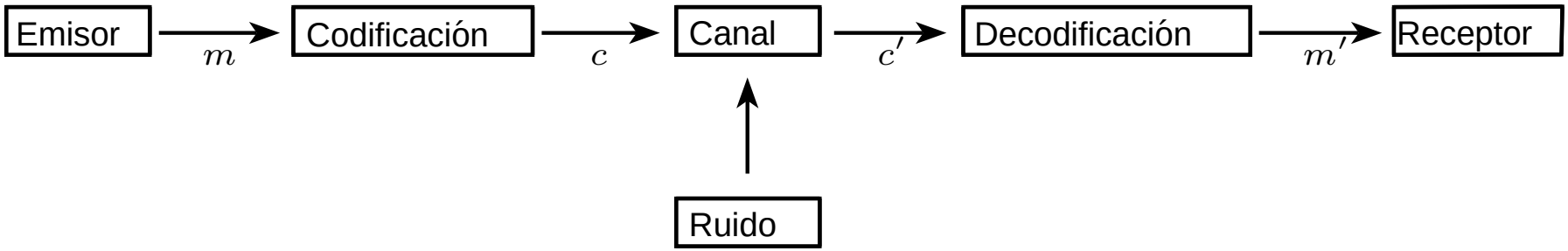
TEORÍA DE CÓDIGOS & ÁLGEBRAS DE GRUPOS

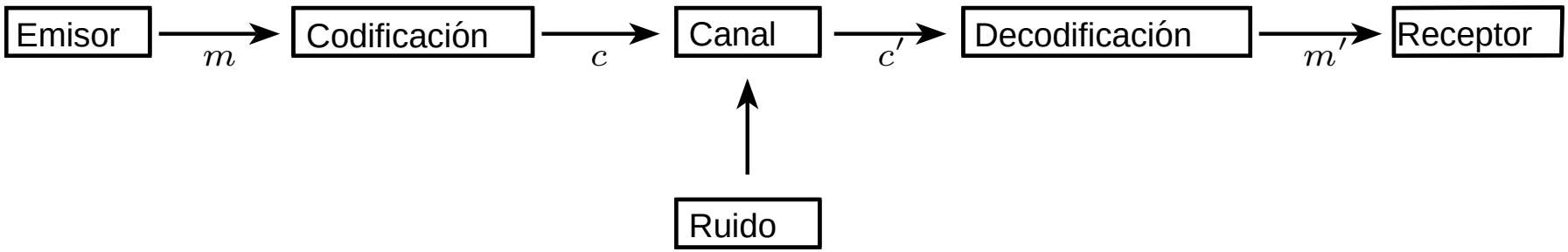
Gerson Leonel Barajas Ávila

Escuela de Matemáticas
Universidad Industrial de Santander
Grupo ALCOM

2016

Índice


Emisor
m
Codificación
c
Canal
c'
Decodificación
m'
Receptor
Ruido



1. ¿Es seguro?
2. ¿Es confiable?

Conceptos Básicos

De igual manera que en lenguaje español, para la construcción de códigos son necesarios los siguientes elemento básicos:

Conceptos Básicos

De igual manera que en lenguaje español, para la construcción de códigos son necesarios los siguientes elemento básicos:

1. Un conjunto finito $\mathcal{A}$ que llamaremos *alfabeto*.
2. Secuencias finitas de símbolos del alfabeto, que llamaremos *palabras*. El número de letras de una palabra es su *longitud*.

Conceptos Básicos

De igual manera que en lenguaje español, para la construcción de códigos son necesarios los siguientes elemento básicos:

1. Un conjunto finito $\mathcal{A}$ que llamaremos *alfabeto*.
2. Secuencias finitas de símbolos del alfabeto, que llamaremos *palabras*. El número de letras de una palabra es su *longitud*.

Un *Código q-ario de lo longitud n* será un subconjunto cualquiera de palabras de longitud n, es decir, un código $\mathcal{C}$ es un subconjunto de $\mathcal{A}^n = \underbrace{\mathcal{A} \times \mathcal{A} \times \cdots \mathcal{A}}_{n-veces}$.

Conceptos Básicos

De igual manera que en lenguaje español, para la construcción de códigos son necesarios los siguientes elemento básicos:

1. Un conjunto finito $\mathcal{A}$ que llamaremos *alfabeto*.
2. Secuencias finitas de símbolos del alfabeto, que llamaremos *palabras*. El número de letras de una palabra es su *longitud*.

Un *Código q-ario de lo longitud n* será un subconjunto cualquiera de palabras de longitud n, es decir, un código $\mathcal{C}$ es un subconjunto de $\mathcal{A}^n = \underbrace{\mathcal{A} \times \mathcal{A} \times \cdots \mathcal{A}}_{n-veces}$.

El número M de elementos del código también es importante, pues cuanto mayor sea M, mayor es la cantidad de información que puede ser trasmitida. Así, un código q-ario, de longitud n que contiene M palabras es llamado (n, M)-código q-ario.

Conceptos Básicos

De igual manera que en lenguaje español, para la construcción de códigos son necesarios los siguientes elemento básicos:

1. Un conjunto finito $\mathcal{A}$ que llamaremos *alfabeto*.
2. Secuencias finitas de símbolos del alfabeto, que llamaremos *palabras*. El número de letras de una palabra es su *longitud*.

Un *Código q-ario de lo longitud n* será un subconjunto cualquiera de palabras de longitud n, es decir, un código $\mathcal{C}$ es un subconjunto de $\mathcal{A}^n = \underbrace{\mathcal{A} \times \mathcal{A} \times \cdots \mathcal{A}}_{n-veces}$.

