Journal of Algebra and Its Applications
(2024) 2450060 (14 pages)

DOI: 10.1142/S0219498824500609

Nilpotent group codes

A. Duarte*

CMCC, Universidade Federal do ABC
R. Santa Adélia, 166 CEP 09210-170
Santo Andre, SP, Brasil
andre.luis@ufabc.edu.br

A. Pereira

Demat, Universidade Federal Rural do Rio de Janeiro
Seropédica, RJ, Brazil, CEP Seropédica - RJ, 23890-000
almp1980@ufrrj.br

C. Polcino Milies

Instituto de Matemática e Estatística
Universidade de São Paulo, Caixa Postal 66281
CEP 05315-970, São Paulo, Brazil
polcino@ime.usp.br

Received 22 April 2022
Revised 6 September 2022
Accepted 24 October 2022
Published 13 December 2022

Communicated by A. Leroy

In this paper, we consider essential idempotents in the finite semisimple group algebra of a nilpotent group, studying conditions for their existence and other implications. Also, we discuss conditions for nilpotent group codes to be equivalent to Abelian ones.

Keywords: Essential idempotents; group code; code equivalence; minimal nilpotent codes.

Mathematics Subject Classification 2020: 11T71

1. Introduction

In what follows, $\mathbb{F} = \mathbb{F}_q$ will always denote a field with q elements, where q is a power of a prime rational integer p, and G a finite group of order n. We shall always assume that $p \nmid n$ so the group algebra $\mathbb{F}G$ will be semisimple.

*Corresponding author.

A code $\mathcal{C} \subset \mathbb{F}^n$ is a left, right, or simply, a group code if there is a listing $G = \{g_1, g_2, \ldots, g_n\}$ of the elements of G such that the image of $\mathcal{C}$ under the map

$$(x_1, x_2, \ldots, x_n) \in \mathbb{F}^n \overset{\varphi}{\longmapsto} x_1 g_1 + x_2 g_2 + \cdots + x_n g_n \in \mathbb{F}G,$$

is a left, right or two-sided ideal of $\mathbb{F}G$, respectively. While working in the group algebra, we shall use indistinctly the terms *left*, *right or simply group code* and *left*, *right or two-sided-ideal* as synonyms, respectively.

Essential idempotents were introduced in [3], which they were used to understand relations among the special case of cyclic codes and Abelian codes in general. In particular, it was shown that minimal Abelian codes are equivalent to cyclic codes of the same length.

We consider the existence and properties of essential idempotents in finite semisimple group algebras of nilpotent groups and show that many of the properties of these idempotents in the Abelian context can be extended, in a natural way, to the present case.

In 1995, Sabin and Lomonaco [9] showed that every group code in a semisimple group algebra of a metacyclic group is equivalent, in a sense we will make precise below, to an Abelian code. In 2009, Bernal *et al.* [1] provided a criterion to decide when a linear code is permutation equivalent to a group code and they used this to show that if a finite group G can be written as a product of two Abelian subgroups, then every group code in the group algebra of G is permutation equivalent to an Abelian code. Nebe and Schäfer generalize in [6, Theorem 1] the criterion of Bernal *et al.* to monomial equivalence.

In Sec. 3, we study monomial and permutation equivalence of group codes and explore this concepts to give other criteria for group codes to be permutation equivalent to Abelian ones and monomial equivalent to cyclic codes.

Finally, in Sec. 4, we consider minimal nilpotent codes and show that, in many cases, these are permutation equivalent to Abelian codes.

2. Essential Idempotents

Let G be a finite group of order n and $\mathbb{F} = \mathbb{F}_q$ a field with q elements, where q is a power of a prime rational integer p such that $p \nmid n$. Recall that two idempotents $\alpha, \beta \in \mathbb{F}G$ are said to be *orthogonal* if $\alpha\beta = \beta\alpha = 0$. If a nonzero central idempotent $e \in \mathbb{F}G$ satisfies that: e has no decomposition into $\alpha + \beta$, where α, β are nonzero orthogonal idempotents in $\mathbb{F}G$, we say that e is a *primitive central idempotent of* $\mathbb{F}G$.

If $H \neq \{1\}$ is a subgroup of G such that $|H|$ is invertible in $\mathbb{F}$, then

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

is an idempotent of $\mathbb{F}G$.

If H is a normal subgroup of G, then $\widehat{H}$ is central and it is a sum of primitive central idempotents called its *constituents*.

Definition 2.1. A primitive central idempotent $e \in \mathbb{F}G$ such that $e \cdot \widehat{H} = 0$, for all $\{1\} \neq H \lhd G$, is an *essential idempotent.* A minimal ideal of $\mathbb{F}G$ is called an *essential ideal* if it is generated by an essential idempotent and *non-essential* otherwise.

We recall some results about essential idempotents in the case G is Abelian.

Proposition 2.2 ([3, Proposition 2.3]). *Let $e \in \mathbb{F}G$ be a primitive central idempotent. Then e is essential if and only if the map $\pi : G \to Ge$, given by $g \mapsto ge$, is a group isomorphism.*

As a direct consequence we have the following.

Theorem 2.3 ([3, Corollary 2.4]). *If A is an Abelian group and $\mathbb{F}A$ contains an essential idempotent, then A is cyclic.*

Corollary 2.4 ([3, Corollary 2.5]). *Let A be an Abelian non-cyclic group. Then, for any finite field $\mathbb{F}$, all the minimal codes of $\mathbb{F}A$ are repetition codes.*

We shall show that similar results hold when G is a nilpotent group.

