Códigos (II)

XXVII Escuela Venezolana de Matemáticas – EMALCA

Edgar Martínez-Moro

Sept. 2014

imUVa Instituto de Investigación en Matemáticas

Universidad de Valladolid

Códigos sobre anillos

A partir de ahora A sera un anillo de cadena con ideal maximal $\mathfrak{m}$. Consideraremos siempre fijado un generador del ideal maximal θ. Los ideales de A son $\langle \theta^i \rangle$ con $i = 1, 2, \ldots, \beta$ donde β es el índice de nilpotencia. Los divisores de cero corresponden al ideal $\langle \theta \rangle$ y los elementos en $A \setminus \langle \theta \rangle$ son las unidades.

Para todo elemento no nulo $a \in A$ existe un único exponente tal que $a = u\theta^i$ con u una unidad única módulo $\theta^{\beta-1}$. Claramente para cada par de índices $1 \leq i < j \leq \beta$ si $c\theta^i \in \langle \theta^j \rangle$ entonces $c \in \langle \theta^{j-i} \rangle$.

álgebra lineal sobre anillos de cadena

El rango de McCoy de una matriz $\mathcal{M}$ con entradas en un anillo de cadena A es el mayor entero positivo t tal que existe un menor de la matriz que es una unidad. En caso de que no exista ningun menor que sea una unidad el rango de McCoy es 0. Notaremos el rango de McCoy de la matriz $\mathcal{M}$ por $\operatorname{rg}_{Mc}(\mathcal{M})$.

– Teorema –

Consideremos $\mathbf{v}_1, \ldots, \mathbf{v}_m \in A^n \setminus \theta A^n$. El conjunto $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ es linealmente dependiente si y sólo si $\{\overline{\mathbf{v}_1}, \ldots, \overline{\mathbf{v}_m}\}$ son linealmente dependientes en $\mathbb{K} = A/\mathfrak{m}$.

álgebra lineal sobre anillos de cadena

El rango de McCoy de una matriz $\mathcal{M}$ con entradas en un anillo de cadena A es el mayor entero positivo t tal que existe un menor de la matriz que es una unidad. En caso de que no exista ningun menor que sea una unidad el rango de McCoy es 0. Notaremos el rango de McCoy de la matriz $\mathcal{M}$ por $\operatorname{rg}_{Mc}(\mathcal{M})$.

– Teorema –

Consideremos $\mathbf{v}_1, \ldots, \mathbf{v}_m \in A^n \setminus \theta A^n$. El conjunto $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ es linealmente dependiente si y sólo si $\{\overline{\mathbf{v}_1}, \ldots, \overline{\mathbf{v}_m}\}$ son linealmente dependientes en $\mathbb{K} = A/\mathfrak{m}$.

– Corolario –

Dada una matriz $\mathcal{M}$ con entradas en el anillo A las siguientes proposiciones son equivalentes.

1. $\mathrm{rg}_{Mc}(\mathcal{M}) = t$.
2. El rango de $\overline{\mathcal{M}}$ es t.
3. $\mathcal{M}$ tiene t filas linealmente independientes y $t+1$ filas son siempre linealmente dependientes.
4. $\mathcal{M}$ tiene t columnas linealmente independientes y $t+1$ columnas son siempre linealmente dependientes.

Es fácil ver que la regla de Cramer para sistemas sobre un anillo de cadena A se cumple. Como corolario tenemos que

$$|\{\mathbf{x} \in A^n \mid \mathcal{M} \cdot \mathbf{x}^T = 0\}| = |A|^{n-m}.$$

Códigos lineales sobre A

Un código lineal $\mathcal{C}$ sobre A de longitud n es un A-submódulo de A^n. Para un entero positivo k denotaremos por Id_k la matriz identidad de tamao $k \times k$.

Sea $\mathcal{C}$ un código lineal sobre A. Una matriz G se denomina matriz generatriz de $\mathcal{C}$ si las filas de G generan linealmente a $\mathcal{C}$ y ninguna de ellas se puede poner como una combinación lineal de las demás.

