Indian J Pure Appl Math
https://doi.org/10.1007/s13226-021-00187-5

ORIGINAL RESEARCH PAPER

Essential idempotents in group algebras and coding theory

Raul A. Ferraz · C. Polcino Milies

Dedicated to Prof. I.B.S. Passi on the occasion of his 80th birthday

Received: 17 July 2020 / Accepted: 4 November 2020

Abstract We consider a special class of idempotent of semisimple group algebras which we call essential. We give some criteria to decide when a primitive idempotent is essential; then we consider group algebras of cyclic group over finite fields, establish the number of essential idempotents in this case and find a relation among essential idempotents in different algebras. Finally we apply this ideas to coding theory and compute examples of codes with the best known weight.

1 Introduction

In our first section we discuss a special kind of primitive idempotents in the semisimple group algebra of a finite group, that we call *essential*, which were primary motivated by the study of coding theory but that might be of interest in their own right. These idempotents were considered by Bakshi, Raka and Sharma in [2], where they were called *non-degenerate*, in the special case of group algebras of cyclic groups over finite fields.

In the third section we give some results relating this type of idempotents to special codes that were extensively studied in the literature and proceed, in the following section, to establish a correspondence between essential idempotents of related group algebras. Finally, we give examples to show that essential idempotents can be used to produce examples of codes of maximum weight in a rather simple way.

Some of the results we survey have already been published; these we quote with a reference. The new ones are given with the corresponding proofs.

We first discuss briefly some basic definitions in coding theory and their relations to group algebras.

Let $\mathbb{F}$ denote a finite field with q elements. A *linear code* of length n over $\mathbb{F}$ is a proper subspace of $\mathbb{F}^n$.

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

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

Given a code $\mathcal{C}$, its minimal distance is the number

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

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

Communicated by Gadadhar Misra.

R. A. Ferraz (✉) · C. P. Milies
Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66.281, São Paulo CEP 05314-970, Brazil
E-mail: raul@ime.usp.br

C. P. Milies
E-mail: polcino@usp.br

Published online: 29 November 2021

Theorem 1 *Let $\mathcal{C}$ be a code with minimal distance d and set $\kappa = \lfloor (d-1)/2 \rfloor$.*
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 over a field with q elements, of length n and dimension m, having minimal distance d is called a q-ary (n, M, d)-code.

A natural goal, when designing a code is to look for efficiency (in the sense that it should contain 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 $\mathbb{F}^n$ 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 special class of linear codes was introduced in 1957 by E. Prange [30]. 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 in use are of this kind.

Given a word $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ its *right shift* is the word $(x_n, x_1, \ldots, x_{n-1})$. A linear code $\mathcal{C}$ is *cyclic* if, for every word in the code its right shift is also in the code. Notice that this implies that if a given word $(x_1, x_2, \ldots, x_n)$ is in the code, then all words obtained by circular permutations are also in the code.

The map

$$\varphi : \mathbb{F}^n \to \frac{\mathbb{F}[X]}{(X^n - 1)}$$

given by $\varphi(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) = a_0 + a_1 X + \ldots + a_{n-2} X^{n-2} + a_{n-1} X^{n-1}$ is a linear isomorphism and it is easy to see that a linear code $\mathcal{C}$ of length n over $\mathbb{F}$ is cyclic if and only if its image $\varphi(\mathcal{C})$ is an ideal of the factor ring $\mathbb{F}[X]/(X^n - 1)$.

Since this ring, in turn, is isomorphic to the group algebra of the cyclic group C_n, of order n, over $\mathbb{F}_q$, one can think of cyclic codes as ideals of $\mathbb{F}_q C$.

S.D. Berman in 1967 [4] and MacWilliams in 1970 [22] introduced independently the notion of an *Abelian code*: one such code, over a field $\mathbb{F}$ is an ideal of the group algebra $\mathbb{F}A$ of a finite Abelian group A.

It is then natural to further extend this definition. A *group code* over a field $\mathbb{F}$ is an ideal of the group algebra $\mathbb{F}G$ of a finite group G.

These codes have been extensively studied by many authors for example, among others, in [7,13,14,18–20,24,29,30].

2 Codes and Group algebras

All groups considered throughout this paper will be finite, and we shall always assume that all fields $\mathbb{F}$ are such that $char(\mathbb{F}) \nmid |G|$.

For an element α in the group algebra $\mathbb{F}G$, the *weight* of α is the number of elements in its support; i.e., if $\alpha = \sum_{g \in G} \alpha_g g$, then

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

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

Given two elements $\alpha = \sum_{g \in G} \alpha_g g$ and $\sum_{g \in G} \beta_g g$, regarding $\mathbb{F}G$ as a vector space with basis G, the Hamming distance from α to β is

$$d(\alpha, \beta) = |\{g \mid \alpha_g \neq \beta_g, g \in G\}| = \omega(\alpha - \beta, 0),$$

and thus, for an ideal I in $\mathbb{F}G$, we have that

$$d(I) = min\{\omega(\alpha) \in I \mid \alpha \neq 0\} = \omega(I),$$

the *minimum weight* of I.

Since we are always assuming that $char(\mathbb{F}) \nmid |G|$, the group algebra $\mathbb{F}G$ is *semisimple* (see [27, Theorem 3.4.7]) meaning that every ideal is a direct summand or, equivalently, that every ideal is generated by an idempotent element.

Moreover, $\mathbb{F}G$ can be written as a (unique) direct sum of a finite number of two-sided ideals $\{A_i\}_{1\leq i\leq r}$, called the *simple components* of $\mathbb{F}G$, which are simple algebras, and also a direct sum (in more than one way) of minimal left ideals.

This implies that there exists a unique family $\{e_1, \ldots, e_r\}$ of orthogonal idempotents in $\mathbb{F}G$ which are central, such that none of them can be written as a sum of two non-zero central idempotents, and such that $\sum_{i=1}^{r} e_i = 1$. These are called the *primitive central idempotents* of $\mathbb{F}G$.

Each two-sided ideal of $\mathbb{F}G$ is a direct sum of some of the simple components and thus, every central idempotent is a sum of primitive central idempotents called its *constituents*.

Each decomposition as direct sums of left ideals determines a family of non-central idempotents with similar properties, called a family of *primitive idempotents* of $\mathbb{F}G$.

There is a natural way of exhibiting idempotents of $\mathbb{F}G$ from subgroups of G. If H is a subgroup of G, then the element

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

is an idempotent and it is central if and only if H is normal in G.

As shown in [27, Proposition 3.6.7] we have that $(\mathbb{F}G)(1-\widehat{H}) = \Delta(G, H)$, the kernel of the natural projection $\pi : \mathbb{F}G \to \mathbb{F}[G/H]$ and it is easy to see that $(\mathbb{F}G)\widehat{H} \cong \mathbb{F}[G/H]$ via the map $\psi : (\mathbb{F}G)\widehat{H} \to \mathbb{F}[G/H]$ defined by $g\widehat{H} \mapsto gH \in G/H$, so

$$\mathbb{F}G = (\mathbb{F}G)\widehat{H}\oplus \cong (\mathbb{F}G)[G/H] \oplus \Delta(G : H).$$

and

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

In particular, if we take H to be G', the commutator subgroup of G we have the following.

