# Essential idempotents in group algebras and minimal cyclic codes

César Polcino Milies

Universidad de São Paulo

# Basic Facts

The basic elements to build a code are the following:

The basic elements to build a code are the following:

- A finite set, $A$ called the **alphabet**. We shall denote by $q = |A|$ the number of elements in $A$.

The basic elements to build a code are the following:

- A finite set, $A$ called the **alphabet**. We shall denote by $q = |A|$ the number of elements in $A$.
- Finite sequences of elements of the alphabet, that are called **words**. The number of elements in a word is called its **length**. We shall only consider codes in which all the words have the same length $n$.

The basic elements to build a code are the following:

- A finite set, $A$ called the **alphabet**. We shall denote by $q = |A|$ the number of elements in $A$.
- Finite sequences of elements of the alphabet, that are called **words**. The number of elements in a word is called its **length**. We shall only consider codes in which all the words have the same length $n$.
- A **$q$-ary block code of length $n$** is any subset of the set of all words of length $n$, i.e., the code $\mathcal{C}$ is a subset:

$$\mathcal{C} \subset A^n = \underbrace{A \times A \times \ \cdots \times A}_{n \ \ veces}.$$

# A classical scheme due to Shannon

$$\boxed{\text{Information}} \longrightarrow \boxed{\text{codification}} \xrightarrow{\text{signal}} \underset{\substack{\uparrow \\ \boxed{\text{noise}}}}{\boxed{\text{channel}}} \xrightarrow{\text{signal}} \boxed{\text{decodification}} \longrightarrow \boxed{\text{receiver}}$$

# A classical scheme due to Shannon

$$\begin{tikzcd}
\boxed{\text{Information}} \arrow[r] & \boxed{\text{codification}} \arrow[r, "\text{signal}"] & \boxed{\text{channel}} \arrow[r, "\text{signal}"] & \boxed{\text{decodification}} \arrow[r] & \boxed{\text{receiver}} \\
 & & \boxed{\text{noise}} \arrow[u] & &
\end{tikzcd}$$

The basic idea in coding theory, is to add information to the message, called **redundancy**, in such a way that it will turn possible to detect errors and correct them.

# Linear Codes

- We shall take, as an alphabet $A$, a finite field $\mathbb{F}$.

# Linear Codes

- We shall take, as an alphabet $A$, a finite field $\mathbb{F}$.
- In this case, $\mathbb{F}^n$ is an $n$-dimensional vector space over $\mathbb{F}$.

# Linear Codes

- We shall take, as an alphabet $A$, a finite field $\mathbb{F}$.
- In this case, $\mathbb{F}^n$ is an $n$-dimensional vector space over $\mathbb{F}$.
- We shall take, as codes, subespaces of $\mathbb{F}^n$ of dimensión $m < n$.

# Linear Codes

- We shall take, as an alphabet $A$, a finite field $\mathbb{F}$.
- In this case, $\mathbb{F}^n$ is an $n$-dimensional vector space over $\mathbb{F}$.
- We shall take, as codes, subespaces of $\mathbb{F}^n$ of dimensión $m < n$.

## Definition

A code $\mathcal{C}$ as above is called a **linear code** over $\mathbb{F}$.

If $d$ the minimum distance of $\mathcal{C}$, we shall call it a **(n,m,d)-code.**

## Definition

Given two elements $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in $A^n$, the number of coordinates in which the two elements differ is called the **Hamming distance** from $x$ to $y$; i.e.:

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

### Definition

Given two elements $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in $A^n$, the number of coordinates in which the two elements differ is called the **Hamming distance** from $x$ to $y$; i.e.:

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

### Definition

Given a code $\mathcal{C} \subset A^n$ the **minimum distance** of $\mathcal{C}$ is the number:

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

## Theorem

Let $\mathcal{C}$ be a code with minimum distance $d$ and set

$$\kappa = \left[ \frac{d-1}{2} \right]$$

where $[x]$ denotes the integral part of the real number $x$; i.e., the greatest integer smaller than or equal to $x$.

Then $\mathcal{C}$ is capable of detecting $d-1$ errors and correcting $\kappa$ errores.

**Theorem**

Let $\mathcal{C}$ be a code with minimum distance $d$ and set

$$\kappa = \left[ \frac{d-1}{2} \right]$$

where $[x]$ denotes the integral part of the real number $x$; i.e., the greatest integer smaller than or equal to $x$.

