Left Metacyclic Ideals

Samir Assuena

Centro Universiário da FEI

Joint work with César Polcino Milies

samir.assuena@fei.edu.br

CIMPA RESEARCH SCHOOL

ALGEBRAIC METHODS IN CODING THEORY

www.fei.edu.br

Metacyclic Groups

Definition

A group G is **metacyclic** *if G contains a cyclic normal subgroup H such that the factor group G/H is also cyclic.*

The dihedral groups and groups all whose Sylow subgroups are cyclic are examples of such groups.

Metacyclic Groups

Let G be a metacyclic group, $H = \langle a \rangle$ its cyclic normal subgroup, and set $G/H = \langle bH \rangle$. Then G has the following presentation

$$G = \left\langle a, b \mid a^m = 1, b^n = a^s, bab^{-1} = a^r \right\rangle$$

and the integers *m*,*n*,*s*, *r* satisfy the relations

$$s \mid m, \quad m \mid s(r-1) \quad , \quad r < m, \quad \gcd(r, m) = 1.$$

When $s = m$, we say G is *split*. In this case, $G = \langle a \rangle \rtimes \langle b \rangle$.

Group Codes

Definition

A **group code** *over a field $\mathbb{F}$ is any ideal I of the group algebra $\mathbb{F}G$ of a finite group G. A code is said to be metacyclic, abelian, or dihedral in case the given group G is of that kind. If I is two-sided, then it is called a* **central** *code. A* **minimal code** *is an ideal I (left, two-sided) which is minimal in the set of all (left, two-sided) ideals of $\mathbb{F}G$.*

centro universitário FEI

www.fei.edu.br

Group Codes

The **weight** of an element $\alpha = \sum_{g \in G} \alpha_g g$ is

$$w(\alpha) = \mid \{g \mid \alpha_g \neq 0,\ g \in G\} \mid$$

that is, the number of elements of the support of α. The **weight** of an ideal I is

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

centro universitário FEI

www.fei.edu.br

Metacyclic Codes

Definition

Let G_1 and G_2 be finite groups of the same order and let $\mathbb{F}$ be a field. Let $\mathbb{F}G_1$ and $\mathbb{F}G_2$ be the corresponding group algebras. A **combinatorial equivalence** *is a linear isomorphism $\phi : \mathbb{F}G_1 \longrightarrow \mathbb{F}G_2$ induced by a bijection $\phi : G_1 \longrightarrow G_2$. Codes $C_1 \subset \mathbb{F}G_1$ and $C_2 \subset \mathbb{F}G_2$ are* **combinatorially equivalent** *if there exists a combinatorial equivalence $\phi : \mathbb{F}G_1 \longrightarrow \mathbb{F}G_2$ such that $\phi(C_1) = C_2$.*

www.fei.edu.br

Metacyclic Codes

Theorem (Sabin and Lomonaco)

Metacyclic Central Codes are combinatorially equivalent to abelian codes.

Metacyclic Codes

Let $\mathbb{F}_q$ be a finite field. For a subgroup S of a group $\mathcal{G}$ such that $gcd(q, \mid S \mid) = 1$, we set

$$\widehat{S} = \frac{1}{|S|} \sum_{x \in S} x.$$

Then $\widehat{S}$ is an idempotent of $\mathbb{F}_q\mathcal{G}$ and is central if and only if S is a normal subgroup.

Metacyclic Codes

Let G be a split metaclyclic group of order $p^m\ell^n$ with presentation

$$G = \left\langle a, b \mid a^{p^m} = 1 = b^{\ell^n}, bab^{-1} = a^r \right\rangle$$

and $\mathbb{F}_q$ be a finite field with q elements such that $gcd(q, p^m\ell^n) = 1$. In this case, the group algebra $\mathbb{F}_qG$ is semisimple and it can be decomposed as direct sum of simple rings.

www.fei.edu.br

Metacyclic Codes

Set $H = \langle a \rangle$ and let

$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}$$

be the descending chain of all subgroups of H, i.e., $H_j = \langle a^{p^j} \rangle$, $0 \leq j \leq m$. Consider the idempotents

$$e_0 = \widehat{H} \quad \text{and} \quad e_j = \widehat{H_j} - \widehat{H_{j-1}}, \;\; 1 \leq j \leq m,$$

which are central in $\mathbb{F}_q G$.

centro universitário FEI

www.fei.edu.br

Metacyclic Codes

Write $\widehat{H} = \widehat{a}$ and $\widehat{\langle b \rangle} = \widehat{b}$, so the elements $\widehat{b}e_j$, $1 \leq j \leq m$, are non central idempotents of $\mathbb{F}_q G$.