El número M de elementos del código también es importante, pues cuanto mayor sea M, mayor es la cantidad de información que puede ser trasmitida. Así, un código q-ario, de longitud n que contiene M palabras es llamado (n, M)-código q-ario.

$c \in \mathcal{C} \subset \mathcal{A}^n$, es de la forma $c = (a_1, a_2, \ldots, a_n)$, donde $a_i \in \mathcal{A}$, $1 \leq i \leq n$. Escribiremos a c como una secuencia de elementos en $\mathcal{A}$, es decir, de la forma $c = a_1 a_2 \ldots a_n$.

Definición

Sean $x = x_1x_2 \dots x_n$, $y = y_1y_2 \dots y_n$ dos palabras de un código $\mathcal{C} \subset \mathcal{A}^n$. La distancia de Hamming entre x e y, denotada por $d(x, y)$, se define por

Definición

Sean $x = x_1x_2 \dots x_n$, $y = y_1y_2 \dots y_n$ *dos palabras de un código* $\mathcal{C} \subset \mathcal{A}^n$. *La distancia de Hamming entre* x *e* y, *denotada por* $d(x, y)$, *se define por*

$$d(x, y) = \#\{1 \leq i \leq n : x_i \neq y_i\}.$$

Definición

Sean $x = x_1x_2 \dots x_n$, $y = y_1y_2 \dots y_n$ dos palabras de un código $\mathcal{C} \subset \mathcal{A}^n$. La distancia de Hamming entre x e y, denotada por $d(x, y)$, se define por

$$d(x, y) = \#\{1 \leq i \leq n : x_i \neq y_i\}.$$

Proposición

La función d es una métrica en $\mathcal{C}$, es decir que para todo x , y , z en $\mathcal{C}$, satisface las siguientes propiedades.

Definición

Sean $x = x_1x_2 \dots x_n$, $y = y_1y_2 \dots y_n$ *dos palabras de un código* $\mathcal{C} \subset \mathcal{A}^n$. *La distancia de Hamming entre* x *e* y, *denotada por* $d(x, y)$, *se define por*

$$d(x, y) = \#\{1 \leq i \leq n : x_i \neq y_i\}.$$

Proposición

La función d *es una métrica en* $\mathcal{C}$, *es decir que para todo* $x\,, y\,, z$ *en* $\mathcal{C}$, *satisface las siguientes propiedades.*

(i) $d(x, y) \geq 0$.

(ii) $d(x, y) = 0$ *si y solo si* $x = y$

(iii) $d(x, y) = d(y, x)$

(iv) $d(x, y) \leq d(x, z) + d(z, y)$

Ejemplo

Sea $\mathcal{C} = \{001, 011, 111\}$ *un código y supongamos que un emisor envía el mensaje* 111*, pero en la trasmisión de dicho mensaje, un ruido altera la codificación y/o decodificación, permitiendo así que el emisor reciba el mensaje* 110*.*

Ejemplo

Sea $\mathcal{C} = \{001, 011, 111\}$ *un código y supongamos que un emisor envía el mensaje* 111*, pero en la trasmisión de dicho mensaje, un ruido altera la codificación y/o decodificación, permitiendo así que el emisor reciba el mensaje* 110*.*

En este caso el receptor se da cuenta que el mensaje recibido es erróneo, puesto que $110 \notin \mathcal{C}$ *(Código detector).*

Ejemplo

Sea $\mathcal{C} = \{001, 011, 111\}$ *un código y supongamos que un emisor envía el mensaje* 111*, pero en la trasmisión de dicho mensaje, un ruido altera la codificación y/o decodificación, permitiendo así que el emisor reciba el mensaje* 110*.*

En este caso el receptor se da cuenta que el mensaje recibido es erróneo, puesto que $110 \notin \mathcal{C}$ *(Código detector).*

¿Cuál fue el mensaje enviado?

Ejemplo

Sea $\mathcal{C} = \{001, 011, 111\}$ *un código y supongamos que un emisor envía el mensaje* 111*, pero en la trasmisión de dicho mensaje, un ruido altera la codificación y/o decodificación, permitiendo así que el emisor reciba el mensaje* 110*.*

En este caso el receptor se da cuenta que el mensaje recibido es erróneo, puesto que $110 \notin \mathcal{C}$ *(Código detector).*

¿Cuál fue el mensaje enviado?

Pero este método no siempre nos ayuda a corregir, consideremos la situación en que el emisor envía el mensaje 111*, pero en su trasmisión se altera, recibiendo así el receptor el mensaje* 101*, este último detecta el error puesto que* $101 \notin \mathcal{C}$*. Ahora veamos que:*

Ejemplo

Sea $\mathcal{C} = \{001, 011, 111\}$ *un código y supongamos que un emisor envía el mensaje* 111*, pero en la trasmisión de dicho mensaje, un ruido altera la codificación y/o decodificación, permitiendo así que el emisor reciba el mensaje* 110*.*

En este caso el receptor se da cuenta que el mensaje recibido es erróneo, puesto que $110 \notin \mathcal{C}$ *(Código detector).*

¿Cuál fue el mensaje enviado?

Pero este método no siempre nos ayuda a corregir, consideremos la situación en que el emisor envía el mensaje 111*, pero en su trasmisión se altera, recibiendo así el receptor el mensaje* 101*, este último detecta el error puesto que* $101 \notin \mathcal{C}$*. Ahora veamos que:*

$d((101), (001)) = 1 = d((101), (111))$*. Por tal razón, a pesar que se puede detectar el error, este no puede ser corregido.*

Definición (Código Lineal)

Sea $\mathcal{A} = \mathbb{F}_q$ un alfabeto, si $\mathcal{C}$ es un subespacio de $\mathbb{F}_q^n$, entonces es llamado un código lineal.

