Revista Integración, temas de matemáticas
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 37, N° 1, 2019, pág. 153–166

DOI: http://dx.doi.org/10.18273/revint.v37n1-2019008

Group algebras and coding theory: a short survey

César Polcino Milies*
Universidade de São Paulo, Instituto de Matemática e Estatística, R. do Matão 1010, Brazil.

Abstract. We study codes constructed from ideals in group algebras and we are particularly interested in their dimensions and weights. First we introduced a special kind of idempotents and study the ideals they generate. We use this information to show that there exist abelian non-cyclic groups that give codes which are more convenient than the cyclic ones. Finally, we discuss briefly some facts about non-abelian codes.
Keywords: code, Hamming distance, weight, group algebra, ideal, group code.
MSC2010: 16S34, 20C05, 94B15.

Álgebras de grupo y teoría de códigos: una breve reseña

Resumen. Estudiamos códigos construidos a partir de ideales de álgebras de grupo y estamos particularmente interesados en sus dimensiones y pesos. Introducimos inicialmente un tipo especial de idempotentes y estudiamos los ideales que generan. Usamos esta información para mostrar que existen grupos abelianos no cíclicos que son más convenientes que los cíclicos. Finalmente, discutimos brevemente algunos resultados sobre códigos no abelianos.
Palabras clave: códigos, distancia de Hamming, peso, álgebra de grupo, ideal, código de grupo.

1. Introduction

Group algebras play a very large role in the theory of error-correcting codes. In this very short survey we cover only one aspect of this role: we focus on the relationship between weight and dimension of group codes. This type of codes have recently been the object of active research (see [2], [6], [7], [8], [9], [10], [11], [12], [13], [19], [20], [24], [27]).

We start from the most basic definitions to render the paper accessible to the general mathematical reader. It should be noted that some important concepts of the theory, such as encoding and decoding, are not treated here since they are of no direct interest to our objectives

* E-mail: polcinomilies@gmail.com
Received: 21 December 2018, Accepted: 15 January 2019.
To cite this article: C. Polcino Milies, Group algebras and coding theory: a short survey, *Rev. Integr. temas mat.* 37 (2019), No. 1, 153–166. doi: 10.18273/revint.v37n1-2019008.

2. A brief history

Already at the early days of computing, a method was devised to prevent a computer from working with wrong data.

Each "word" of information sent to the computer was composed of a series of digits equal to either 0 or 1 (or **bits**, as they are called in this context). One such word could be, for example 10011001. Then, an extra digit was added at the end of each word, called the *parity-check digit* which would be equal to 0 or 1 depending on whether the number of bits equal to 1 in the given word were even or odd, In the case of our example, the parity check would be 0 and the extended word would be 100110010.

In this way, every extended word sent to the computer would now have nine digits and an even number of bits equal to 1.

On receiving each word, the computer would check the number of digits equal to 1, and in case this number were odd it would know that there was a mistake in this word and stop the task.

Of course this method has some inconveniences. First, if *two* mistakes were committed the error would not be detected. Also, even if the existence of a mistake is detected, it is not possible to determine which is the wrong bit in the word.

This was the method used in 1947 at the *Bell Telephone Laboratories*, where the engineer **Richard W. Hammming** worked. In those days computers were much slower than nowadays and their time was disputed among the users of the machine. Hamming's priority was rather low, so he had to submit his "jobs" to stand in a queue over the weekend to be processed when possible. The computer would work on each job and if an error was detected it, would just stop and proceed to the next job.

In an interview [18], Hamming recalls how the idea of error correcting codes came to him:

> Two weekends in a row I came and found that all my stuff had been dumped and nothing was done. I was really aroused and annoyed and I wanted those answers and two weekends had been lost. And so I said, "Damn it, if the machine can detect an error, why can't it locate the position of the error and correct it?" [1]

He started to work on this question and his idea was to add to each word not just one parity-check digit but more digits that he called *redundancy* which would allow to locate the error and hence correct it. Still in 1947, in an internal memorandum of the *Bell Telephone Company* he developed a code in which the information to be transmitted was composed of words of four bits and contained another four bits of redundancy.

Let $a_1a_2a_3a_4$ be a word to be transmitted. First, write it as a matrix of size 2×2 :

$$\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$$

[1] Quoted in T. Thompson, [30, p.17], where the reader can find more information on this story.