G está expresada en forma estándar si después de una permutación de las coordenadas adecuada tiene la siguiente forma

$$\begin{pmatrix} \mathrm{Id}_{k_0} & C_{0,1} & C_{0,2} & C_{0,3} & \dots & C_{0,\beta-1} & C_{0,\beta} \\ 0 & \theta\mathrm{Id}_{k_1} & \theta C_{1,2} & \theta C_{1,3} & \dots & \theta C_{1,\beta-1} & \theta C_{1,\beta} \\ 0 & 0 & \theta^2\mathrm{Id}_{k_2} & \theta^2 C_{2,3} & \dots & \theta^2 C_{2,\beta-1} & \theta^2 C_{2,\beta} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \theta^{\beta-1} Id_{k_{\beta-1}} & \theta^{\beta-1} C_{\beta-1,\beta} \end{pmatrix} = \begin{pmatrix} C_0 \\ \theta C_1 \\ \theta^2 C_2 \\ \vdots \\ \theta^{\beta-1} C_{\beta-1} \end{pmatrix}.$$

Códigos lineales sobre A

Un código lineal $\mathcal{C}$ sobre A de longitud n es un A-submódulo de A^n. Para un entero positivo k denotaremos por Id_k la matriz identidad de tamao $k \times k$.

Sea $\mathcal{C}$ un código lineal sobre A. Una matriz G se denomina matriz generatriz de $\mathcal{C}$ si las filas de G generan linealmente a $\mathcal{C}$ y ninguna de ellas se puede poner como una combinación lineal de las demás.

G está expresada en forma estándar si después de una permutación de las coordenadas adecuada tiene la siguiente forma

$$\begin{pmatrix} \mathrm{Id}_{k_0} & C_{0,1} & C_{0,2} & C_{0,3} & \dots & C_{0,\beta-1} & C_{0,\beta} \\ 0 & \theta\mathrm{Id}_{k_1} & \theta C_{1,2} & \theta C_{1,3} & \dots & \theta C_{1,\beta-1} & \theta C_{1,\beta} \\ 0 & 0 & \theta^2\mathrm{Id}_{k_2} & \theta^2 C_{2,3} & \dots & \theta^2 C_{2,\beta-1} & \theta^2 C_{2,\beta} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \theta^{\beta-1} Id_{k_{\beta-1}} & \theta^{\beta-1} C_{\beta-1,\beta} \end{pmatrix} = \begin{pmatrix} C_0 \\ \theta C_1 \\ \theta^2 C_2 \\ \vdots \\ \theta^{\beta-1} C_{\beta-1} \end{pmatrix}.$$

Códigos lineales sobre A

Un código lineal $\mathcal{C}$ sobre A de longitud n es un A-submódulo de A^n. Para un entero positivo k denotaremos por Id_k la matriz identidad de tamao $k \times k$.

Sea $\mathcal{C}$ un código lineal sobre A. Una matriz G se denomina matriz generatriz de $\mathcal{C}$ si las filas de G generan linealmente a $\mathcal{C}$ y ninguna de ellas se puede poner como una combinación lineal de las demás.

G está expresada en forma estándar si después de una permutación de las coordenadas adecuada tiene la siguiente forma

$$\begin{pmatrix} \mathrm{Id}_{k_0} & C_{0,1} & C_{0,2} & C_{0,3} & \dots & C_{0,\beta-1} & C_{0,\beta} \\ 0 & \theta\mathrm{Id}_{k_1} & \theta C_{1,2} & \theta C_{1,3} & \dots & \theta C_{1,\beta-1} & \theta C_{1,\beta} \\ 0 & 0 & \theta^2\mathrm{Id}_{k_2} & \theta^2 C_{2,3} & \dots & \theta^2 C_{2,\beta-1} & \theta^2 C_{2,\beta} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \theta^{\beta-1} Id_{k_{\beta-1}} & \theta^{\beta-1} C_{\beta-1,\beta} \end{pmatrix} = \begin{pmatrix} C_0 \\ \theta C_1 \\ \theta^2 C_2 \\ \vdots \\ \theta^{\beta-1} C_{\beta-1} \end{pmatrix}.$$

Asociaremos a G la matriz C dada por

$$C = \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ \vdots \\ C_{\beta-1} \end{pmatrix},$$

cuyas submatrices son únicas módulo $\theta^{\beta-1}$ y sus proyecciones sobre $\mathbb{K}$ son únicas.

– Proposición –

Cualquier código $\mathcal{C}$ sobre un anillo de cadena A tiene una matriz generatriz en forma estándar.