Proposition

Let e be a central idempotent. Then the left ideal $\mathbb{F}_q G \cdot \widehat{b}e$ is minimal if and only if the ideal $\mathbb{F}_q G \cdot e$ is minimal as a two-sided ideal.

Proposition

The left codes $\mathbb{F}_q G \cdot \widehat{b}e_j$ and $\mathbb{F}_q G \cdot (1 - \widehat{b})e_j$ are combinatorially equivalent to cyclic codes.

Metacyclic Codes

Lemma

For all $j,\ 1 \leq j \leq m$, the elements $\alpha_j = e_j + \widehat{b}a(1-\widehat{b})e_j$ are units inside the ideals $\mathbb{F}_q G \cdot e_j$.

So, we can construct non central idempotents using the units α_j as follows $\alpha_j \left(\widehat{b}e_j\right) \alpha_j^{-1}$ and $\alpha_j^{-1} \left(\widehat{b}e_j\right) \alpha_j$.

Metacyclic Codes

The non central idempotents are

$$(\widehat{b} \pm \widehat{b}a(1-\widehat{b}))e_j,\ 1 \leq j \leq m.$$

The dimension of $\mathbb{F}_q G \cdot \widehat{b}e_j$ over $\mathbb{F}_q$ is $p^j - p^{j-1} = \varphi(p^j)$, where φ denotes Euler's totient function. Hence the dimension of $\mathbb{F}_q G \cdot (\widehat{b} \pm \widehat{b}a(1-\widehat{b}))e_j$ over $\mathbb{F}_q$ is also $\varphi(p^j)$.

centro universitário FEI

www.fei.edu.br

Metacyclic Codes

Proposition

Write $f = (\widehat{b} + \widehat{b}a(1 - \widehat{b}))e_j$. *If* e_j *is a central primitive idempotent of* $\mathbb{F}_q \langle a \rangle$, *then the set*

$$\mathcal{B} = \{f, af, a^2 f, \cdots, a^{\varphi(p^j)-1} f\}$$

is a basis of the left ideal $\mathbb{F}_q G \cdot f$ *over* $\mathbb{F}_q$.

centro universitário FEI

www.fei.edu.br

Examples

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

Examples

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

Central primitive idempotents over $\mathbb{F}_5$:

$f_1 = \widehat{b}\widehat{a}, \quad f_2 = (1 - \widehat{b})\widehat{a}, \quad e_1 = 1 - \widehat{a};$

$$\mathbb{F}_5 G \cong \mathbb{F}_5 \oplus \mathbb{F}_{25} \oplus M_3(\mathbb{F}_{25}).$$

Examples

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

Central primitive idempotents over $\mathbb{F}_5$:

$f_1 = \widehat{b}\widehat{a}, \quad f_2 = (1 - \widehat{b})\widehat{a}, \quad e_1 = 1 - \widehat{a};$

$$\mathbb{F}_5 G \cong \mathbb{F}_5 \oplus \mathbb{F}_{25} \oplus M_3(\mathbb{F}_{25}).$$

$f = (\widehat{b} + \widehat{b}a(1 - \widehat{b}))e_1;$

Examples

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

Central primitive idempotents over $\mathbb{F}_5$:

$f_1 = \widehat{b}\widehat{a}, \qquad f_2 = (1 - \widehat{b})\widehat{a}, \qquad e_1 = 1 - \widehat{a};$

$$\mathbb{F}_5 G \cong \mathbb{F}_5 \oplus \mathbb{F}_{25} \oplus M_3(\mathbb{F}_{25}).$$

$f = (\widehat{b} + \widehat{b}a(1 - \widehat{b}))e_1;$

$\mathcal{B} = \{f, af, a^2 f, a^3 f, a^4 f, a^5 f\}$ basis of the left ideal $\mathbb{F}_5 G \cdot f$.

Examples

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

Central primitive idempotents over $\mathbb{F}_5$:

$f_1 = \widehat{b}\widehat{a}, \quad f_2 = (1 - \widehat{b})\widehat{a}, \quad e_1 = 1 - \widehat{a};$

$$\mathbb{F}_5 G \cong \mathbb{F}_5 \oplus \mathbb{F}_{25} \oplus M_3(\mathbb{F}_{25}).$$

$f = (\widehat{b} + \widehat{b}a(1 - \widehat{b}))e_1;$

$\mathcal{B} = \{f, af, a^2 f, a^3 f, a^4 f, a^5 f\}$ basis of the left ideal $\mathbb{F}_5 G \cdot f$.

