Left Metacyclic Ideals

Samir Assuena
Centro Universitário da FEI
Joint work with César Polcino Milies
samir.assuena@fei.edu.br

CIMPA RESEARCH SCHOOL
ALGEBRAIC METHODS IN CODING THEORY
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.
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

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

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

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

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

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 $\mathbb{F}G$. 
Group Codes

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

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

that is, the number of elements of the support of $\alpha$. The **weight** of an ideal $I$ is

$$w(I) = \min \{w(\alpha) \mid \alpha \neq 0, \ \alpha \in I\}.$$
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 $\phi : \mathbb{F}G_1 \rightarrow \mathbb{F}G_2$ induced by a bijection $\phi : G_1 \rightarrow G_2$. 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 $\phi : \mathbb{F}G_1 \rightarrow \mathbb{F}G_2$ such that $\phi(C_1) = C_2$. 
Theorem (Sabin and Lomonaco)

*Metacyclic Central Codes are combinatorially equivalent to abelian codes.*
Let $\mathbb{F}_q$ be a finite field. For a subgroup $S$ of a group $G$ such that $gcd(q, |S|) = 1$, we set

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

Then $\hat{S}$ is an idempotent of $\mathbb{F}_qG$ and is central if and only if $S$ is a normal subgroup.
Let $G$ be a split metacyclic group of order $p^m \ell^n$ with presentation

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

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 $\mathbb{F}_q G$ is semisimple and it can be decomposed as direct sum of simple rings.
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

$$e_0 = \widehat{H} \quad \text{and} \quad e_j = \widehat{H}_j - \widehat{H}_{j-1}, \quad 1 \leq j \leq m,$$

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

**Proposition**

Let $e$ be a central idempotent. Then the left ideal $\mathbb{F}_q G \cdot \hat{b}e$ 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 $\mathbb{F}_q G \cdot \hat{b}e_j$ and $\mathbb{F}_q G \cdot (1 - \hat{b})e_j$ are combinatorially equivalent to cyclic codes.
For all $j$, $1 \leq j \leq m$, the elements $\alpha_j = e_j + \hat{b}a(1 - \hat{b})e_j$ are units inside the ideals $\mathbb{F}_q G \cdot e_j$.

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

\[(\hat{b} \pm \hat{b}a(1 - \hat{b}))e_j, \ 1 \leq j \leq m.\]

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

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

$$B = \{ f, af, a^2 f, \ldots, a^{\varphi(p^j)} f \}$$

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

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

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

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

$$\mathbb{F}_5 G \cong \mathbb{F}_5 \oplus \mathbb{F}_{25} \oplus M_3(\mathbb{F}_{25}).$$
**Example 1:** Set $G = \langle a, b \mid a^7 = 1 = b^3, bab^{-1} = a^2 \rangle$.

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

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

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

$f = (\hat{b} + \hat{ba}(1 - \hat{b}))e_1;$
Example 1: Set \( G = \langle a, b \mid a^7 = 1 = b^3, bab^{-1} = a^2 \rangle \).

Central primitive idempotents over \( \mathbb{F}_5 \):

\[
f_1 = \hat{b}\hat{a}, \quad f_2 = (1 - \hat{b})\hat{a}, \quad e_1 = 1 - \hat{a};
\]

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

\[
f = (\hat{b} + \hat{b}a(1 - \hat{b}))e_1;
\]

\( \mathcal{B} = \{ f, af, a^2f, a^3f, a^4f, a^5f \} \) basis of the left ideal \( \mathbb{F}_5 G \cdot f \).
Example 1: Set $G = \langle a, b \mid a^7 = 1 = b^3, bab^{-1} = a^2 \rangle$.

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

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

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

$f = (\hat{b} + \hat{ba}(1 - \hat{b}))e_1$;

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

We have found a minimal $[21,6,10]$ left code.
Example 2: Set $G = \langle a, b \mid a^7 = 1 = b^3, bab^{-1} = a^2 \rangle$. 
Example 2: Set $G = \langle a, b \mid a^7 = 1 = b^3, bab^{-1} = a^2 \rangle$.

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

\[ f_1 = \hat{b}\hat{a}, \quad f_2 = (1 - \hat{b})\hat{a}, \]
\[ f_3 = \frac{1}{7} (3 + (\xi + \xi^2 + \xi^4)\Gamma_a + (\xi^3 + \xi^5 + \xi^6)\Gamma_a^3), \]
\[ f_4 = \frac{1}{7} (3 + (\xi^3 + \xi^5 + \xi^6)\Gamma_a + (\xi + \xi^2 + \xi^4)\Gamma_a^3), \]

where $\xi$ is a primitive 7th root of unity;

\[ \mathbb{F}_2 G \cong \mathbb{F}_2 \oplus \mathbb{F}_4 \oplus M_3(\mathbb{F}_2) \oplus M_3(\mathbb{F}_2). \]
Examples

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

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

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

$\mathcal{B} = \{f, af, a^2f, a^3f, a^4f, a^5f\}$ basis of the left ideal $\mathbb{F}_2 G \cdot f$.

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

\[ D = \langle a, b \mid a^{p^m} = 1 = b^2, \ bab = a^{-1} \rangle. \]
Dihedral Codes

\[ D = \langle a, b \mid a^{p^m} = 1 = b^2, \ bab = a^{-1} \rangle. \]

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

\[
\begin{align*}
e_{11} & = \left( \frac{1+b}{2} \right) e, & e_{12} & = \left( \frac{1+b}{2} \right) a \left( \frac{1-b}{2} \right) e, \\
e_{21} & = 4((a - a^{-1})e)^{-2} \left( \frac{1-b}{2} \right) a \left( \frac{1+b}{2} \right) e, & e_{22} & = \left( \frac{1-b}{2} \right) e.
\end{align*}
\]

form a set of matrix units for \((\mathbb{F}D)e\).
**Example 3:** Let $D_9$ be dihedral group of order 18, set

$$e = e_1 = \widehat{H_1} - \widehat{H_0}, f = e_{11} - e_{22}.$$
Example 3: Let $D_9$ be dihedral group of order 18, set
\[ e = e_1 = \hat{H}_1 - \hat{H}_0, \quad f = e_{11} - e_{22}. \]

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

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

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

Set $e = 1 - \hat{a}$ and set $f = e_{11} - e_{12}$. 
**Example 4:** Let $D_6$ be dihedral group of order 6.

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

The set $\{f, af\}$ is a basis of the minimal left ideal $l = \mathbb{F}_q D_6 \cdot f$. 
Example 4: Let $D_6$ be dihedral group of order 6. 

Set $e = 1 - \hat{a}$ 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!!!!