Semisimple Group Codes

César Polcino Milies

Universidade de São Paulo

Basic Facts

The basic elements to build a code are the following:

Basic Facts

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.

Basic Facts

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.

Basic Facts

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:

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

A classical scheme due to Shannon

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

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 error-correcting 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.

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 κ 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 κ errores.

Definition

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

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

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:

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

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:

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

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

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:

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

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

$$[a_0 + a_1 X + \ldots + a_{n-2} X^{n-2} + a_{n-1} X^{n-1}].$$

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:

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

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

$$[a_0 + a_1 X + \ldots + a_{n-2}X^{n-2} + a_{n-1}X^{n-1}].$$

φ is an isomorphism of $\mathbb{F}$-vector spaces. Hence *A code $\mathcal{C} \subset \mathbb{F}^n$ is*

It is easy to show that

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

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 $\mathbb{F}C_n$.

Definition

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

The ideals generated by the primitive idempotents; i.e. the ideals of the form $I_i = \mathbb{F}Ge_i$ are the minimal ideals of $\mathbb{F}G$.

The ideals generated by the primitive idempotents; i.e. the ideals of the form $I_i = \mathbb{F}Ge_i$ are the minimal ideals of $\mathbb{F}G$.

Also, every ideal of $\mathbb{F}G$ is of the form $I = \mathbb{F}Ge$, where $e \in \mathbb{F}G$ is an idempotent element.

The ideals generated by the primitive idempotents; i.e. the ideals of the form $I_i = \mathbb{F}Ge_i$ are the minimal ideals of $\mathbb{F}G$.

Also, every ideal of $\mathbb{F}G$ is of the form $I = \mathbb{F}Ge$, where $e \in \mathbb{F}G$ is an idempotent element.

Hence:

If we assume that $char(\mathbb{F}) \nmid |G|$, then to study group codes is equivalent to study ideals in group algebras, generated by idempotent elements

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

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

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

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

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

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

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

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

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:

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

As we shall see, they will be very useful.

Code Parameters

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 $H \subset H^*$ 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 $(FG)e$.

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 $H \subset H^*$ and set $e = \widehat{H} - \widehat{H^*}$. Let $\mathcal{A}$ be a transversal of H^* in G and τ 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 $H_i \subset H_i^*$, be normal subgroups of a group $G, 1 \leq i \leq k$, such that $H_i^* \cap N_i^* = \{1\}$, where N_i denotes the subgroup generated by all H_j^* with $j \neq i$. Set $e = (\widehat{H_1} - \widehat{H_1^*})(\widehat{H_2} - \widehat{H_2^*}) \cdots (\widehat{H_k} - \widehat{H_k^*})$.
Then,
$dim_F(FG)e =$

$$\frac{|G|}{|H_1 H_2 \cdots H_k|} \left(1 - \frac{|H_1|}{|H_1^*|}\right) \left(1 - \frac{|H_2|}{|H_2^*|}\right) \cdots \left(1 - \frac{|H_k|}{|H_k^*|}\right)$$

and

$$w\left((FG)e\right) \ = \ 2^k |H_1 H_2 \cdots H_k|.$$

Let $H_i \subset H_i^*$, be normal subgroups of a group G, $1 \leq i \leq k$, such that $H_i^* \cap N_i^* = \{1\}$, where N_i denotes the subgroup generated by all H_j^* with $j \neq i$. Set $e = (\widehat{H_1} - \widehat{H_1^*})(\widehat{H_2} - \widehat{H_2^*}) \cdots (\widehat{H_k} - \widehat{H_k^*})$. Let $\mathcal{A}$ be a transversal of H^* in G and τ_i a transversal of H_i in H_i^* containing 1, $1 \leq i \leq k$. Then

$$\mathcal{B} = \{a(1-t_1)(1-t_2)\cdots(1-t_k)\widehat{H} \mid a \in \mathcal{A}, t_i \in \tau_i, t_i \neq 1, 1 \leq i \leq k\}$$

is a basis of $(\mathbb{F}G)e$ over $\mathbb{F}$.

