Essential idempotents and Nilpotent Group Codes

César Polcino Milies

Universidade de São Paulo

Cyclic Codes

Definition

A linear code $\mathcal{C} \subset \mathbb{F}^n$ is called a **cyclic code** if for every vector $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ in the code, we have that also the vector $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is in the code.

Definition

A linear code $\mathcal{C} \subset \mathbb{F}^n$ is called a **cyclic code** if for every vector $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ in the code, we have that also the vector $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is in the code.

Notice that the definition implies that if $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ is in the code, then all the vectors obtained from this one by a cyclic permutation of its coordinates are also in the code.

Let

$$\mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle};$$

We shall denote by $[f]$ the class of the polynomial $f \in \mathbb{F}[X]$ in $\mathcal{R}_n$.

Let

$$\mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle};$$

We shall denote by $[f]$ the class of the polynomial $f \in \mathbb{F}[X]$ in $\mathcal{R}_n$. The mapping:

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

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in \mathbb{F}[X] \quad \mapsto \quad [a_0 + a_1 X + \ldots + a_{n-2} X^{n-2} + a_{n-1} X^{n-1}].$$

Let

$$\mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1\rangle};$$

We shall denote by $[f]$ the class of the polynomial $f \in \mathbb{F}[X]$ in $\mathcal{R}_n$. The mapping:

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

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in \mathbb{F}[X] \quad \mapsto \quad [a_0 + a_1 X + \ldots + a_{n-2}X^{n-2} + a_{n-1}X^{n-1}].$$

φ is an isomorphism of $\mathbb{F}$-vector spaces. Hence *A code $\mathcal{C} \subset \mathbb{F}^n$ is cyclic if and only if $\varphi(\mathcal{C})$ is an ideal of $\mathcal{R}_n$.*

In the case when $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ is a cyclic group of order n, and $\mathbb{F}$ is a field, the elements of $\mathbb{F}C_n$ are of the form:

$$\alpha = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_{n-1} a^{n-1}.$$

In the case when $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ is a cyclic group of order n, and $\mathbb{F}$ is a field, the elements of $\mathbb{F}C_n$ are of the form:

$$\alpha = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_{n-1} a^{n-1}.$$

It is easy to show that

$$\mathbb{F}C_n \;\cong\; \mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle};$$

In the case when $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \dots, a^{n-1}\}$ is a cyclic group of order n, and $\mathbb{F}$ is a field, the elements of $\mathbb{F}C_n$ are of the form:

$$\alpha = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_{n-1} a^{n-1}.$$

It is easy to show that

$$\mathbb{F}C_n \ \cong \ \mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle};$$

Hence, to study cyclic codes is equivalent to study ideals of a group algebra of the form $\mathbb{F}C_n$.

Group Codes

Definition

A **group code** is an ideal of a finite group algebra.

Definition

A **group code** is an ideal of a finite group algebra.

S.D. Berman 1967.

F.J. MacWilliams 1970.

Definition

A **group code** is an ideal of a finite group algebra.

S.D. Berman 1967.
F.J. MacWilliams 1970.

In what follows, we shall always assume that $char(K) \not| \, |G|$ so all group algebras considered here will be semisimple and thus, all ideals of $\mathbb{F}G$ are of the form $I = \mathbb{F}Ge$, where $e \in \mathbb{F}G$ is an idempotent element.

Idempotents from subgroups

Let H be a subgroup of a finite group G and let $\mathbb{F}$ be a field such that $car(\mathbb{F}) \not| \, |G|$. The element

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

is an idempotent of the group algebra $\mathbb{F}G$, called the **idempotent determined by** H.

Idempotents from subgroups

Let H be a subgroup of a finite group G and let $\mathbb{F}$ be a field such that $car(\mathbb{F}) \not| \, |G|$. The element

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

is an idempotent of the group algebra $\mathbb{F}G$, called the **idempotent determined by** H.

$\widehat{H}$ is central if and only if H is normal in G.