Assume that G is a nilpotent group and let $\mathcal{F}$ be the family of all minimal normal subgroups of G. We define

$$e(G) = \prod_{K \in \mathcal{F}} (1 - \widehat{K}) \in \mathbb{F}G.$$

Lemma 2.5. *With the notation above, $e(G)$ is the sum of all the essential idempotents of $\mathbb{F}G$.*

Proof. Let e be a minimal central idempotent of $\mathbb{F}G$. If e is essential, we have

$$e \cdot e(G) = \prod_{K \in \mathcal{F}} e(1 - \widehat{K}) = \prod_{K \in \mathcal{F}} e = e.$$

On the other hand, if e is not essential, there exists a normal subgroup H in G such that $e\widehat{H} = e$. If K is a minimal normal subgroup of G contained in H we have

$$e(1 - \widehat{K}) = e\widehat{H}(1 - \widehat{K}) = e\widehat{H} - e\widehat{H}\widehat{K} = e\widehat{H} - e\widehat{H} = 0.$$

Consequently, $e \cdot e(G) = 0$.

Since a minimal central idempotent e is a constituent of a central idempotent f if and only if $ef = e$, the result follows. $\square$

Theorem 2.6. *Let e be a primitive central idempotent of $\mathbb{F}G$. Then, $e \in \mathbb{F}G$ is an essential idempotent if and only if $e \cdot e(G) = e$.*

Proof. Let $e \in \mathbb{F}G$ be an essential idempotent. Then, by Lemma 2.5, it follows that $e \cdot e(G) = e$.

Conversely, assume, by way of contradiction, that we have $e \cdot e(G) = e$ but e is non-essential. Then, there exists a normal subgroup H of G such that $e\widehat{H} = e$. Moreover, for any minimal normal subgroup $K_i \subset H$ we have $\widehat{H}(1 - \widehat{K_i}) = 0$. Hence, $\widehat{H} \cdot e(G) = 0$ and

$$e \cdot e(G) = (e \cdot \widehat{H}) \cdot e(G) = e \cdot (\widehat{H} \cdot e(G)) = 0,$$

a contradiction. □

Theorem 2.7. *$\mathbb{F}G$ contains essential idempotents if and only if the center of G is cyclic.*

Proof. If G is nilpotent, with cyclic center, of order $m = \prod_{i=1}^{r} p_i^{\alpha_i}$, then G is the product of its Sylow subgroups P_i, for all $i = 1, \ldots, r$, all of which have cyclic centers. For each index i there exists a unique minimal normal subgroup K_i of P_i. In this case

$$e(G) = (1 - \widehat{K_1}) \cdots (1 - \widehat{K_r}).$$

Since K_i is a minimal normal subgroup of G, we have $K_i \subset \mathcal{Z}(G)$, for all $i = 1, \ldots, r$. Therefore, K_i is also cyclic. Denote $K_i = \langle a_i \rangle$, where a_i is of order p_i. Then

$$e(G) = \left(1 - \frac{1 + a_1 + \cdots a_1^{p_1 - 1}}{p_1}\right) \cdots \left(1 - \frac{1 + a_r + \cdots a_r^{p_r - 1}}{p_r}\right).$$

Note that the coefficient of $a_1 \cdots a_r$ is $(-1)^r (1/p_1) \cdots (1/p_r) \neq 0$. We conclude that $e(G) \neq 0$. Therefore, its constituents are essential idempotents in $\mathbb{F}G$.

Conversely, when G is a finite nilpotent group with non-cyclic center, we have, by [5, Lemma 2.2], that $e(G) = 0$. Thus, $\mathbb{F}G$ contains no essential idempotents. □

Let $e \in \mathbb{F}G$ be a primitive central idempotent. We define

$$K_e = \{g \in G : ge = e\}. \tag{1}$$

Note that K_e is the kernel of the group homomorphism $\pi : G \to Ge$, given by $g \mapsto ge$. Thus

$$\frac{G}{K_e} \cong Ge.$$

The next lemma will be needed in what follows.

Lemma 2.8. *Let $e \in \mathbb{F}G$ be a primitive central idempotent and K a normal subgroup of G. Then $e \cdot \widehat{K} = e$ if and only if $K \subset K_e$. Furthermore, if $K \not\subset K_e$, then $e\widehat{K} = 0$.*

Proof. If $K \subset K_e$, then for any $k \in K$, we have $ek = e$, so $\widehat{K} = e$. Conversely, if $e\widehat{K} = e$, then $ke = k\widehat{K}e = \widehat{K}e = e$. Finally, if $K \not\subset K_e$, then $e \cdot \widehat{K} \neq e$. As e is a primitive central idempotent, it follows that $e \cdot \widehat{K} = 0$. □

The same techniques as in [3, Theorem 3.1] also give the following.

Theorem 2.9. *Let $e \neq \widehat{G}$ be a primitive central idempotent of $\mathbb{F}G$ and ψ the natural projection $\psi : \mathbb{F}G\widehat{K_e} \to \mathbb{F}[G/K_e]$, given by $g\widehat{K_e} \mapsto gK_e \in G/K_e$. Then, the element $\psi(e)$ is an essential idempotent of $\mathbb{F}[G/K_e]$.*

Corollary 2.10. *Let G be a nilpotent group and $e \neq \widehat{G}$ a primitive central idempotent of $\mathbb{F}G$. Then, the group G/K_e has cyclic center.*

3. Equivalence

Let $\mathbb{F}$ be a field and n a positive integer. Recall that an $\mathbb{F}$-linear transformation $T : \mathbb{F}^n \to \mathbb{F}^n$ is a *monomial transformation* if there exists a permutation $\sigma \in S_n$ and nonzero elements $k_1, k_2, \ldots, k_n$ in $\mathbb{F}$ such that

$$T(x_1, x_2, \ldots, x_n) = (k_1 x_{\sigma(1)}, k_2 x_{\sigma(2)}, \ldots, k_n x_{\sigma(n)}),$$

for all $(x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$.