Definición (Código Lineal)

Sea $\mathcal{A} = \mathbb{F}_q$ un alfabeto, si $\mathcal{C}$ es un subespacio de $\mathbb{F}_q^n$, entonces es llamado un código lineal.

Definición (Código cíclico)

Un código lineal $\mathcal{C} \subset \mathbb{F}_q^n$ es un código cíclico, si para toda palabra $c_0 c_1 \ldots c_{n-2} c_{n-1}$ en el código, se tiene que $c_{n-1} c_0 \ldots c_{n-2}$ está en el código.

Definición (Código Lineal)

Sea $\mathcal{A} = \mathbb{F}_q$ un alfabeto, si $\mathcal{C}$ es un subespacio de $\mathbb{F}_q^n$, entonces es llamado un código lineal.

Definición (Código cíclico)

Un código lineal $\mathcal{C} \subset \mathbb{F}_q^n$ es un código cíclico, si para toda palabra $c_0c_1 \ldots c_{n-2}c_{n-1}$ en el código, se tiene que $c_{n-1}c_0 \ldots c_{n-2}$ está en el código.

Note que la definición implica que si la palabra $c_0c_1 \ldots c_{n-2}c_{n-1}$ está en el código, entonces todos las palabras que se obtienen a partir de esta por una permutación cíclica de sus coordenadas también están en el código.

Observación

Si $\mathcal{C} \subset \mathbb{F}_q^n$ es un código lineal q-ario, a cada palabra código le podemos asignar un polinomio en $\mathbb{F}_q[x]$, mediante la siguiente aplicación.

$$\begin{array}{rccc} \mathbf{\Phi}: & \mathcal{C} \subset \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x] \\ & c = (c_i)_{0 \leq i \leq n-1} & \mapsto & \Phi(c) = \sum_{i=0}^{n-1} c_i x^i. \end{array}$$

Observación

Si $\mathcal{C} \subset \mathbb{F}_q^n$ es un código lineal q-ario, a cada palabra código le podemos asignar un polinomio en $\mathbb{F}_q[x]$, mediante la siguiente aplicación.

$$\begin{array}{rccc} \mathbf{\Phi}: & \mathcal{C} \subset \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x] \\ & c = (c_i)_{0 \leq i \leq n-1} & \mapsto & \Phi(c) = \sum_{i=0}^{n-1} c_i x^i. \end{array}$$

Sea $R_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$ el álgebra de polinomios de grado menor que n.

Observación

Si $\mathcal{C} \subset \mathbb{F}_q^n$ es un código lineal q-ario, a cada palabra código le podemos asignar un polinomio en $\mathbb{F}_q[x]$, mediante la siguiente aplicación.

$$\begin{array}{rccc} \mathbf{\Phi}: & \mathcal{C} \subset \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x] \\ & c = (c_i)_{0 \leq i \leq n-1} & \mapsto & \Phi(c) = \sum_{i=0}^{n-1} c_i x^i. \end{array}$$

Sea $R_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$ el álgebra de polinomios de grado menor que n.

Observación

consideremos la siguiente aplicación:

$$\begin{array}{rccc} \varphi: & \mathbb{F}_q^n & \longrightarrow & R_n \\ & (a_0, a_1, \ldots, a_{n-2}, a_{n-1}) & \mapsto & [a_0 + a_1 x + \cdots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1}]. \end{array}$$

φ es un isomorfismo de $\mathbb{F}$-espacios vectoriales.

Observación

Si $\mathcal{C} \subset \mathbb{F}_q^n$ es un código lineal q-ario, a cada palabra código le podemos asignar un polinomio en $\mathbb{F}_q[x]$, mediante la siguiente aplicación.

$$\begin{array}{rccc} \mathbf{\Phi}: & \mathcal{C} \subset \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x] \\ & c = \underset{0\leq i\leq n-1}{(c_i)} & \mapsto & \Phi(c) = \sum_{i=0}^{n-1} c_i x^i. \end{array}$$

Sea $R_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$ el álgebra de polinomios de grado menor que n.

Observación

consideremos la siguiente aplicación:

$$\begin{array}{rccc} \varphi: & \mathbb{F}_q^n & \longrightarrow & R_n \\ & (a_0, a_1, \ldots, a_{n-2}, a_{n-1}) & \mapsto & [a_0 + a_1 x + \cdots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}]. \end{array}$$

φ es un isomorfismo de $\mathbb{F}$-espacios vectoriales. Por tanto, un Código $\mathcal{C} \in \mathbb{F}_q^n$ es cíclico si y solamente si $\varphi(\mathcal{C})$ es un ideal en R_n.

Sea $C_n =< a : a^n = 1 >= \{1, a, a^2, \ldots, a^{n-1}\}$ un grupo cíclico y $\mathbb{F}$ un cuerpo, los elementos de $\mathbb{F}C_n$ son de la forma:

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

Sea $C_n =< a : a^n = 1 >= \{1, a, a^2, \ldots, a^{n-1}\}$ un grupo cíclico y $\mathbb{F}$ un cuerpo, los elementos de $\mathbb{F}C_n$ son de la forma:

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

Luego,

$$\mathbb{F}C_n \simeq R_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle};$$

Sea $C_n =< a : a^n = 1 >= \{1, a, a^2, \ldots, a^{n-1}\}$ un grupo cíclico y $\mathbb{F}$ un cuerpo, los elementos de $\mathbb{F}C_n$ son de la forma:

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

Luego,

$$\mathbb{F}C_n \simeq R_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle};$$

Por lo tanto, estudiar códigos cíclicos será equivalente a estudiar los ideales de un álgebra de grupo de la forma $\mathbb{F}C_n$.