If H is a normal subgroup of a group G, we have that

$$\mathbb{F}G \cdot \widehat{H} \cong \mathbb{F}[G/H]$$

via the map $\psi : \mathbb{F}G \cdot \widehat{H} \to \mathbb{F}[G/H]$ given by

$$g.\widehat{H} \ \mapsto \ gH \in G/H.$$

If H is a normal subgroup of a group G, we have that

$$\mathbb{F}G \cdot \widehat{H} \cong \mathbb{F}[G/H]$$

via the map $\psi : \mathbb{F}G \cdot \widehat{H} \to \mathbb{F}[G/H]$ given by

$$g.\widehat{H} \;\mapsto\; gH \in G/H.$$

so

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

If H is a normal subgroup of a group G, we have that

$$\mathbb{F}G \cdot \widehat{H} \cong \mathbb{F}[G/H]$$

via the map $\psi : \mathbb{F}G \cdot \widehat{H} \to \mathbb{F}[G/H]$ given by

$$g.\widehat{H} \;\mapsto\; gH \in G/H.$$

so

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

Set $\tau = \{t_1, t_2, \ldots, t_k\}$ a transversal of K in G (where $k = [G:H]$ and we choose $t_1 = 1$),

If H is a normal subgroup of a group G, we have that

$$\mathbb{F}G \cdot \widehat{H} \cong \mathbb{F}[G/H]$$

via the map $\psi : \mathbb{F}G \cdot \widehat{H} \to \mathbb{F}[G/H]$ given by

$$g.\widehat{H} \ \mapsto \ gH \in G/H.$$

so

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

Set $\tau = \{t_1, t_2, \ldots, t_k\}$ a transversal of K in G (where $k = [G : H]$ and we choose $t_1 = 1$), then

$$\{t_i\widehat{H} \mid 1 \leq i \leq k\}$$

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

Then, an element $\alpha \in \mathbb{F}G \cdot e$ can be written in the form

$$\alpha = \sum_{\nu \in \tau} \alpha_\nu \nu \hat{H}.$$

Then, an element $\alpha \in \mathbb{F}G \cdot e$ can be written in the form

$$\alpha = \sum_{\nu \in \tau} \alpha_\nu \nu \hat{H}.$$

If we denote $\tau = \{t_1, t_2, \ldots, t_d\}$ and $H = \{h_1, h_2, \ldots, h_m\}$, the explicit expression of α is

$$\alpha = \alpha_1 t_1 h_1 + \alpha_2 t_2 h_1 + \cdots + \alpha_d t_d h_1 + \cdots + \alpha_1 t_1 h_m + \alpha_2 t_2 h_m + \cdots + \alpha_d t_d h_m.$$

Then, an element $\alpha \in \mathbb{F}G \cdot e$ can be written in the form

$$\alpha = \sum_{\nu \in \tau} \alpha_\nu \nu \hat{H}.$$

If we denote $\tau = \{t_1, t_2, \ldots, t_d\}$ and $H = \{h_1, h_2, \ldots, h_m\}$, the explicit expression of α is

$$\alpha = \alpha_1 t_1 h_1 + \alpha_2 t_2 h_1 + \cdots + \alpha_d t_d h_1 + \cdots + \alpha_1 t_1 h_m + \alpha_2 t_2 h_m + \cdots + \alpha_d t_d h_m.$$

The sequence of coefficients of α, when written in this order, is formed by d repetitions of the subsequence $\alpha_1, \alpha_2, \cdots \alpha_d$, so this is a *repetition code*.

Essential idempotents

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

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

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

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

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

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

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

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

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

In this last case, we have that $\mathbb{F}G \cdot e \subset \mathbb{F}G \cdot \widehat{H}$.

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

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

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

In this last case, we have that $\mathbb{F}G \cdot e \subset \mathbb{F}G \cdot \widehat{H}$.

Hence, the minimal code $\mathbb{F}G \cdot e$ is a **repetition code**.

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

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

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

In this last case, we have that $\mathbb{F}G \cdot e \subset \mathbb{F}G \cdot \widehat{H}$.

Hence, the minimal code $\mathbb{F}G \cdot e$ is a **repetition code**.

.

We shall be interested in primitive idempotents which are not of this type.

Definition

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

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

Definition

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

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

Lemma

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.

Corollary

If G is abelian and $\mathbb{F}G$ contains an essential idempotent, then G is cyclic.

Corollary

If G is abelian and $\mathbb{F}G$ contains an essential idempotent, then G is cyclic.

