Códigos de grupo

Francisco César Polcino Milies
Instituto de Matemáticas e Estatística
Universidade de Sao Paulo, Sao Paulo, Brasil
e-mail: polcino@ime.usp.br

ALTENCOA6-2014
San Juan de Pasto, Colombia
11 al 15 de agosto de 2014

Resumen

En este curso se tratarán los siguientes temas:

1. Conceptos básicos de la teoria de códigos correctores de errores.
2. Códigos Lineares y códigos cíclicos.
3. Álgebras de grupo y códigos de grupo.
4. Álgebras de grupo semisimples e idempotentes primitivos.
5. Códigos a partir de subgrupos.
6. Algunas aplicaciones.

Álgebras de Grupo y Teoria de Códigos

César Polcino Milies

Universidade de São Paulo
Universidade Federal do ABC

Códigos Cíclicos

Definición

Un código lineal $\mathcal{C} \subset \mathbb{F}^n$ se llama un **código cíclico** se, para todo vector $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ en el código, se tiene que también el vector $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ está en el código.

Definición

Un código lineal $\mathcal{C} \subset \mathbb{F}^n$ se llama un **código cíclico** se, para todo vector $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ en el código, se tiene que también el vector $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ está en el código.

Note que la definición implica que si $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ está en el código, entonces todos los vectores que se obrienen a partir de este por una permutación cíclica de sus coordenadas también están en el código.

Sea

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

Denotaremos por $[f]$ la clase del polinomio $f \in \mathbb{F}[X]$ en $\mathcal{R}_n$.

Sea

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

Denotaremos por $[f]$ la clase del polinomio $f \in \mathbb{F}[X]$ en $\mathcal{R}_n$.
La función:

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

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

Sea

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

Denotaremos por $[f]$ la clase del polinomio $f \in \mathbb{F}[X]$ en $\mathcal{R}_n$.
La función:

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

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

φ es un isomorfismo de $\mathbb{F}$-espacios vectoriales. Por lo tanto *Un código $\mathcal{C} \subset \mathbb{F}^n$ es cíclico si y solamente si $\varphi(\mathcal{C})$ es un ideal de $\mathcal{R}_n$.*

En el caso en que $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ es un grupo cíclico de orden n, y $\mathbb{F}$ es un cuerpo, los elementos de $\mathbb{F}C_n$ son de la forma:

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

En el caso en que $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ es un grupo cíclico de orden n, y $\mathbb{F}$ es un cuerpo, los elementos de $\mathbb{F}C_n$ son de la forma:

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

Es muy facil probar que

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

En el caso en que $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ es un grupo cíclico de orden n, y $\mathbb{F}$ es un cuerpo, los elementos de $\mathbb{F}C_n$ son de la forma:

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

Es muy facil probar que

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

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

Álgebras de grupo

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

$$\alpha = \sum_{g \in G} \alpha_g g, \quad \text{donde} \quad \alpha_g \in R.$$

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

$$\alpha = \sum_{g \in G} \alpha_g g, \quad \text{donde} \quad \alpha_g \in R.$$

Dados $\alpha = \sum_{g \in G} \alpha_g g$ e $\beta = \sum_{g \in G} \beta_g g$ tenemos que

$$\alpha = \beta \Longleftrightarrow \alpha_g = \beta_g, \quad \forall g \in G.$$

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

$$\alpha = \sum_{g \in G} \alpha_g g, \quad \text{donde} \quad \alpha_g \in R.$$

Dados $\alpha = \sum_{g \in G} \alpha_g g$ e $\beta = \sum_{g \in G} \beta_g g$ tenemos que

$$\alpha = \beta \Longleftrightarrow \alpha_g = \beta_g, \quad \forall g \in G.$$

Definimos:

$$\left(\sum_{g \in G} \alpha_g g \right) + \left(\sum_{g \in G} \beta_g g \right) = \sum_{g \in G} (\alpha_g + \beta_g) g.$$

$$\left(\sum_{g \in G} \alpha_g g \right) \left(\sum_{g \in G} \beta_g g \right) = \sum_{g,h \in G} (\alpha_g \beta_h) gh.$$

Para λ in R definimos

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

Para λ in R definimos

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

Definición

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

Códigos Cíclicos

Definición

Un **código de grupo** es un ideal de un álgebra de grupo finita.