Then extend it to a matrix of size 3×3 (but without the entry corresponding to position $3, 3$) in such a way that each row and each column has an even number of digits equal to 1:

$$\begin{bmatrix} a_1 & a_2 & b_1 \\ a_3 & a_4 & b_2 \\ c_1 & c_2 & \end{bmatrix}$$

Then the matrix can be written as a 'word' taking it by rows:

$$a_1, a_2, b_1, a_3, a_4, b_2, c_1, c_2.$$

For example, if the initial word is 1101 we dispose it as

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

and extend it to the matrix

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & \end{bmatrix}.$$

Then, the word to be sent to the computer would be 11001110. The computer would then reproduce the 3×3 matrix, check parity of rows and columns and it is an easy exercise to verify that if one error is committed, then it is possible to detect the existence of the error and also its position, so it can be corrected.

In this same memorandum, Hamming asks if it would be possible to correct an error in a word containing four original digits of information, using only three digits of redundancy. His results could not be published in a journal for a general audience because the company applied for the corresponding patents and Hamming had to wait for the end of this process, until 1950 [17].

A positive answer to Hamming's question appeared in a paper by his colleague at the company **Claude Shannon** [29] in 1948. This long work by Shannon is considered today as a paper giving birth to *two* mathematical theories: the Theory of Error-Correcting Codes and Mathematical Information Theory.

Shortly afterwords, **Marcel Golay**, inspired by the work of Shannon, published a paper, one page long, in which he gives two of the most used codes in use to this day. E.R. Berlekamp [3, p. 4] described this paper as the "best page ever published" in Coding Theory.

3. Basic facts

A code is essentially a language devised to communicate with a machine or for communication among machines.

The fundamental elements to produce a code are:

- A finite set $\mathcal{A}$ which we call an **alphabet**; its elements are frequently called **letters**. We denote by $q = |\mathcal{A}|$ the number of elements in $\mathcal{A}$ and say that the code is q**-ary**.

- Finite sequences of elements of $\mathcal{A}$ are called **words**. The number of letters in a word is called its **length**. We shall assume that all the words in the codes considered here have the same length.

A q**-ary code** $\mathcal{C}$ **of length** n is then a set (of our choice) of words of length n; i.e., a code $\mathcal{C}$ is a subset of

$$\mathcal{A}^n = \underbrace{\mathcal{A} \times \mathcal{A} \times \cdots \times \mathcal{A}}_{n \text{ times}}.$$

This set is sometimes called the **ambient space** $\mathcal{F}_q^n$ of the code.

Definition 3.1. Given two words $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in a code $\mathcal{C} \subset \mathcal{A}^n$, the **Hamming distance** from x to y is the number of coordinates in which these elements differ; i.e.:

$$d(x, y) = |\ \{i, 1 \leq i \leq n \mid x_i \neq y_i\}\ |$$

Given a code $\mathcal{C} \subset \mathcal{A}^n$ the **minimal distance** of $\mathcal{C}$ is the number

$$d = min\{d(x, y) \mid x, y \in \mathcal{C}, x \neq y\ \}.$$

For a rational number α we denote by $\lfloor \alpha \rfloor$ the greatest integer m such that $m \leq \alpha$. The first important result in coding theory is the following.

Theorem 3.2. *Let $\mathcal{C}$ be a code with minimal distance d and set*

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Then, it is possible to detect up to $d-1$ errors and correct up to κ errors.

The number κ above is called the **error-correcting capacity** of the code. A q-ary code of length n containing M words and having minimal distance d is called an (n, M, d)-**code**.

A natural goal, when designing a code is to look for efficiency (in the sense that it contains a large number of words, so it can transmit enough information) and also a large minimum distance, so that it can correct a big number of errors.

Unfortunately, these goals conflict with each other, since the ambient space $\mathcal{A}^n$ is finite. The problem of maximizing one of the parameters (n, M, d) when the other two are given is known as the **main problem of Coding Theory**.

A most important class of codes are the so-called **linear codes** which are constructed as follows.

We take, as an alphabet, a finite field $\mathcal{F}_q$ with q elements (where q is now a power of a prime $p = char(\mathcal{F}_q)$). The ambient space $\mathcal{F}_q^n$ is then a vector space of dimension n over $\mathcal{F}_q$.

A **linear code** $\mathcal{C}$ of length n over $\mathcal{F}_q$ is a proper *linear subspace* of $\mathcal{F}_q$. If $dim(\mathcal{C}) = m$, then $m < n$.