Is it possible to determine the primitive central idempotents from the subgroup idempotents?

Remark

Let $\mathbb{F}$ be a field with q elements and A a cyclic group of order p^n, with $(q, n) = 1$. Let

$$A = A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

be the descending chain of all subgroups of A.

Remark

Let $\mathbb{F}$ be a field with q elements and A a cyclic group of order p^n, with $(q, n) = 1$. Let

$$A \;=\; A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

be the descending chain of all subgroups of A.
Set:

$$e_0 \;=\; \widehat{A} \;=\; \frac{1}{p^n}\left(\sum_{a \in A} a\right)$$

$$e_i = \widehat{A_i} - \widehat{A_{i-1}},\; 1 \leq i \leq n.$$

Remark

Let $\mathbb{F}$ be a field with q elements and A a cyclic group of order p^n, with $(q,n)=1$. Let

$$A \ = \ A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

be the descending chain of all subgroups of A.
Set:

$$e_0 \ = \ \widehat{A} \ = \ \frac{1}{p^n}\left(\sum_{a\in A} a\right)$$

$$e_i = \widehat{A_i} - \widehat{A_{i-1}}, \ 1 \leq i \leq n.$$

Then $\{e_0, e_1, \ldots, e_n\}$ is a set of orthogonal idempotents such that

$$e_0 + e_1 + \cdots + e_n \ = \ 1.$$

For each automorphism $\sigma \in Gal(\mathbb{F}(\zeta), \mathbb{F})$, we have $\sigma(\zeta) = \zeta^r$ for some positive integer r.

For each automorphism $\sigma \in Gal(\mathbb{F}(\zeta), \mathbb{F})$, we have $\sigma(\zeta) = \zeta^r$ for some positive integer r.
We define an action of σ on G by:

$$\sigma : g \mapsto g^r$$

For each automorphism $\sigma \in Gal(\mathbb{F}(\zeta), \mathbb{F})$, we have $\sigma(\zeta) = \zeta^r$ for some positive integer r.
We define an action of σ on G by:

$$\sigma : g \mapsto g^r$$

Definition

Two conjugacy classes of G are said to be $\mathbb{F}$-*conjugate* if they correspond under this action. This notion of $\mathbb{F}$-conjugacy is an equivalence relation on the conjugacy classes of G and the corresponding equivalence classes are called $\mathbb{F}$-*classes*.

The number of simple components of the group algebra $\mathbb{F}G$ is the number of $\mathbb{F}$-classes of G.

Definition

Given an element $g \in G$, and a positive integer q then, the $q-$ *cyclotomic class* of g is the set

$$S_g = \{g^{q^j} | 0 \leq j \leq t_g - 1\}$$

where t_g is the least positive integer such that $q^{t_g} \equiv 1 (mod\ o(g))$ and $o(g)$ stands for the order of g.

Definition

Given an element $g \in G$, and a positive integer q then, the $q-$ *cyclotomic class* of g is the set

$$S_g = \{g^{q^j} | 0 \leq j \leq t_g - 1\}$$

where t_g is the least positive integer such that $q^{t_g} \equiv 1 (mod\ o(g))$ and $o(g)$ stands for the order of g.

Remark If G is an abelian group, then elements and conjugacy classes coincide. Hence, in this case if $|\mathbb{F}| = q$, then the $\mathbb{F}$-classes defined above are the same as the q-cyclotomic classes

Theorem (Arora-Pruthi (1997), Ferraz-P.M. (2007))

Let $\mathbb{F}$ be a field with q elements and A a cyclic group of order p^n such that $o(q) = \varphi(p^n)$ in $U(\mathbb{Z}_{p^n})$ (where φ denots Euler's Totient function). Let

$$A \ = \ A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

be the descending chain of all subgroups of A. Then, the set of primitive idempotents of FA is given by:

$$e_0 \ = \ \frac{1}{p^n}\left(\sum_{a\in A} a\right)$$

$$e_i = \widehat{A_i} - \widehat{A_{i-1}}, \ 1 \leq i \leq n.$$

Theorem (Arora and Pruthi (2002), Ferraz-PM (2007))