Then $\mathcal{C}$ is capable of detecting $d-1$ errors and correcting $\kappa$ errores.

**Definition**

The number $\kappa$ is called the **capacity** of the code $\mathcal{C}$.

**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:

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

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

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:

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

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

$\varphi$ 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 $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ 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

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

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.

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

Let $G$ be a finite group and let $\mathbb{F}$ be a field such that $char(\mathbb{F}) \not| \, |G|$.
Let $H$ and $H^*$ be normal subgroups of $G$ such that $H \subset H^*$.
We can define another type of idempotents by:

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

# Code Parameters

**Theorem (R. Ferraz - P.M.)**

Let $G$ be a finite group and let $\mathbb{F}$ be a field such that $char(\mathbb{F}) \nmid |G|$. Let $H$ and $H^*$ be normal subgroups of $G$ such that $H \subset H^*$ and set . Then,

$$dim_F(FG)e = |G/H| - |G/H^*| = \frac{|G|}{|H|}\left(1 - \frac{|H|}{|H^*|}\right)$$

and

$$w((FG)e) = 2|H|$$

where $w((FG)e)$ denotes the minimal distance of $(FG)e$.

**Theorem (R. Ferraz - P.M.)**

Let $G$ be a finite group and let $\mathbb{F}$ be a field such that $char(\mathbb{F}) \nmid |G|$. Let $H$ and $H^*$ be normal subgroups of $G$ such that $H \subset H^*$ and set $e = \widehat{H} - \widehat{H^*}$. Let $\mathcal{A}$ be a transversal of $H^*$ in $G$ and $\tau$ 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 $\mathbb{F}$.

Let $A$ be an abelian $p$-group. For each subgroup $H$ of $A$ such that $A/H \neq \{1\}$ is cyclic, we shall construct an idempotent of $\mathbb{F}A$. Since $A/H$ is a cyclic subgroup of order a power of $p$, there exists a unique subgroup $H^*$ of $A$, containing $H$, such that $|H^*/H| = p$.

Let $A$ be an abelian $p$-group. For each subgroup $H$ of $A$ such that $A/H \neq \{1\}$ is cyclic, we shall construct an idempotent of $\mathbb{F}A$. Since $A/H$ is a cyclic subgroup of order a power of $p$, there exists a unique subgroup $H^*$ of $A$, containing $H$, such that $|H^*/H| = p$. We set

$$e_H = \widehat{H} - \widehat{H^*}.$$

and also

$$e_G = \frac{1}{|G|} \sum_{g \in G} g.$$

Let $A$ be an abelian $p$-group. For each subgroup $H$ of $A$ such that $A/H \neq \{1\}$ is cyclic, we shall construct an idempotent of $\mathbb{F}A$. Since $A/H$ is a cyclic subgroup of order a power of $p$, there exists a unique subgroup $H^*$ of $A$, containing $H$, such that $|H^*/H| = p$. We set

$$e_H = \widehat{H} - \widehat{H^*}.$$

and also

$$e_G = \frac{1}{|G|}\sum_{g \in G} g.$$

It is not difficult to see that this is a set of orthogonal idempotents whose sum is equal to 1

### Definition

Let$g$ be an element of a finite group $G$. The *q-cyclotomic class* of g is the set

$$S_g \;=\; \{g^{q^j} \mid 1 \leq j \leq t_g - 1\},$$

where $t_g$ is the smallest positive integer such that

$$q^{t_g} \equiv 1(mod\ o(g)).$$

### Definition

Let$g$ be an element of a finite group $G$. The *q-cyclotomic class* of g is the set

$$S_g \;=\; \{g^{q^j} \mid 1 \leq j \leq t_g - 1\},$$

where $t_g$ is the smallest positive integer such that

$$q^{t_g} \equiv 1 (mod\ o(g)).$$

### Theorem

Let $G$ be a finite group and $\mathbb{F}$ the field with $q$ elements and assume that $gcd(q, |G|) = 1$. Then, the number of simple components of $\mathbb{F}G$ is equal to the number of $q$-cyclotomic classes of $G$.

**Theorem (Ferraz-PM (2007))**

Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = q$, and let $A$ be a finite abelian group, of exponent $e$. Then the primitive central idempotents can be constructed as above if and only if one of the following holds:

(i) $e = 2$ and $q$ is odd.

(ii) $e = 4$ and $q \equiv 3 \pmod 4$.

(iii) $e = p^n$ and $o(q) = \varphi(p^n)$ in $U(\mathbb{Z}_{p^n})$.

