number of words. Next theorem gives this number for cyclic codes over finite chain rings. We have

$$RG = RGe_0 \oplus ... \oplus RGe_m \simeq \frac{R[x]}{\langle x^n - 1 \rangle} \simeq \frac{R[x]}{\langle f_0 \rangle} \oplus ... \oplus \frac{R[x]}{\langle f_m \rangle},$$

where f_i are irreducible factors of $x^n - 1$ and , after reordering the indexes if necessary, we have $RGe_i \simeq \frac{R[x]}{\langle f_i \rangle}$. Hence, $\mid RGe_i \mid = \mid R \mid^{w_i}$, for $w_i = deg(f_i)$.

Theorem 7.5. [69, Teorema 2.1.7] *Under the same hypothesis of Theorem 7.2, let C be a cyclic code of the form $C = \left\langle a^{k_{i_1}} e_{i_1} \right\rangle \oplus ... \oplus \left\langle a^{k_{i_r}} e_{i_r} \right\rangle$ in RG. The the number of words in C is $\mid C \mid = \mid \overline{R} \mid^{\sum_{s=1}^{r} (t - k_{i_s}) w_{i_s}}$.*

Considering $* : RG \longrightarrow RG$ the classical involution, Silva also gives a description of the dual cyclic codes in RG as follows.

Theorem 7.6. [69, Teorema 2.2.3] *Under the same hypothesis of Theorem 7.4, the dual code of a cyclic code* $C = \langle a^{k_0} e_0 \rangle \oplus ... \oplus \langle a^{k_m} e_m \rangle$, *with* $0 \leq k_i \leq t$, *is* $C^{\perp} = \oplus \sum_{r=0}^{m} \langle a^{t-k_r} {e_r}^* \rangle$.

As in [19], Silva in [69, Section 2.2] states the conditions for the ring R under which the group ring RG admits self-dual codes.

Chapter 3 of [69] is dedicated to codes over chain rings of length p^n, for a prime p, extending the results of Ferraz and Milies [28] and of Melo [49] to this context. Silva also proves in [69, Teorema 3.0.14] some facts about the size of such codes and computes minimum weight of these codes [69, Teoremas 3.0.15 to 3.0.18], similarly to Theorem 5.14. He also discusses about free codes in RG in [69, Section 3.1] and about MDS codes of length p^n over R in [69, Section 3.2]. Finally, in [69, Chapter 4], Silva proves all such results for cyclic codes of length $2p^n$ over finite chain rings.

There are also interesting discussion on equivalence of linear codes over rings in [20, 21, 76, 78].

References

[1] S.K. Arora, M. Pruthi, *Minimal codes of prime power length*. Finite Fields and their Applications **3** (1997) 99-113.

[2] S.K. Arora, M. Pruthi, *Minimal cyclic codes of length* $2p^n$. Finite Fields and their Applications **5** (1999) 177-187.

[3] S. Assuena, *Códigos Metacíclicos*. Tese de Doutorado, Instituto de Matemática e Estatística da Universidade de São Paulo, 2013.

[4] G.K. Bakshi and M. Raka, *Minimal cyclic codes of length* 2^n. Ranchi University Math. Journal **33** (2002) 1-18.

[5] G.K. Bakshi and M. Raka, *Minimal cyclic codes of length* $p^n q$. Finite Fields and their Applications **9** (2003) 432-448.

[6] G.K. Bakshi, M. Raka and A.Sharma, *Idempotent generators of Irreducible Cyclic Codes*. Number Theory and Discrete Geometry, RMS Lecture Notes Series **6** (2008), 13-18.

[7] G.T. Bastos, M. Guerreiro, *Comparação de técnicas para o cálculo de idempotentes geradores de códigos cíclicos*. Atas do CNMAC 2014 (to appear).

[8] G.T. Bastos, M. Guerreiro, *Idempotents generators for minimal cyclic codes of length $p^n q$*. Proceedings of the 4th International Castle Meeting on Coding Theory and Applications, Palmela, Portugal, September 2014 (to appear).