It is easy to see that, in this case, the number of words in $\mathcal{C}$ is q^m, so we refer to one such code, for briefness, as an (n, m, d)-code.

A special class of linear codes was introduced in 1957 by **E. Prange** [25]. Originally these codes were introduced because they allowed for efficient implementation, but they also have a rich algebraic structure and can be used in many different ways. Many practical codes actually in use are of this kind.

Given a word $(x_1, x_2, \dots x_{n-1}, x_n) \in \mathcal{F}_q^n$, its *right shift* is the word $(x_n, x_1, \dots x_{n-1})$. A linear code $\mathcal{C}$ is **cyclic** if, for every word in the code its right shift is also in the code; i.e., if

$$(x_1, x_2, \dots x_{n-1}, x_n) \in \mathcal{C} \Rightarrow (x_n, x_1, \dots x_{n-1}) \in \mathcal{C}.$$

Notice that this implies that if a given word $(x_1, x_2, \dots x_{n-1}, x_n)$ is in the code, then *all* its circular permutations are in the code.

The map $\varphi : \mathcal{F}_q^n \to \mathcal{F}_q[X]/\langle X^n - 1\rangle$ given by

$$\varphi((a_0, a_1, \dots, a_{n-2}, a_{n-1})) = [a_0 + a_1X + \dots + a_{n-2}X^{n-2} + a_{n-1}X^{n-1}],$$

where $[f]$ denotes the class of the polynomial $f \in \mathbb{F}_q[X]$ in $\mathcal{R}_n$, is a linear isomorphism, and it is easy to see that a linear subspace $\mathcal{C}$ in $\mathcal{F}_q^n$ is a cyclic code if and only if $\varphi(\mathcal{C})$ is an ideal of $\mathcal{F}_q[X]/\langle X^n - 1\rangle$. Hence, the study of cyclic codes of length n over $\mathcal{F}_q^n$ is the same as the study of ideals in the quotient ring $\mathcal{F}_q[X]/\langle X^n - 1\rangle$.

On the other hand, if C_n denotes the cyclic group of order n and $\mathcal{F}_qC_n$ its group algebra over $\mathcal{F}_q$, it is well-known that

$$\mathcal{F}_q[X]/\langle X^n - 1\rangle \cong \mathcal{F}_qC_n.$$

Hence, the study of cyclic codes of length n over the field $\mathcal{F}_q$ can also be regarded as the study of ideals in the group ring $\mathcal{F}_qC_n$.

4. Group Codes

The concept of codes as ideals in group algebras of cyclic groups can be extended naturally to other classes of groups. This was first done in 1967 by S.D. Berman ([4], [5]) and independently by F.J. MacWilliams [21] in 1970.

Recall that the group algebra of a finite group G over a field R is the set of all formal linear combinations:

$$\alpha = \sum_{g\in G} \alpha_g g, \quad \text{where} \quad \alpha_g \in R, \text{for all} \quad g \in G.$$

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

$$\alpha = \beta \iff \alpha_g = \beta_g, \quad \forall g \in G.$$

We define:

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

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

For λ in R we define

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

The set RG, with the operations above, is called the **group algebra** of G over R.

The elements of the group G form a basis of the group algebra RG over R. So if we enumerate them in any given order $G=\{g_1,g_2,\ldots,g_n\}$, we can think of a word $(x_1,x_2,\ldots,x_n)$ in a space $\mathcal{F}_q^n$ as corresponding to the element $\alpha=x_1g_1+x_2g_2+\cdots+x_ng_n$.

With this correspondence in mind, we define:

Let G be a finite group and $\mathcal{F}_q$ a finite field. A **group code** or, more precisely, a G-**code** over $\mathcal{F}_q$ is an ideal of the group algebra $\mathcal{F}_qG$.

We recall that the *support* of an element $\alpha=\sum_{g\in G}\alpha_g g$ in the group $\mathbb{F}_qG$ of a group G over a field $\mathbb{F}_q$ is the set

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

The *Hamming distance* between two elements $\alpha=\sum_{g\in A}\alpha_g g,\ \beta=\sum_{g\in A}\beta_g g$ in $\mathbb{F}_qG$ is

$$d(\alpha,\beta)\ =\ |\{g\mid \alpha_g\neq\beta_g, g\in A\}|,$$

and the *weight* of an element α is $w(\alpha)=d(\alpha,0)=|supp(\alpha)|$; then,

$$\omega(\alpha)=|\{g\in G\mid \alpha_g\neq 0\}|.$$

Notice that, for linear codes, it is easy to see that the minimum distance of a code coincides with its minimum weight.