Ideales en Álgebras de Grupo

Definición

Un álgebra A se dice semisimple si todo ideal de A es un sumando directo.

Definición

Un álgebra A se dice semisimple si todo ideal de A es un sumando directo.

Dado un ideal J en A, existe otro ideal L tal que $A = J \oplus L$. Escribiendo $1 = e + f$, con $e \in J$ y $f \in L$, es facil provar que $e^2 = e$ y que $J = Ae$.

Definición

Un álgebra A se dice semisimple si todo ideal de A es un sumando directo.

Dado un ideal J en A, existe otro ideal L tal que $A = J \oplus L$.
Escribiendo $1 = e + f$, con $e \in J$ y $f \in L$, es facil provar que $e^2 = e$ y que $J = Ae$.
En un álgebra semisimple A, todo ideal es generado por un elemento idempotente.

Definición

Un álgebra A se dice semisimple si todo ideal de A es un sumando directo.

Dado un ideal J en A, existe otro ideal L tal que $A = J \oplus L$.
Escribiendo $1 = e + f$, con $e \in J$ y $f \in L$, es facil provar que $e^2 = e$ y que $J = Ae$.
En un álgebra semisimple A, todo ideal es generado por un elemento idempotente.

Teorema

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

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

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

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

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

1. $e_i^2 = e_i, 1 \leq i \leq n$ (son idempotentes).
2. $e_i e_j = 0$ if $i \neq j$ (son ortogonales dos a dos).

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

1. $e_i^2 = e_i, 1 \leq i \leq n$ (son idempotentes).
2. $e_i e_j = 0$ if $i \neq j$ (son ortogonales dos a dos).
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 o indescomponible).

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

1. $e_i^2 = e_i, 1 \leq i \leq n$ (son idempotentes).
2. $e_i e_j = 0$ if $i \neq j$ (son ortogonales dos a dos).
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 o indescomponible).
4. $1 = e_1 + e_2 + \cdots + e_n$

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

1. $e_i^2 = e_i, 1 \leq i \leq n$ (son idempotentes).
2. $e_i e_j = 0$ if $i \neq j$ (son ortogonales dos a dos).
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 o indescomponible).
4. $1 = e_1 + e_2 + \cdots + e_n$

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

Los ideales generados por los idempotentes centrales primitivos; i.e. los ideales de la forma $I_i = \mathbb{F}Ge_i$ son los ideales bilaterales minimales de A.

Los ideales generados por los idempotentes centrales primitivos; i.e. los ideales de la forma $I_i = \mathbb{F}Ge_i$ son los ideales bilaterales minimales de A.

Todo ideal bilateral de $\mathcal{A}$ es de la forma $I = Ae$, donde $e \in A$ es un elemento idempotente central.

Los ideales generados por los idempotentes centrales primitivos; i.e. los ideales de la forma $I_i = \mathbb{F}Ge_i$ son los ideales bilaterales minimales de A.

Todo ideal bilateral de $\mathcal{A}$ es de la forma $I = Ae$, donde $e \in A$ es un elemento idempotente central.

Existe un resultado similar para ideales a la izquierda (o a la derecha).

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

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

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

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

1. $e_i^2 = e_i, 1 \leq i \leq n$ (son idempotentes).
2. $e_i e_j = 0$ if $i \neq j$ (son ortogonales dos a dos).

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

1. $e_i^2 = e_i, 1 \leq i \leq n$ (son idempotentes).
2. $e_i e_j = 0$ if $i \neq j$ (son ortogonales dos a dos).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes ortogonales, entonces $e_i = e_i'$ o $e_i = e_i$" (cada idempotente es primitivo).

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

1. $e_i^2 = e_i, 1 \leq i \leq n$ (son idempotentes).
2. $e_i e_j = 0$ if $i \neq j$ (son ortogonales dos a dos).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes 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 A es semisimple, entonces existe un conjunto de elementos $e_1, e_2, \ldots, e_n$ in $\mathbb{F}G$ tales que:

1. $e_i^2 = e_i, 1 \leq i \leq n$ (son idempotentes).
2. $e_i e_j = 0$ if $i \neq j$ (son ortogonales dos a dos).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes 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 un conjunto completo de idempotentes primitivos de $\mathbb{F}G$.