Two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $\mathbb{F}^n$ are *monomially equivalent* if there exists a monomial transformation $T : \mathbb{F}^n \to \mathbb{F}^n$ such that $T(C_1) = C_2$.

In the particular case when $k_i = 1$, for all $1 \leq i \leq n$, the codes are said to be *permutation equivalent*.

All ideals in a semisimple group algebra $\mathbb{F}G$ are permutation equivalent to Abelian codes whenever G has an Abelian decomposition, i.e., when $G = AB$, where A and B are Abelian subgroups of G (see [1]). On the other hand, it was shown in [6] that there exists a nilpotent code which is not monomially equivalent (and thus also not permutation equivalent) to an Abelian code. In what follows, we give other conditions for group codes (not necessarily nilpotent) to be permutation equivalent to Abelian codes and, in the next section, we explore some consequences.

For a permutation $\sigma \in S_n$ and an element $\alpha = \sum_{i=1}^{n} x_i g_i \in \mathbb{F}G$ we denote

$$\sigma(\alpha) = \sum_{i=1}^{n} x_i g_{\sigma(i)}.$$

Given an ideal I in a group algebra $\mathbb{F}G$, define

$$P\mathrm{Aut}(I) = \{\sigma \in S_n \mid \sigma(\alpha) \in I,\ \forall\, \alpha \in I\}.$$

Let H and K be two subgroups of G. Recall that, G is said to be a *semidirect product* of H by K, denoted by $G = H \rtimes K$, if we have

(i) $G = HK = KH$,
(ii) $H \cap K = \{1\}$,
(iii) H normal in G.

Also, recall that $T \subset G$ is a left (or right) *transversal* of H in G if T is a complete set of representatives of left (or right) cosets of the subgroup H.

Theorem 3.1. *Let e be an idempotent of $\mathbb{F}G$ and $H = \{g \in G \mid eg = e\}$ a subgroup of G of order m. If $G = H \rtimes T$ is a semidirect product, then $\mathcal{C} = \mathbb{F}Ge$ is permutation* *equivalent to a left group code over $T \times C_m$, where C_m denotes the cyclic group of order m.*

Proof. Let $t = |T|$. We can choose a listing of G such that $T = \{g_1 = 1, g_{m+1}, g_{2m+1}, \ldots, g_{(t-1)m+1}\}$ and

$$\begin{aligned} H &= \{g_1, g_2, g_3, \ldots, g_m\}, \\ g_{m+1}H &= \{g_{m+1}, g_{m+2}, g_{m+3}, \ldots, g_{2m}\}, \\ g_{2m+1}H &= \{g_{2m+1}, g_{2m+2}, g_{2m+3}, \ldots, g_{3m}\}, \\ &\vdots \\ g_{(t-1)m+1}H &= \{g_{(t-1)m+1}, g_{(t-1)m+2}, g_{(t-1)m+3}, \ldots, g_{tm}\}, \end{aligned}$$

are the left cosets of H in G. Denote $I_T = \{1, m+1, 2m+1, \ldots, (t-1)m+1\}$ the set of indices of T.

Note that $e\widehat{H} = e$, so we have $\mathcal{C} = \mathbb{F}Ge \subset \mathbb{F}G\widehat{H}$. As we know that $\{\widehat{H}, g_{m+1}\widehat{H}, g_{2m+1}\widehat{H}, \ldots, g_{(t-1)m+1}\widehat{H}\}$ is a basis of $\mathbb{F}G\widehat{H}$ over $\mathbb{F}$ (see [8]), if we choose a basis $\{v_1, v_2, \ldots, v_d\}$ of $\mathcal{C}$ over $\mathbb{F}$, we can write

$$v_i = \sum_{j \in I_T} a_{ij} g_j \widehat{H},$$

with $a_{ij} \in \mathbb{F}$, for all $1 \le i \le d$ and $j \in I_T$.

Set $\sigma = (1, 2, 3, \ldots, m)(m+1, \ldots, 2m) \ldots (m(t-1)+1, \ldots, mt) \in S_n$. Since $\sigma(v_i) = v_i$, for all $1 \le i \le d$, it follows that $\sigma \in P\mathrm{Aut}(\mathcal{C})$ and it has order m.

Note that for every $x \in \{1, 2, 3, \ldots, n\}$ there are unique $j \in I_T$ and $0 \le \ell < m$ such that $x = j + \ell$. For each $g_i \in T$ and $x = j + \ell$ with $j \in I_T$ and $0 \le \ell < m$, we compute $g_i g_j = g_k$ and define a permutation $\sigma_i \in S_n$ by

$$\sigma_i(x) = k + \ell.$$

Since $\mathcal{C}$ is a left ideal of $\mathbb{F}G$ and $\tilde{T} = \{\sigma_i \,|\, i \in I_T\}$ is a group, we have $\tilde{T}$ is a subgroup of $\mathrm{PAut}(\mathcal{C})$.

We claim first that $\tilde{G} = \tilde{T}\langle\sigma\rangle$ is a direct product. For each $j \in I_T$ and $0 \le \ell < m$, we have

$$\sigma_i\sigma(j+\ell) = \begin{cases} \sigma_i(j+\ell+1), & \text{if } \ell < m-1 \\ \sigma_i(j), & \text{if } \ell = m-1 \end{cases} = \begin{cases} k+\ell+1 & \text{if } \ell < m-1, \\ k & \text{if } \ell = m-1, \end{cases}$$

whenever $g_i g_j = g_k$. On the other hand,

$$\sigma\sigma_i(j+\ell) = \sigma(k+\ell) = \begin{cases} k+\ell+1, & \text{if } \ell < m-1, \\ k, & \text{if } \ell = m-1. \end{cases}$$

It follows that $\sigma\sigma_i = \sigma_i\sigma$ for any $i \in I_T$.