Proposition 1 *([27, Prop. 3.6.11]) Let $\mathbb{F}G$ be a semisimple group algebra. Then*

$$\mathbb{F}G = (\mathbb{F}G)\widehat{G'} \oplus \Delta(G : G'),$$

where $(\mathbb{F}G)\widehat{G'} \cong \mathbb{F}[G/G']$ is the sum of all commutative components of $\mathbb{F}G$ and $\Delta(G : G')$ is the sum of all the non commutative ones.

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 $(\mathbb{F}G)\widehat{H}$ over $\mathbb{F}$.

Hence, an element in the ideal $(\mathbb{F}G)\widehat{H}$ is of the form $\alpha = \sum_{t\in\tau} a_t t\widehat{H}$ which means that, when written in the basis G of $\mathbb{F}G$, 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.

In the case of the rational group algebra of a finite Abelian p-group G, it is known that the set of primitive idempotents of $\mathbb{Q}G$ is the set of all elements of the form

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

where H, H^* are pairs of subgroups of G such that $H \subset H^*$ and the factor group H^*/H is cyclic of order p, together with the element $\widehat{G}$ which is called the *principal idempotent* of $\mathbb{Q}G$ [16, Theorem VII.1.4].

In [14] we gave necessary and sufficient conditions for this same formulas to describe the set of primitive idempotents of the group algebra of a finite Abelian group over a finite field. Information about these kind of ideals is well-known.

Proposition 2 *[12] Let G be a finite group and F a field such that $char(F)$ does not divide $|G|$. Let H and H^* be normal subgroups of G such that $H \subset H^*$ and set $e = \widehat{H} - \widehat{H^*}$. Then:*

(i) $dim_F(FG)e = |G/H| - |G/H^*|$

(ii) $w((FG)e) = 2|H|$.
(iii) *If $\mathcal{A}$ is 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 $(\mathbb{F}G)e$ over $\mathbb{F}$.

Since $\widehat{H} - \widehat{H^*} = (\widehat{H} - \widehat{H^*})H$ we have that $(\mathbb{F}G)((\widehat{H} - \widehat{H^*}) \subset (\mathbb{F}G)\widehat{H}$ so, from the point of view of coding theory these ideals give also repetition codes.

These results suggest that, though minimal ideals of group algebras have been the subject of several papers on coding theory, they might not be good candidates to obtain interesting codes.

3 Essential idempotents

As noted above, if H is normal subgroup of G, then $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents.

Let e be a primitive central idempotent of $\mathbb{F}G$. Then:

- If e is not a constituent of $\widehat{H}$ we have $e\widehat{H} = 0$.
- If e is a constituent of $\widehat{H}$ we have $e\widehat{H} = e$.

In this last case, we have that $(\mathbb{F}G)e \subset (\mathbb{F}G)\widehat{H}$ and thus the minimal code $(\mathbb{F}G)e$ is a repetition code.

We are interested, of course, in codes which are not of this type.

Definition 1 A primitive idempotent e in the group algebra $\mathbb{F}G$, is called an **essential idempotent** if $e\widehat{H} = 0$, for every subgroup $H \neq (1)$ in G.

A minimal ideal of $\mathbb{F}G$ is called an **essential ideal** if it is generated by an essential idempotent and **non essential** otherwise.

Notice that, if e is a central idempotent, then the map $\pi : G \to Ge$, given by $\pi(g) = g \cdot e$ is a group epimorphism. We can use this map to characterize essential idempotents.

Proposition 3 *Let $e \in \mathbb{F}G$ be a primitive central idempotent. Then e is essential if and only if the map $\pi : G \to Ge$, is a group isomorphism.*

Though the proof of this result is very simple, it has an interesting consequence, whose proof is also almost immediate.

Corollary 1 *([9, Corollary 2.4]) If G is Abelian and $\mathbb{F}G$ contains an essential idempotent, then G is cyclic.*

Hence, if G is Abelian but not cyclic, all the minimal ideals of A give repetition codes.

On the other hand, as we show below, if G is cyclic, then $\mathbb{F}G$ always contains essential idempotents. To do so, assume that G is cyclic of order $n = p_1^{n_1} \cdots p_t^{n_t}$. Then, G can be written as a direct product $G = C_1 \times \cdots \times C_t$, where C_i is cyclic, of order $p_i^{n_i}$, $1 \leq i \leq t$. Let K_i be the minimal subgroup of C_i; i.e. the unique subgroup of order p_i in C_i and denote by a_i a generator of this subgroup, $1 \leq i \leq t$. Set

$$\begin{aligned} e_0 &= (1 - \widehat{K_1}) \cdots (1 - \widehat{K_t}) \\ &= \left(1 - \frac{(1 + a_1 + \cdots + a_1^{p_1^{n_1-1}})}{p_1}\right) \cdots \left(1 - \frac{(1 + a_t + \cdots + a_t^{p_t^{n_t-1}})}{p_t}\right). \end{aligned}$$

Then e_0 is a non zero central idempotent and it is easy to see that a primitive idempotent $e \in \mathbb{F}G$ is essential if and only if $e \cdot e_0 = e$ [9, theorem 2.6]. This implies that e_0 is the sum of all essential idempotents of $\mathbb{F}G$ and thus $(\mathbb{F}G)e_0$ is the sum of all the essential ideals of $\mathbb{F}G$.

Since $e_0 \neq 0$ it follows that, when G is cyclic, $\mathbb{F}G$ always contains essential idempotents.

Let $\mathbb{F}$ be a field, G a finite Abelian group and $e \neq \widehat{A}$ an idempotent in $\mathbb{F}G$. Set

$$H_e = \{g \in G \mid ge = e\}.$$

Clearly, H_e is the unique maximal subgroup of G such that $H_e e = e$ and it can be shown easily that $H_e = G$ if and only if $e = \widehat{G}$, the principal idempotent of $\mathbb{F}G$. Actually, H_e is the kernel of the irreducible representation associated to the simple component $(\mathbb{F}G)e$.

Theorem 2 *([9, Theorem 3.1]) Let $e \neq \widehat{G}$ be a primitive idempotent of $\mathbb{F}G$ and $\psi : \mathbb{F}G \to \mathbb{F}[G/H_e]$ the natural projection. Then, the element $\psi(e)$ is an essential idempotent of $\mathbb{F}[G/H_e]$.*

This result readily shows that G/H_e is cyclic.
Let G_1 and G_2 denote two finite groups of the same order, $\mathbb{F}$ a field, and let $\gamma : G_1 \to G_2$ be a bijection. Denote by $\overline{\gamma} : \mathbb{F}G_1 \to \mathbb{F}G_2$ 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 $I_1 \subset \mathbb{F}G_1$ and $I_2 \subset \mathbb{F}G_2$ 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 [30].

The subgroup H_e constructed above can be used to prove the following.

Theorem 3 *([9, Theorem 3.3]) Every minimal ideal in the semisimple group algebra $\mathbb{F}A$ of a finite Abelian group A is permutation equivalent to a minimal ideal in the group algebra $\mathbb{F}C$ of a cyclic group C of the same order.*

For quite some time after the introduction of Abelian codes by Berman and MacWilliams, there was no evidence that non cyclic Abelian groups could provide better codes than those which are cyclic. The results above show that such codes should be searched among those which are non minimal and they do exist; see [18,23] and [29].