Asociaremos a G la matriz C dada por

$$C = \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ \vdots \\ C_{\beta-1} \end{pmatrix},$$

cuyas submatrices son únicas módulo $\theta^{\beta-1}$ y sus proyecciones sobre $\mathbb{K}$ son únicas.

– Proposición –

Cualquier código $\mathcal{C}$ sobre un anillo de cadena A tiene una matriz generatriz en forma estándar.

Dado un código $\mathcal{C}$ sobre un anillo de cadena A y un elemento $a \in A$ definimos $(\mathcal{C} : a)$ como es siguiente conjunto (cociente de submodulos)

$$(\mathcal{C} : a) = \{b \in A \mid a \cdot b \in \mathcal{C}\}.$$

Dado un código $\mathcal{C}$ sobre un anillo de cadena A con θ un generador de $\mathfrak{m}$ ideal maximal de A con índice de nilpotencia β lo asociamos la siguiente torre de códigos

$$\mathcal{C} = (\mathcal{C} : \theta^0) \subseteq \cdots \subseteq (\mathcal{C} : \theta^i) \subseteq \cdots \subseteq (\mathcal{C} : \theta^{\beta-1})$$

y sobre $\mathbb{K} = A/\mathfrak{m}$

$$\overline{\mathcal{C}} = \overline{(\mathcal{C} : \theta^0)} \subseteq \cdots \subseteq \overline{(\mathcal{C} : \theta^i)} \subseteq \cdots \subseteq \overline{(\mathcal{C} : \theta^{\beta-1})}$$

Dado un código $\mathcal{C}$ sobre un anillo de cadena A y un elemento $a \in A$ definimos $(\mathcal{C} : a)$ como es siguiente conjunto (cociente de submodulos)

$$(\mathcal{C} : a) = \{b \in A \mid a \cdot b \in \mathcal{C}\}.$$

Dado un código $\mathcal{C}$ sobre un anillo de cadena A con θ un generador de $\mathfrak{m}$ ideal maximal de A con índice de nilpotencia β lo asociamos la siguiente torre de códigos

$$\mathcal{C} = (\mathcal{C} : \theta^0) \subseteq \cdots \subseteq (\mathcal{C} : \theta^i) \subseteq \cdots \subseteq (\mathcal{C} : \theta^{\beta-1})$$

y sobre $\mathbb{K} = A/\mathfrak{m}$

$$\overline{\mathcal{C}} = \overline{(\mathcal{C} : \theta^0)} \subseteq \cdots \subseteq \overline{(\mathcal{C} : \theta^i)} \subseteq \cdots \subseteq \overline{(\mathcal{C} : \theta^{\beta-1})}$$

– Lema –

1. Consideremos un código $\mathcal{C}$ con matriz generatriz G en forma estándar y matriz asociada C. Para cada valor de $i = 1, 2, \ldots, \beta - 1$ el código $\overline{(\mathcal{C} : \theta^i)}$ tiene matriz generatriz $\begin{pmatrix} \overline{C_0} \\ \overline{C_1} \\ \overline{C_2} \\ \vdots \\ \overline{C_i} \end{pmatrix}$, y su dimensión es $\sum_{j=0}^{i} k_j$.
2. Si la cadena $\mathcal{E}_0 \subseteq \mathcal{E}_1 \subseteq \cdots \subseteq \mathcal{E}_{\beta-1}$ está formada por códigos de longitud n sobre $\mathbb{K}$ entonces existe un código $\mathcal{C}$ sobre A con

$$\overline{(\mathcal{C} : \theta^i)} = \mathcal{E}_i, \qquad i = 0, 1, \ldots, \beta - 1.$$

– Teorema –

Sea $\mathcal{C}$ un código de longitud n sobre un anillo de cadena A. Entonces:

1. Los parámetros k_i para $i = 0, 1, \ldots, k_{\beta-1}$ son independientes de la matriz generatriz en forma estándar G elegida.
2. Cualquier palabra $\mathbf{c} \in \mathcal{C}$ se puede escribir de forma única como

$$\mathbf{c} = (\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{\beta-1}) \cdot G, \quad \mathbf{v}_i \in (A/\theta^{\beta-i}A)^{k_i} \simeq (\theta^i R)^{k_i}.$$

3. $$|\mathcal{C}| = |\mathbb{K}|^{\sum_{i=0}^{\beta-1} k_i(\beta-i)}.$$

Dualidad

Con las notaciones anteriores definimos

$$k_0(\mathcal{C}) = \dim(\overline{\mathcal{C}})$$
$$k_i(\mathcal{C}) = \dim(\overline{(\mathcal{C} : \theta^i)}) - \dim(\overline{(\mathcal{C} : \theta^{i-1})}), \quad 1 \leq i \leq \beta - 1.$$

– Teorema –

Consideremos $\mathcal{C}$ un código sobre un anillo de cadena A con matriz generatriz G en forma estándar.