(iv) $e = 2p^n$ and $o(q) = \varphi(p^n)$ in $U(\mathbb{Z}_{2p^n})$.

# 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 $\mathbb{F}G \cdot e \subset \mathbb{F}G \cdot \widehat{H}$.

Denote by $T$ a transversal of $H$ in $G$. Then, an element $\alpha \in \mathbb{F}G \cdot e$ can be written in the form

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

Denote by $T$ a transversal of $H$ in $G$. Then, an element $\alpha \in \mathbb{F}G \cdot e$ can be written in the form

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

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

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

Denote by $T$ a transversal of $H$ in $G$. Then, an element $\alpha \in \mathbb{F}G \cdot e$ can be written in the form

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

If we denote $T = \{t_1, t_2, \dots, t_d\}$ and $H = \{h_1, h_2, \dots, h_m\}$, the explicit expression of $\alpha$ 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 $\alpha$, when written in this order, is formed by $d$ repetitions of the subsequence $\alpha_1, \alpha_2, \cdots \alpha_d$. In terms of coding theory, this means that the code given by the minimal ideal $\mathbb{F}Ge$ is a **repetition code**. We shall be interested in idempotents that 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.

These idempotents were first considered by Bakshi, Raka and Sharma in a paper from 2008, where they were called *non-degenerate*.

## 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.

These idempotents were first considered by Bakshi, Raka and Sharma in a paper from 2008, where they were called *non-degenerate*.

## 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.

### 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.

These idempotents were first considered by Bakshi, Raka and Sharma in a paper from 2008, where they were called *non-degenerate*.

### 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.

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 $e \cdot e_0 = e$.

# Galois Descent

Let $\mathbb{F}$ be a field and $C_n$ a cyclic group of order $n$ such that $char(\mathbb{F})$ does not divide $n$. There is a well-known method to determine the primitive idempotents os $\mathbb{F}C_n$.

# Galois Descent

Let $\mathbb{F}$ be a field and $C_n$ a cyclic group of order $n$ such that $char(\mathbb{F})$ does not divide $n$. There is a well-known method to determine the primitive idempotents os $\mathbb{F}C_n$.

If $\zeta$ 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

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

# Galois Descent

Let $\mathbb{F}$ be a field and $C_n$ a cyclic group of order $n$ such that $char(\mathbb{F})$ does not divide $n$. There is a well-known method to determine the primitive idempotents os $\mathbb{F}C_n$.

If $\zeta$ 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

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

# Galois Descent

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).

## Galois Descent

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

$$\epsilon_i = \sum_{\sigma \in Gal(\mathbb{F}(\zeta^i):\mathbb{F})} \sigma(e_i) = \frac{1}{n} \sum_{j=0}^{n-1} tr_{\mathbb{F}(\zeta^i)|\mathbb{F}}(\zeta^{-ij}) g^j, \quad 1 \leq i \leq t,$$

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

### Theorem

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

## Theorem

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

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

### Theorem

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

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

### Theorem

Let $C$ be a cyclic group of order $n$ and $\mathbb{F}$ a field such that char($\mathbb{F}$) does not divide $n$. Given two essential idempotents $\epsilon_h, \epsilon_k \in \mathbb{F}C$, there exists an integer $i$ with $(n, i) = 1$ and the automorphism $\psi_i : \mathbb{F}C \to \mathbb{F}C$ defined as above is such that $\psi_i(\epsilon_h) = \epsilon_k$. Conversely, if $\epsilon$ is an essential idempotent and $\psi_i$ is an automorphism as above, then $\psi_i(\epsilon)$ is also an essential idempotent

## Theorem

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

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

# An application

Let $\mathbb{F}$ be a field, $A$ be a finite abelian group such that $char(\mathbb{F})$ does not divide $|A|$ and $e \neq \widehat{A}$ an idempotent in $\mathbb{F}A$. Let

$$\mathcal{H}_e = \{H < A \mid e\widehat{H} = e\}$$

and set

$$H_e = \prod_{H \in \mathcal{H}_e} H.$$

Let $\mathbb{F}$ be a field, $A$ be a finite abelian group such that $char(\mathbb{F})$ does not divide $|A|$ and $e \neq \widehat{A}$ an idempotent in $\mathbb{F}A$. Let

$$\mathcal{H}_e = \{H < A \mid e\widehat{H} = e\}$$

and set

$$H_e = \prod_{H \in \mathcal{H}_e} H.$$

Then $e.\widehat{H_e} = e$ and thus $H_e \in \mathcal{H}_e$ so $H \subset H_e$, for all $H \in \mathcal{H}_e$. Hence $H_e$ is the maximal subgroup of $A$ such that $e\widehat{H} = \widehat{H}$. Actually, the converse also holds:

Let $\mathbb{F}$ be a field, $A$ be a finite abelian group such that $char(\mathbb{F})$ does not divide $|A|$ and $e \neq \widehat{A}$ an idempotent in $\mathbb{F}A$. Let

$$\mathcal{H}_e = \{H < A \mid e\widehat{H} = e\}$$

and set

$$H_e = \prod_{H \in \mathcal{H}_e} H.$$

Then $e.\widehat{H_e} = e$ and thus $H_e \in \mathcal{H}_e$ so $H \subset H_e$, for all $H \in \mathcal{H}_e$. Hence $H_e$ is the maximal subgroup of $A$ such that $e\widehat{H} = \widehat{H}$. Actually, the converse also holds:

**Proposition**

Let $\mathbb{F}$ be a field, $A$ an abelian group and $e$ an idempotent in $\mathbb{F}A$. Let $K$ be a subgroup of $A$. Then, $e\widehat{K} = e$ if and only if $K \subset H_e$.

## Remark

Let $\alpha$ be in $\mathbb{F}A \cdot \widehat{H_e}$, and $T$ be a transversal of $H_e$ in $A$. Then $\alpha$ can be written in the form

$$\alpha = \sum_{\tau \in T} \sum_{h \in H_e} \alpha_{\tau h} \tau h.$$

As $\alpha \in \mathbb{F}A \cdot \widehat{H_e}$, then for every $\tau \in T$ and $h \in H_e$ we have $\alpha_{\tau h} = \alpha_\tau$.
So

$$\alpha = |H_e| \sum_{\tau \in T} \alpha_\tau \tau \cdot \widehat{H_e}.$$

## Remark

Let $\alpha$ be in $\mathbb{F}A \cdot \widehat{H_e}$, and $T$ be a transversal of $H_e$ in $A$. Then $\alpha$ can be written in the form

$$\alpha = \sum_{\tau \in T} \sum_{h \in H_e} \alpha_{\tau h} \tau h.$$

As $\alpha \in \mathbb{F}A \cdot \widehat{H_e}$, then for every $\tau \in T$ and $h \in H_e$ we have $\alpha_{\tau h} = \alpha_\tau$.
So

$$\alpha = |H_e| \sum_{\tau \in T} \alpha_\tau \tau \cdot \widehat{H_e}.$$

Thus, if $\psi$ denotes natural projection, we have

$$\psi(\alpha) = |H_e| \sum \alpha_\tau \bar{\tau}.$$

## Corollary

Let $e \neq \widehat{A}$ be a primitive idempotent of $\mathbb{F}A$. Then, the factor group $A/H_e$ is cyclic.

## Corollary

Let $e \neq \widehat{A}$ be a primitive idempotent of $\mathbb{F}A$. Then, the factor group $A/H_e$ is cyclic.

## Definition (Sabin and Lomonaco (1995))

Let $G_1$ and $G_2$ denote two finite groups of the same order and let $\mathbb{F}$ be a field. Two ideals (codes) $I_1 \subset \mathbb{F}G_1$ and $I_2 \subset \mathbb{F}G_2$ are said to be **combinatorially equivalent** if there exists a bijection $\gamma : G_1 \to G_2$ whose linear extension $\overline{\gamma} : \mathbb{F}G_1 \to \mathbb{F}G_2$ is such that $\overline{\gamma}(I_1) = I_2$. The map $\overline{\gamma}$ is called a **combinatorial equivalence** between $I_1$ and $I_2$.

**Theorem (G. Chalom, R. Ferraz and PM)**

Every minimal ideal in the group algebra of a finite abelian group is combinatorially equivalent to a minimal ideal in the group algebra of a cyclic group of the same order.

# Cyclic codes vs Abelian Codes

We shall compare cyclic and Abelian codes of length $p^2$ under the hypotheses that $o(q) = \varphi(p^2)$ in $U(\mathbb{Z}_{p^n})$.

We shall compare cyclic and Abelian codes of length $p^2$ under the hypotheses that $o(q) = \varphi(p^2)$ in $U(\mathbb{Z}_{p^n})$.