In our last section we will also give examples of codes from metacyclic groups that are not equivalent to Abelian ones.

Let $\mathbb{F}$ be a field and C_n a cyclic group of order n such that $char(\mathbb{F}) \nmid n$. A well-known method to determine the primitive idempotents of $\mathbb{F}C_n$ is the so-called Galois descent. We shall give a criteria to determine essential idempotents from this point of view and, as a consequence, compute the number of these idempotents in $\mathbb{F}C_n$. If ζ denotes a primitive root of unity of order n, then $\mathbb{F}(\zeta)$ is a splitting field for C_n, and the primitive idempotents of $\mathbb{F}C_n$ are given by

$$e_i = \frac{1}{n}\sum_{j=0}^{n-1} \zeta^{-ij} g^j, \quad 0 \leq i \leq n-1.$$

For each element $\sigma \in Gal(\mathbb{F}(\zeta^i) : \mathbb{F})$ set

$$\sigma(e_i) = \frac{1}{n}\sum_{j=0}^{n-1} \sigma(\zeta^{-i})^j g^j, \quad 0 \leq i \leq n-1.$$

Recall that two primitive idempotents of $\mathbb{F}(\zeta)C_n$ are equivalent if there exists $\sigma \in Gal(\mathbb{F}(\zeta^i) : \mathbb{F})$ which maps one to the other. Let $e_1, \ldots, e_t$ be a set of representatives of classes of primitive idempotents (reordering, if necessary).

Then, the set of primitive elements of $\mathbb{F}C_n$ is given by the formulas

$$\varepsilon_i = \sum_{\sigma \in Gal(\mathbb{F}(\zeta^i):\mathbb{F})} \sigma(e_i), \quad 1 \leq i \leq t.$$

Notice that, for each fixed index i we have:

$$\begin{aligned}\varepsilon_i &= \sum_{\sigma \in Gal(\mathbb{F}(\zeta^i):\mathbb{F})} \sigma(e_i) \;=\; \frac{1}{n} \sum_{\sigma \in Gal(\mathbb{F}(\zeta^i):\mathbb{F})} \sum_{j=0}^{n-1} \sigma(\zeta^{-i})^j g^j \\ &= \frac{1}{n}\sum_{j=0}^{n-1} \sum_{\sigma \in Gal(\mathbb{F}(\zeta^i):\mathbb{F})} \sigma(\zeta^{-i})^j g^j \;=\; \frac{1}{n}\sum_{j=0}^{n-1} tr_{\mathbb{F}(\zeta^i)|\mathbb{F}}(\zeta^{-ij}) g^j,\end{aligned}$$

where $tr_{\mathbb{F}(\zeta^i)|\mathbb{F}}$ denotes the trace map of $\mathbb{F}(\zeta^i)$ over $\mathbb{F}$.

Let $C_n = \langle g \rangle$ denote a cyclic group of order n. If i is a positive integer such that $(n, i) = 1$, then the map $\psi_i : C_n \to C_n$ defined by $g \mapsto g^i$ is an automorphism of C that extends linearly to an automorphism of $\mathbb{F}C_n$, which we shall also denote by ψ_i:

$$\sum_{g \in C_n} a_g g \overset{\psi_i}{\mapsto} \sum_{g \in C_n} a_g \psi_i(g). \tag{1}$$

Lemma 1 *If $\varepsilon_i = \frac{1}{n}\sum_{j=0}^{n-1} tr_{\mathbb{F}(\zeta^i)|\mathbb{F}}(\zeta^{-ij})g^j$ is an essential idempotent, then ζ^i is a primitive root of unity of order precisely equal to n.*

Proof Assume, by way of contradiction, that $o(\zeta^i) = d < n$ and set $r = n/d$. Then

$$1 = \zeta^{id} = \zeta^{i(2d)} = \cdots = \zeta^{i(r-1)d},$$

so

$$\begin{aligned}\varepsilon_i &= \frac{1}{n}\sum_{j=0}^{d-1} tr_{\mathbb{F}(\zeta^i)|\mathbb{F}}(\zeta^{-ij})(1 + g^d + g^{2d} + \cdots + g^{d(r-1)})g^j \\ &= \left(\frac{1}{n}\sum_{j=0}^{d-1} tr_{\mathbb{F}(\zeta^i)|\mathbb{F}}(\zeta^{-ij})g^j\right)\widehat{\langle g^d \rangle}.\end{aligned}$$

Hence, $\varepsilon_i \cdot \widehat{\langle g^d \rangle} = \varepsilon_i$, so ε_i is not essential. □

Theorem 4 *Let C_n be a cyclic group of order n and $\mathbb{F}$ a field such that $char(\mathbb{F}) \nmid n$. Given two essential idempotents $\varepsilon_h, \varepsilon_k \in \mathbb{F}C_n$, there exists an integer i with $(n, i) = 1$ and the automorphism $\psi_i : \mathbb{F}C_n \to \mathbb{F}C_n$ defined as above is such that $\psi_i(\varepsilon_h) = \varepsilon_k$. Conversely, if ε is an essential idempotent and ψ_i is an automorphism as above, then $\psi_i(\varepsilon)$ is also an essential idempotent.*

Proof Write

$$\varepsilon_h = \frac{1}{n}\sum_{j=0}^{n-1} tr_{\mathbb{F}(\zeta^h)|\mathbb{F}}(\zeta^{-hj})g^j \text{ and } \varepsilon_k = \frac{1}{n}\sum_{j=0}^{n-1} tr_{\mathbb{F}(\zeta^k)|\mathbb{F}}(\zeta^{-kj})g^j$$

It follows again from the lemma that $(h, n) = (k, n) = 1$ so, there exist integers r, s such that

$$h \equiv s \cdot k (\bmod n) \text{ and } k \equiv r \cdot h (\bmod n).$$

Also, $\mathbb{F}(\zeta^h) = \mathbb{F}(\zeta^k)$ hence, to simplify notations, we shall write $tr_{\mathbb{F}(\zeta^h)|\mathbb{F}} = tr_{\mathbb{F}(\zeta^k)|\mathbb{F}}$ simply as tr.
Now, writing $\ell = sj$ we have

$$\psi_s(\varepsilon_h) = \frac{1}{n}\sum_{j=0}^{n-1} tr(\zeta^{-hj})g^{sj} = \frac{1}{n}\sum_{\ell=0}^{n-1} tr(\zeta)^{-(rh)\ell}g^{\ell} = \varepsilon_{rh} = \varepsilon_k.$$

Since for every such automorphism ψ_i we have that $\psi_i(\widehat{H}) = \widehat{H}$ for every subgroup H of C_n, the converse follows immediately □

Now we can give another description of essential idempotents.