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

1. $e_i^2 = e_i, 1 \leq i \leq n$ (son idempotentes).
2. $e_i e_j = 0$ if $i \neq j$ (son ortogonales dos a dos).
3. Si $e_i = e_i' + e_i''$ con e_i', e_i'' idempotentes 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 un conjunto completo de idempotentes primitivos de $\mathbb{F}G$.

Todo ideal a izquierd de $\mathcal{A}$ es de la forma $I = Ae$, donde $e \in A$ es un elemento idempotente central.

Por lo tanto:

Si suponemos que $char(\mathbb{F}) \nmid |G|$, entonces el estudio de códigos de grupo es equivalente al estudio de ideales de álgebras de grupo y estos son siempre genereados por elementos idempotentes.

Idempotentes a partir de subgrupos

Sea H un subgrupo de un grupo finito G y sea $\mathbb{F}$ un cuerpo tal que $car(\mathbb{F}) \nmid |G|$. El 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.

Idempotentes a partir de subgrupos

Sea H un subgrupo de un grupo finito G y sea $\mathbb{F}$ un cuerpo tal que $car(\mathbb{F}) \nmid |G|$. El 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.

Si H es un subgrupo normal del grupo G, tenemos que

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

Si H es un subgrupo normal del grupo G, tenemos que

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

luego

$$\boxed{dim_{\mathbb{F}} \left((\mathbb{F}G) \cdot \widehat{H} \right) = \frac{|G|}{|H|} = [G : H].}$$

Si H es un subgrupo normal del grupo G, tenemos que

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

luego

$$\boxed{dim_{\mathbb{F}} \left((\mathbb{F}G) \cdot \widehat{H} \right) = \frac{|G|}{|H|} = [G : H].}$$

Sea $\tau = \{t_1, t_2, \ldots, t_k\}$ un transversal de K en G (donde $k = [G : H]$ y elegimos $t_1 = 1$),

Si H es un subgrupo normal del grupo G, tenemos que

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

luego

$$\boxed{dim_{\mathbb{F}} \left((\mathbb{F}G) \cdot \widehat{H} \right) = \frac{|G|}{|H|} = [G : H].}$$

Sea $\tau = \{t_1, t_2, \ldots, t_k\}$ un transversal de K en G (donde $k = [G : H]$ y elegimos $t_1 = 1$), entonces

$$\{t_i \widehat{H} \mid 1 \leq i \leq k\}$$

es una base de $(\mathbb{F}G) \cdot \widehat{H}$.

Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid |G|$.
Sean todavia H y H^* subgrupos normales de G tales que $H \subset H^*$.
Podemos definir otro tipo de idempotentes por:

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

Como veremos, estos serán muy útiles.

Parámeteros del código

Teorema (R. Ferraz - P.M.)

Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid |G|$. Sean H y H^* subgrupos normales de G tales que $H \subset H^*$ e sea

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

Entonces:

Parámeteros del código

Teorema (R. Ferraz - P.M.)

Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid |G|$. Sean H y H^* subgrupos normales de G tales que $H \subset H^*$ e sea

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

Entonces:

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

Parámeteros del código

Teorema (R. Ferraz - P.M.)

Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid |G|$. Sean H y H^* subgrupos normales de G tales que $H \subset H^*$ e sea

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

Entonces:

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

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

donde $w((FG)e)$ denota distancia mínima de $(FG)e$.

Teorema

Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid |G|$. Sean H y H^* subgrupos normales de G tales que $H \subset H^*$ e sea

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

Sean $\mathcal{A}$ un transversal de H^* en G y τ un transversal de H en H^* que contene el elemento 1. Entonces

$$\mathcal{B} = \{a(1-t)\widehat{H} \mid a \in \mathcal{A}, t \in \tau \setminus \{1\}\}$$

es una base de $(\mathbb{F}G)e$ sobre $\mathbb{F}$.

Es posible determinar los idempotentes centrales primitivos a partir de los idempotentes determnados por subgrupos?