Given an ideal $I\subset\mathbb{F}_qG$, the *weight distribution* of I is the map which assigns, to each possible weight t, the number of elements of I having weight t.

It is well-known that, due to Maschke's Theorem (see [23, Corollary 3.2.8]), the structure of the group algebra $\mathcal{F}_qG$ changes dramatically, depending on weather q and $|G|$ are, or not, relatively prime.

We shall always assume, throughout, that $gcd(q,|G|)=1$. In this case the group algebra $\mathcal{F}_qG$ is semisimple, meaning that every ideal (right, left or two-sided) is a direct summand and is thus a principal ideal, generated by an idempotent element.

Morover, it can be shown that:

(i) $\mathbb{F}_q G$ is a direct sum of a finite number of two-sided ideals $\{A_i\}_{1\leq i\leq r}$, called the **simple components** of $\mathbb{F}_q G$. Each A_i is a simple algebra.

(ii) Any two-sided ideal of $\mathbb{F}_q G$ is a direct sum of some of the members of the family $\{B_i\}_{1\leq i\leq r}$.

(iii) Each simple component A_i is isomorphic to a full matrix ring of the form $M_{n_i}(\mathcal{F}_i)$, where $\mathcal{F}_i$ is a field containing an isomorphic copy of $\mathbb{F}_q$ in its center.

Since every simple component is generated by an idempotent element, the results above can be translated as follows:

Let G be a finite group, and let $\mathbb{F}_q$ be a field such that $char(\mathbb{F}_q) \nmid |G|$; and let $\mathcal{F}G = \oplus_{i=1}^{s} A_i$ be the decomposition of the group algebra as a direct sum of minimal two-sided ideals. Then, there exists a family $\{e_1, \ldots, e_s\}$ of elements of $\mathcal{F}G$ such that:

(i) $e_i \neq 0$ is a central idempotent, $1 \leq i \leq t$.

(ii) If $i \neq j$, then $e_i e_j = 0$.

(iii) $1 = e_1 + \cdots + e_t$.

(iv) e_i cannot be written as $e_i = e_i' + e_i''$, where e_i', e_i'' are central idempotents such that both $e_i', e_i'' \neq 0$ and $e_i' e_i'' = 0$, $1 \leq i \leq t$.

(v) $A_i = Ae_i$, $1 \leq i \leq s$.

The idempotents above are called the **primitive central idempotents** of $\mathbb{F}_q G$.

There is a rather standard way of constructing idempotents in group algebras. If H is a subgroup of G, then

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

is an idempotent of $\mathcal{F}G$, and $\widehat{H}$ is central if and only if H is normal in G.

It is well-known that [23, Proposition 3.6.7]

$$(\mathcal{F}G) \cdot \widehat{H} \cong \mathcal{F}[G/H],$$

so,

$$dim_{\mathcal{F}} \left((\mathcal{F}G) \cdot \widehat{H} \right) = [G : H].$$

Also, it is easy to see that if τ is a transversal of H in G, i.e., a complete set of representatives of cosets of H in G, then

$$\{t\widehat{H} \mid t \in \tau\}$$

is a basis of $(\mathcal{F}G) \cdot \widehat{H}$ over $\mathcal{F}$.

Unfortunately, an element in such an ideal is of the form $\alpha = \sum_{t\in\tau} a_t \widehat{H}$, which means that, when written in the basis G of $\mathcal{F}G$, it has the same coefficient along all the elements of the form th for a fixed $t \in \tau$ and any $h \in H$. Thus, this kind of ideals defines repetition codes, which are not particularly interesting.

There is another kind of idempotents that will define more significant codes.

Theorem 4.1 ([13]). *Let G be a finite group and $\mathcal{F}$ a field such that $char(\mathcal{F}) \nmid |G|$. Let H and H^* be normal subgroups of G such that $H \subset H^*$, and set $e = \widehat{H} - \widehat{H^*}$. Then,*

$$dim_F(\mathcal{F}G)e \;=\; |G/H| - |G/H^*|$$

and

$$w((\ FG)e) \;=\; 2|H|.$$

Let $\mathcal{A}$ be a transversal of H^* in G and τ a transversal of H in H^* containing 1. Then,

$$\mathcal{B} \;=\; \{a(1-t)\widehat{H} \mid a \in \mathcal{A}, t \in \tau \setminus \{1\}\}$$

is a basis of $(\mathcal{F}G)e$ over $\mathcal{F}$.