Theorem 5 *An idempotent $\varepsilon_i = \frac{1}{n}\sum_{j=0}^{n-1} tr_{\mathbb{F}(\zeta^i)|\mathbb{F}}(\zeta^{-ij})g^j$ is an essential idempotent if and only if ζ^i is a primitive root of unity of order precisely equal to n.*

Proof Necessity is just the content of the lemma above.
To prove the converse, notice that exists at least one essential idempotent in $\mathbb{F}C_n$, which must be of the form

$$\varepsilon_h = \frac{1}{n}\sum_{j=0}^{n-1} tr_{\mathbb{F}(\zeta^h)|\mathbb{F}}(\zeta^{-hj})g^j, \quad \text{with } (h,n)=1.$$

For every integer k, with $(k,n)=1$, the proof of the previous theorem shows that there exists another integer r such that $\psi_r(\varepsilon_h)=\varepsilon_k$. Hence, for every such k, the idempotent e_k is essential. □

We are ready to compute the number of essential idempotents in the group algebra of a cyclic group.

Let φ denote Euler's totient function. Notice that, according to Theorem 5 there are $\varphi(n)$ possibilities for an idempotent of the form $\varepsilon_i = \frac{1}{n}\sum_{j=0}^{n-1} tr_{\mathbb{F}(\zeta^i)|\mathbb{F}}(\zeta^{-ij})g^j$ to be essential, one for each exponent i such that ζ^i is primitive of order n. However, two expressions of this type, for idempotents e_h, e_k, can give the same idempotent.

Write them in the form

$$\varepsilon_h = \sum_{\sigma\in Gal(\mathbb{F}(\zeta^h):\mathbb{F})} \sigma(e_h), \quad \varepsilon_k = \sum_{\sigma\in Gal(\mathbb{F}(\zeta^k):\mathbb{F})} \sigma(e_k).$$

Notice that, since ζ^h and ζ^k are primitive roots of order n, we have that $\mathbb{F}(\zeta^h)=\mathbb{F}(\zeta^k)=\mathbb{F}(\zeta)$.

Clearly, the above idempotents are equal if and only if there exists an automorphism $\sigma \in Gal(\mathbb{F}(\zeta):\mathbb{F})$ such that $\sigma(e_h)=e_k$. Since the elements of $Gal(\mathbb{F}(\zeta):\mathbb{F})$ do not fix idempotents of $\mathbb{F}(\zeta)C_n$, there are precisely $|Gal(\mathbb{F}(\zeta):\mathbb{F})|$ idempotents of $\mathbb{F}C_n$ equal to e_i.

Hence, we have proved the following.

Theorem 6 *The number of essential idempotents in the group algebra $\mathbb{F}C_n$ is precisely*

$$\frac{\varphi(n)}{|Gal(\mathbb{F}(\zeta):\mathbb{F})|}.$$

4 Binary Codes of a special type

In this section we show that essential idempotents play a deceive role in the construction of some important classes of binary codes.

Recall that a binary linear code of dimension k and length n is called *simplex* if a generating matrix for the code contains all possible non zero columns of length k. Since these are 2^k-1 in number, this matrix must be of size $k\times(2^k-1)$ so, we must have $n=2^k-1$.

Theorem 7 *([9]) Let $\mathcal{C}$ be a binary linear code of dimension k and length $n=2^k-1$. Then $\mathcal{C}$ is a simplex code if and only if it is cyclic and essential.*

Our next result needs the following elementary lemmas, whose proofs can be found in [10].

Lemma 2 *Let $\mathcal{C}$ be a binary linear code of length n and dimension k. Let $f=X^k+a_{k-1}X^{k-1}+\cdots+a_1X+a_0\in\mathbb{F}_2[X]$ be an irreducible polynomial of order 2^k-1. Then, it is possible to order the non zero elements of $\mathcal{C}$ as $\{v_1,\ldots,v_{2^k-1}\}$ so that*

$$v_t = a_{k-1}v_{t-1}+\cdots a_1v_{t-k+1}+a_0v_{t-k},$$

where the subindexes are taken modulo 2^k-1

Lemma 3 *Let $\mathbb{F}_q$ be a finite field with q elements,*

$$f = X^k - a_{k-1}X^{k-1} - \cdots - a_1X - a_0 \in \mathbb{F}_q[X]$$

an irreducible polynomial of order q^k-1 and for each arbitrary sequence $(x_0,\ldots,x_{k-1})$ of elements of $\mathbb{F}_q$. Set:

$$x_\ell = a_{k-1}x_{\ell-1}+\cdots+a_0x_{\ell-k}, \quad \text{for } \ell\geq k.$$

Let W be the set of all sequences constructed in this way and $C_{q^k-1} = \langle g \rangle$ a cyclic group of order $q^k - 1$. Then, the set

$$I = \left\{ \sum_{j=0}^{q^k-2} x_j g^j \mid (x_0, \ldots, x_{q^k-2}) \in W \right\},$$

is an essential ideal of $\mathbb{F}_q C_{q^k-1}$.

Lemma 4 *Let $\mathcal{C}$ be a cyclic code of length n and dimension k. Then*

$$\sum_{v \in \mathcal{C}} w(v) = nq^{k-1}(q-1).$$

If $\mathcal{C}$ is of constant weight, then

$$w(\mathcal{C}) = \frac{nq^{k-1}(q-1)}{q^k - 1}.$$

Let $\mathcal{C}$ be binary a code of length n and dimension k with elements ordered as in Lemma 2. Write its elements in coordinates, as rows of a matrix:

$$M = \begin{bmatrix} v_{1,1} & v_{1,2} & \ldots & v_{1,n} \\ v_{2,1} & v_{i,2} & \ldots & v_{i,n} \\ & & \ldots & \end{bmatrix}.$$

We shall be interested in those codes for which this matrix contains no column equal to 0. More precisely, we give the following.

Definition 2 Let $\mathcal{C} = \{v_1, \ldots, v_m\}$ be a linear code, whose elements we write as $v_i = (v_{i,1}, v_{i,2}, \ldots v_{i,n})$, $1 \leq i \leq k-1$, $1 \leq i \leq k-1$. We say that $\mathcal{C}$ contains no zero column if, for each index j, $1 \leq j \leq n$, there exists at least one vector $v_i \in \mathcal{C}$ such that $v_{i,j} \neq 0$.

Now, we can state the following.

Theorem 8 *Let $\mathcal{C}$ be a binary linear code of constant weight, without zero columns. Then $\mathcal{C}$ is equivalent to a cyclic code which is either essential or a repetition of an essential one.*

5 A correspondence

Let $\mathbb{F}_q$ be the finite field with q elements, $C = C_n$ the cyclic group of order n, with generator g and assume that $(q, n) = 1$. Throughout this section, m will always denote the multiplicative order of $\overline{q}$ in the unit group $U(\mathbb{Z}_n)$. Also, we set $N = q^m - 1$ and $\ell = N/n$. Notice that the multiplicative order of q, modulo N is also m because, if $s < m$ is a positive integer such that $N|(q^s - 1)$, then also $n|(q^s - 1)$, a contradiction.

If $\mathbb{F}$ is any field such that char $(\mathbb{F}) \nmid |C|$, e is a primitive idempotent of $\mathbb{F}C$ and $\Phi : \mathbb{F}[X] \to (\mathbb{F}C)e$ denotes the morphism given by $\Phi(f) = f(ge), \forall f \in \mathbb{F}[X]$, it is easy to see that

$$(\mathbb{F}C)e \cong \frac{\mathbb{F}[X]}{(p(X))},$$

where $p \in \mathbb{F}[X]$ is the generator of $Ker(\Phi)$ and thus the minimal polynomial of ge over $\mathbb{F}$. As e is primitive, $(\mathbb{F}C)e$ is a field and hence $p(X)$ is irreducible in $\mathbb{F}[X]$.