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

Sean $\mathbb{F}$ un cuerpo con q elementos y A un grupo cíclico de orden p^n, p un primo impar, tal que $o(q) = \varphi(p^n)$ en $U(\mathbb{Z}_{p^n})$ (donde φ denota la función de Euler). Sea

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

la cadena descendente de todos los subgrupos de A. Entonces, el conjunto de idempotentes primitivos de FA es el siguiente:

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

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

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

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

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

Sea A un p-grupo abeliano. Para cada subgrupo H de A tal que $A/H \neq \{1\}$ es cíclico, podemos construir un idempotente de $\mathbb{F}A$. Como A/H es un subgrupo cíclico de oreden una potencia de p, existe un único subgrupo H^* de A, que contiene H y tal que $|H^*/H| = p$.

Sea A un p-grupo abeliano. Para cada subgrupo H de A tal que $A/H \neq \{1\}$ es cíclico, podemos construir un idempotente de $\mathbb{F}A$. Como A/H es un subgrupo cíclico de oreden una potencia de p, existe un único subgrupo H^* de A, que contiene H y tal que $|H^*/H| = p$.
Escribimos

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

y también

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

Teorema (Ferraz-PM (2007))

Sea p un primo impar e sea A un p-grupo abeliano de exponente e. Entonces, el conjunto de idempotentes dado en el teorema anterior es el conjunto de los idempotentes primitivos de $\mathbb{F}A$ si y solamente si vale una de las siguientes condiciones:

(i) $e = 2p^r$, $p \neq 2$ y q es impar.

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

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

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

Teorem (Ferraz-PM (2007))

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 abeliano elemental y B es un p-grupo. Enbtonces, los idempotentes primitivos de FA son productos de la forma $e.f$, donde e es un idempotente primitivo de FE y f un idempotente primitivo de FB.

Algunas aplicaciones

César Polcino Milies

Universidade de São Paulo

Preliminares

Parámeteros del código

Teorema (R. Ferraz - P.M.)

Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que $car(\mathbb{F}) \nmid |G|$. Sean H y H^* subgrupos normales de G tales que $H \subset H^*$ e sea

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

Entonces:

Parámeteros del código

Teorema (R. Ferraz - P.M.)

Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que $car(\mathbb{F}) \nmid |G|$. Sean H y H^* subgrupos normales de G tales que $H \subset H^*$ e sea

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

Entonces:

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

Parámeteros del código

Teorema (R. Ferraz - P.M.)

Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que $car(\mathbb{F}) \nmid |G|$. Sean H y H^* subgrupos normales de G tales que $H \subset H^*$ e sea

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

Entonces:

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

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

donde $w((FG)e)$ denota distancia mínima de $(FG)e$.

Teorema

Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que $car(\mathbb{F}) \nmid |G|$. Sean H y H^* subgrupos normales de G tales que $H \subset H^*$ e sea

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

Sean $\mathcal{A}$ un transversal de H^* en G y τ un transversal de H en H^* que contene el elemento 1. Entonces

$$\mathcal{B} = \{a(1-t)\widehat{H} \mid a \in \mathcal{A}, t \in \tau \setminus \{1\}\}$$

es una base de $(\mathbb{F}G)e$ sobre $\mathbb{F}$.

Sea A un p-grupo abeliano. Para cada subgrupo H de A tal que $A/H \neq \{1\}$ es cíclico, vamos a construir un idempotente de $\mathbb{F}A$. Como A/H es cíclico, de orden una potencia de p, existe un único subgrupo H^* de A, que contiene H, tal que $|H^*/H| = p$.

Sea A un p-grupo abeliano. Para cada subgrupo H de A tal que $A/H \neq \{1\}$ es cíclico, vamos a construir un idempotente de $\mathbb{F}A$. Como A/H es cíclico, de orden una potencia de p, existe un único subgrupo H^* de A, que contiene H, tal que $|H^*/H| = p$. Construimos los idempotentes

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

y también

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

Sea A un p-grupo abeliano. Para cada subgrupo H de A tal que $A/H \neq \{1\}$ es cíclico, vamos a construir un idempotente de $\mathbb{F}A$. Como A/H es cíclico, de orden una potencia de p, existe un único subgrupo H^* de A, que contiene H, tal que $|H^*/H| = p$. Construimos los idempotentes

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

y también

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

No es difícil ver que este es un conjunto de idempotentes ortogonales cuja suma es 1.