We have found a minimal [21,6,10] left code.

Examples

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

Examples

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

Central primitive idempotents over $\mathbb{F}_2$:

$$f_1 = \widehat{b}\widehat{a}, \qquad f_2 = (1 - \widehat{b})\widehat{a},$$
$$f_3 = \frac{1}{7}\left(3 + (\xi + \xi^2 + \xi^4)\Gamma_a + (\xi^3 + \xi^5 + \xi^6)\Gamma_{a^3}\right),$$
$$f_4 = \frac{1}{7}\left(3 + (\xi^3 + \xi^5 + \xi^6)\Gamma_a + (\xi + \xi^2 + \xi^4)\Gamma_{a^3}\right),$$ where ξ is a primitive 7th root of unity;

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

centro universitário FEI

www.fei.edu.br

Examples

Take $e_1 = 1 + \widehat{a}$ which is not a central primitive idempotent and $f = (\widehat{b} + \widehat{b}a(1 + \widehat{b}))e_1$;

$\mathcal{B} = \{f, af, a^2f, a^3f, a^4f, a^5f\}$ basis of the left ideal $\mathbb{F}_2G \cdot f$.

Examples

Take $e_1 = 1 + \widehat{a}$ which is not a central primitive idempotent and $f = (\widehat{b} + \widehat{b}a(1 + \widehat{b}))e_1$;

$\mathcal{B} = \{f, af, a^2f, a^3f, a^4f, a^5f\}$ basis of the left ideal $\mathbb{F}_2G \cdot f$.

This is a [21,6,8]-code, which is not minimal and it has the same weight of the best known [21,6]-code.

centro universitário FEI

www.fei.edu.br

Dihedral Codes

$$D = \left\langle a, b \mid a^{p^m} = 1 = b^2,\ bab = a^{-1} \right\rangle.$$

Dihedral Codes

$$D = \left\langle a, b \mid a^{p^m} = 1 = b^2,\ bab = a^{-1} \right\rangle.$$

Suppose that $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \overline{q} \rangle$. The elements

$$e_{11} = \left(\tfrac{1+b}{2}\right) e, \qquad e_{12} = \left(\tfrac{1+b}{2}\right) a \left(\tfrac{1-b}{2}\right) e,$$
$$e_{21} = 4((a - a^{-1})e)^{-2} \left(\tfrac{1-b}{2}\right) a \left(\tfrac{1+b}{2}\right) e, \qquad e_{22} = \left(\tfrac{1-b}{2}\right) e.$$

form a set of matrix units for $(\mathbb{F}D)e$.

Dihedral Codes

Example 3: Let D_9 be dihedral group of order 18, set

$e = e_1 = \widehat{H_1} - \widehat{H_0}$, $f = e_{11} - e_{22}$.

Dihedral Codes

Example 3: Let D_9 be dihedral group of order 18, set $e = e_1 = \widehat{H_1} - \widehat{H_0}$, $f = e_{11} - e_{22}$.

The set $\{f, af\}$ is a basis of the minimal left ideal $I = \mathbb{F}_q D_9 \cdot f$.

Example 3: Let D_9 be dihedral group of order 18, set $e = e_1 = \widehat{H_1} - \widehat{H_0}$, $f = e_{11} - e_{22}$.

The set $\{f, af\}$ is a basis of the minimal left ideal $I = \mathbb{F}_q D_9 \cdot f$.

If the characteristic of $\mathbb{F}_q$ is different from 2,3,5 and 7, the weight of I of weight 15 and it is the same as that of the best known code of same dimension and this code is not equivalent to any abelian code.

Dihedral Codes

Example 4: Let D_6 be dihedral group of order 6.

Dihedral Codes

Example 4: Let D_6 be dihedral group of order 6.

Set $e = 1 - \widehat{a}$ and set $f = e_{11} - e_{12}$.

Dihedral Codes

Example 4: Let D_6 be dihedral group of order 6.

Set $e = 1 - \widehat{a}$ and set $f = e_{11} - e_{12}$.

The set $\{f, af\}$ is a basis of the minimal left ideal $I = \mathbb{F}_q D_6 \cdot f$.

Dihedral Codes

Example 4: Let D_6 be dihedral group of order 6.

Set $e = 1 - \widehat{a}$ and set $f = e_{11} - e_{12}$.

The set $\{f, af\}$ is a basis of the minimal left ideal $I = \mathbb{F}_q D_6 \cdot f$.

If the characteristic of $\mathbb{F}_q$ is different from 2,3,5 and 7, the weight of I of weight 5 and it is the same as that of the best known code of same dimension.

Thank you!!!!