[9] S.D. Berman, *Semisimple cyclic and abelian codes, II*. Kybernetika **3** (1967) 21-30.

[10] S. D. Berman, *On the theory of group codes*. Kibernetika, **3** (1967) 31-39.

[11] J.J. Bernal, A. del Rio, J.J. Simón, *An intrinsical description of group codes*. Designs, Codes and Cryptography **51** (3) (2009) 289-300.

[12] E. Biglieri and M. Elia, *On the construction of group block codes*. Annales des Télécommunications, **50** Issue 9-10 (1995) 817-823.

[13] O. Broche and A. del Rio, *Wedderburn decomposition of finite group algebras*. Finite Fields and their Applications **13** (2007) 71-79.

[14] A. R. Calderbank and N. J. A. Sloane, *Modular and p-adic codes*. Designs, Codes and Cryptography **6** (1995) 21-35.

[15] G. Chalom, R. Ferraz, M. Guerreiro and C. Polcino Milies, *Minimal binary abelian codes of length $p^n q^n$*. Preprint in arxiv:1205.5699v1 [cs.IT] 2012.

[16] G. Chalom, R.A. Ferraz and C. Polcino Milies, *Essencial idempotents in group algebras and minimal cyclic codes*. Preprint.

[17] J. H. Conway and N. J. A. Sloane, *Self-dual codes over the integers modulo 4*. J. Combinatorial Theory Series A, **62** (1993) 30-45.

[18] H. Q. Dinh, *Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$*. IEEE Transactions on Information Theory **53** (2007) 147-161.

[19] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*. IEEE Transactions on Information Theory, **50** (2004) 1728-1744.

[20] H. Q. Dinh and S. R. López-Permouth, *On the equivalence of codes over finite rings*. AAECC **15** (2004) No. 1 37-50.

[21] H. Q. Dinh and S. R. López-Permouth, *On the equivalence of codes over rings and modules*. Finite Fields and their Applications **10** (2004) No. 4 615-625.

[22] V. Drensky and P. Lakatos, *Monomial ideals, group algebras and error-correcting codes*. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science **357** (1989) 181-188.

[23] F.S. Dutra, *Sobre códigos diedrais e quatérnios*. Tese de Doutorado, Universidade Federal de Minas Gerais, 2006.

[24] M. Elia and C. García Pillado, *Ideal Group codes and their Syndrome Decoding*. Proceedings of the 21st International Symposium on Mathematical Theory of Networks and Systems, Groningen, The Netherlands, July 2014.

[25] R.A. Ferraz, F.S. Dutra and C.Polcino Milies, *Semisimple group codes and dihedral codes*. Algebra and Discrete Mathematics **3** (2009) 28-48.

[26] R.A. Ferraz, M. Guerreiro and C. Polcino Milies, *Minimal codes in binary abelian group algebras*. Information Theory Workshop (ITW) IEEE (2011) 225-228.

[27] R.A. Ferraz, M. Guerreiro, C. Polcino Milies, *G-equivalence in group algebras and minimal abelian codes*. IEEE Transactions on Information Theory **60** (1) (2014) 252-260.

[28] R.A. Ferraz and C. Polcino Milies, *Idempotents in group algebras and minimal abelian codes*. Finite Fields and their Applications **13** (2007) 382-393.

[29] G.D. Forney and M. Trott, *The dynamics of group codes : state spaces, trellis diagrams and canonical encoders*. IEEE Trans. Inform. Theory **39** (1993) 1491-1593.

[30] C. García Pillado, S. González, V. T. Markov, C. Martínez and A. A. Nechaev, *When are all group codes of a noncommutative group abelian (a computational approach)?*. Journal of Mathematical Sciences **186** No. 4 (2012) 578-585.

[31] C. García Pillado, S. González, V. T. Markov, C. Martínez and A. A. Nechaev, *Group codes over non-abelian groups*. Journal of Algebra and its Applications **12** No. 7 (2013) 20 pages.