Sean G un grupo y R un anillo conmutativo, con unidad. Denotaremos por RG el conjunto de todas las combinaciones lineales formales:

$$RG = \left\{ \sum_{g \in G} \alpha_g g : \alpha_g \in R \text{ y } \alpha_g \neq 0 \text{ para un número finito de } \alpha_g \right\}.$$

Sean G un grupo y R un anillo conmutativo, con unidad. Denotaremos por RG el conjunto de todas las combinaciones lineales formales:

$$RG = \left\{ \sum_{g \in G} \alpha_g g : \alpha_g \in R \text{ y } \alpha_g \neq 0 \text{ para un número finito de } \alpha_g \right\}.$$

Dados $\alpha = \sum_{g \in G} \alpha_g g$ y $\beta = \sum_{g \in G} \beta_g g$ tenemos que $\alpha = \beta$ si y solo si $\alpha_g = \beta_g$ para todo $g \in G$.

Sean G un grupo y R un anillo conmutativo, con unidad. Denotaremos por RG el conjunto de todas las combinaciones lineales formales:

$$RG = \left\{ \sum_{g \in G} \alpha_g g : \alpha_g \in R \text{ y } \alpha_g \neq 0 \text{ para un número finito de } \alpha_g \right\}.$$

Dados $\alpha = \sum_{g \in G} \alpha_g g$ y $\beta = \sum_{g \in G} \beta_g g$ tenemos que $\alpha = \beta$ si y solo si $\alpha_g = \beta_g$ para todo $g \in G$.

Sean $\alpha_g, \beta_g \in R$ y $g, h \in G$, definimos las operaciones de suma "$+$" y producto "$\cdot$", de la siguiente forma

$$(+) \quad (\sum_{g \in G} \alpha_g g) + (\sum_{g \in G} \beta_g g) = \sum (\alpha_g + \beta_g) g,$$

$$(\cdot) \quad \sum_{g \in G} \alpha_g g \sum_{h \in G} \beta_h h = \sum_{g,h \in G} (\alpha_g \beta_h) gh = \sum_{u \in G} c_u u, \text{ donde}$$

$$c_u = \sum_{gh = u} \alpha_g \beta_h.$$

Para λ en R definimos

$$\lambda(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} (\lambda\alpha_g)g.$$

Para λ en R definimos

$$\lambda(\sum_{g\in G}\alpha_g g) = \sum_{g\in G}(\lambda\alpha_g)g.$$

Definición

El conjunto RG, con las operaciones definidas anteriormente, es un álgebra sobre R, llamada el álgebra de grupo de G sobre R.

Definición

Un álgebra $\mathcal{B}$ se dice semisimple si todo ideal de $\mathcal{B}$ es un sumando directo.

Definición

Un álgebra $\mathcal{B}$ se dice semisimple si todo ideal de $\mathcal{B}$ es un sumando directo.

Dado un ideal J en $\mathcal{B}$, existe otro ideal L tal que $\mathcal{B} = J \bigoplus L$.
Escribiendo $1 = e + f$, con $e \in J$ y $f \in L$, podemos ver que e es un idempotente.

Definición

Un álgebra $\mathcal{B}$ se dice semisimple si todo ideal de $\mathcal{B}$ es un sumando directo.

Dado un ideal J en $\mathcal{B}$, existe otro ideal L tal que $\mathcal{B} = J \bigoplus L$.
Escribiendo $1 = e + f$, con $e \in J$ y $f \in L$, podemos ver que e es un idempotente.

En un álgebra semisimple $\mathcal{B}$, todo ideal es generado por un elemento idempotente.

Definición

Un álgebra $\mathcal{B}$ se dice semisimple si todo ideal de $\mathcal{B}$ es un sumando directo.

Dado un ideal J en $\mathcal{B}$, existe otro ideal L tal que $\mathcal{B} = J \bigoplus L$.
Escribiendo $1 = e + f$, con $e \in J$ y $f \in L$, podemos ver que e es un idempotente.

En un álgebra semisimple $\mathcal{B}$, todo ideal es generado por un elemento idempotente.

Teorema (Maschke)

Un álgebra de grupo $\mathbb{F}G$ es semisimple si y solamente si la característica de $\mathbb{F}$ no divide el orden de G.

Cuando $\mathbb{F}G$ es semisimple, entonces existe un único conjunto de elementos centrales $e_1, e_2, \ldots, e_n$ en $\mathbb{F}G$ tales que:

Cuando $\mathbb{F}G$ es semisimple, entonces existe un único conjunto de elementos centrales $e_1, e_2, \ldots, e_n$ en $\mathbb{F}G$ tales que:

1. $e_i^2 = e_1$, $1 \leq i \leq n$ (idempotentes).

Cuando $\mathbb{F}G$ es semisimple, entonces existe un único conjunto de elementos centrales $e_1, e_2, \ldots, e_n$ en $\mathbb{F}G$ tales que:

1. $e_i^2 = e_1$, $1 \leq i \leq n$ (idempotentes).
2. $e_i e_j = 0$ si $i \neq j$ (ortogonales).

Cuando $\mathbb{F}G$ es semisimple, entonces existe un único conjunto de elementos centrales $e_1, e_2, \ldots, e_n$ en $\mathbb{F}G$ tales que:

1. $e_i^2 = e_1$, $1 \leq i \leq n$ (idempotentes).
2. $e_i e_j = 0$ si $i \neq j$ (ortogonales).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes centrales ortogonales, entonces $e_i = e_i'$ o $e_i = e_i''$ (cada idempotente es primitivo).