If $\gamma \in \tilde{T} \cap \langle\sigma\rangle$, then $\gamma = \sigma_i = \sigma^\mu$ for some integer $0 \leq \mu < m$. However $\sigma^\mu(1) \in \{1, 2, 3, \ldots, m\}$ and $\sigma_i(1) = i \in I_T$. We conclude that $i = 1$ which implies that $\sigma_i = \gamma$ is the identity. Then $\tilde{G} = \tilde{T} \times \langle\sigma\rangle$ is a direct product. As $\tilde{T} \cong T$ and $\langle\sigma\rangle$ is cyclic of order m, we have $|\tilde{G}| = tm = n$.

Now we claim that $\tilde{G}$ is a regular subgroup of S_n. Let $x \in \{1, 2, 3, \ldots, n\}$ and $\gamma \in \tilde{G}$. If $\gamma = \sigma_i\sigma^\mu$ ($i \in I_T$, $\mu < m$) and $x = j + \ell$, with j and ℓ as before, then

$$\gamma(x) = \sigma_i(\sigma^\mu(j+\ell)) = \begin{cases} \sigma_i(j+\ell+\mu), & \text{if } \ell+\mu < m, \\ \sigma_i(j+r), & \text{if } \ell+\mu \geq m, \end{cases}$$

where r is the remainder when $\ell + \mu$ is divided by m. This implies that

$$\gamma(x) = \begin{cases} k+\ell+\mu, & \text{if } \ell+\mu < m, \\ k+r, & \text{if } \ell+\mu \geq m, \end{cases}$$

where $g_i g_j = g_k$. If $\gamma(x) = x$ then either $j+\ell = k+\ell+\mu$, if $\ell+\mu < m$ or $j+\ell = k+r$, if $\ell+\mu \geq m$. Since $j, k \in I_T$ are indices of the transversal T of H in G, we conclude that $j = k$ implying that γ is the identity. In the second case, as above $j = k$, so $j + \ell = j + r$ with $\ell + \mu \geq m$. Using the division algorithm, we have $\ell + \mu = m + r$, which implies $m = \mu$, a contradiction.

Finally, as $T \times C_m$ is isomorphic to a regular subgroup $\tilde{G}$ of $P\mathrm{Aut}(\mathcal{C})$, by [1, Theorem 2.1], we conclude that $\mathcal{C}$ is equivalent to a left group code over $T \times C_m$. □

Example 3.2. The group

$$G = \langle a, b, c \,|\, a^5 = b^7 = c^3 = 1, ab = ba, ac = ca, = 1, cbc^{-1} = b^4\rangle,$$

is metacyclic, and so is metabelian since every metacyclic group is metabelian. Olteanu and Van Gelder, in [7, Example 5.2], considered the group algebra $\mathbb{F}_2G$ and exibited a best $[105, 3, 60]$-code in the group above, and stated "*it is unclear whether this code can be realized as an Abelian code or not.*"

By [7, Theorem 3.1] and the algorithm exhibited, the idempotent that generates the ideal considered is

$$e = (1 + b + b^2 + b^4)\widehat{\langle a, c\rangle}.$$

The subgroup $T = \langle b\rangle$ is a left transversal of $H = \{g \in G \,|\, eg = e\} = \langle a, c\rangle$ in G. By Theorem 3.1 we conclude that this group code over G is also a group code over C_{105} which implies that this code is, in particular, Abelian.

The example above suggests the following result.

Corollary 3.3. *Let e be an idempotent of $\mathbb{F}G$ and $H = \{g \in G \,|\, eg = e\}$ a subgroup of G of order m. If $G = H \rtimes \tau$ is a semidirect product with τ Abelian, then $\mathcal{C} = \mathbb{F}Ge$ is permutation equivalent to an Abelian code.*

It was shown in [3] that every minimal Abelian code is permutation equivalent to a minimal cyclic code. In what follows, we give a condition for ideals of an arbitrary finite semisimple group algebra to be monomially equivalent to cyclic codes. We need some technical results.

Lemma 3.4. *Let I be an ideal of the group algebra $\mathbb{F}G$ of dimension t. If I contains a basis $\{u_i\}_{i=1}^t$ whose elements have disjoint supports, then there exist elements $g_1, \ldots, g_t \in G$ and some $1 \leq i \leq t$ such that $\{g_1u_1, \ldots, g_tu_1\}$ is also a basis of I and its elements have disjoint supports.*

Proof. We may assume, without loss of generality, that the basis has been ordered in such a way so that $\mathrm{supp}(u_1)$ has a minimal number of elements.

Also, since for every $g \in G$, the set $\{gu_1, \ldots, gu_t\}$ is a basis of I, and clearly its elements have disjoint supports, we may also assume that $1 \in \mathrm{supp}(u_1)$.

Set $g_1 = 1$, and choose an element $g_i \in \mathrm{supp}(u_i)$, where $2 \leq i \leq t$. Since $g_iu_1 \in I$ we can write

$$g_iu_1 = \sum_{j=1}^{t} a_ju_j, \quad 1 \leq i \leq t.$$

As the elements of the basis have disjoint supports, for each index i, we have

$$\mathrm{supp}(g_iu_1) = \bigcup_{a_j \neq 0} \mathrm{supp}(u_j).$$

But $|\mathrm{supp}(g_iu_1)| = |\mathrm{supp}(u_1)|$ is minimal and $g_i \in \mathrm{supp}(u_1) \cap \mathrm{supp}(u_i)$; so $\mathrm{supp}(g_1u_1) = \mathrm{supp}(u_i)$, and thus $g_iu_1 = a_iu_i$.