1. Si definimos

$$H_{i,j} = -\sum_{k=i+1}^{j-1} H_{i,k} C^T_{\beta-j,\beta-k} - C^T_{\beta-j,\beta-i}, \quad 0 \leq i < j \leq \beta$$

entonces la matriz H

$$\begin{pmatrix} H_{0,\beta} & H_{0,\beta-1} & \cdots & H_{0,1} & \mathrm{Id}_{n-k(\mathcal{C})} \\ \theta H_{1,\beta} & \theta H_{1,\beta-1} & \cdots & \theta \mathrm{Id}_{n-k_{\beta-1}(\mathcal{C})} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \theta^{\beta-1} H_{\beta-1,\beta} & \theta^{\beta-1} \mathrm{Id}_{n-k_1(\mathcal{C})} & \cdots & 0 & 0 \end{pmatrix} = \begin{pmatrix} H_0 \\ \theta H_1 \\ \vdots \\ \theta^{\beta-1} H_{\beta-1} \end{pmatrix},$$

es una matriz de paridad de $\mathcal{C}$.

– Teorema (cont) –

2. $\overline{(\mathcal{C}^{\perp} : \theta^{i})} = \left(\overline{(\mathcal{C} : \theta^{\beta-1-i})}\right)^{\perp}$,
   $k_0(\mathcal{C}^{\perp}) = n - k_0(\mathcal{C})$,
   $k_i(\mathcal{C}^{\perp}) = k_{\beta-1}(\mathcal{C})$ para $1 \leq i \leq \beta - 1$.
3. $$|\mathcal{C}|^{\perp} = \frac{|A^n|}{|\mathcal{C}|} \quad \text{y} \quad (\mathcal{C}^{\perp})^{\perp} = \mathcal{C}.$$

Asociaremos a la matriz de paridad H la siguiente matriz:

$$C(\perp) = \begin{pmatrix} H_0 \\ H_1 \\ H_2 \\ \vdots \\ H_{\beta-1} \end{pmatrix}.$$

– Corolario –

Sea $\mathcal{C}$ un código con matriz generatriz G y matriz de paridad H y matrices asociadas C y $C(\perp)$ respectivamente. Entonces $\overline{\mathcal{C}}$ tiene matriz generatriz $\overline{A_0}$ y matriz de paridad $\overline{C(\perp)}$.

Asociaremos a la matriz de paridad H la siguiente matriz:

$$C(\perp) = \begin{pmatrix} H_0 \\ H_1 \\ H_2 \\ \vdots \\ H_{\beta-1} \end{pmatrix}.$$

– Corolario –

Sea $\mathcal{C}$ un código con matriz generatriz G y matriz de paridad H y matrices asociadas C y $C(\perp)$ respectivamente. Entonces $\overline{\mathcal{C}}$ tiene matriz generatriz $\overline{A_0}$ y matriz de paridad $\overline{C(\perp)}$.

Códigos libres

– Proposición –

Consideremos $\mathcal{C}$ un código sobre un anillo de cadena A. Los siguientes enunciados son equivalentes.

1. $\mathcal{C}$ es un código libre (como submódulo).
2. Si la matriz G es una matriz generatriz de $\mathcal{C}$ en forma estándar entonces $G = (\mathrm{Id}\,, C)$ para alguna matriz C (es decir, es sistemática).
3. $k(\mathcal{C}) = k_0(\mathcal{C})$.
4. $\overline{\mathcal{C}} = \overline{(\mathcal{C} : \theta)} = \cdots = \overline{(\mathcal{C} : \theta^{\beta-1})}$.
5. $\mathcal{C}^{\perp}$ es un código libre.