Cuando $\mathbb{F}G$ es semisimple, entonces existe un único conjunto de elementos centrales $e_1, e_2, \ldots, e_n$ en $\mathbb{F}G$ tales que:

1. $e_i^2 = e_1$, $1 \leq i \leq n$ (idempotentes).
2. $e_i e_j = 0$ si $i \neq j$ (ortogonales).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes centrales ortogonales, entonces $e_i = e_i'$ o $e_i = e_i''$ (cada idempotente es primitivo).
4. $1 = e_1 + e_2 + \cdots + e_n$.

Cuando $\mathbb{F}G$ es semisimple, entonces existe un único conjunto de elementos centrales $e_1, e_2, \ldots, e_n$ en $\mathbb{F}G$ tales que:

1. $e_i^2 = e_1$, $1 \leq i \leq n$ (idempotentes).
2. $e_i e_j = 0$ si $i \neq j$ (ortogonales).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes centrales ortogonales, entonces $e_i = e_i'$ o $e_i = e_i''$ (cada idempotente es primitivo).
4. $1 = e_1 + e_2 + \cdots + e_n$.

Este conjunto es llamado el *conjunto completo de idempotentes centrales idempotentes primitivos* de $\mathbb{F}G$.

Cuando $\mathbb{F}G$ es semisimple, entonces existe un único conjunto de elementos centrales $e_1, e_2, \ldots, e_n$ en $\mathbb{F}G$ tales que:

1. $e_i^2 = e_1$, $1 \leq i \leq n$ (idempotentes).
2. $e_i e_j = 0$ si $i \neq j$ (ortogonales).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes centrales ortogonales, entonces $e_i = e_i'$ o $e_i = e_i''$ (cada idempotente es primitivo).
4. $1 = e_1 + e_2 + \cdots + e_n$.

Este conjunto es llamado el *conjunto completo de idempotentes centrales idempotentes primitivos* de $\mathbb{F}G$.

Los ideales generados por los idempotentes centrales primitivos son ideales bilaterales minimales del álgebra.

Cuando $\mathbb{F}G$ es semisimple, entonces existe un único conjunto de elementos centrales $e_1, e_2, \ldots, e_n$ en $\mathbb{F}G$ tales que:

1. $e_i^2 = e_1$, $1 \leq i \leq n$ (idempotentes).
2. $e_i e_j = 0$ si $i \neq j$ (ortogonales).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes centrales ortogonales, entonces $e_i = e_i'$ o $e_i = e_i''$ (cada idempotente es primitivo).
4. $1 = e_1 + e_2 + \cdots + e_n$.

Este conjunto es llamado el *conjunto completo de idempotentes centrales idempotentes primitivos* de $\mathbb{F}G$.

Los ideales generados por los idempotentes centrales primitivos son ideales bilaterales minimales del álgebra.

Todo ideal bilateral de $\mathbb{F}G$ es de la forma $I = \mathbb{F}Ge$, donde $e \in \mathbb{F}G$ es un elemento idempotente central.

Cuando $\mathbb{F}G$ es semisimple, entonces existe un único conjunto de elementos centrales $e_1, e_2, \ldots, e_n$ en $\mathbb{F}G$ tales que:

1. $e_i^2 = e_1$, $1 \leq i \leq n$ (idempotentes).
2. $e_i e_j = 0$ si $i \neq j$ (ortogonales).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes centrales ortogonales, entonces $e_i = e_i'$ o $e_i = e_i''$ (cada idempotente es primitivo).
4. $1 = e_1 + e_2 + \cdots + e_n$.

Este conjunto es llamado el *conjunto completo de idempotentes centrales idempotentes primitivos* de $\mathbb{F}G$.

Los ideales generados por los idempotentes centrales primitivos son ideales bilaterales minimales del álgebra.

Todo ideal bilateral de $\mathbb{F}G$ es de la forma $I = \mathbb{F}Ge$, donde $e \in \mathbb{F}G$ es un elemento idempotente central.

Por lo tanto si $char(\mathbb{F}) \not| |G|$, el estudio de códigos sobre el álgebras de grupo $\mathbb{F}G$ es equivalente al estudio de sus ideales, los cuales a su vez son generados por elementos idempotentes.

Sean H un subgrupo de un grupo finito G y $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \not| |G|$. Elemento

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

es un idempotente del álgebra $\mathbb{F}G$, llamado el *idempotente determinado por* H.

Sean H un subgrupo de un grupo finito G y $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \not| |G|$. Elemento

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

es un idempotente del álgebra $\mathbb{F}G$, llamado el *idempotente determinado por* H.

$\widehat{H}$ es central si y solamente si H es normal en G.

Sean H un subgrupo de un grupo finito G y $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid |G|$. Elemento

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

es un idempotente del álgebra $\mathbb{F}G$, llamado el *idempotente determinado por* H.

$\widehat{H}$ es central si y solamente si H es normal en G.

Lema

Sean $\mathbb{F}_q$ un cuerpo, p un primo, $A = \langle a \rangle$ un grupo de orden p^n, con $n \geq 1$, y

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

la cadena decreciente de todos los subgrupos de A. Entonces los elementos

Sean H un subgrupo de un grupo finito G y $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid |G|$. Elemento

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

es un idempotente del álgebra $\mathbb{F}G$, llamado el *idempotente determinado por* H.

$\widehat{H}$ es central si y solamente si H es normal en G.

Lema

Sean $\mathbb{F}_q$ un cuerpo, p un primo, $A = \langle a \rangle$ un grupo de orden p^n, con $n \geq 1$, y

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

la cadena decreciente de todos los subgrupos de A. Entonces los elementos

$$e_0 = \widehat{A} \quad y \quad e_i = \widehat{A_i} - \widehat{A_{i-1}}, \quad 1 \leq i \leq n$$

Sean H un subgrupo de un grupo finito G y $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid |G|$. Elemento

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

es un idempotente del álgebra $\mathbb{F}G$, llamado el *idempotente determinado por* H.