Proposition 4 *With the notation above, if e is an essential idempotent, then the dimension of $(\mathbb{F}_q C)e$ is precisely m.*

Proof On the one hand, it is clear that $dim[(\mathbb{F}_qC)e]$ equals the degree of p. On the other hand, as ge is a root of p, all the distinct root of this polynomial are $ge, g^qe, \dots g^{q^{r-1}}e$, where r is the least positive integer such that $g^{q^r}e = ge$ [21, Theorem 3.33]. It follows, from Proposition 3, that also $g^{q^r} = g$ and hence, that $g^{q^r-1} = 1$. So, r is the least positive integer such that $q^r \equiv 1 \pmod n$ and thus, the order of $\overline{q}$ in $U(\mathbb{Z}_n)$. Since $deg(p) = r$, the result follows. □

Theorem 9 *Let C denote a cyclic group of order n and generator g and let e_0 be the sum of all essential idempotents in $\mathbb{F}_qC$. Then:*
(i) $dim(\mathbb{F}_qC)e_0 = \varphi(n)$ where φ denotes Euler's Totient function.
(ii) There exist precisely $\varphi(n)/m$ essential idempotents in $\mathbb{F}_qC$.

Proof Let $n = p_1^{n_1} \cdots p_t^{n_t}$ be the factorization of n as a product of prime integers and let C_i denote the cyclic group of order ${p_i}^{n_i}$, $1 \le i \le t$. Recall that $e_0 = (1 - \widehat{K_1}) \cdots (1 - \widehat{K_t})$, where K_i is the only subgroup of order p_i in C_i, $1 \le i \le t$.

First, we claim that if R is a finite dimensional algebra over $\mathbb{F}_q$, taking dimensions over $\mathbb{F}_q$, we have $dim(RC_i \cdot (1 - \widehat{K_i})) = dim(R).\varphi(p_i^{n_i})$.

In fact, notice that $RC_i \cdot \widehat{K_i} \cong R[C_i/K_i]$ so $dim(RC_i \cdot \widehat{K_i}) = |C_i|/|K_i| = dim(R).p_i^{n_i-1}$. Also,

$$RC_i = RC_i \cdot \widehat{K_i} \oplus RC_i \cdot (1 - \widehat{K_1})$$

and thus

$$\begin{aligned} dim(RC_i(1 - \widehat{K_i})) &= dim(R).(|C_i| - dim(\mathbb{F}_qC_i \cdot \widehat{K_i})) \\ &= dim(R)(p_i^{n_i} - p_i^{n_i-1}) = dim(R).\varphi(n). \end{aligned}$$

We shall prove (i) by induction on t. The case when $t = 1$ follows immediately from the claim above, setting $i = 1$ and $R = \mathbb{F}_q$.

Now, assume that the statement is true for $t - 1$ and set

$$R = \mathbb{F}_q[C_1 \times \cdots \times C_{t-1}](1 - \widehat{K_1}) \cdots (1 - \widehat{K_{t-1}}).$$

Then,

$$\begin{aligned} dim(\mathbb{F}_qC)e_0 &= dim(RC_t.(1 - \widehat{K_t}) = dim(R).\varphi(p_t^{n_t})) \\ &= \varphi(p_1^{n_1} \cdots p_{t-1}^{n_{t-1}})\varphi(p_t^{n_t}) = \varphi(n). \end{aligned}$$

If $\mathbb{F}$ is a finite field with q elements we have $|Gal(\mathbb{F}(\zeta) : \mathbb{F})| = o(\overline{q}) = m$ so (ii) follows immediately from Theorem 6. □

Since $\mathbb{F}_q$ contains q elements and $dim(\mathbb{F}_qC)e = m$, it follows that $(\mathbb{F}_qC)e$ is a field with q^m elements. If we denote by $U_e = U((\mathbb{F}_qC)e)$, the group of invertible elements of $(\mathbb{F}_qC)e$, we have that U_e is a cyclic group of order $|U_e| = q^m - 1 = N$. Let γ be a generator of U_e.

As e is essential, we have that $C \cong Ce$, so Ce is a subgroup of order n of U_e and the coset $\gamma(Ce)$ is a generator of the factor group U_e/Ce, which is of order ℓ. Hence, ℓ is the least positive integer such that $\gamma^\ell \in Ce$. Thus, there exists an integer k, with $1 \le k \le n - 1$, such that $\gamma^\ell = g^ke$. Also, we can write

$$U_e = \{g^j\gamma^i \mid 0 \le j \le n - 1,\ 0 \le i \le \ell - 1\}.$$

In the particular case when $n = q^k - 1$ for some positive integer k we have that $m = k$ and then $N = n$ and $\ell = 1$. This implies that

$$(\mathbb{F}C)e = \{0\} \cup \{g^je \mid 0 \le j \le n - 1\}, \tag{2}$$

showing that, in this case, all non-zero elements of an essential ideal are of equal weight.

Denote by C_n and C_N the cyclic groups of orders n and N, with generators g and h respectively. In what follows, we compare essential idempotents in $\mathbb{F}_qC_n$ and $\mathbb{F}_qC_N$

First, note that $N = \ell n$ and thus $\langle h^\ell \rangle$ is a subgroup of C_N of order n, hence isomorphic to C_n. Let σ be such an isomorphism and denote also by $\sigma : \mathbb{F}_q\langle h^\ell \rangle \to \mathbb{F}_qC_n$ the isomorphism induced linearly by σ.

The set $\{1, h, \ldots, h^{\ell-1}\}$ is a transversal of $\langle h^\ell \rangle$ and thus, every element $\alpha \in \mathbb{F}_q C_N$ can be written uniquely in the form

$$\alpha = \sum_{i=0}^{\ell-1} \alpha_i h^i \quad \text{with } \alpha_i \in \mathbb{F}_q \langle h^\ell \rangle,\ 0 \leq i \leq \ell - 1. \tag{3}$$

We wish to prove the following.

Theorem 10 *With the notations above, given an essential idempotent $e \in \mathbb{F}_q C_n$ there exists an element $\beta \in U_e$ such that $\{e, \beta, \ldots \beta^{\ell-1}\}$ is a transversal of $C_n \cdot e$ in U_e and the element*

$$e_N = \frac{1}{\ell} \sum_{i=0}^{\ell-1} \sigma^{-1}(\beta^i) h^i$$

is an essential idempotent of $\mathbb{F}_q C_N$.

Conversely if $e_N = \sum_{i=0}^{\ell-1} \alpha_i h^i$ is an essential idempotent of $\mathbb{F}_q C_N$, then $e = \ell.\sigma(\alpha_0)$ is an essential idempotent of $\mathbb{F}_q C_n$ and the set $\{\sigma(\alpha_0), \sigma(\alpha_1), \ldots, \sigma(\alpha_{\ell-1})\}$ is a transversal of $C_n \cdot e$ in U_e.

To do so, we need an elementary fact about cyclic groups. We begin with the following.