Corollary

If G is abelian, non-cyclic, then every minimal ideal gives a repetition code.

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 $p_i^{n_i}$, $1 \leq i \leq t$.

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

$$e_0 = (1 - \widehat{K_1}) \cdots (1 - \widehat{K_t})$$

Then e_0 is a non-zero central idempotent.

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

$$e_0 = (1 - \widehat{K_1}) \cdots (1 - \widehat{K_t})$$

Then e_0 is a non-zero central idempotent.

Proposition

Let G be a cyclic group. Then, a primitive idempotent $e \in \mathbb{F}G$ is essential if and only if $e \cdot e_0 = e$.

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

$$e_0 = (1 - \widehat{K_1}) \cdots (1 - \widehat{K_t})$$

Then e_0 is a non-zero central idempotent.

Proposition

Let G be a cyclic group. Then, a primitive idempotent $e \in \mathbb{F}G$ is essential if and only if $e \cdot e_0 = e$.

Notice that the previous theorem actually shows that e_0 is the sum of all essential idempotents so, the simple components of the ideal $\mathbb{F}C.e_0$ are precisely the essential ideals of $\mathbb{F}C$.

Theorem

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.

Theorem

Let $\mathcal{C}$ be a binary linear code of **constant weight**, whose generating matrix has no zero columns.

Theorem

Let $\mathcal{C}$ be a binary linear code of **constant weight**, whose generating matrix has no zero columns.
Then $\mathcal{C}$ is equivalent to a cyclic code which is either essencial or a repetition code of an essencial code.

Nilpotent Codes

Let G be a nilpotent group and let $\mathcal{F}$ be the family of all minimal normal subgroups of G. For a field $\mathbb{F}$ such that $char(\mathbb{F}) \nmid |G|$, we define

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

Let G be a nilpotent group and let $\mathcal{F}$ be the family of all minimal normal subgroups of G. For a field $\mathbb{F}$ such that $char(\mathbb{F}) \nmid |G|$, we define

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

Lemma

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

Theorem

Let G be a nilpotent group. Suppose that e is a primitive central idempotent of $\mathbb{F}G$. Then, $e \in \mathbb{F}G$ is an essential idempotent if and only if $e.e(G) = e$.

Theorem

Let G be a nilpotent group. Suppose that e is a primitive central idempotent of $\mathbb{F}G$. Then, $e \in \mathbb{F}G$ is an essential idempotent if and only if $e.e(G) = e$.

Theorem

Let G be a finite nilpotent group. Then $\mathbb{F}G$ contains essential idempotents if and only if the center of G is cyclic.

Let G be a finite group and R a finite semisimple ring such that $|G|$ is invertible in R. Let $e \in RG$ be a primitive central idempotent.

Let G be a finite group and R a finite semisimple ring such that $|G|$ is invertible in R. Let $e \in RG$ be a primitive central idempotent.

We define

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

Let G be a finite group and R a finite semisimple ring such that $|G|$ is invertible in R. Let $e \in RG$ be a primitive central idempotent.

We define

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

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

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

Lemma

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

Equivalence

Definitions

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

Definitions

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 $T(C_1) = C_2$.

Definitions

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 $k_i = 1, \;\; 1 \leq i \leq n$, the codes are said to be **permutation equivalent**.

When a group G canbe written as a product $G = AB$, where A and B are abelian subgroups of G then all ideals in a semisimple group algebra $\mathbb{F}G$ are permutation equivalent to abelian codes ([1], [6]).

When a group G canbe written as a product $G = AB$, where A and B are abelian subgroups of G then all ideals in a semisimple group algebra $\mathbb{F}G$ are permutation equivalent to abelian codes ([1], [6]).

On the other hand, it was shown in [4], that there exists a nilpotent code which is not monomially equivalent (and thus also not permutation equivalent) to an abelian code.

When a group G canbe written as a product $G = AB$, where A and B are abelian subgroups of G then all ideals in a semisimple group algebra $\mathbb{F}G$ are permutation equivalent to abelian codes ([1], [6]).

On the other hand, it was shown in [4], 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 e Abelian codes.