In the case when G is an abelian group, it is possible to decide when *all* primitive central idempotents can be obtained in this way.

Let A be an abelian p-group. For each subgroup H of A such that $A/H \neq \{1\}$ is cyclic, we shall construct an idempotent of $\mathcal{F}A$. Since A/H is a cyclic subgroup of order a power of p, there exists a unique subgroup H^* of A, containing H, such that $|H^*/H| = p$.

We set

$$e_H = \widehat{H} - \widehat{H^*},$$

and also

$$e_G = \frac{1}{|G|}\sum_{g\in G} g.$$

Theorem 4.2 ([13]). *Let p be an odd prime and let A be an abelian p-group of exponent p^r. Then, the set of idemponts above is the set of primitive idempotents of $\mathcal{F}_qA$ if and only if one of the following holds:*

(i) $p^r = 2$, *and q is odd.*

(ii) $p^r = 4$ *and* $q \equiv 3$ *(mod 4).*

(iii) $o(q) = \varphi(p^n)$ *in* $U(\mathbb{Z}_{p^n})$ *(where φ denotes Euler's Totient function).*

In the particular case when G is a cyclic group of order p^n, with $gcd(p, q) = 1$, the theorem above gives the following

Corollary 4.3 ([13], [26]). *Let $\mathcal{F}$ be a field with q elements and A a cyclic group of order p^n such that $o(q) = \varphi(p^n)$ in $U(\mathbb{Z}_{p^n})$. Let*

$$A \;=\; A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

be the descending chain of all subgroups of A. Then, the set of primitive idempotents of FA is given by

$$e_0 \;=\; \frac{1}{p^n}\left(\sum_{a\in A} a\right),$$

$$e_i = \widehat{A_i} - \widehat{A_{i-1}},\ 1 \leq i \leq n.$$

A similar result holds for cyclic groups of order $2p^n$ (see [1], [13]).

Since the introduction of abelian codes by Berman and MacWiliams, untill recent times there were no evidence that they would produce better codes than the cyclic ones. This was mainly due to the fact that most of the codes that were constructed were defined from minimal ideals and, as we shall see, these are not the ones that should be taken into account for this purpose.

Let G_1 and G_2 denote two finite groups of the same order, $\mathcal{F}$ a field, and let $\gamma : G_1 \to G_2$ be a bijection. Denote by $\overline{\gamma} : \mathcal{F}G_1 \to \mathcal{F}G_2$ its linear extension to the corresponding group algebras.

Clearly, $\overline{\gamma}$ is a Hamming isometry; i.e., elements corresponding under this map have the same Hamming weight. Ideals $I_1 \subset \mathcal{F}G_1$ and $I_2 \subset \mathcal{F}G_2$ such that $\overline{\gamma}(I_1) = I_2$ are thus equivalent, in the sense that they have the same dimension and the same weight distribution. In this case, the codes I_1 and I_2 are said to be *permutation equivalent* and were called *combinatorially equivalent* in [28]. We have the following

Theorem 4.4 ([7]). *Every minimal ideal in the semisimple group algebra $\mathcal{F}_qA$ of a finite abelian group A is permutation equivalent to a minimal ideal in the group algebra $\mathcal{F}_qC$ of a cyclic group C of the same order.*

However, when working with non-minimal ideals, the situation is quite different.

As mentioned in the previous section, when we stated the Main Problem of Coding Theory, we wish to build codes with a good error correcting capacity and dimension as big as possible. Since one of this numbers decreases as the other increases, to compare efficiency of codes with different weights and dimensions, it seems rather natural to make the following

Definition 4.5. For a code $\mathcal{C}$, we call **convenience** of $\mathcal{C}$ the number

$$conv(\mathcal{C}) = dim(\mathcal{C}) \cdot w(\mathcal{C}).$$

Notice that this notion makes sense if one wishes to compare codes with dimensions or weights that are somehow close. However one might have a code with a high convenience where one of the parameter is quite big and the other rather small. Certainly, this would not be a useful code.