Let $\mathbb{F}$ be a field with q elements and A a cyclic group of order $2p^n$, p an odd prime, such that $o(q) = \varphi(p^n)$ in $U(\mathbb{Z}_{2p^n})$.
Write $G = C \times A$ where A denotes the p-Sylow subgroup of G and $C = \{1, t\}$ is the 2-Sylow subgroup.
If e_i, $0 \leq i \leq n$ denotes the set of primitive idempotents of $\mathbb{F}A$, then the primitive idempotents of $\mathbb{F}G$ are

$$\frac{(1+t)}{2} \cdot e_i \quad \text{and} \quad \frac{(1-t)}{2} \cdot e_i \quad 0 \leq i \leq n.$$

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

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

Theorem (Ferraz-PM (2007))

Let p be an odd prime and let A be an Abelian p-group of exponent p^r. Then, the set of idemponts above is the set of primitive idempotents of $\mathbb{F}A$ if and only if one of the following holds:

(i) $p^r = 2$, and q is odd.

(ii) $p^r = 4$ and $q \equiv 3 \pmod 4$.

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

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 $U(\mathbb{Z}_{2p^n})$.

Proposition (Ferraz-Goodaire-PM)

Let $A = \langle t \rangle$ be a cyclic group of order 2^m and $\mathbb{F}$ a field such that $char(\mathbb{F}) \not| \, |A|$ then:

(i) If $m = 1$, for any such field $\mathbb{F}$, there are precisely two F-classes in A.

(ii) If $m > 1$, the number of $\mathbb{Q}$-classes of A is $m + 1$ and at least $2m - 1$ for any finite field $\mathbb{F}$. This minimal number is achieved if $\mathbb{F}$ has order $q \equiv 3 \pmod{8}$.

Proposition (Ferraz-Goodaire-PM)

Let $A = \langle t \rangle$ be a cyclic group of order 2^m and $\mathbb{F}$ a field such that $char(\mathbb{F}) \not| \, |A|$ then:

(i) If $m = 1$, for any such field $\mathbb{F}$, there are precisely two F-classes in A.

(ii) If $m > 1$, the number of $\mathbb{Q}$-classes of A is $m + 1$ and at least $2m - 1$ for any finite field $\mathbb{F}$. This minimal number is achieved if $\mathbb{F}$ has order $q \equiv 3 \pmod{8}$.

Lemma

If $q \equiv 3$ $(mod\ 8)$, then -2 has a square root módulo q.
In what follows, this square root will be denoted by α (in both cases).

Theorem *(J. do Prado)*

In the case when $q \equiv 3 (mod\ 8)$ and $A =< a >$, the primitive idempotents of $\mathbb{F}G$ are:

Theorem *(J. do Prado)*

In the case when $q \equiv 3 (mod\ 8)$ and $A =< a >$, the primitive idempotents of $\mathbb{F}G$ are:

$$
\begin{aligned}
\epsilon_0 &= \widehat{A}, \\
\epsilon_1 &= \frac{1 - a + a^2 - \cdots - a^{2^m - 1}}{2^m}, \\
\epsilon_2 &= \frac{1 - a^2 + a^4 - \cdots - a^{2^m - 2}}{2^{m-1}}, \\
\epsilon_3 &= (1 - a^4)\frac{(1 + a^{2^3} + \cdots + a^{2^m - 2^3})(2 + \alpha a + \alpha a^3)}{2^m}, \\
\epsilon_3' &= (1 - a^4)\frac{(1 + a^{2^3} + \cdots + a^{2^m - 2^3})(2 - \alpha a - \alpha a^3)}{2^m},
\end{aligned}
$$