Distancia de Hamming

Llamaremos soporte de un elemento $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in A^n$ a $\mathrm{sop}(\mathbf{x}) = \{i \mid x_i \neq 0\}$. El soporte de un conjunto en A^n será la unión de todos los soportes de sus elementos y la distancia de Hamming de un código $\mathcal{C}$ será entonces

$$\mathrm{d}(\mathcal{C}) = \mathrm{mín}\{|\mathrm{sop}(\mathbf{c})| \mid \mathbf{c} \in \mathcal{C},\ \mathbf{c} \neq \mathbf{0}\}.$$

– Lema –

Sea $\alpha = \theta^{\beta-1}$. La aplicación

$$\begin{array}{rccc} \xi: & \alpha A^n & \longrightarrow & \mathbb{K} \\ & \alpha \cdot \mathbf{x} & \mapsto & \overline{\mathbf{x}} \end{array}$$

es un isomorfismo que preserva la distancia de Hamming.

Distancia de Hamming

Llamaremos soporte de un elemento $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in A^n$ a $\mathrm{sop}(\mathbf{x}) = \{i \mid x_i \neq 0\}$. El soporte de un conjunto en A^n será la unión de todos los soportes de sus elementos y la distancia de Hamming de un código $\mathcal{C}$ será entonces

$$\mathrm{d}(\mathcal{C}) = \mathrm{mín}\{|\mathrm{sop}(\mathbf{c})| \mid \mathbf{c} \in \mathcal{C},\ \mathbf{c} \neq \mathbf{0}\}.$$

– Lema –

Sea $\alpha = \theta^{\beta-1}$. La aplicación

$$\begin{array}{rccc} \xi: & \alpha A^n & \longrightarrow & \mathbb{K} \\ & \alpha \cdot \mathbf{x} & \mapsto & \overline{\mathbf{x}} \end{array}$$

es un isomorfismo que preserva la distancia de Hamming.

Llamaremos soporte minimal de un conjunto $S \subseteq A^n$ a aquellos elementos de S no nulos con soporte mínimo respecto a la inclusión. Lo denotaremos por $\mathrm{Msop}(S)$. Es claro que

$$\mathrm{d}(\mathcal{C}) = \text{mín}\{|R| \mid R \in \mathrm{Msop}(\mathcal{C})\}.$$

– Teorema –

Sea $\mathcal{C}$ un código sobre el anillo de cadena A.

1. $\mathrm{Msop}(\mathcal{C}) = \mathrm{Msop}(\mathcal{C} \cap \theta^i\mathcal{C})$ y $\mathrm{d}(\mathcal{C}) = \mathrm{d}(\mathcal{C} \cap \theta^i\mathcal{C})$ para $0 \leq i \leq \beta - 1$.
2. $\mathrm{Msop}(\mathcal{C}) = \mathrm{Msop}\left(\overline{(\mathcal{C} : \alpha)}\right)$ y $\mathrm{d}(\mathcal{C}) = \mathrm{d}\left(\overline{(\mathcal{C} : \alpha)}\right)$.
3. Si $\overline{\mathcal{C}} \neq \{\mathbf{0}\}$ entonces $\mathrm{d}(\mathcal{C}) \leq \mathrm{d}(\overline{\mathcal{C}})$.

Llamaremos soporte minimal de un conjunto $S \subseteq A^n$ a aquellos elementos de S no nulos con soporte mínimo respecto a la inclusión. Lo denotaremos por $\mathrm{Msop}(S)$. Es claro que

$$\mathrm{d}(\mathcal{C}) = \text{mín}\{|R| \mid R \in \mathrm{Msop}(\mathcal{C})\}.$$

– Teorema –

Sea $\mathcal{C}$ un código sobre el anillo de cadena A.

1. $\mathrm{Msop}(\mathcal{C}) = \mathrm{Msop}(\mathcal{C} \cap \theta^i\mathcal{C})$ y $\mathrm{d}(\mathcal{C}) = \mathrm{d}(\mathcal{C} \cap \theta^i\mathcal{C})$ para $0 \leq i \leq \beta - 1$.
2. $\mathrm{Msop}(\mathcal{C}) = \mathrm{Msop}\left(\overline{(\mathcal{C} : \alpha)}\right)$ y $\mathrm{d}(\mathcal{C}) = \mathrm{d}\left(\overline{(\mathcal{C} : \alpha)}\right)$.
3. Si $\overline{\mathcal{C}} \neq \{\mathbf{0}\}$ entonces $\mathrm{d}(\mathcal{C}) \leq \mathrm{d}(\overline{\mathcal{C}})$.