Consequently, it follows immediately that $\{g_1u_1, \ldots, g_tu_1\}$ is a basis of I and clearly its elements have disjoint supports. $\square$

For an element $\sigma \in S_n$ we consider the permutation matrix $[\sigma] = (\sigma_{ij}) \in M_n(\mathbb{F})$ defined by

$$\sigma_{ij} = \begin{cases} 1, & \text{if } j = \sigma(i) \\ 0, & \text{otherwise.} \end{cases}$$

The proof of the next result is a straightforward computation.

Lemma 3.5. *Let $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ and $\pi \in S_n$. Then*

$$[\pi] \cdot \mathrm{Diag}(\lambda_1, \ldots, \lambda_n) = \mathrm{Diag}(\lambda_{\pi(1)}, \ldots, \lambda_{\pi(n)}) \cdot [\pi].$$

Theorem 3.6. *Let G be a finite group of order n and let $\mathbb{F}$ be a finite field such that char$(\mathbb{F}) \not| |G|$. Suppose that $I \neq (0)$ is a code in $\mathbb{F}G$ with a basis whose elements have disjoint supports. Then I is monomially equivalent to a cyclic code.*

Proof. Let $\{u_i\}_{i=1}^t$ be a basis of I whose elements have disjoint supports. By Lemma 3.4, the code I contains a basis of the form $\{g_1u_1, \ldots, g_tu_1\}$.

Since $I \neq (0)$ there exists $0 \neq \alpha \in I$. Also, for any arbitrary element $g \in \mathrm{supp}(\alpha)$ we have $h \in \mathrm{supp}(hg^{-1}\alpha)$, for all $h \in G$. Since $hg^{-1}\alpha \in I$, it follows that $G = \cup_{i=1}^{t}\mathrm{supp}(g_i u_1)$.

So, the subsets $\mathrm{supp}(g_i u_1)$, for all $1 \leq i \leq t$, form a partition of G, since they are disjoint, and clearly all these sets have cardinality n/t. Then we enumerate the elements of G so that we can write

$$\begin{aligned}
\mathrm{supp}(g_1 u_1) &= \{g_1, \quad g_{t+1}, \quad g_{2t+1}, \quad \ldots, \quad g_{(m-1)t+1}\},\\
\mathrm{supp}(g_2 u_1) &= \{g_2, \quad g_{t+2}, \quad g_{2t+2}, \quad \ldots, \quad g_{(m-1)t+2}\},\\
&\vdots\\
\mathrm{supp}(g_t u_1) &= \{g_t, \quad g_{2t}, \quad g_{3t}, \quad \ldots, \quad g_{mt}\}
\end{aligned}$$

and thus $g_i u_1 = \sum_{j=0}^{m-1} a_{j+1} g_{jt+i}$, with $a_i \in \mathbb{F}$.

As we did before, we can define an action of S_n on G by $\tau(g_i) = g_{\tau(i)}$, for all $\tau \in S_n$, and extend it linearly to $\mathbb{F}G$. Take the n-cycle $\sigma = (1, 2, \ldots, n) \in S_n$. Set

$$M = \left(\begin{array}{ccccc|ccccc|c|ccccc}
a_m^{-1}a_1 & 0 & 0 & \cdots & 0 & & & & & & & & & & & \\
0 & 1 & 0 & \cdots & 0 & & & & & & & & & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & & & & & & & & & & & \\
0 & 0 & 0 & \cdots & 1 & & & & & & & & & & & \\
\hline
 & & & & & a_2^{-1}a_3 & 0 & 0 & \cdots & 0 & & & & & & \\
 & & & & & 0 & 1 & 0 & \cdots & 0 & & & & & & \\
 & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & \\
 & & & & & 0 & 0 & 0 & \cdots & 1 & & & & & & \\
\hline
 & & & & & & & & & & \ddots & & & & & \\
\hline
 & & & & & & & & & & & a_{m-1}^{-1}a_m & 0 & 0 & \cdots & 0 \\
 & & & & & & & & & & & 0 & 1 & 0 & \cdots & 0 \\
 & & & & & & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots \\
 & & & & & & & & & & & 0 & 0 & 0 & \cdots & 1
\end{array}\right).$$

As M is a diagonal matrix, we can identify $M \cdot [\sigma] \in GL_n(\mathbb{F})$ with the element $(\lambda_1, \ldots, \lambda_m).\sigma$ in the group $(\mathbb{F})^n \rtimes S_n$, where $(\lambda_1, \ldots, \lambda_m)$ is the diagonal of M.

Since $(M \cdot [\sigma]^{-1})g_i u_1 = g_{i+1}u_1$, where $1 \leq i \leq t-1$, and $(M \cdot [\sigma]^{-1})g_t u_1 = u_1$, we have $M \cdot [\sigma]^{-1}(I) = I$ which implies that $M \cdot [\sigma] \in M\mathrm{Aut}(I)$.

We claim that $M \cdot [\sigma]^{-1}$ has order n. Note that if $M = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$, then by Lemma 3.5, we have

$$[\sigma]^{-1} \cdot M = \mathrm{Diag}(\lambda_{\sigma^{-1}(1)}, \ldots, \lambda_{\sigma^{-1}(n)}) \cdot [\sigma]^{-1}.$$

Now, $(M[\sigma]^{-1})^n = \prod_{k=0}^{n-1} \mathrm{Diag}(\lambda_{\sigma^{-k}(1)}, \dots, \lambda_{\sigma^{-k}(n)})[\sigma]^{-n}$ and the ij-entry is

$$\begin{cases} \displaystyle\prod_{k=0}^{n-1} \lambda_{\sigma^{-k}(i)}, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$$

Since $\prod_{k=0}^{n-1} \lambda_{\sigma^{-k}(i)} = (a_m^{-1}a_1)(a_1^{-1}a_2)\cdots(a_{m-1}^{-1}a_m) = 1$ for all $1 \le i \le n$, it follows that $(M[\sigma]^{-1})^n$ is the identity matrix. As n is the order of $[\sigma]$, we conclude that $M[\sigma]^{-1}$ has order n.