Lemma 5 *Let n and N be positive integers such that $n|N$ and let i be an integer such that $(n, i) = 1$. If $\ell = N/n$, then the equation*

$$\ell.X \equiv \ell.i \ (\mathit{mod}\ N)$$

has precisely $\varphi(N)/\varphi(n)$ invertible solutions in $\mathbb{Z}_N$.

Proof Notice that $N = n\ell$, so X is a solution of the equation of the statement if and only if it is a solution of the equation $X \equiv i \ (\mathrm{mod}\ n)$. Since this equation has the unique root $X = \bar{i}$ in $\mathbb{Z}_n$, it follows that the solutions of the given equation, in $\mathbb{Z}_N$, are $i, i + n, i + 2n, \ldots i + (\ell - 1)n$.

Let N_1 denote the greatest divisor of N that has the same prime divisors as n, and write $N = N_1 N_2$. By the Chinese Remainder Theorem we have that

$$\mathbb{Z}_N \cong \mathbb{Z}_{N_1} \oplus \mathbb{Z}_{N_2}$$

as rings. Denote by ϕ this isomorphism, which maps an element $a \in \mathbb{Z}_N$ to a pair (a', a'') , where a', a'' denote the classes of a modulo N_1 and N_2 respectively.

Since $\ell n = N$, the set of solutions $i, i + n, i + 2n, \ldots i + (\ell - 1)n$, in $\mathbb{Z}_N$ is the same as the set $i + n\mathbb{Z}_N$.

Claim 1. $\phi(n\mathbb{Z}_N) = n\mathbb{Z}_{N_1} \oplus \mathbb{Z}_{N_2}$. To prove our claim, we shall show that, given integers a_1, a_2, there exists a unique integer a, $0 \leq a \leq \ell - 1$ such that

$$\begin{aligned} na &\equiv na_1 \ (\mathrm{mod}\ N_1), \\ na &\equiv a_2 \ (\mathrm{mod}\ N_2). \end{aligned}$$

In fact, the first equation is equivalent to the congruence $a \equiv a_1 \ (\mathrm{mod}\ N_1/n)$ and, since n is invertible modulo N_2 the second equation is equivalent to the congruence $a \equiv n^{-1}a_2 \ (\mathrm{mod}\ N_2)$. Hence the given system is equivalent to

$$\begin{aligned} a &\equiv a_1 \ \ (\mathrm{mod}\ N_1/n), \\ a &\equiv n^{-1}a_2 \ (\mathrm{mod}\ N_2). \end{aligned}$$

Since $(N_1/n, N_2) = 1$, the Chinese Remainder Theorem shows that this system has a unique solution modulo $N_1 N_2/n = \ell$.

Claim 2. $\phi(i + n\mathbb{Z}_N) = \{(i + a_1 n, a_2) \mid 0 \le a_1 \le N_1/n - 1,\ 0 \le a_2 \le N_2 - 1\}$.
To see this, it is enough to notice that

$$\{i + a_2 \mid 0 \le a_2 \le N_2 - 1\} = \{a_2 \mid 0 \le a_2 \le N_2 - 1\} \text{ in } \mathbb{Z}_{N_2}$$

and use Claim 1 above.

Proof of Lemma. By Claim 2 an element $i + an \in i + n\mathbb{Z}_N$ is invertible in $\mathbb{Z}_N$ if and only if $i + a_1 n$ is invertible in $\mathbb{Z}_{N_1}$ and a_2 is invertible in $\mathbb{Z}_{N_2}$.

As $(i + a_1 n, N_1) = 1$ all elements of this form are invertible in $\mathbb{Z}_{N_1}$, hence they are N_1/n in number. The number of invertible elements in $\mathbb{Z}_{N_2}$ is $\varphi(N_2)$.

Thus, the total number of invertible elements is $N_1/n.\varphi(N_2)$. As n and N_1 have the same prime divisors, $N_1/n = \varphi(N_1)/\varphi(n)$ and $\varphi(N_1)\varphi(N_2)/\varphi(n) = \varphi(N)/\varphi(n)$, as stated. □

Lemma 6 *Let C_N be a cyclic group of order N, C_n a subgroup of C_N of order n and set $\ell = N/n$. Given a generator g of C_n there exist precisely $\varphi(N)/\varphi(n)$ elements x which are generators of C_N and such that $x^\ell = g$.*

Proof Let g be a generator of C_n. If t_0 is any generator of C_N, the element t_0^ℓ is a generator of C_n. Hence, there exists a positive integer i such that $(i, n) = 1$ and $g = t_0^{i\ell}$.

A generator t of C_N such that $t^\ell = g$ must be of the form $t = t_0^X$, with X invertible in $\mathbb{Z}_N$ and $t_0^{\ell X} = t_0^{\ell i}$; i.e., X must be an invertible solution of the equation

$$\ell.X \equiv \ell.i \ (\bmod N).$$

The result now follows from the previous lemma. □

Proof of Theorem 10. Let e be an essential idempotent of $\mathbb{F}C_n$. Then, $g^{-1}e$ is a generator of the subgroup $C_n e$, of order n in U_e. By Lemma 6, there exists a generator $\beta \in U_e$ such that $\beta^\ell = g^{-1}e$. Set

$$e_N = \frac{1}{\ell}\sum_{i=0}^{\ell-1} \sigma^{-1}(\beta^i)h^i.$$

Recall that the isomorphism $\sigma : \mathbb{F}_q\langle h^\ell\rangle \to \mathbb{F}_q C_n$ is such that $\sigma(h^\ell) = g$ so $\sigma^{-1}(g) = h^\ell$. We compute

$$\sigma^{-1}(\beta)h.e_N = \sigma^{-1}(\beta)h.\frac{1}{\ell}\sum_{i=0}^{\ell-1}\sigma^{-1}(\beta^i)h^i = \frac{1}{\ell}\left(\sum_{i=1}^{\ell-1}\sigma^{-1}(\beta^i)h^i + \sigma^{-1}(\beta^\ell)h^\ell\right)$$
$$= \frac{1}{\ell}\left(\sum_{i=1}^{\ell-1}\sigma^{-1}(\beta^i)h^i + \sigma^{-1}(e)\right) = e_N.$$

Hence, we also have

$$[\sigma^{-1}(\beta)h]^j.e_N = e_N \quad \text{for every integer } j.$$

Then

$$e_N^2 = \left(\frac{1}{\ell}\sum_{i=0}^{\ell-1}\sigma^{-1}(\beta^i)h^i\right)e_N = \frac{1}{\ell}\sum_{i=0}^{\ell-1}\sigma^{-1}(\beta^i)h^i.e_N = \frac{1}{\ell}\ell.e_N = e_N.$$

Thus, e_N is an idempotent.
We have shown above that $\sigma^{-1}(\beta)h.e_N = e_N$ so also $h^i e_N = \sigma^{-1}(\beta^{-i})e_N$ for every integer i. We shall use this remark to prove that the set

$$J = \{0\} \cup \{h^i e_N \mid i \in \mathbb{Z}\}$$

is an ideal of $\mathbb{F}_q C_N$.