[32] C. García Pillado, S. González, V. T. Markov, C. Martínez and A. A. Nechaev, *New examples of non-abelian group codes*. Proceedings of the 4th International Castle Meeting on Coding Theory and Applications, Palmela, Portugal, September 2014 (to appear).

[33] M. Greferath, *An introduction to ring-linear coding theory.*In: Ed. M. Sala et al. *Gröbner Bases, Coging and Cryptography*, Springer-Verlag, Berlin Heidelberg, 2009.

[34] E.G. Goodaire, E. Jespers and C. Polcino Milies, *Alternative Loop Rings*. North-Holland Mathematics Studies **184**, Amsterdam, Holland: Elsevier, 1996.

[35] R. W. Hamming, *Error detecting and error correcting codes*. The Bell System Technical Journal, **26** (1950) 147-160.

[36] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*. IEEE Transactions on Information Theory **40** (1994) 301-319.

[37] E. Jespers, G. Leal and A. Paques, *Central idempotents in the rational group algebra of a finite nilpotent group*. Journal of Algebra and its Applications **2** No. 1 (2003) 57-62.

[38] P. Kanwar, S.R. López-Permouth, *Cyclic codes over the integers modulo p^m*. Finite Fields and its Applications **3** (1997) 334-352.

[39] A.V. Kelarev, *Ring constructions and applications*. River Edge-NJ, World Scientific, 2002.

[40] A.V. Kelarev and P. Solé, *Error-correcting codes as ideals in group rings*. Contemporary Math., **273** (2001), 11-18.

[41] P. Kumar, S.K. Arora, *λ-mapping and primitive idempotents in semisimple rings R_m*. Communications in Algebra **41** (10) (2013) 3679-3694.

[42] Z. H. Liu, *Notes on linear codes over finite chain rings*. Acta Mathematicae Applicatae Sinica, **27** (2011) 141-148.

[43] V.O. J. Luchetta, *Códigos cíclicos como ideais em álgebras de grupo*. Dissertação de Mestrado, Instituto de Matemática e Estatística da Universidade de São Paulo, 2005.

[44] B.R. McDonald, *Finite Rings with Identity*. Pure and Applied Mathematics **28** Marcel Dekker Inc., New York, 1974.

[45] F.J. MacWilliams, *Codes and ideals in group algebra*. Combinatorial Mathematics and its Applications, University of North Carolina Press, 1969.

[46] F.J. MacWilliams, *Binary codes which are ideals in the group algebra of an abelian group*. Bell System Tech. Journal **44** (1970) 987-1011.

[47] P.A. Martin, *Grupos, Corpos e Teoria de Galois*. Editora Livraria da Física, São Paulo, 2010.

[48] E. Martínez-Moro and I. F. Rúa, *On repeated-root multivariable codes over a finite chain ring*. Des. Codes Cryptogr. **45** (2007) 219-227.

[49] F.D. de Melo, *Sobre códigos cíclicos e abelianos*. Tese de Doutorado, Instituto de Matemática e Estatística da Universidade de São Paulo, 2012.

[50] F.D. de Melo and C. Polcino Milies, *On Cyclic and Abelian Codes*. IEEE Transactions on Information Theory **59** (11) (2013) 7314-7319.

[51] R.L. Miller, *Minimal codes in abelian group algebras*. Journal of Combinatorial Theory, Series A **26** (1979) 166-178.

[52] R. Nascimento, *Códigos de peso constante*. Tese de Doutorado, Instituto de Matemática e Estatística da Universidade de São Paulo, 2014.

[53] G. Norton and A. Sălăgean-Mandache, *On the structure of linear cyclic codes over finite chain rings*. Appl. Algebra Eng. Commun. Comput. **10** (2000) 489-506.

[54] A. Olivieri, A. del Río and J.J. Simón, *On monomial characters and central idempotents of rational group algebras*. Comm. Algebra **32** (4) (2004) 1531-1550.

[55] V. Pless, Z. Qian, *Cyclic codes and quadratic residue codes over* $\mathbb{Z}_4$. IEEE Transactions on Information Theory **42** (1996) 1594-1600.