Let $H = \langle M \cdot \sigma\rangle \subseteq M\mathrm{Aut}(C)$ and $\phi : (\mathbb{F})^n \rtimes S_n \to S_n$, where $\phi(A\cdot\pi) = \pi$. Since every n-cycle generates a transitive group, we get $\phi(H) = \langle\sigma\rangle$ is a regular subgroup of S_n. By [6, Theorem 1], we conclude that I is monomially equivalent to a cyclic code. □

In what follows, we shall denote by G_1 and G_2 two groups of the same order and by K_1 and K_2 normal subgroups of them, such that $G_1/K_1 \cong G_2/K_2$. Hence

$$\mathbb{F}[G_1/K_1] \cong \mathbb{F}[G_2/K_2]$$

and

$$\mathbb{F}G_1 \cdot \widehat{K_1} \cong \mathbb{F}[G_1/K_1] \cong \mathbb{F}[G_2/K_2] \cong \mathbb{F}G_2\widehat{K_2}.$$

Denote by $\mu : \mathbb{F}[G_1/K_1] \to \mathbb{F}[G_2/K_2]$ the linear extension of the isomorphism $G_1/K_1 \cong G_2/K_2$ and by $\theta : \mathbb{F}G_1 \cdot \widehat{K_1} \to \mathbb{F}G_2\widehat{K_2}$ isomorphism above.

Let $\mathcal{T}_1 = \{g_1, \dots, g_t\}$ be a transversal of K_1 in G_1. Choose any $\eta_i \in G_2$ such that $\eta_i K_2 = \mu(g_i K_1)$. Then $\mathcal{T}_2 = \{\eta_1, \dots, \eta_t\}$ is a transversal of K_2 in G_2. Suppose that $f : K_1 \to K_2$ is a bijection map. We can define a map $\eta : G_1 \to G_2$ by $\eta(g_i k) = \eta_i f(k)$, for all $g_i \in \mathcal{T}_1$ and $k \in K_1$.

If $\alpha \in \mathbb{F}G_1 \cdot \widehat{K_1}$, then we can write

$$\alpha = \sum_{i=0}^{t-1} \alpha_i g_i \widehat{K_1},$$

implying that

$$\theta(\alpha) = \sum_{i=1}^{t} \alpha_i \eta_i \widehat{K_2} = \sum_{i=1}^{t} \alpha_i \eta_i \left(\frac{1}{|K_2|} \sum_{k' \in K_2} k' \right) = \frac{1}{|K_1|} \sum_{i=1}^{t} \alpha_i \eta_i \left(\sum_{k \in K_1} f(k) \right).$$

By comparing the expressions for α and $\theta(\alpha)$, we see that the linear extension $\overline{\eta} : \mathbb{F}G_1 \to \mathbb{F}G_2$ of η coincides with θ in $\mathbb{F}G_1.\widehat{K_1}$.

Theorem 3.7. *Let K_1 and K_2 and G_1 and G_2, be as above. If e_1 is an idempotent of $\mathbb{F}G_1$ where $e_1 \in \mathbb{F}G_1\widehat{K_1}$, then $\mathbb{F}G_1 e_1$ is permutation equivalent to $\mathbb{F}G_2 e_2$, with $e_2 = \theta(e_1)$.*

Proof. Since $\mathbb{F}G_1 e_1 \subset \mathbb{F}G_1\widehat{K_1}$, we have

$$\theta(\mathbb{F}G_1 \cdot e_1) = \theta(\mathbb{F}G_1\widehat{K_1})\theta(e_1) = \mathbb{F}G_2\widehat{K_2} \cdot e_2 = \mathbb{F}G_2 \cdot e_2.$$ □

4. Minimal Nilpotent Codes

In this section, we shall prove that every primitive central idempotent which is not essential generates a code which is permutation equivalent to an Abelian code. Then we shall determine a condition on nilpotent groups so that every minimal nilpotent code is permutation equivalent to an Abelian code.

It was proved in [3] that every minimal Abelian code is permutation equivalent to a cyclic code. The idea of the proof is as follows. For a primitive idempotent e of the Abelian group algebra $\mathbb{F}A$, consider a cyclic group C of the same order as A and a subgroup H of C such that $G/K_e \cong C/H$.

To use a similar argument in the case of nilpotent groups, we would need that, for any primitive central idempotent $e \in \mathbb{F}G$, there should exist a nilpotent group N, with cyclic center, and a subgroup of H of N such that $G/K_e \cong N/H$. However, as shown in the next example, this is not always the case.

Example 4.1. Consider the group $G = C_4 \rtimes C_4$ with presentation

$$G = \langle a, b \,|\, a^4 = b^4 = 1, bab^{-1} = a^{-1} \rangle$$

and center $\mathcal{Z}(G) = \{1, a^2, b^2, a^2b^2\}$. The element $e = 2 + 5b^2 + 5a^2 + 2a^2b^2 \in \mathbb{F}_7G$ is a central idempotent. Notice that

$$a^ib^je = \begin{cases} a^{i \bmod 2}\, b^{j \bmod 2} e, & \text{if } i, j = 0, 1, \\ 6a^{i \bmod 2}\, b^{j \bmod 2}\, e, & \text{if } i = 0, 1 \text{ and } j = 2, 3, \\ 6a^{i \bmod 2}\, b^{j \bmod 2}\, e, & \text{if } i = 2, 3 \text{ and } j = 0, 1, \\ a^{i \bmod 2}\, b^{j \bmod 2}\, e, & \text{if } i, j = 2, 3. \end{cases}$$