First, we claim that, given $k_1, k_2 \in \mathbb{F}_q$ and $i_1, i_2 \in \mathbb{Z}$ then either $k_1 h^{i_1} e_N + k_2 h^{i_2} e_N = 0$ or there exists an integer i such that $k_1 h^{i_1} e_N + k_2 h^{i_2} e_N = h^i e_N$. In fact, using the remark above, we have

$$k_1 h^{i_1} e_N + k_2 h^{i_2} e_N = k_1 \sigma^{-1}(\beta^{-i_1}) e_N + k_2 \sigma^{-1}(\beta^{-i_2}) e_N = \sigma^{-1}(k_1 \beta^{-i_1} + k_2 \beta^{-i_2}) e_N.$$

As $\beta \in U_e$ it follows that $k_1 \beta^{-i_1} + k_2 \beta^{-i_2} \in \mathbb{F}_q C_n \cdot e = \{0\} \cup U_e$. If $k_1 \beta^{-i_1} + k_2 \beta^{-i_2} \neq 0$, it is in U_e which is generated by β, so there exists an integer i such that $k_1 \beta^{-i_1} + k_2 \beta^{-i_2} = \beta^{-i}$, proving the claim.

Since $C_N = \langle h \rangle$ it now follows immediately that J is an ideal. Notice that, given the description of the elements in J, it follows that J is a field with unit e_N,

We now observe that $\mathbb{F}_q C_N \cdot e_N = J$. In fact, since $e_N \in J$ it follows that $\mathbb{F}_q C_N \cdot e_N \subset J$. Also, it is clear that $J \subset \mathbb{F}_q C_N \cdot e_N$. Since $\mathbb{F}_q C_N \cdot e_N = J$ is a field, it is a minimal ideal, so e_N is primitive.

To prove that e_N is esencial we use Proposition 3 and show that the map $\pi : C_N \to C_N e_N$ given by $\pi(h^i) = h^i e_N$ is injective (and hence, also an isomorphism). In fact, if $h^i e_N = h^j e_N$ then $\sigma^{-1}(\beta^{-i}) e_N = \sigma^{-1}(\beta^{-j}) e_N$ so $\sigma^{-1}(\beta^{-i} - \beta^{-j}) e_N = 0$. If $\beta^{-i} - \beta^{-j} \neq 0$ then $h^k e_N = 0$ for some integer k, a contradiction. As $0 \leq i, j \leq N - 1$ this implies $i = j$.

To prove the converse we notice that, given an essential idempotent e_n in $\mathbb{F}_q C_n$ and a generator β of $U(\mathbb{F}_q C_n \cdot e_n)$, it was shown that the element

$$e_N = \frac{1}{\ell} \sum_{i=0}^{\ell-1} \sigma^{-1}(\beta^i) h^i$$

is an essential idempotent of $\mathbb{F}_q C_N$. Since we have shown in Theorem 9 that there exist $\varphi(n)/m$ essential idempotents in $\mathbb{F}_q C_n$ and there are $\varphi(N)/\varphi(n)$ possible choices for β, as shown in Lemma 6, so the number of essential idempotents of $\mathbb{F}_q C_N$ that can be constructed in this way is

$$\frac{\varphi(n)}{m} \cdot \frac{\varphi(N)}{\varphi(n)} = \frac{\varphi(N)}{m}.$$

As this is precisely the number of essential idempotents of $\mathbb{F}_q C_N$, it follows that all of them are of this form.

The fact that the set $\{\sigma(\alpha_0), \sigma(\alpha_1), \ldots, \sigma(\alpha_{\ell-1})\}$ is a transversal of $C_n \cdot e$ in U_e now follows again from the proof of the direct direction. □

6 Examples

In this section we offer some examples of interesting codes that can be constructed easily using group algebras and essential idempotents. C. Garca Pillado, S. Gonzlez, C. Martnez, V. Markov, and A. Nechaev, [15] showed that if a group G can be written as a product $G = AB$ where both A and B are Abelian, then central idempotents generate codes that are equivalent to Abelian ones. Hence, we focus below on ideals generated by non-central idempotents.

Example 1. Let $D_9 = \langle a, b \mid a^9 = 1 = b^2,\ bab = a^{-1} \rangle$ be dihedral group of order 18, set $H_0 = \langle a \rangle$, $H_1 = \langle a^3 \rangle$ and $H_0 = \{1\}$. Then

$$e_{11} = \left(\frac{1+b}{2}\right)\widehat{A}, \quad e_{22} = \left(\frac{1-b}{2}\right)\widehat{A}, \quad e_j = \widehat{H_j} - \widehat{H_{j-1}}, \quad j = 0, 1$$

are the primitive central idempotents of $\mathbb{F}_q D$ ([12, Theorem 3.3]).

Set $f = e_{11} - e_{22}$ and consider the ideal $I = \mathbb{F}_q D_9 \cdot f$.

It is possible to show that if the characteristic of $\mathbb{F}_q$ is different from 2,3,5 and 7, then $dim[I] = 2$ and $w(I) = 15$. The weight of this code is the same as that of the best known code of same dimension (see [17]), for example in the case when the field is $\mathbb{F}_{11}$.

Also, it is possible to prove that these codes are not equivalent to any Abelian code [1, Example 4]. For detailed proofs, see [1].

Example 2. Let us consider the metacyclic group

$$G = \langle a, b \mid a^9 = 1, b^3 = 1, ba = a^4 b \rangle.$$

Olteanu and Van Gelder [25] gave an example of a binary [27,18,2]-code constructed as a left ideal of $\mathbb{F}_2 G$, generated by the non central idempotent $e = a^{-1}ba + aba^{-1}$ which was obtained using the program PrimitiveIdempotentsNilpotent of the GAP program Wedderga [32].

Since $G' = \langle a^3 \rangle$, using Proposition 1 it is easy to see that

$$\mathbb{F}_2 G \cong \mathbb{F}_2 \oplus 4\mathbb{F}_4 \oplus M_3(\mathbb{F}_4),$$

where the only non commutative component is generated by the idempotent $e' = 1 - \widehat{G'} = a^3 + a^6$. Since the dimension of this simple component over $\mathbb{F}_2$ is already 18, it cannot contain a proper left ideal of that dimension. Actually, it is possible to verify, via hand calculations, that the given element is not even an idempotent.

This is due to a small gap in the GAP program. A possible way to repair this gap consists in replacing the last part of the source code:

```
### Construct the idempotents
L := List( Product3Lists([T_odd,T_even,T_E]) , i -> (AverageSum(FG,b_odd])*beta*eps)^i);
return L;
end);
```

by the following:

```
### Construct the idempotents

b_summ := One(FG)*b_odd;

for i in [2..Order(b_odd)] do

    b_summ := b_summ+((One(FG) )*b_odd)^ i ;

od;

b_hat := (Order(b_odd)*One(FG))^-1*b_summ;

L := List( Product3Lists([T_odd,T_even,T_E]) , i -> (b_hat*beta*eps)^i);

return L;
end);
```

After this correction, the program gives three non central idempotents in the component:

$$\begin{aligned} e_1 &= a^3 + a^{-1}ba + a^{-3} + ab^{-1}a^{-1} + aba^{-1} + a^{-1}b^{-1}a, \\ e_2 &= b + a^3 + b^{-1} + a^{-3} + ab^{-1}a^{-1} + aba^{-1}, \\ e_3 &= b + a^3 + b^{-1} + a^{-1}ba + a^{-3} + a^{-1}b^{-1}a. \end{aligned}$$

each of which gives a [27,6,6]-code over F_2.