$\widehat{H}$ es central si y solamente si H es normal en G.

Lema

Sean $\mathbb{F}_q$ un cuerpo, p un primo, $A = \langle a \rangle$ un grupo de orden p^n, con $n \geq 1$, y

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

la cadena decreciente de todos los subgrupos de A. Entonces los elementos

$$e_0 = \widehat{A} \quad y \quad e_i = \widehat{A_i} - \widehat{A_{i-1}}, \quad 1 \leq i \leq n$$

forman un conjunto de idempotentes en $\mathbb{F}A$ tales que $e_0 + e_1 + \cdots + e_n = 1$.

Ejemplo

Sea A un grupo cíclico de orden 3^3 y $\mathbb{F}_q$ un cuerpo. Entonces

$$
\begin{aligned}
A_0 &= \langle a \rangle = \{1, a, a^2, \ldots, a^{26}\} \\
A_1 &= \langle a^3 \rangle = \{1, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24}\} \\
A_2 &= \langle a^9 \rangle = \{1, a^9, a^{18}\} \\
A_3 &= \langle a^{27} \rangle = \{1\}.
\end{aligned}
$$

Ejemplo

Sea A un grupo cíclico de orden 3^3 y $\mathbb{F}_q$ un cuerpo. Entonces

$$
\begin{aligned}
A_0 &= \langle a \rangle = \{1, a, a^2, \ldots, a^{26}\} \\
A_1 &= \langle a^3 \rangle = \{1, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24}\} \\
A_2 &= \langle a^9 \rangle = \{1, a^9, a^{18}\} \\
A_3 &= \langle a^{27} \rangle = \{1\}.
\end{aligned}
$$

Así,

Ejemplo

Sea A un grupo cíclico de orden 3^3 y $\mathbb{F}_q$ un cuerpo. Entonces

$$
\begin{aligned}
A_0 &= \langle a \rangle = \{1, a, a^2, \ldots, a^{26}\} \\
A_1 &= \langle a^3 \rangle = \{1, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24}\} \\
A_2 &= \langle a^9 \rangle = \{1, a^9, a^{18}\} \\
A_3 &= \langle a^{27} \rangle = \{1\}.
\end{aligned}
$$

Así,

$$
\begin{aligned}
e_0 &= \frac{1}{27}\left(1 + a + a^2 + \cdots + a^{26}\right) \\
e_1 &= \widehat{A_1} - \widehat{A_0} = \frac{1}{27}\left(2 - a - a^2 + 2a^3 - a^4 - \cdots - a^{23} + 2a^{24} - a^{25} - a^{26}\right) \\
e_2 &= \widehat{A_2} - \widehat{A_1} = \frac{1}{9}\left(2 - a^3 - a^6 + 2a^9 - a^{12} - a^{15} + 2a^{18} - a^{21} - a^{24}\right) \\
e_3 &= \widehat{A_3} - \widehat{A_2} = \frac{1}{3}\left(2 - a^9 - a^{18}\right)
\end{aligned}
$$

El método permite obtener los idempotentes primitivos en $\mathbb{Q}A$, pero en general, no funciona sobre cuerpos finitos.

El método permite obtener los idempotentes primitivos en $\mathbb{Q}A$, pero en general, no funciona sobre cuerpos finitos.
Para ilustrar esto, consideremos el polinomio $f(x) = x^3 - 1$ sobre el cuerpo de 7 elementos $\mathbb{F}_7$, el cual se expresa como

$$x^3 - 1 = (x - 1)(x - 2)(x - 4),$$

El método permite obtener los idempotentes primitivos en $\mathbb{Q}A$, pero en general, no funciona sobre cuerpos finitos.
Para ilustrar esto, consideremos el polinomio $f(x) = x^3 - 1$ sobre el cuerpo de 7 elementos $\mathbb{F}_7$, el cual se expresa como

$$x^3 - 1 = (x-1)(x-2)(x-4),$$

y así,

$$\mathbb{F}_7 C_3 \simeq \frac{\mathbb{F}[x]}{(x^3-1)} \simeq \frac{\mathbb{F}[x]}{(x-1)} \oplus \frac{\mathbb{F}[x]}{(x-2)} \oplus \frac{\mathbb{F}[x]}{(x-4)}$$

El método permite obtener los idempotentes primitivos en $\mathbb{Q}A$, pero en general, no funciona sobre cuerpos finitos.
Para ilustrar esto, consideremos el polinomio $f(x) = x^3 - 1$ sobre el cuerpo de 7 elementos $\mathbb{F}_7$, el cual se expresa como

$$x^3 - 1 = (x-1)(x-2)(x-4),$$

y así,

$$\mathbb{F}_7 C_3 \simeq \frac{\mathbb{F}[x]}{(x^3-1)} \simeq \frac{\mathbb{F}[x]}{(x-1)} \oplus \frac{\mathbb{F}[x]}{(x-2)} \oplus \frac{\mathbb{F}[x]}{(x-4)}$$

Por otro lado sobre $\mathbb{Q}[x]$, el polinomio $(x^3 - 1)$ se descompone como $(x - 1)(x^2 + x + 1)$. Por tanto si ζ denota una raíz primitiva de la unidad de orden 3 tenemos que

$$\mathbb{Q}C_3 \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta).$$

El método permite obtener los idempotentes primitivos en $\mathbb{Q}A$, pero en general, no funciona sobre cuerpos finitos.
Para ilustrar esto, consideremos el polinomio $f(x) = x^3 - 1$ sobre el cuerpo de 7 elementos $\mathbb{F}_7$, el cual se expresa como

$$x^3 - 1 = (x-1)(x-2)(x-4),$$

y así,

$$\mathbb{F}_7 C_3 \simeq \frac{\mathbb{F}[x]}{(x^3-1)} \simeq \frac{\mathbb{F}[x]}{(x-1)} \oplus \frac{\mathbb{F}[x]}{(x-2)} \oplus \frac{\mathbb{F}[x]}{(x-4)}$$