Set $G =< a >$, with $a^{p^2} = 1$, a cyclic code of order p^2 and let $\mathcal{F}_q$ be any field as in the hypotheses of the Theorem above. Then, from the Corollary, there exist in $\mathcal{F}G$ only three principal idempotents:

$$e_0 = \widehat{G}, \;\; e_1 = \widehat{G_1} - \widehat{G} \;\; , \;\; e_2 = \widehat{G_2} - \widehat{G_1}.$$

So the maximal ideals are:

$$I = I_0 \oplus I_1 \;\text{ and }\; J = I_1 \oplus I_2,$$

with $dim(I) = p$, $w(I) = p$ and $dim(J) = p^2 - 1$, $w(J) = 2$, and thus $conv(I) = p^2$ and $conv(J) = 2(p^2 - 1)$.

On the other hand, also from the Theorem above, it can be shown that if we set $A = C_p \times C_p$, then the principal idempotents of $\mathcal{F}_q A$ are

$$e_0 = \widehat{A},\ e_1 = \widehat{a} - \widehat{A},\ e_2 = \widehat{b} - \widehat{A},$$

and

$$f_j = \widehat{ab^j} - \widehat{A},\ 1 \leq j \leq p-1,$$

where a and b denote the respective generators of both direct factors.

We have that

$$w(\mathcal{F}_q A) = p^2, \qquad dim((\mathcal{F}_q)e_0) = 1;$$

and for the other minimal ideals $\mathfrak{L}_i = (\mathcal{F}_q A)e_i$, $i = 1, 2$, $\mathfrak{M}_j = (\mathcal{F}_q A)f_j$, $1 \leq j \leq p-1$, we have:

$$\begin{aligned} w(\mathfrak{L}_i) &= 2p, \qquad dim(\mathfrak{L}_i) = p-1,\ i = 1, 2, \\ w(\mathfrak{M}_j) &= 2p, \qquad dim(\mathfrak{M}_j) = p-1,\ 1 \leq j \leq p-1. \end{aligned}$$

If $H =< h >$ and $K =< k >$ are two subgroups of order p of $C_p \times C_p$, the corresponding idempotents are $e = \widehat{H} - \widehat{A}$, $f = \widehat{K} - \widehat{A}$. Set

$$\mathfrak{N} = (\mathcal{F}A)e \oplus (\mathcal{F}A)f.$$

Then, we have the following

Proposition 4.6 ([22]). *The weight and dimension of $I = (\mathcal{F}G)e \oplus (\mathcal{F}G)f$ are*

$$w(\mathfrak{N}) = dim(\mathfrak{N}) = 2p-2,\ \textit{so } conv(\mathfrak{N}) = 4(p-1)^2.$$

Hence, if $p > 3$, we have that $conv(\mathfrak{N})$ is greater than $conv(I)$ for all proper ideal I of $\mathcal{F}_q C_{p^2}$.

5. Non Abelian groups

Codes in group algebras of non-abelian groups have been considered for quite some time. Lomonaco and Sabin [28] studied metacyclic groups and showed that central idempotents generate codes that are combinatorially equivalent to abelian codes.

More recently, C. García Pillado, S. González, C. Martínez, V. Markov, and A. Nechaev, [15] showed that this is also the case for groups G that can be written as $G = AB$, where both A and B are abelian.

Hence, one should focus on ideals generated by non-central idempotents. We offer a couple of examples in this direction taken from [2].

Example 5.1. Set $G = \langle a, b \mid a^7 = 1 = b^3, bab^{-1} = a^2 \rangle$.

It can be shown that the central primitive idempotents of $\mathcal{F}_2G$ are

$$f_1 = \widehat{b}\widehat{a}, f_2 = (1-\widehat{b})\widehat{a}, f_3 = \frac{1}{7}\left(3 + (\xi+\xi^2+\xi^4)\Gamma_a + (\xi^3+\xi^5+\xi^6)\Gamma_{a^3}\right)$$

and

$$f_4 = \frac{1}{7}\left(3 + (\xi^3+\xi^5+\xi^6)\Gamma_a + (\xi+\xi^2+\xi^4)\Gamma_{a^3}\right),$$

where ξ is a primitive 7th root of unity.