Definición

Sea g un elemento de un grupo finito G. A *clase q-ciclotómica* de g es el conjunto

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

donde t_g es el menor entero positivo tal que

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

Definición

Sea g un elemento de un grupo finito G. A *clase q-ciclotómica* de g es el conjunto

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

donde t_g es el menor entero positivo tal que

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

Teorema

Sea G un grupo finito y $\mathbb{F}$ el cuerpo con q elementos y supongamos que $gcd(q, |G|) = 1$. Entonces, el número de componentes simples de $\mathbb{F}G$ es igual al número de clases q-ciclotómicas de G.

Teorema (Ferraz-PM (2007))

Sea $\mathbb{F}$ un cuerpo finito con $|\mathbb{F}| = q$, y sea A un grupo abeliano finito, de exponente e. Entonces, el conjunto de los idempotentes primitivos de $\mathbb{F}G$ es el construído a partir de subgrupos si y sólo si vale una de las siguientes condiciones:

(i) $e = 2$ y q es impar.

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

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

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

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

Sean $\mathbb{F}$ el cuerpo con q elementos y A un grupo cíclico de orden p^n tales que $o(q) = \varphi(p^n)$ en $U(\mathbb{Z}_{p^n})$ (donde φ denota la función de Euler). Sea

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

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

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

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

Teorema

Sean $G_i \subset G_{i-1}$ subgrupos consecutivos en la cadena de subgrupos de G y $e_i = \widehat{G}_i - \widehat{G_{i-1}}$. Entonces

$$w((RG)e_i) = 2 \mid G_i \mid, \text{ para } i \neq 0$$

y

$$w((RG)e_0) = \mid G \mid, \text{ for } 0 \leq k \leq t-1.$$

Teorema

Sean $G_i \subset G_{i-1}$ subgrupos consecutivos en la cadena de subgrupos de G y $e_i = \widehat{G}_i - \widehat{G_{i-1}}$. Entonces

$$w((RG)e_i) = 2 \mid G_i \mid, \text{ para } i \neq 0$$

y

$$w((RG)e_0) = \mid G \mid, \text{ for } 0 \leq k \leq t-1.$$

Teorema (F. Melo - PM (2013))

Considere $I = I_0 \oplus ... \oplus I_j$,con $0 \leq j \leq n-1$. Entonces,

Teorema

Sean $G_i \subset G_{i-1}$ subgrupos consecutivos en la cadena de subgrupos de G y $e_i = \widehat{G}_i - \widehat{G_{i-1}}$. Entonces

$$w((RG)e_i) = 2 \mid G_i \mid, \text{ para } i \neq 0$$

y

$$w((RG)e_0) = \mid G \mid, \text{ for } 0 \leq k \leq t-1.$$

Teorema (F. Melo - PM (2013))

Considere $I = I_0 \oplus ... \oplus I_j$,con $0 \leq j \leq n-1$. Entonces,

$$w(I_0 \oplus I_1 \oplus ... \oplus I_j) = \mid G_j \mid .$$

Teorema (F. Melo - PM (2013))

Si $I = I_{j_1} \oplus ... \oplus I_{j_l}$, $j_r < j_{r+1}$, para $1 \leq r \leq l$ con $\{j_1, ..., j_l\} \subsetneq \{0, 1, ..., j_l\}$, entonces

Teorema (F. Melo - PM (2013))

Si $I = I_{j_1} \oplus ... \oplus I_{j_l}$, $j_r < j_{r+1}$, para $1 \leq r \leq l$ con $\{j_1, ..., j_l\} \subsetneq \{0, 1, ..., j_l\}$, entonces

$$w(I) = 2 \mid G_{j_l} \mid .$$

Códigos cíclicos vs Códigos Abelianos

Vamos a comparar códigos cíclicos e códigos abelianos no cíclicos de longitud 2^n, sobre un cuerpo con q elementos, siempre con la hipótesis de que $o(q) = \varphi(p^2)$ in $U(\mathbb{Z}_{p^n})$.

Vamos a comparar códigos cíclicos e códigos abelianos no cíclicos de longitud 2^n, sobre un cuerpo con q elementos, siempre con la hipótesis de que $o(q) = \varphi(p^2)$ in $U(\mathbb{Z}_{p^n})$.