Códigos cíclicos sobre anillos de cadena

Utilizaremos para simplificar la notación A_n para denotar $A[x]/\langle x^n-1\rangle$ y $\mathbb{K}_n$ para denotar a $\mathbb{K}[x]/\langle x^n-1\rangle$. Claramente A_n y A^n son isomorfos como grupos abelianos con la suma ordinaria en ambos casos y es claro que un código de longitud n sobre A es cíclico si y sólo si se puede ver como un ideal en A_n. También es fácil de ver que si $\mathcal{C}$ es un código cíclico en A^n entonces $\overline{\mathcal{C}}$ es un código cíclico en $\mathbb{K}^n$, es más, los códigos

$$(\mathcal{C} : \theta^i), \qquad i = 0, 1, \ldots, \beta - 1$$

son también cíclicos.

Diremos que el conjunto

$$S = \{\theta^{a_0} g_{a_0}, \theta^{a_1} g_{a_1}, \ldots, \theta^{a_s} g_{a_s}\}$$

es un conjunto de generadores en forma estándar para el código cíclico $\mathcal{C} = \langle S \rangle$ si $0 \leq s < \beta$ y además

1. $0 \leq a_0 < a_1 < \cdots < a_s < \beta$;
2. $g_{a_i} \in A[x]$ es mónico para todo $i = 0, 1, \ldots, s$;
3. $\deg(g_{a_i}) > \deg(g_{a_{i+1}})$ para todo $i = 0, 1, \ldots, s-1$;
4. $g_{a_s} | g_{a_{s-1}} | \ldots | g_{a_0} | x^n - 1$.

– Lema –

Si $\mathcal{C}$ es un código cíclico no nulo entonces también lo es $\overline{(\mathcal{C} : \theta^{\beta-1})}$.

– Lema –

Sea $S = \{\theta^{a_0} g_{a_0}, \theta^{a_1} g_{a_1}, \ldots, \theta^{a_s} g_{a_s}\}$ un sistema de generadores del código cíclico $\mathcal{C}$ en forma estándar. Si $i < a_0$ entonces $\overline{(\mathcal{C} : \theta^i)} = \{\mathbf{0}\}$, en el resto de los casos $\overline{(\mathcal{C} : \theta^i)} = \langle \overline{g_{a_j}} \rangle$ donde j es maximal con la propiedad $a_j \leq i$.

– Lema –

Si $\mathcal{C}$ es un código cíclico no nulo entonces también lo es $\overline{(\mathcal{C} : \theta^{\beta-1})}$.

– Lema –

Sea $S = \{\theta^{a_0} g_{a_0}, \theta^{a_1} g_{a_1}, \ldots, \theta^{a_s} g_{a_s}\}$ un sistema de generadores del código cíclico $\mathcal{C}$ en forma estándar. Si $i < a_0$ entonces $\overline{(\mathcal{C} : \theta^i)} = \{\mathbf{0}\}$, en el resto de los casos $\overline{(\mathcal{C} : \theta^i)} = \langle \overline{g_{a_j}} \rangle$ donde j es maximal con la propiedad $a_j \leq i$.

Para cada divisor $f|x^n-1 \in \mathbb{K}[x]$ existe un polinomio único en $g \in A[x]$ con $\overline{g} = f$ y $g|x^n-1$ pues x^n-1 es libre de cuadrados. A dicho g le llamaremos (polinomio) levantamiento de Hensel de f.

– Teorema –

Un código cíclico no nulo tiene un único conjunto generador en forma estándar.

Para cada divisor $f|x^n-1 \in \mathbb{K}[x]$ existe un polinomio único en $g \in A[x]$ con $\overline{g}=f$ y $g|x^n-1$ pues x^n-1 es libre de cuadrados. A dicho g le llamaremos (polinomio) levantamiento de Hensel de f.

– Teorema –

Un código cíclico no nulo tiene un único conjunto generador en forma estándar.

– Teorema –

Sea $S = \{\theta^{a_0} g_{a_0}, \theta^{a_1} g_{a_1}, \ldots, \theta^{a_s} g_{a_s}\}$ un sistema de generadores en forma estándar del código cíclico $\mathcal{C}$.