It can be shown also that

$$\mathcal{F}_2G \cong \mathcal{F}_2 \oplus \mathcal{F}_4 \oplus M_3(\mathcal{F}_2) \oplus M_3(\mathcal{F}_2).$$

Take $e_1 = 1 + \widehat{a}$, which is not a central primitive idempotent, and compute

$$\begin{aligned} f &= (\widehat{b} + \widehat{b}a(1+\widehat{b}))e_1 = (\widehat{b} + \widehat{b}a(1+\widehat{b}))(1+\widehat{a}) \\ &= 1 + b + b^2 + a + a^2b + a^4b + a + ab + ab^2 + a^2b + a^2b^2 + a^2 + a^4b^2 \\ &\quad + a^4 + a^4b + \widehat{G}. \end{aligned}$$

The weight of f is $w(f) = 12$, and it can be shown that the weight distribution of this ideal is

weight	0	8	12
words	1	21	42

This is a [21,6,8]-code, which has the same weight of the best known [21,6]-code (see [16]).

Example 5.2. Let

$$D_6 = \langle a, b \mid a^3 = 1 = b^2, bab = a^2 \rangle$$

be the dihedral group of order 6, and let $\mathcal{F}_q$ be a finite field with q elements such that $\mathcal{U}(\mathbb{Z}_3) = \langle \overline{q} \rangle$. By [11, Theorem 3.3]), the central primitive idempotents of $\mathcal{F}_qD_6$ are

$$e_{11} = \left(\frac{1+b}{2}\right)\widehat{A}, \quad e_{22} = \left(\frac{1-b}{2}\right)\widehat{A}, \quad , \quad e_1 = 1 - e_{11} - e_{22},$$

and we can write $f = e_{11} - e_{12}$ and set $I = \mathcal{F}_qD_6 \cdot f$. Since $dim[I] = 2$, the set $\{f, af\}$ is a basis over $\mathcal{F}_q$, and an element $\alpha \in \mathcal{F}_qD_6 \cdot f$ can be written as

$$\begin{aligned} \alpha = \alpha_0 f + \alpha_1 af = \frac{1}{12}[&(4\alpha_0 + \alpha_1)\,1 + (-5\alpha_0 + 4\alpha_1)\,a + (\alpha_0 - 5\alpha_1)\,a^2 \\ &+ (4\alpha_0 - 5\alpha_1)\,b + (\alpha_0 + 4\alpha_1)\,ab + (-5\alpha_0 + \alpha_1)\,a^2b]. \end{aligned}$$

If $q = 11$, a direct computation show us that $w(I) = 5$, the weight of the best known [6,2]-code according to [16]. This is also the case for any field of characteristic different from 2, 3, 5 and 7.

5.1. Idempotents and left ideals in matrix algebras

Since the building blocks of finite semisimple group algebras are matrix algebras over finite fields, it is natural to try to determine all non-central idempotents defining left ideals in this kind of rings. These can be obtained as follows.

Let $E(n,k)$ denote the set of all matrices $A = (a_{ij})$ such that there exist k rows, at positions denoted $i_1, i_2, \ldots, i_k$, verifying:

(i) Every row of A, except these, is a row of zeros.

(ii) $a_{i_j i_j} = 1$ and $a_{i_j,h} = 0$ if $h < i_j$, $1 \leq j \leq k$.

(iii) $a_{i_j,h} = 0$ for $h = i_s$, $j+1 \leq s \leq k$.

The set of numbers $i_1, i_2, \ldots, i_k$ will be called the *pivotal positions* of A.

For example, $E(4,3)$ is the set of all matrices of the form:

$$\begin{bmatrix} 1 & 0 & 0 & a_{14} \\ & 1 & 0 & a_{24} \\ & & 1 & a_{34} \\ & & & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & a_{13} & 0 \\ & 1 & a_{23} & 0 \\ & & 0 & 0 \\ & & & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & a_{12} & 0 & 0 \\ & 0 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix}$$

with $a_{ij} \in \mathcal{F}_q$.

Theorem 5.3 ([14]). *The elements of the set $E(n,k)$ are idempotent generators of the different left ideals of rank k of $M_n(\mathcal{F}_q)$. Moreover, each left ideal of rank k has $q^{(n-k)k}$ different idempotent generators.*

References

[1] Arora S.K., Pruthi M., "Minimal cyclic codes of length $2p^n$", *Finite Fields Appl.* 5 (1999), No. 2, 177–187.

[2] Assuena S. and Polcino Milies C., "Good codes from metacyclic groups", *Contemporary Math.*, to appear.

[3] Berlekamp E.R., *Key papers in the development of Coding Theory*, I.E.E.E. Press, New York, 1974.

[4] Berman S.D., "On the theory of group codes", *Kibernetika* 3 (1967), No. 1, 31–39.

[5] Berman S.D., "Semisimple cyclic and abelian codes II", *Kibernetika* 3 (1967), No. 3, 17–23.