Then, $\mathbb{F}_7G$ is generated by the set $\mathcal{B} = \{e, ae, be, abe\}$ as an $\mathbb{F}$-vector space. Since e, ae, be and abe have disjoint supports, we have $\mathcal{B}$ as a basis of $\mathbb{F}_7G$. Due to

$$(ae)(be) = 2ab + 5a^3b + 5ab^3 + 2a^3b^3 \neq 2 + 5a^2 + 5b^2 + 2a^3b = (be)(ae)$$

it follows that $\mathbb{F}_7Ge \cong M_2(\mathbb{F}_7)$ implying that e is a primitive central idempotent. Note that $K_e = \{g \in G | ge = e\} = \{1, a^2b^2\}$ and $G/K_e \cong Q_8$ the quaternion group of order 8. By [2] there exist six groups of order 16 with cyclic center:

$$\begin{aligned} C_{16} &= \langle g \rangle; \\ D_8 &= \langle a, b \,|\, a^8 = b^2 = 1, bab = a^{-1} \rangle; \\ Q_{16} &= \langle a, b \,|\, a^8 = 1, b^2 = a^4, bab^{-1} = a^{-1} \rangle; \\ SD_{16} &= \langle a, b \,|\, a^8 = b^2 = 1, bab = a^3 \rangle; \\ M_4(2) &= \langle a, b \,|\, a^8 = b^2 = 1, bab = a^5 \rangle; \\ C_4 \circ D_4 &= \langle a, b, c \,|\, a^4 = c^2 = 1, b^2 = a^2, ab = ba, ac = ca, cbc = a^2b \rangle. \end{aligned}$$

It follows from [8, Corollary 1.5.19] that there exists a unique minimal normal subgroup in each of these subgroups. The correspondent factor groups are isomorphic to

$$C_8,\ D_4,\ D_4,\ D_4,\ C_2 \times C_4,\ C_2^3,$$

respectively. Then, it is not possible to find a group N of order 16 with cyclic center and a subgroup H for which $G/K_e \cong N/H$. However, since the elements of $\mathcal{B}$ have disjoint supports of the same cardinality, by Theorem 3.6, we can conclude that $\mathbb{F}Ge$ is monomially equivalent to a cyclic code.

As the example above suggests, it is of interest to determine when minimal nilpotent codes are equivalent to Abelian codes. The following result gives an answer to this question.

Theorem 4.2. *Let $e \in \mathbb{F}G$ be a primitive central idempotent which is not essential. If $G = H \rtimes A$, where $H = \{g \in G \,|\, eg = e\}$ and A is Abelian, then $\mathbb{F}Ge$ is permutation equivalent to an Abelian code.*

Proof. Since e is non-essential, it follows that $K_e \neq \{1\}$. As e is central, we have $H = K_e$. By Theorem 3.1, we get $\mathbb{F}Ge$ is permutation equivalent to an Abelian code. $\square$

As an immediate consequence, we have the following.

Corollary 4.3. *If G is a finite nilpotent group which has a non-cyclic center and $G = K_e \rtimes A_e$, where A_e is Abelian, for all primitive central idempotent $e \in \mathbb{F}G$, then every minimal code in $\mathbb{F}G$ is permutation equivalent to an Abelian code.*

We shall see that, at least under some restrictive hypotheses, all nilpotent codes are permutation equivalent to cyclic codes.

For an element $g \in G$ we denote by C_g its conjugacy class and by C_g^+ the sum of all elements in the class C_g. Moreover, for an element $g \in G$ we denote by g^+ the sum of all distinct powers of g.

We need the following.

Lemma 4.4 ([5, Lemma 2.3]). *Let G be a finite group and $g \in G$. If $g^{-1}C_g \cap \mathcal{Z}(G) \neq \{1\}$, then G contains a central element z of prime order so that $C_g^+ = C_g^+\widehat{z}$.*

Let G be a finite nilpotent group and let $e \in \mathbb{F}G$ be a primitive central idempotent. Let H be the subgroup of G such that $H/K_e = \mathcal{Z}(G/K_e)$. We already know, from Corollary 2.10, that H/K_e is cyclic.

Lemma 4.5. *With $e \in \mathbb{F}G$ as above, if G/K_e is nilpotent of class $c \leq 2$, then* $\mathrm{supp}(e) \subset H$.

Proof. If $c = 1$, then G/K_e is cyclic and we are done. Now, assume that $c = 2$. Let $\mathcal{C}$ be a full set of representatives of the conjugacy classes of G/K_e and $\psi : \mathbb{F}G \to$

$\mathbb{F}(G/K_e)$, the linear extension of the natural projection $G \to G/K_e$. Denote by $\overline{e}$ the image of e by ψ.

Theorem 2.9 shows that $\bar{e}$ is an essential idempotent and thus, in particular, a primitive central idempotent. Since $H/K_e = \mathcal{Z}(G/K_e)$, we can write

$$\overline{e} = \sum_{\bar{g} \in H/K_e} \beta_g \bar{g} + \sum_{\bar{g} \in \mathcal{C} \setminus (H/K_e)} \beta_g C_{\bar{g}}^{+},$$

where $C_{\bar{g}}$ denotes the conjugacy class of $\bar{g} \in G/K_e$ and $\beta_g \in \mathbb{F}$ for $\bar{g} \in \mathcal{C}$.