$$
\begin{aligned}
\epsilon_4 &= (1-a^8)\frac{(1+a^{2^4}+\cdots+a^{2^m-2^4})(2+\alpha a^2+\alpha a^{3,2})}{2^{m-1}}, \\
\epsilon_4' &= (1-a^8)\frac{(1+a^{2^4}+\cdots+a^{2^m-2^4})(2-\alpha a^2-\alpha a^{3,2})}{2^{m-1}}, \\
& \cdots \\
\epsilon_{m-1} &= (1-a^{2^{m-2}})\frac{(1+a^{2^{m-1}})(2+\alpha a^{2^{m-4}}+\alpha a^{3,2^{m-4}})}{2^4}, \\
\epsilon_{m-1}' &= (1-a^{2^{m-2}})\frac{(1+a^{2^{m-1}})(2-\alpha a^{2^{m-4}}-\alpha a^{3,2^{m-4}})}{2^4}, \\
\epsilon_m &= (1-a^{2^{m-1}})\frac{(2+\alpha a^{2^{m-3}}+\alpha a^{3,2^{m-3}})}{2^3}, \\
\epsilon_m' &= (1-a^{2^{m-1}})\frac{(2-\alpha a^{2^{m-3}}-\alpha a^{3,2^{m-3}})}{2^3}.
\end{aligned}
$$

Theorem

The minimal ideals of $\mathbb{F}A$ are:

$$I_i = (\mathbb{F}A)\epsilon_i, \;\; i = 0, 1, 2,$$

$$J_j = (\mathbb{F}A)\epsilon_j, \quad \text{and} \quad L_j = (\mathbb{F}A)\epsilon_j', \quad \text{for} \quad 3 \leq j \leq m$$

and

Theorem

The minimal ideals of $\mathbb{F}A$ are:

$$I_i = (\mathbb{F}A)\epsilon_i, \;\; i = 0, 1, 2,$$

$$J_j = (\mathbb{F}A)\epsilon_j, \quad \text{and} \quad L_j = (\mathbb{F}A)\epsilon_j', \quad \text{for} \quad 3 \leq j \leq m$$

and

(i) $dim(I_i) = 1$ and $w(I_i) = 2^m$, for $i = 1, 0$; $dim(I_2) = 2$ and $w(I_2) = 2^{m-1}$.

Theorem

The minimal ideals of $\mathbb{F}A$ are:

$$I_i = (\mathbb{F}A)\epsilon_i, \; i = 0, 1, 2,$$

$$J_j = (\mathbb{F}A)\epsilon_j, \quad \text{and} \quad L_j = (\mathbb{F}A)\epsilon_j', \quad \text{for} \quad 3 \leq j \leq m$$

and

(i) $dim(I_i) = 1$ and $w(I_i) = 2^m$, for $i = 1, 0$; $dim(I_2) = 2$ and $w(I_2) = 2^{m-1}$.

(ii)

$$dim(J_j) = dim(L_j) = 2^{j-2}$$

$$w(J_j) = w(L_j) = w(\epsilon_j) = 3 \cdot 2^{m-j+1}, \text{ for } 3 \leq j \leq m.$$

Proposition

The set:

$$\begin{aligned}\mathcal{B}_j &= \left\{\epsilon_j, a\epsilon_j, a^2\epsilon_j, \ldots, a^{2^{j-3}-1}\epsilon_j\right\} \\ &\bigcup \left\{a^{2^{j-2}}\epsilon_j, a^{2^{j-2}+1}\epsilon_j, a^{2^{j-2}+2}\epsilon_j, \ldots, a^{2^{j-2}+2^{j-3}-1}\epsilon_j\right\}\end{aligned}$$

is a basis of J_j.

Similarly exchanging above ϵ_j by ϵ'_j, we obtain a basis of L_j.