Por otro lado sobre $\mathbb{Q}[x]$, el polinomio $(x^3 - 1)$ se descompone como $(x - 1)(x^2 + x + 1)$. Por tanto si ζ denota una raíz primitiva de la unidad de orden 3 tenemos que

$$\mathbb{Q}C_3 \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta).$$

Así, el grupo cíclico de orden 3 sobre $\mathbb{Q}$ contiene solo dos idempotentes centrales primitivos no triviales, mientras el álgebra de grupo del mismo grupo sobre $\mathbb{F}_7$ contiene tres de tales elementos.

Así, los $n+1$ idempotentes dados del lema anterior, serán el conjunto de idempotentes primitivos de $\mathbb{F}A$, siempre que $\mathbb{F}A$ tenga exactamente $n+1$ componentes. Dado que el exponente de A es p^n, tenemos que esto sucede si y solo si q y p^n están relacionados como en el siguiente corolario.

Corolario

Sea $\mathbb{F}$ un cuerpo finito con $|\mathbb{F}| = q$, y A un grupo cíclico de orden p^n. Entonces, el conjunto de idempotentes definidos en el lema anterior es el conjunto de idempotentes primitivos de A si y solo si una de las siguientes condiciones se cumple

(i) $p = 2$, *o bien* $n = 1$ *y* q *es impar o* $n = 2$ *y* $q \equiv 3 \pmod 4$.

Así, los $n+1$ idempotentes dados del lema anterior, serán el conjunto de idempotentes primitivos de $\mathbb{F}A$, siempre que $\mathbb{F}A$ tenga exactamente $n+1$ componentes. Dado que el exponente de A es p^n, tenemos que esto sucede si y solo si q y p^n están relacionados como en el siguiente corolario.

Corolario

Sea $\mathbb{F}$ un cuerpo finito con $|\mathbb{F}| = q$, y A un grupo cíclico de orden p^n. Entonces, el conjunto de idempotentes definidos en el lema anterior es el conjunto de idempotentes primitivos de A si y solo si una de las siguientes condiciones se cumple

(i) $p = 2$, *o bien* $n = 1$ *y* q *es impar o* $n = 2$ *y* $q \equiv 3 \pmod 4$.

(ii) p *es un número primo impar y* $o(q) = \Phi(p^n)$ *en* $U(\mathbb{Z}_{p^n})$.

Así, los $n+1$ idempotentes dados del lema anterior, serán el conjunto de idempotentes primitivos de $\mathbb{F}A$, siempre que $\mathbb{F}A$ tenga exactamente $n+1$ componentes. Dado que el exponente de A es p^n, tenemos que esto sucede si y solo si q y p^n están relacionados como en el siguiente corolario.

Corolario

Sea $\mathbb{F}$ un cuerpo finito con $|\mathbb{F}| = q$, y A un grupo cíclico de orden p^n. Entonces, el conjunto de idempotentes definidos en el lema anterior es el conjunto de idempotentes primitivos de A si y solo si una de las siguientes condiciones se cumple

(i) $p = 2$, *o bien* $n = 1$ *y* q *es impar o* $n = 2$ *y* $q \equiv 3 \pmod 4$.

(ii) p *es un número primo impar y* $o(q) = \Phi(p^n)$ *en* $U(\mathbb{Z}_{p^n})$.

Como una consecuencia inmediata, tenemos el siguiente resultado de Pruthi y Arora.

Teorema

Sean $\mathbb{F}$ un cuerpo con q elementos y A u n grupo cíclico de orden p^n tal que $o(q) = \Phi(p^n)$ en $U(\mathbb{Z}_{p^n})$. Sea

$$A = A_0 \supset A_1 \supset \cdots \supset A_n$$

la cadena decreciente de todos los subgrupos de A. Entonces, el conjunto de idempotentes primitivos de $\mathbb{F}A$ esta dado por

$$e_0 = \frac{1}{p^n}\left(\sum_{a\in A} a\right) \quad y \quad e_i = \widehat{A_i} - \widehat{A_{i-1}} \quad 1 \leq i \leq n$$

Dado que

$$\mathbb{F}G = F(C \times A) \cong (\mathbb{F}C)A \cong (\mathbb{F} \bigoplus \mathbb{F})A,$$

Dado que

$$\mathbb{F}G = F(C \times A) \cong (\mathbb{F}C)A \cong (\mathbb{F} \bigoplus \mathbb{F})A,$$

Tenemos el siguiente resultado:

Dado que

$$\mathbb{F}G = F(C \times A) \cong (\mathbb{F}C)A \cong (\mathbb{F} \bigoplus \mathbb{F})A,$$

Tenemos el siguiente resultado:

Teorema (Arora - Pruthi & Ferraz - Polcino)

Sea $\mathbb{F}$ un cuerpo finito con q elementos y G un grupo cíclico de orden $2p^n$, p un primo impar, tal que $o(q) = \Phi(p^n)$ en $U(\mathbb{Z}_{2p^n})$. Escribimos $G = C \times A$, donde A es el subgrupo p-sylow de G y $C = \{1, t\}$ es un 2-subgrupo sylow. Si e_i, $0 \leq i \leq n$, denotan los idempotentes primitivos de $\mathbb{F}A$ entonces, los idempotentes primitivos de $\mathbb{F}G$ son

$$\frac{1+t}{2}e_i \quad y \quad \frac{1-t}{2}e_i, \quad 0 \leq i \leq n.$$

Códigos abelianos

Queremos extender estos resultados a los grupos abelianos finitos. Vamos a considerar el caso de los p-grupos.