Observación

Note que, en $\mathbb{F}C_{p^2}$ existen precisamente tres idempotentes primitivos, a saber:

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

Vamos a comparar códigos cíclicos e códigos abelianos no cíclicos de longitud 2^n, sobre un cuerpo con q elementos, siempre con la hipótesis de que $o(q) = \varphi(p^2)$ in $U(\mathbb{Z}_{p^n})$.

Observación

Note que, en $\mathbb{F}C_{p^2}$ existen precisamente tres idempotentes primitivos, a saber:

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

Para cada peso posible, los ideales de mayor dimensión correspondientes son:

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

con $dim(I) = p$, $w(I) = p$ y $dim(J) = p^2 - 1$, $w(J) = 2$.

Ahora vamos a considerar códigos no cíclicos de longitud p^2; esto es, ideales de $\mathbb{F}G$ donde

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

Ahora vamos a considerar códigos no cíclicos de longitud p^2; esto es, ideales de $\mathbb{F}G$ donde

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

Para determinar los idempotentes primitivos de $\mathbb{F}G$, precisamos encontrar los subgrupos H de G tales que G/H es cíclico.

Ahora vamos a considerar códigos no cíclicos de longitud p^2; esto es, ideales de $\mathbb{F}G$ donde

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

Para determinar los idempotentes primitivos de $\mathbb{F}G$, precisamos encontrar los subgrupos H de G tales que G/H es cíclico. Estos subgrupos son, precisamente

$$\widehat{< a >} \qquad \widehat{< b >}$$

y todos los subgrupos de la forma

$$\widehat{< ab^i >} - \widehat{G}, \quad \text{con} \quad 1 \leq i \leq p-1.$$

Los idempotentes de $\mathbb{F}G$ son:

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

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

Los pesos y las respectivas dimensiones de estos códigos son las siguientes:

Los pesos y las respectivas dimensiones de estos códigos son las siguientes:

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

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

Los pesos y las respectivas dimensiones de estos códigos son las siguientes:

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

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

Dados dos subgrupos cualquiera H, K elegidos entre los anteriores, tenemos que $G = H \times K$.

Los pesos y las respectivas dimensiones de estos códigos son las siguientes:

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

Dados dos subgrupos cualquiera H, K elegidos entre los anteriores, tenemos que $G = H \times K$.
Escribamos $H =< h >$ y $K =< k >$. Los idempotents centrales correspondientes son $e = \widehat{H} - \widehat{G}$, $f = \widehat{K} - \widehat{G}$. Considere

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

Teorema (F. Melo e P.M)

EL peso y la dimensión de $I = (\mathbb{F}G)e \oplus (\mathbb{F}G)f$ están dados por las fórmulas:

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

Teorema (F. Melo e P.M)

EL peso y la dimensión de $I = (\mathbb{F}G)e \oplus (\mathbb{F}G)f$ están dados por las fórmulas:

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

Definición

La **conveniencia** de um código $\mathcal{C}$ es el número

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

Para los códigos cíclicos no minimales tenemos:

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

Para los códigos cíclicos no minimales tenemos:

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

Para la suma de dos códigos abelianos no cíclicos tenemos:

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

Para los códigos cíclicos no minimales tenemos:

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

Para la suma de dos códigos abelianos no cíclicos tenemos:

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

Luego, si $p > 3$, tenemos que $conv(\mathfrak{N})$ es mayor que $conv(I)$ para todo ideal propio I de $\mathbb{F}_q C_{p^2}$.

Códigos dihedrales

En esta sección vamos a considerar grupoes dihedrales de orden $2p^m$, con p primo, es decir, grupos de la forma:

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

Teorema (Dutra, Ferraz, P.M.)