Let G be a nonabelian group with an involution $g \mapsto g^*$ (an antiautomorphism of order two) which is such that $gg^* \in \mathbb{Z}(G)$, the centre of G, for all $g \in G$. Let $g_0 \in \mathbb{Z}(G)$ be an element fixed by $*$ and let u be an element not in G.

Let G be a nonabelian group with an involution $g \mapsto g^*$ (an antiautomorphism of order two) which is such that $gg^* \in \mathbb{Z}(G)$, the centre of G, for all $g \in G$. Let $g_0 \in \mathbb{Z}(G)$ be an element fixed by $*$ and let u be an element not in G.

Let $L = G \cup Gu$ with multiplication defined by

Let G be a nonabelian group with an involution $g \mapsto g^*$ (an antiautomorphism of order two) which is such that $gg^* \in \mathbb{Z}(G)$, the centre of G, for all $g \in G$. Let $g_0 \in \mathbb{Z}(G)$ be an element fixed by $*$ and let u be an element not in G.
Let $L = G \cup Gu$ with multiplication defined by

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^*)u \\ (gu)(hu) &= g_0 h^* g \end{aligned}$$

for $g, h \in G$.

Let G be a nonabelian group with an involution $g \mapsto g^*$ (an antiautomorphism of order two) which is such that $gg^* \in \mathbb{Z}(G)$, the centre of G, for all $g \in G$. Let $g_0 \in \mathbb{Z}(G)$ be an element fixed by $*$ and let u be an element not in G.
Let $L = G \cup Gu$ with multiplication defined by

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^*)u \\ (gu)(hu) &= g_0 h^* g \end{aligned}$$

for $g, h \in G$.
Then L is a Moufang loop, denoted $M(G, *, g_0)$.

If $G/\mathcal{C}Z(G) \cong C_2 \times C_2$, then the commutator subgroup $G' = \{1, s\}$ is central of order two, the map $*\colon G \longrightarrow G$ defined by

$$g^* = \begin{cases} g & \text{if } g \in \mathcal{C}Z(G) \\ sg & \text{if } g \notin \mathcal{C}Z(G), \end{cases} \tag{1}$$

is an involution (an SLC group).

If $G/\mathcal{C}Z(G) \cong C_2 \times C_2$, then the commutator subgroup $G' = \{1, s\}$ is central of order two, the map $*\colon G \to G$ defined by

$$g^* = \begin{cases} g & \text{if } g \in \mathcal{C}Z(G) \\ sg & \text{if } g \notin \mathcal{C}Z(G), \end{cases} \tag{1}$$

is an involution (an SLC group).

The loop $L = M(G, *, g_0)$ is an RA (ring alternative) loop; that is, over any (commutative associative) coefficient ring R (with 1), the loop ring RL is alternative, but not associative. Moreover, all RA loops can be constructed in this way.

There are exactly seven classes of finite RA loops which are indecomposable in the sense that they are not the direct products of nontrivial subloops.

There are exactly seven classes of finite RA loops which are indecomposable in the sense that they are not the direct products of nontrivial subloops.

In six of these classes, the groups G defining the RA loops $M(G, *, g_0)$ come from one of the five classes $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathcal{D}_4, \mathcal{D}_5$ described below.

There are exactly seven classes of finite RA loops which are indecomposable in the sense that they are not the direct products of nontrivial subloops.

In six of these classes, the groups G defining the RA loops $M(G, *, g_0)$ come from one of the five classes $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathcal{D}_4, \mathcal{D}_5$ described below.

In the seventh class of indecomposable loops, the groups are the direct products of a group in dd_5 with a cyclic group.

In each class of groups, the groups are generated by their centre, which is the direct product of at most three cyclic groups, and two other elements x and y.