### Remark

Note that in $\mathbb{F}C_{p^2}$ there exist precisely three primitive idempotents, namely:

$$e_0 = \widehat{G}, \;\; e_1 = \widehat{G_1} - \widehat{G} \;\; \text{e} \;\; e_2 = \widehat{G_2} - \widehat{G_1}.$$

We shall compare cyclic and Abelian codes of length $p^2$ under the hypotheses that $o(q) = \varphi(p^2)$ in $U(\mathbb{Z}_{p^n})$.

**Remark**

Note that in $\mathbb{F}C_{p^2}$ there exist precisely three primitive idempotents, namely:

$$e_0 = \widehat{G}, \;\; e_1 = \widehat{G_1} - \widehat{G} \quad \text{e} \quad e_2 = \widehat{G_2} - \widehat{G_1}.$$

Ideals of maximum dimension for each possible weight are:

$$I = I_0 \oplus I_1 \quad \text{e} \quad J = I_1 \oplus I_2$$

with $dim(I) = p$, $w(I) = p$ e $dim(J) = p^2 - 1$, $w(J) = 2$.

Now we consider Abelian non-cyclic codes of length $p^2$; i.e., ideals of $\mathbb{F}G$ where

$$G = (C_p \times C_p) = < a > \times < b > .$$

Now we consider Abelian non-cyclic codes of length $p^2$; i.e., ideals of $\mathbb{F}G$ where

$$G = (C_p \times C_p) =< a > \times < b > .$$

To find the primitive idempotents of $\mathbb{F}G$, we need to find subgroups $H$ of $G$ such that $G/H$ is cyclic.

Now we consider Abelian non-cyclic codes of length $p^2$; i.e., ideals of $\mathbb{F}G$ where

$$G = (C_p \times C_p) = < a > \times < b > .$$

To find the primitive idempotents of $\mathbb{F}G$, we need to find subgroups $H$ of $G$ such that $G/H$ is cyclic.

The idempotents of $\mathbb{F}G$ are:

$$e_0 = \widehat{G},\ e_1 = \widehat{< a >} - \widehat{G},\ e_2 = \widehat{< b >} - \widehat{G},$$

$$f_i = \widehat{< ab^i >} - \widehat{G}, 1 \leq i \leq p-1.$$

Weights and dimensions of minimal codes are:

Weights and dimensions of minimal codes are:

$$dim(\mathbb{F}G)e_0 = 1 \quad \text{e} \quad dim(\mathbb{F}G)e_1 = dim(\mathbb{F}G)f_i = p - 1,$$
$$w((\mathbb{F}G)e_0) = p^2 \quad \text{e} \quad w((\mathbb{F}G)e_1) = w((\mathbb{F}G)f_i) = 2p.$$

Weights and dimensions of minimal codes are:

$$dim(\mathbb{F}G)e_0 = 1 \quad \text{e} \quad dim(\mathbb{F}G)e_1 = dim(\mathbb{F}G)f_i = p - 1,$$
$$w((\mathbb{F}G)e_0) = p^2 \quad \text{e} \quad w((\mathbb{F}G)e_1) = w((\mathbb{F}G)f_i) = 2p.$$

Given any two subgroups $H$, $K$ as above, then $G = H \times K$.

Weights and dimensions of minimal codes are:

$$dim(\mathbb{F}G)e_0 = 1 \quad \text{e} \quad dim(\mathbb{F}G)e_1 = dim(\mathbb{F}G)f_i = p-1,$$
$$w((\mathbb{F}G)e_0) = p^2 \quad \text{e} \quad w((\mathbb{F}G)e_1) = w((\mathbb{F}G)f_i) = 2p.$$

Given any two subgroups $H$, $K$ as above, then $G = H \times K$. Write $H =< h >$ and $K =< k >$. The corresponding central idempotents are $e = \widehat{H} - \widehat{G}$, $f = \widehat{K} - \widehat{G}$. Consider

$$I = (\mathbb{F}G)e \oplus (\mathbb{F}G)f,$$

**Teorema (F. Melo e P.M)**

The weight and dimension of $I = (\mathbb{F}G)e \oplus (\mathbb{F}G)f$ are

$$w(I) = dim(I) = 2p - 2,$$

## Teorema (F. Melo e P.M)

The weight and dimension of $I = (\mathbb{F}G)e \oplus (\mathbb{F}G)f$ are

$$w(I) = dim(I) = 2p - 2,$$

## Definition

The **convenience** of a code $\mathcal{C}$ is the number

$$conv(\mathcal{C}) = w(\mathcal{C})dim(\mathcal{C}).$$

For the cyclic non-minimal codes we have:

$$conv(I_0 \oplus I_1) = p^2 \text{ e } conv(I_1 \oplus I_2) = 2(p^2 - 1).$$

For the cyclic non-minimal codes we have:

$$conv(I_0 \oplus I_1) = p^2 \text{ e } conv(I_1 \oplus I_2) = 2(p^2 - 1).$$

For the sum of two minimal Abelian (non-cyclic) codes we have:

$$conv(\mathfrak{M}) = 4(p - 1)^2.$$

For the cyclic non-minimal codes we have:

$$conv(I_0 \oplus I_1) = p^2 \text{ e } conv(I_1 \oplus I_2) = 2(p^2 - 1).$$

For the sum of two minimal Abelian (non-cyclic) codes we have:

$$conv(\mathfrak{M}) = 4(p-1)^2.$$

Hence, if $p > 3$, we have that $conv(\mathfrak{M})$ is bigger than $conv(I)$ for any proper ideal $I$ of $\mathbb{F}_q C_{p^2}$.

# Group algebras over finite fields

In this section, $\mathbb{F}_q$ will always denote a finite field with $q$ elements, $C = C_n$ the cyclic of order $n$, with generator $g$ and we shall assume that $(q, n) = 1$.

**Proposition**

Let $C$ be a cyclic group of order $n$ and let $m$ be the multiplicative order of $\overline{q}$ in the unit group $U(\mathbb{Z}_n)$. If $e$ is an essential idempotent, then the dimension of $\mathbb{F}_q C \cdot e$ is precisely $m$.

In this section, $\mathbb{F}_q$ will always denote a finite field with $q$ elements, $C = C_n$ the cyclic of order $n$, with generator $g$ and we shall assume that $(q, n) = 1$.

### Proposition

Let $C$ be a cyclic group of order $n$ and let $m$ be the multiplicative order of $\overline{q}$ in the unit group $U(\mathbb{Z}_n)$. If $e$ is an essential idempotent, then the dimension of $\mathbb{F}_q C \cdot e$ is precisely $m$.

### Theorem

Let $C_n$ denote a cyclic group of order $n$ and generator $g$. Then:
$(i)$ $dim(\mathbb{F}_q C_n)e_0 = \varphi(n)$ where $\varphi$ denotes Euler's Totient function.
$(ii)$ There exist precisely $\varphi(n)/m$ essential idempotents in $\mathbb{F}_q C$.

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

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

As $e$ is essential, we have that $C \cong C \cdot e$, so $C \cdot e$ is a subgroup of order $n$ of $U_e$. Set $\ell = N/n$.
Denote by $C_n$ and $C_N$ the cyclic groups of orders $n$ and $N$, with generators $g$ and $h$ respectively.

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

As $e$ is essential, we have that $C \cong C \cdot e$, so $C \cdot e$ is a subgroup of order $n$ of $U_e$. Set $\ell = N/n$.
Denote by $C_n$ and $C_N$ the cyclic groups of orders $n$ and $N$, with generators $g$ and $h$ respectively.

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 $\sigma$ be such an isomorphism and denote also by $\sigma : \mathbb{F}_q\langle h^\ell \rangle \to \mathbb{F}_q C_n$ the isomorphism induced linearly by $\sigma$.

## Theorem

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 $U_e$.

- G. K. Bakshi, M. Raka, A. Sharma, Idempotent 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.
- S.D. Berman, On the theory of group codes, *Kibernetika*, **3**, 1 (1967) 31–39.
- S.D. Berman, Semisimple cyclic and abelian codes II, *Kibernetika*, **3** , (1967) 17–23.
- F. Melo and C. Polcino Milies, On Cyclic and Abelian Codes, *IEEE Transactions on Information Theory*, **59**, 11 (2013), 7314-7319.
- F.J. MacWilliams, Binary codes which are ideals in the group algebra of an abelian group, *Bell System Tech. J.*, **49** (1970), 987–1011.
- C. Polcino Milies and S.K. Sehgal, *An introduction to group rings*, Algebras and Applications, Kluwer Academic Publishers, Dortrecht, 2002.
- R.E. Sabin and S.J. Lomonaco, Metacyclic Error-correcting Codes, *Applicable Algebra in Engeneering, Communication and Computing*, **6** (1995), 191–210.