Theorem

Let G be a finite group of order n, $\mathbb{F}$ a field and $e \in \mathbb{F}G$ an idempotent. If there exists a subgroup H of G such that $char(\mathbb{F}) \not| \ |H|$ and $e\widehat{H} = e$, then $\mathbb{F}Ge$ is permutation equivalent to an abelian code.

Olteanu and Van Gelder, [4] considered the group algebra $\mathbb{F}_2 G$ with

$$G = \langle a, b, c \mid a^7 = 1, b^3 = 1, c^5 = 1, ba = a^4 b, [a, c] = 1, [b, c] = 1 \rangle,$$

which is metabelian, and exibited a best [105,3,60]-code in the group algebra above.

Olteanu and Van Gelder, [4] considered the group algebra $\mathbb{F}_2 G$ with

$$G = \langle a, b, c \mid a^7 = 1, b^3 = 1, c^5 = 1, ba = a^4 b, [a, c] = 1, [b, c] = 1 \rangle,$$

which is metabelian, and exibited a best [105,3,60]-code in the group algebra above.

They stated "*it is unclear whether this code can be realized as an Abelian code or not.*"

Olteanu and Van Gelder, [4] considered the group algebra $\mathbb{F}_2 G$ with

$$G = \langle a, b, c \mid a^7 = 1, b^3 = 1, c^5 = 1, ba = a^4 b, [a, c] = 1, [b, c] = 1 \rangle,$$

which is metabelian, and exibited a best [105,3,60]-code in the group algebra above.

They stated "*it is unclear whether this code can be realized as an Abelian code or not.*"

The subgroup $H = \langle b, c, aba^{-2} \rangle$ is non-normal, but if we denote by e the idempotent generator for the given code, it can be shown that $e\widehat{H} = e$. Hence, this code is equivalent to an Abelian code.

Lemma

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 support, then there exist elements $g_1, \cdots, g_t \in G$ such that $\{g_1 u_1, \cdots, g_t u_1\}$ is also a basis of I and its elements have disjoint support.

Lemma

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 support, then there exist elements $g_1, \cdots, g_t \in G$ such that $\{g_1 u_1, \cdots, g_t u_1\}$ is also a basis of I and its elements have disjoint support.

Theorem

Let G be a finite group of order n and let $\mathbb{F}$ be a finite field such that $char(\mathbb{F}) \nmid |G|$. Suppose that $I \neq (0)$ is a code in $\mathbb{F}G$ with a basis whose elements have disjoint support. Then, I is monomially equivalent to a cyclic code.

Theorem

Let G be a finite nilpotent group. Let $e \in \mathbb{F}G$ be a primitive central idempotent which is not essential. Then $\mathbb{F}Ge$ is permutation equivalent to an abelian code.

Theorem

Let G be a finite nilpotent group. Let $e \in \mathbb{F}G$ be a primitive central idempotent which is not essential. Then $\mathbb{F}Ge$ is permutation equivalent to an abelian code.

Corollary

If G is a finite nilpotent group which has a non-cyclic center, then every minimal code in $\mathbb{F}G$ is permutation equivalent to an abelian code.

Theorem

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 $C \subset \mathbb{F}G$ is permutation equivalent to a cyclic code C' in $\mathbb{F}C_n$.

Bibliography

[1] J. J. Bernal, A. del Río and J. J. Simón, An Intrinsical Description of Group Codes, *Des. Codes Cryptogr.*, **51**(3) 289-300 (2009).

[2] A. Duarte, *On Nilpotent Codes*, PhD Thesis, Universidade Federal do ABC, São Paulo, 2021.

[3] C. Gladys, R. A. Ferraz, C. Polcino Milies, Essential Idempotents and Simplex Codes, *Algebra Comb. Discrete Appl.*, **4**(2) 181-188 (2016).

[4] G. Nebe, A.Schäfer, A Nilpotent non Abelian Group Code, *Algebra and Discrete Math.* , **18**(2) (2014), 268-273.

[5] G. Olteanu and I. Van Gelder, Construction of minimal non-abelian left group codes, *Designs Codes and Cryptogr.*, **75** (2015), 359-373.

[6] C. G. Pillado, S. Gonzales and C. Martínez, V. Markov and A. Nechaev, Group codes over non-Abelian groups, *J.of Algebra and Its Appl.*, **12** (7) (2013),