In each class of groups, the groups are generated by their centre, which is the direct product of at most three cyclic groups, and two other elements x and y.

$$\mathcal{D}_1 : \langle x, y, t_1 \mid x^2 = y^2 = t_1^{2^m} = 1, m \geq 1\rangle$$
$$\mathcal{D}_2 : \langle x, y, t_1 \mid x^2 = y^2 = t_1, t_1^{2^m} = 1, m \geq 1\rangle$$
$$\mathcal{D}_3 : \langle x, y, t_1, t_2 \mid x^2 = t_1^{2^{m_1}} = t_2^{2^{m_2}} = 1, y^2 = t_2, m_1, m_2 \geq 1\rangle$$
$$\mathcal{D}_4 : \langle x, y, t_1, t_2 \mid x^2 = t_1, y^2 = t_2, t_1^{2^{m_1}} = t_2^{2^{m_2}} = 1, m_1, m_2 \geq 1\rangle$$
$$\mathcal{D}_5 : \langle x, y, t_1, t_2, t_3 \mid x^2 = t_2, y^2 = t_3, t_1^{2^{m_1}} = t_2^{2^{m_2}} = t_3^{2^{m_3}} = 1, m_1, m_2, m_2 \geq 1\rangle.$$

Theorem

Let $L = M(G, *, g_0)$ be an RA loop and F a field of characteristic different from 2. Then $FG = \oplus_{i=1}^{n} A_i$ is the direct sum of simple algebras A_i, each A_i is invariant under the involution $*$.

Theorem

Let $L = M(G, *, g_0)$ be an RA loop and F a field of characteristic different from 2. Then $FG = \oplus_{i=1}^{n} A_i$ is the direct sum of simple algebras A_i, each A_i is invariant under the involution $*$.

Moreover, $FL = \oplus_{i=1}^{n}(A_i + A_i u)$ for some $u \in L \setminus G$ with each $A_i + A_i u$ the direct sum of two fields or a simple Cayley algebra.

Theorem (Ferraz, Goodaire and PM)

Suppose that $L = M(G, *, 1)$ is the class $\mathcal{L}_1$ of loops corresponding to a group of type $\mathcal{D}_1$. Then $\mathbb{Q}G$ is the direct sum of $8m$ fields and the split Cayley algebra.

Theorem (Ferraz, Goodaire and PM)

Suppose that $L = M(G, *, 1)$ is the class $\mathcal{L}_1$ of loops corresponding to a group of type $\mathcal{D}_1$. Then $\mathbb{Q}G$ is the direct sum of $8m$ fields and the split Cayley algebra.
If $L = M(G, *, 1)$ is the corresponding indecomposable RA loop, then $\mathbb{F}L$ is the direct sum of $2(8m-12) = 16m-24$ fields and 5 split Cayley algebras.

Theorem (Ferraz, Goodaire and PM)

Suppose that $L = M(G,*,1)$ is the class $\mathcal{L}_1$ of loops corresponding to a group of type $\mathcal{D}_1$. Then $\mathbb{Q}G$ is the direct sum of $8m$ fields and the split Cayley algebra.
If $L = M(G,*,1)$ is the corresponding indecomposable RA loop, then $\mathbb{F}L$ is the direct sum of $2(8m-12) = 16m-24$ fields and 5 split Cayley algebras.

If $L = M(G,*,g_0)$ is an RA loop of type $\mathcal{L}_2$, then $\mathbb{Q}L$ is the direct sum of $4m+4$ fields and one Cayley algebra.
The loop algebra $\mathbb{F}L$ of the corresponding RA loop L is the direct sum of $8m-4$ fields and four Cayley algebras.

Theorem (Goodaire,Ferraz and PM)

Let K be any field (of characteristic not 2) and let L be a loop from the class $\mathcal{L}_6$ with $m_1 = 1, m_2 = 2$ and $m_3 = 1$ and let M be a loop of the same order, in the class $\mathcal{L}_5$.

Theorem (Goodaire,Ferraz and PM)

Let K be any field (of characteristic not 2) and let L be a loop from the class $\mathcal{L}_6$ with $m_1 = 1, m_2 = 2$ and $m_3 = 1$ and let M be a loop of the same order, in the class $\mathcal{L}_5$.

Then $KL \cong KM$ but $L \ncong M$.