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos, tal que $\mathrm{mdc}(2p^m, q) = 1$ y $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$. Sea $A = \langle a \rangle$, y sea

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

la cadena de subgrupos de A. Considere:

$$e_0 = \widehat{A} \quad , \quad e_j = \widehat{H_j} - \widehat{H_{j-1}}, \ \ 1 \leq j \leq m.$$

y

$$e_{11} = \left(\frac{1+b}{2}\right) e_0 \quad e \quad e_{22} = \left(\frac{1-b}{2}\right) e_0.$$

Entonces, el conjunto de idempotentes centrales primitivos de $\mathbb{F}_q D_{p^m}$ es

$$\{e_{11}, e_{22}\} \cup \{e_j, \ 1 \leq j \leq m\}.$$

Teorema

Para cada idempotente central e_j de $\mathbb{F}_q D_{p^m}$ differente de e_{11}, e_{22} los elementos

$$e_{11}^j = \frac{1+b}{2} e_j \quad \text{y} \quad e_2^j = \frac{1-b}{2} e_j$$

son idempotnentes primitivos no centrales.

Teorema

Para cada idempotente central e_j de $\mathbb{F}_q D_{p^m}$ differente de e_{11}, e_{22} los elementos

$$e_{11}^j = \frac{1+b}{2} e_j \quad \text{y} \quad e_2^j = \frac{1-b}{2} e_j$$

son idempotnentes primitivos no centrales.

Teorema (Assuena- P.M.)

Con la notación anterior, considere $e_{12}^j = \frac{1+b}{2} e_j \frac{1-b}{2}$.
Entonces $f_j = e_{11}^j - e_{12}^j$ es un idempotente no central primitivo y, para $I = (\mathbb{F}_q D_{p^m}) f_j$ tenemos que:

$$dim(I) = \varphi(p^j) \quad \text{and} \quad w(I) = 10|H_j|.$$

Definition

Sea $\mathbb{F}$ un cuerpo y sean G_1, G_2 grupos finitos del mismo orden. Una **equivalencia combinatoria** es un isomorfismo de espacios vectoriales $\phi : \mathbb{F}G_1 \longrightarrow \mathbb{F}G_2$ tal que $\phi(G_1) = G_2$.

Definition

Sea $\mathbb{F}$ un cuerpo y sean G_1, G_2 grupos finitos del mismo orden. Una **equivalencia combinatoria** es un isomorfismo de espacios vectoriales $\phi : \mathbb{F}G_1 \longrightarrow \mathbb{F}G_2$ tal que $\phi(G_1) = G_2$.
Dos códigos $\mathcal{C}_1 \subset \mathbb{F}G_1$ y $\mathcal{C}_2 \subset \mathbb{F}G_2$, son **combinatoriamente equivalentes** si existe una equivalencia combinatoria $\phi : \mathbb{F}G_1 \longrightarrow \mathbb{F}G_2$ tal que $\phi(\mathcal{C}_1) = \mathcal{C}_2$.

Teorema (Assuena- P.M.)

Sea D_{p^m} o grupo dihedral:

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

y sea $\mathbb{F}_q$ un cuerpo finito con q elementos, tal que $\mathrm{mdc}(2p^m, q) = 1$ y $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$.
Entonces, en cada componente simple de $\mathbb{F}_q D_{p^m}$, exisite un ideal a la izquierda minimal (un código izquierdo) que no es combinatoriamente equivalente a un código abeliano.

Una familia de ejemplos

Sean $\mathbb{F}_q$un cuerpo finito con q elementos y D_9 el grupo dihedral de orden 18. Si $\gcd(2p^m, q) = 1$, $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$ y la caracteristica de $\mathbb{F}_q$ no es 2, 3, 5 e 7, entonces:

- $dim[\mathbb{F}_q D_9(e_{11}^1 - e_{12}^1)] = \varphi(3) = 2$;
- $w[\mathbb{F}_q D_9(e_{11}^1 - e_{12}^1)] = 15$.

Una familia de ejemplos

Sean $\mathbb{F}_q$un cuerpo finito con q elementos y D_9 el grupo dihedral de orden 18. Si $\gcd(2p^m, q) = 1$, $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$ y la caracteristica de $\mathbb{F}_q$ no es 2, 3, 5 e 7, entonces:

- $dim[\mathbb{F}_q D_9(e_{11}^1 - e_{12}^1)] = \varphi(3) = 2$;
- $w[\mathbb{F}_q D_9(e_{11}^1 - e_{12}^1)] = 15$.

En **www.codetables.de** hay códigos sobre $\mathbb{F}_5$ y $\mathbb{F}_7$ de esta longitud y dimensión y el mejor peso conocido es precisamente 15.