1. Consideremos

$$T = \bigcup_{i=0}^{s} \left\{ \theta^{a_i} g_{a_i} x^{d_{i-1}-d_i-1}, \ldots, \theta^{a_i} g_{a_i} x, \theta^{a_i} g_{a_i} \right\}$$

con $d_i = \deg(g_{a_i})$ para $i = 1, \ldots, s$ y $d_{-1} = n$, $d_{s+1} = 0$.
El conjunto T define una matriz generatriz del código $\mathcal{C}$.

– Teorema (cont.) –

2. Cualquier palabra del código $\mathbf{c} \in \mathcal{C}$ puede ser escrita de forma única como

$$\mathbf{c} = \sum_{j=0}^{s} h_j g_{a_j} \theta^{a_j}$$

con $h_j \in (A/A\theta^{\beta - a_j})[x] \cong A\theta^{a_j}[x]$ y $\deg(h_j) < d_{j-1} - d_j$.

3. $k_i(\mathcal{C}) = d_{j-1} - d_j$ si $i = a_j$ para algún j y $k_i(\mathcal{C}) = 0$ en el resto de los casos. Además

$$|\mathcal{C}| = |\mathbb{K}|^{\sum_{j=0}^{s} (\beta - a_j)(d_{j-1} - d_j)}.$$

Dualidad

El dual de un código cíclico es también cíclico.

Sea $f \in A[x]$ un polinomio no nulo. Llamaremos polinomio recíproco de f a

$$f^\star = x^{\deg(f)} f\left(\frac{1}{x}\right).$$

Si el termino constante f_0 de f es una unidad definimos

$$f^\sharp = \frac{f^\star}{f_0}.$$

– Proposición –

Sea $\{\theta^{a_0} g_{a_0}, \theta^{a_1} g_{a_1}, \ldots, \theta^{a_s} g_{a_s}\}$ un sistema de generadores en forma estándar del código cíclico $\mathcal{C}$. Definamos $a_{s+1} = \beta$ y $g_{a_{-1}} = x^n - 1$. Para $j = 0, 1, \ldots, s+1$ definamos $b_j = \beta - a_{s+1-j}$ y

$$h_{b_j} = \left(\frac{x^n - 1}{g_{a_{s-j}}} \right)^{\sharp}.$$

Entonces $\{\theta^{b_0} h_{b_0}, \theta^{b_1} h_{b_1}, \ldots, \theta^{b_{s+1}} h_{b_{s+1}}\}$ un sistema de generadores en forma estándar del código cíclico $\mathcal{C}^{\perp}$.

Sea $f \in \mathbb{K}[x]$ un polinomio mónico con $f | x^n - 1$. El código cíclico $\mathcal{C} = \langle g \rangle$ donde g el el levantamiento de Hensel de f se llama levantamiento de Hensel del código (cíclico) $\langle f \rangle$.

– Proposición –

Sea $\mathcal{C}$ un código sobre el anillo A. Los siguientes enunciados son equivalentes:

1. $\mathcal{C}$ es el levantamiento de Hensel de un código cíclico.
2. $\mathcal{C}$ es cíclico y libre.
3. Existe un $g \in A[x]$ con $g | x^n - 1$ y $\mathcal{C} = \langle g \rangle$.
4. Existe un $g \in A[x]$ mónico tal que $\{g\}$ es un sistema de generadores en forma estándar del código $\mathcal{C}$.
5. $\mathcal{C}^{\perp}$ es el levantamiento de Hensel de un código cíclico.

Raíces de la unidad

Tomemos $A = GR(p^{al}, p^a)$ y m un entero positivo tal que $l|m$ y $n|p^m - 1$, el anillo $GR(p^{am}, p^a)$ es una extensión de A en la que $x^n - 1$ tiene n raíces. Podemos levantar una raíz primitiva de la unidad en el cuerpo finito $\mathbb{F}_{p^m}$ a una raíz ξ de $x^n - 1$ en el anillo $GR(p^{am}, p^a)$ que también será primitiva. Para cada elección de $i = 0, 1, \ldots, n-1$ denotaremos por $m_i(x)$ al polinomio mínimo de $\overline{\xi}^i$ en $\mathbb{F}_{p^l}[x]$. Si denotamos por U un conjunto de representantes de las clases de conjugación de $\overline{\xi}$ es bien conocido que

$$x^n - 1 = \prod_U m_i(x).$$

Denotaremos por $M_i(x) \in A[x]$ al levantamiento de Hensel de $m_i(x)$ para cada $i = 1, 2, \ldots, n-1$. Los polinomios $M_i(x)$ son básicos irreducibles.