Again, as $H/K_e = \mathcal{Z}(G/K_e) \neq G/K_e$, we have, for any $\bar{g} \in \mathcal{C} \setminus (H/K_e)$, an element $\bar{x} \in G/K_e$ such that $\bar{1} \neq [\bar{g}, \bar{x}] \in \bar{g}^{-1} C_{\bar{g}} \cap \mathcal{Z}(G/K_e)$. So, by Lemma 4.4, there exists $\omega_g \in \mathcal{Z}(G/K_e)$ of prime order such that $C_{\bar{g}}^{+} = C_{\bar{g}}^{+} \cdot \widehat{\omega_g}$. Then, we can rewrite $\overline{e}$ as

$$\bar{e} = \sum_{\bar{g} \in H/K_e} \beta_g \bar{g} + \sum_{\bar{g} \in \mathcal{C} \setminus (H/K_e)} \beta_g C_{\bar{g}}^{+} \widehat{\omega_g}.$$

Since $\overline{e} \in \mathbb{F}(G/K_e)$ is an essential idempotent, it follows from Theorem 2.6 that $\overline{e} \cdot e(G/K_e) = \overline{e}$. As every minimal normal subgroup of G/K_e is central, we have $e(G/K_e) \in \mathbb{F}(H/K_e)$. Then

$$\begin{aligned} \bar{e} = \bar{e} \cdot e(G/K_e) &= \sum_{\bar{g} \in H/K_e} \beta_g \bar{g} \cdot e(G/K_e) + \sum_{\bar{g} \in \mathcal{C} \setminus (H/K_e)} \beta_g C_{\bar{g}}^{+} \widehat{\omega_g} \cdot e(G/K_e) \\ &= \sum_{\bar{g} \in H/K_e} \beta_g \bar{g} \cdot e(G/K_e), \end{aligned}$$

because $\widehat{\omega_g} \cdot e(G/K_e) = 0$, for all $\bar{g} \in \mathcal{C} \setminus (H/K_e)$. By the last formula we conclude that $\overline{e} \in \mathbb{F}(H/K_e)$. We can write $e = \alpha + \beta$, where $\mathrm{supp}(\alpha) \subset H$ and $\mathrm{supp}(\beta) \subset G \setminus H$. Then, $\overline{e} = \overline{\alpha} + \overline{\beta}$, which implies, by comparing supports, that $\overline{\beta} = \overline{0}$. As the kernel of $\psi : \mathbb{F}G \to \mathbb{F}(G/K_e)$ is $\mathbb{F}G(1 - \widehat{K_e})$, we get $\beta \in \mathbb{F}G(1 - \widehat{K_e})$ and hence $\beta \widehat{K_e} = 0$. Since $e\widehat{K_e} = e$, it follows that $\alpha + \beta = \alpha \widehat{K_e} \in \mathbb{F}H$. Consequently, $\beta = 0$. $\square$

We are now ready to prove the following.

Theorem 4.6. *Let G be a finite nilpotent group of order n and $e \in \mathbb{F}G$ be a primitive central idempotent such that G/K_e is of class $c \leq 2$. Then every code $\mathcal{C} = \mathbb{F}Ge$ is permutation equivalent to a cyclic code C' in $\mathbb{F}C_n$.*

Proof. By Lemma 4.5, we have $\mathrm{supp}(e) \subset H$. Then $e \in \mathbb{F}H$ and H/K_e is cyclic. By Theorem 3.7, we have $\mathbb{F}He$ is permutation equivalent to a code in $\mathbb{F}C_m e'$, where $m = |H|$ and e' is an idempotent.

Let $\psi : \mathbb{F}He \to \mathbb{F}C_m e'$ be a permutation equivalence and $\tau_1 = \{g_1, \ldots, g_t\}$ a transversal of H in G. Let C_n be a cyclic group of order $n = |G|$ and C_m be its unique subgroup of order m. Set $\tau_2 = \{h_1, \ldots, h_t\}$ a transversal of C_m in C_n.

We can now define a permutation equivalence $\tilde{\psi} : \mathbb{F}Ge \to \mathbb{F}C_n e'$ by

$$\tilde{\psi}(g\alpha) = h_i \psi(h\alpha),$$

for all $g = g_i h$, $h \in H$, $\alpha \in \mathbb{F}He$. □

Acknowledgments

The first author was partially supported by CAPES 001 and the third author by FAPESP, proc. 2015/09162-9. The authors are very grateful to the referee and the editor for their valuable comments and suggestions to improve the quality of this paper. Research support by CAPES and FAPESP, Brazil, is gratefully acknowledged.

References

[1] J. J. Bernal, A. del Río and J. J. Simón, An intrinsical description of group codes, *Des. Codes Cryptogr.* **51**(3) (2009) 289–300.
[2] L. Esteban, R. Tapia-Rojo, A. Sancho and L. J. Boya, Groups of order less than 32, revisited, *Rev. Real Acad. Ciencias Zaragoza*, **66** (2011) 63–104.
[3] C. Gladys, R. A. Ferraz and C. Polcino Milies, Essential idempotents and simplex codes, *Algebra Comb. Discrete Appl.* **4**(2) (2016) 181–188.
[4] The GAP Group, GAP Groups, Algorithms, and Programming, Version 4.5.6 (2012), http://www.gap-system.org.
[5] E. Jespers, G. Leal and A. Paques, Central idempotents in the rational group algebra of a finite nilpotent group, *J. Algebra Appl.* **2** (2003) 57–62.
[6] G. Nebe and A. Schäfer, A nilpotent non Abelian group code, *Algebra Discrete Math.* **18**(2) (2014) 268–273.
[7] G. Olteanu and I. Van Gelder, Construction of minimal non-Abelian left group codes, *Designs Codes Cryptogr.* **75** (2015) 359–373.
[8] C. Polcino Milies and S. K. Sehgal, *An Introduction to Group Rings* (Kluwer Academic Publishers, Dordrecht, 2002), xii+371 pp.
[9] R. E. Sabin and S. J. Lomonaco, Metacyclic error-correcting codes, *Appl. Algebra Eng. Commun. Comput.* **6**(3) (1995) 191–210.