[6] Bernhardt F., Landrock P. and Manz O., "The extended Golay codes considered as ideals", *J. Combin. Theory Ser. A* 55 (1990), No. 2, 235–246.

[7] Chalom G., Ferraz R. and Polcino Milies C., "Essential idempotents and simplex codes", *J. Algebra Comb. Discrete Struct. Appl.* 4 (2017), No. 2, 181–188.

[8] Charpin P., "The Reed-Solomon code as ideals in a modular algebra", *C.R. Acad. Sci. Paris, Ser. I. Math.* 294 (1982), 597–600.

[9] Dougherty S., Gildea J., Taylor R. and Tylyshchak A., "Group rings, G-codes and constructions of self-dual and formally self-dual codes", *Des. Codes Cryptogr.* 86 (2018), No. 9, 2115–2138.

[10] Drensky V. and Lakatos P., "Monomial ideals, group algebras and error correcting codes", in *Lect. Notes in Comput. Sci.* 257, Springer, Berlin (1989), 181–188.

[11] Dutra F.S., Ferraz R.A., Polcino Milies C., "Semisimple group codes and dihedral codes", *Algebra Discrete Math.* (2009), No. 3, 28–48.

[12] Ferraz R., Guerreiro M. and Polcino Milies C., "G-equivalence in group algebras and minimal abelian codes", *IEEE Trans. on Inform. Theory* 60 (2014), No. 1, 252–260.

[13] Ferraz R. and Polcino Milies C., "Idempotents in group algebras and minimal abelian codes", *Finite Fields Appl.* 13 (2007), No. 2, 382–393.

[14] Ferraz R., Polcino Milies C. and Taufer E., "Left ideals in matrix rings over finite fields", *preprint*, arXiv:1711.09289.

[15] García Pillado C., González S., Martínez C., Markov V. and Nechaev A., "Group codes over non-abelian groups", *J. Algebra Appl.* 12 (2013), No. 7, 20 pp.

[16] Grassl M., *Bounds on the minimum distance of linear codes and quantum codes*. Online available at http://www.codetables.de/BKLC/index.html [21 December 2018]

[17] Hamming R.W., "Error-detecting and error-correcting codes", *Bell System Tech. J.* 29 (1950), No. 2, 147–160.

[18] Hamming R.W., Interview, February 1977.

[19] Keralev A. and Solé P., "Error-correcting codes as ideals in group rings", in *Contemporary. Math.* 273, Amer. Math. Soc. (2001), 11–18.

[20] Landrock P. and Manz O., "Classical codes as ideals in group algebras", *Des. Codes Cryptogr.* 2 (1992), No. 3, 273–285.

[21] MacWilliams F.J., "Binary codes which are ideals in the group algebra of an abelian group", *Bell System Tech. J.* 49 (1970), 987–1011.

[22] Polcino Milies C. and de Melo F., "On Cyclic and Abelian Codes", *IEEE Trans. Inform. Theory* 59 (2013), No. 11, 7314–7319.

[23] Polcino Milies C. and Sehgal S.K., *An introduction to group rings*, Algebras and Applications, Kluwer Academic Publishers, Dortrecht, 2002.

[24] Poli A., "Codes dans les algebras de groups abelienes (codes semisimples, et codes modulaires)", in Information Theory (Proc. Internat. CNRS Colloq., Cachan 1977) Colloq. Internat. CNRS 276 (1978), 261–271.

[25] Prange E., *Cyclic error-correcting codes in two symbols*, AFCRC-TN-57-103, USAF, Cambridge Research Laboratories, New York, 1957.

[26] Pruthi M. and Arora S.K., "Minimal codes of prime power length", *Finite Fields Appl.* 3 (1997), No. 2, 99–113.

[27] Sabin R.E., "On determining all codes in semi-simple group rings", in *Lecture Notes in Comput. Sci.* 673, Springer (1993), 279–290.

[28] Sabin R.E. and Lomonaco S.J., "Metacyclic Error-correcting Codes", *Appl. Algebra Engrg. Comm. Comput.* 6 (1995), No. 3, 191–210.

[29] Shannon C.E., "A mathematical theory of communication", *Bell System Tech. J.* 27 (1948), 379–423.

[30] Thompson T.M., *From error-correcting codes through sphere packings to simple groups*, Carus Mathematical Monographs 21, Mathematical Association of America, Washington, 1983.