The oversight on this example as well as the correction to the GAP program were given by R. Budaibes [6]. It should be noted that this example has already been quoted in [8].

Example 3. Consider the group

$$G = \langle x, y, t_1;\ x^3 = y^3 = t^3 = 1,\ s = [x, y] = t \rangle.$$

This is an instance of a family of p-groups such that $G/\mathcal{Z}(G) \cong C_p \times C_p$, where $\mathcal{Z}(G)$ denotes the center of G and C_p the cyclic group of order p, that was characterized in [11] and whose use in Coding Theory was explored in in E. Taufer's PhD thesis [31].

We have that $|G| = 27$ and $G' = \{1, s, s^2\}$ and it is not difficult to show that, also in this case,

$$\mathbb{F}G \cong \mathbb{F} \oplus 4\mathbb{F}_4 \oplus M_3(\mathbb{F}_4),$$

and that the central idempotent which is a generator of the non commutative component is $e = 1 - \widehat{G'} = s + s^2$.

Then, $e_1 = (1 + x + x^2)(1 + y)e$ is an idempotent inside the non commutative component and $\{e_1, ye_1, y^2e_1, se_1, yse_1, y^2se_1\}$ is a basis of the ideal it generates.

This ideal contains 36 words whose weight is 12 and 27 words whose weight is 16. Thus, it is a *two-weight code*, and it has the best known weight for binary codes of this dimension, according to [17].

References

1. S. Assuena and C. Polcino Milies, Good Codes from Metacyclic Groups, *Contemporary Math.*, 727 (2019), 39–47.
2. G. K. Bakshi, M. Raka, A. Sharma, Idempotents Generators of Irreducible Cyclic Codes, *Proc. Int. Conf. Number Theory and Discrete Geometry*, Ramanujan Lecture Notes, **6**, (2008), 13–18, ed. R. Balasubramanian, S. G. Dani, P. M. Gruber, R. J. Hans-Gill.
3. S.D. Berman, On the theory of group codes, *Kibernetika*, **1**, (1967) 31–39.
4. S.D. Berman, Semisimple cyclic and abelian codes, *Kibernetika*, **1**, (1967) 17–23.
5. A. Bonisoli, Every equidistant linear code is a sequence of dual Hamming codes. *Ars Combin.* **18** (1984), 181-186.
6. R. Budaibes, *Idempotentes primitivos em Algebras de Grupo Finitas e Codigos Minimais*, PhD Thesis, Inst. de Matemática e Estatística, Univ. São Paulo, 2019.
7. Y. Cao, Y. Cao and F.W. Fu, Concatenated structure of left dihedral codes, *Finite Fields Appl.*, **38** (2016), 93-115.
8. Y. Cao , Y. Cao, F.W. Fu, and J. Gao, On a Class of Left Metacyclic Codes, *IEEE Trans. Inf. Theory*, **62** (2016) 6786-6799.
9. G. Chalom, R. Ferraz and C. Polcino Milies, Essential idempotents and simplex codes, *J. Algebra, Discrete Structures and Appl.*, **4**, 2 (2017), 181-188.
10. G. Chalom, R. Ferraz and C. Polcino Milies, Essential idempotents and codes of constant weight, *São Paulo J. of Math. Sci,*, 11(2) (2018), 253-260.
11. M. Cornelissen and C. Polcino Milies, Finitely Generated Groups G such that $G/\mathcal{Z}G \cong Cp \times Cp$, *Commun. Algebra*, **42**, 1 (2014), 378-388
12. F.S. Dutra, R. Ferraz and C. Polcino Milies, Semisimple Group Codes and Dihedral Codes, *Algebra and Discrete Math.*, **3** (2009), 28–48.
13. R. Ferraz, M. Guerreiro and C. Polcino Milies, G-equivalence in group algebras and minimal Abelian codes, *IEEE Trans. Information Theory,* **60**, 1, (2014), 252-260 .
14. R. Ferraz and C. Polcino Milies, Idempotents in group algebras and minimal Abelian codes, *Finite Fields and Appl.*, , 13 (2007), 382-393.
15. C. García Pillado, S. Gonzalez, C. Martínez, V. Markov, and A. Nechaev, Group codes over non-abelian groups, *J. Algebra Appl.*, **12**, (2013).
16. E.G. Goodaire, E. Jespers and C. Polcino Milies, *Alternative Loop Rings*, North Holland Math. Studies N. 184, Elsevier, Amsterdam, 1996.
17. M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*. Available online at http://www.codetables.de.
18. M. Jensen, The concatenational structure of cyclic and abelian codes, *IEEE Trans. Informormation Theory*, 31 (1985), 788-793.
19. A.V. Keralev and P. Sole, Error-correcting codes as ideals in group rings, *Contemporary Math.*, **273** (2001), 11-18.
20. P. Landrock and O. Manz, Classical codes as ideals in group rings. *Designs, Codes and Criptpgraphy*, **2** (1992), 273-285.
21. R. Lidl and H. Niederreiter, *Finite Fields*, Encycl. of Math. and its Appl, Vol. 20, Cambridge University Press, Cambridge, 1997.
22. F.J. MacWilliams, Binary codes which are ideals in the group algebra of an Abelian group, *Bell System Tech. J.*, 49 (1970), 987-1011.
23. F. Melo and C. Polcino Milies, On cyclic and Abelian codes, *IEEE Transactions on Information Theory*, **59**, 11 (2013), 7314-7319.
24. R.L. Miller, Minimal codes in Abelian group algebras, *J. Combinatorial Theory*, 26 (1979), 166-178.
25. Olteanu, G. ; Van Gelder, I. Construction of minimal non-Abelian left group codes, *Des. Codes Cryptogr.*, **75** (2015),359-373.
26. C. Polcino Milies, Group algebras and coding theory: a short survey, *Revista Integración*, **37**, 1 (2019), 153 - 166
27. C. Polcino Milies and S.K Sehgal, *An introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002, 371 pp.
28. E. Prange, Cyclic error-correcting codes in two symbols, AFCRC-TN-57-103, USAF, Cambridge Research Laboratories, New York (1957)
29. R.E. Sabin, Minimum distance bounds for Abelian codes, in *Applicable Algebra in Engeneering, Communications and Computing*, Springer, New York, 1992.
30. R.E. Sabin and S.J. Lomonaco, Metacyclic error-correcting codes, *Appl. Algebra Eng. Commun. Comput.* **6** (1995), 191-210.
31. E. Taufer, *Ideais em anéis de matrizes finitos e aplicações à Teoria de Códigos*, PhD Thesis, Inst. de Matemática e Estatística, Univ. São Paulo, 2018.
32. O.Broche, A. Herman, A. Konovalov, A. Olivieri, G. Olteanu, Á. del Río, I. Van Gelder: Wedderga - Wedderburn Decomposition of Group Algebras. Version 4.6.0 (2013). http://www.cs.st-andrews.ac.uk/alexk/wedderga, http://www.gap-system.org/Packages/wedderga.html.