Códigos abelianos

Queremos extender estos resultados a los grupos abelianos finitos. Vamos a considerar el caso de los p-grupos.

Sea A un p-grupo abeliano. Para cada subgrupo H de A tal que $A/H \neq \{1\}$ es cíclico, construiremos un idempotente de $\mathbb{F}A$.
Recordemos que dado A/H un grupo cíclico de orden una potencia de p, tenemos que existe un único subgrupo H^* de A que contiene a H, tal que $|H^*/H| = p$.
Definamos $e_H = \widehat{H} - \widehat{H^*}$ claramente $e_H \neq 0$ y tendremos lo siguiente

Códigos abelianos

Queremos extender estos resultados a los grupos abelianos finitos. Vamos a considerar el caso de los p-grupos.

Sea A un p-grupo abeliano. Para cada subgrupo H de A tal que $A/H \neq \{1\}$ es cíclico, construiremos un idempotente de $\mathbb{F}A$.
Recordemos que dado A/H un grupo cíclico de orden una potencia de p, tenemos que existe un único subgrupo H^* de A que contiene a H, tal que $|H^*/H| = p$.
Definamos $e_H = \widehat{H} - \widehat{H^*}$ claramente $e_H \neq 0$ y tendremos lo siguiente

Lema

Los elementos e_H definidos anteriormente, junto con $e_A = \widehat{A}$ forman un conjunto de idempotents ortogonales dos a dos de $\mathbb{F}A$ cuya suma es igual a 1.

Teorema

Sea p un primo impar y sea A un p-grupo abeliano de exponente p^r. Entonces, el conjunto de idempotentes enunciado anteriormente es el conjunto de idempotentes primitivos de $\mathbb{F}A$ si y solo si se cumple uno de los siguientes enunciados

(i) $p^r = 2$ *y* q *es impar.*

(ii) $p^r = 4$ *y* $q \equiv 3(mod\, 4)$.

(iii) p *es primo impar y* $o(q) = \Phi(p^n)$ *en* $U(\mathbb{Z}_{p^n})$.

Teorema

Sea p un primo impar y sea A un p-grupo abeliano de exponente p^r. Entonces, el conjunto de idempotentes enunciado anteriormente es el conjunto de idempotentes primitivos de $\mathbb{F}A$ si y solo si se cumple uno de los siguientes enunciados

(i) $p^r = 2$ y q es impar.

(ii) $p^r = 4$ y $q \equiv 3(mod\, 4)$.

(iii) p es primo impar y $o(q) = \Phi(p^n)$ en $U(\mathbb{Z}_{p^n})$.

Teorema

Sea p un primo impar y sea A un p-grupo abeliano de exponente $2p^r$. Escribimos $A = E \times B$, donde E es un 2-grupo elemental y B es un p-grupo. Entonces los idempotentes primitivos de $\mathbb{F}A$ son productos de la forma ef, donde e es un idempotente primitivo de $\mathbb{F}E$ y f un idempotente primitivo de $\mathbb{F}B$

Note que los idempotentes primitivos de $\mathbb{F}B$ son dados por el teorema anterior y, escribimos $E =< a_1 > \times \cdots \times < a_n >$, un producto de grupos cíclicos de orden 2, entonces los idempotentes primitivos de $\mathbb{F}E$ son todos los productos de la forma $e = e_1 e_2 \cdots e_n$, donde

Note que los idempotentes primitivos de $\mathbb{F}B$ son dados por el teorema anterior y, escribimos $E =< a_1 > \times \cdots \times < a_n >$, un producto de grupos cíclicos de orden 2, entonces los idempotentes primitivos de $\mathbb{F}E$ son todos los productos de la forma $e = e_1 e_2 \cdots e_n$, donde

$$e_i = \frac{1 + a_i}{2} \quad o \quad e_i = \frac{1 - a_i}{2}, \quad 1 \leq i \leq n.$$

Note que los idempotentes primitivos de $\mathbb{F}B$ son dados por el teorema anterior y, escribimos $E =< a_1 > \times \cdots \times < a_n >$, un producto de grupos cíclicos de orden 2, entonces los idempotentes primitivos de $\mathbb{F}E$ son todos los productos de la forma $e = e_1 e_2 \cdots e_n$, donde

$$e_i = \frac{1 + a_i}{2} \quad o \quad e_i = \frac{1 - a_i}{2}, \quad 1 \leq i \leq n.$$

Cabe señalar que, en vista de este corolario, estos son los únicos casos en los que los idempotentes primitivos de álgebras de grupos abelianos finitos se pueden calcular de esta manera.

Gracias por su atención

Bibliografía

- Arora S. K; Pruthi M. Minimal cyclic codes of length $2p^n$. Finite Fields Appl. 5 (1999) 177-187.
- Ferraz, Raul A. Simple components and central units in group algebras. J. Algebra, 279 (2004) 191-203.
- Ferraz, Raul A; Polcino Milies, César. Idempotents in group algebras and minimal abelian codes. Finite Fields and Their Applications, 13 (2007) 382-393.
- Polcino Milies, César; Sehgal, Sudarshan K. An introduction to group rings. Algebras and Applications, 1. Kluwer Academic Publishers, Dordrecht, 2002. xii+371 pp. ISBN: 1-4020-0238-6 MR1896125 (2003b:16026).
- Pruthi, M; Arora S. K. Minimal codes of prime power length. Finite Fields Appl. 3 (1997) 99-113.