– Lema –

1. Para cada $i = 1, 2, \ldots, n-1$

$$\{j \in \{1, \ldots, n-1\} \mid M_i(\xi^j) = 0\} =$$

$$\{j \in \{1, \ldots, n-1\} \mid m_i(\overline{\xi^j}) = 0\}.$$

2. Para cada $i = 1, 2, \ldots, n-1$ $M_i(x)$ es el polinomio mínimo de ξ^i.
3. U un conjunto de representantes de las clases de conjugación de ξ en el anillo $GR(p^{am}, p^a)$.

– Lema (cont) –

4. Sean $f \in A[x]$ y $\{i_1, \ldots, i_v\} \subseteq U$. Si $f(\xi^{i_j}) = 0$ para $j = 1, \ldots, v$ entonces

$$\left(\prod_{j=1}^{v} M_{i_j}(x) \right) | f.$$

5. Sea $f \in A[x]$ con $f | x^n - 1$ y $L \subseteq U$. Entonces $f = \prod_{i \in L} M_i(x)$ si y sólo si $L = \{i \in U | f(\xi^i) = 0\}$.

6. Para $k = 1, \ldots, a-1$,

$$M_i(x) \mod p^k \in (A/p^k A)[x] \cong GR(p^{kl}, p^k)[x]$$

es el polinomio mínimo de ξ^i módulo p^k.

– Teorema –

Sea U un conjunto de representantes de las clases de conjugación de las raíces de $x^n - 1$ en A y $\mathcal{C}$ un submódulo de A^n. El submódulo $\mathcal{C}$ es un código cíclico si y sólo si existen enteros no negativos $0 \leq a_0 < \cdots < a_s < a_{s+1} = a$ y una partición $\{L_{a_j} \mid j = 0, \ldots, s+1\}$ del conjunto U tal que

$$\mathcal{C} = \{\mathbf{c} \in A_n \mid p^{a-a_j}\mathbf{c}(\xi^{i_j}) = 0,\ i_j \in L_{a_j},\ j = 0, \ldots, s+1\}.$$

Códigos Kerdock y Preparata

$$\begin{array}{rccc} \mathfrak{G}: & \mathbb{Z}_4 & \longrightarrow & \mathbb{F}_2^2 \\ & 0 & & \mathfrak{G}(0) = 00 \\ & 1 & & \mathfrak{G}(1) = 01 \\ & 2 & & \mathfrak{G}(2) = 11 \\ & 3 & & \mathfrak{G}(3) = 10 \end{array}$$

La aplicación de Gray no es lineal y define una métrica (métrica de Lee) sobre $\mathbb{Z}_4$ dada por el peso $w_L(x) = w_H(\mathfrak{G}(x))$ para cada $x \in \mathbb{Z}_4$, donde w_H denota el peso de Hamming. La métrica de Lee se extiende de manera natural a $\mathbb{Z}_4^n$ coordenada a coordenada.

Sea $h(x)$ un polinomio básico irreducible de grado r en $\mathbb{Z}_4[x]$. Sea $f(x)$ el polinomio recíproco de

$$\frac{x^n - 1}{(x-1)h(x)}.$$

Definimos $K(r+1)$ el código cíclico de longitud $2^r - 1$ sobre $\mathbb{Z}_4$ generado por $f(x)$. Notaremos por $\hat{K}(r+1)$ al código que se obtiene al aadir un dígito de paridad $K(r+1)$. El código de Kerdock se define como su imagen mediante la aplicación de Gray, es decir $\mathcal{K}(r+1) = \mathfrak{G}(\hat{K}(r+1))$. Es un código de longitud 2^{r+1} con 4^{r+1} palabras.

Para $r \geq 3$ e impar, si tomamos $P(r+1) = \hat{K}(r+1)^{\perp}$ como códigos sobre $\mathbb{Z}_4$ y consideramos su imagen mediante la aplicación de Gray $\mathcal{P}(r+1) = \mathfrak{G}(P(r+1))$ obtenemos los códigos de tipo Preparata.