[56] C. Polcino Milies and S.K. Sehgal, *An Introduction to Group Rings*. Kluwer Academic Publishers, Dordrecht, 2002.

[57] A. Poli, *Ideaux principaux nilpotents de dimension maximale dans l´algebre* $\mathbb{F}_q[X]$ *d´um groupe abelien fini* G. Communications in Algebra, **12** (4) (1984) 391-401.

[58] A. Poli, *Important algebraic calculations for n-variables polynomial codes*. Discrete Mathematics **56** (1985) 255-263.

[59] J. do Prado, *Idempotentes geradores de códigos minimais*. Tese de Doutorado, Instituto de Matemática e Estatística da Universidade de São Paulo, 2010.

[60] M. Pruthi, *Cyclic codes of length* 2^m. Proc. Indian Acad. Sci. (Math. Sci.) **111** (2001) 371-379.

[61] J.J. Rotman, *An Introduction to the Theory of Groups*, 4th Ed., Springer-Verlag, New York, 1995.

[62] R.E. Sabin, *On row-cyclic codes with algebraic structure*. Designs, Codes and Cryptography **4** (1994) 145-155.

[63] R.E. Sabin and S.J. Lomonaco, *Metacyclic Error-Correcting Codes*. AAECC **6** (1995) 191-210.

[64] A. Schäfer, *Two-sided and abelian group ring codes*. Master of Science Thesis, Aachen University, Germany, 2012.

[65] C. Shannon, *A Mathematical Theory of Communication*, The Bell System Technical Journal, bf 27 (1948) 379-423 July and 623-656 October.

[66] A. Sharma, G.K. Bakshi, V.C. Dumir and M. Raka, *Cyclotomic numbers and primitive idempotents in the ring* $GF(q)[x]/ < x^{p^n} - 1 >$. Finite Fields Appl. **10** (2004) 653-673.

[67] A. Sharma, G.K. Bakshi and M. Raka, *The weight distribution of irreducible cyclic codes of length* 2^m. Finite Fields and Applications **13** (2007) 1086-1095.

[68] A. Sharma, G.K. Bakshi, V.C. Dumir and M. Raka, *Irreducible cyclic codes of length* 2^n. Ars Combinatoria **86** (2008) 133-146.

[69] A.T. Silva, *Códigos cíclicos sobre anéis de cadeia*. Tese de Doutorado, Instituto de Matemática e Estatística da Universidade de São Paulo, 2012.

[70] A.T. Silva and C. Polcino Milies, *On cyclic codes over finite chain rings*. Preprint.

[71] R. Singh and M. Pruthi, *Primitive idempotents of irreducible quadratic residue cyclic codes of length* $p^n q^m$. International Journal of Algebra, **5** N.6 (2011) 285 - 294.

[72] P. Solé (Editor), *Codes over Rings*. Series on Coding Theory and Cryptology **6**. Proceedings of the CIMPA Summer School, Ankara, Turkey, 2008.

[73] G. Vega, *Determining the number of one-weight cyclic codes when length and dimension are given*. Lecture Notes in Computer Science **4547** (2007) 284-293.

[74] Z. Wan, *Cyclic codes over Galois rings*. Alg. Colloquium **6** (1999) 291-304.

[75] H.N. Ward, *Visible codes*. Archiv der Mathematik **54** Issue 3 (1990) 307-312.

[76] H.N. Ward and J.A. Wood, *Characters and the equivalence of codes*. J. Comb. Theory Series A **73** (1996) No. 2 348-352.

[77] J.A. Wood, *Duality for modules over finite rings and applications to coding theory*. American Journal of Mathematics **121** (1999) 555-575.

[78] J.A. Wood *Code equivalence characterizes finite Frobenius rings*. Proc. Amer. Math. Soc. **136** (2008) 699-706.

[79] J.A. Wood, *The structure of linear codes of constant weight*. Trans. Amer. Math. Soc. **354** (2002) No. 3 1007-1026.