CÓDIGOS CONVOLUCIONALES Y GEOMETRÍA ALGEBRAICA

J.M. MUÑOZ PORRAS, J.A. DOMÍNGUEZ PÉREZ

Resumen. Las técnicas de Geometría Algebraica utilizadas para construir códigos de Goppa sobre una curva algebraica sobre un cuerpo finito $\mathbb{F}_q$ pueden extenderse a la construcción de códigos convolucionales sobre el cuerpo infinito de funciones racionales en una variable $\mathbb{F}_q(z)$. De este modo es posible constuir códigos convolucionales sobre la recta proyectiva que alcanzan la cota de Singleton generalizada.

1. Introducción a la Teoría de Códigos Convolucionales

Dado un cuerpo finito $\mathbb{F}_q$ de q elementos, un $[n,k]$-*codificador lineal* es una aplicación lineal inyectiva

$$\begin{aligned} G\colon \mathbb{F}_q^k &\hookrightarrow \mathbb{F}_q^n \\ u &\mapsto x = u \cdot G\,, \end{aligned}$$

cuya imagen define el $[n,k]$-*código lineal* $\mathcal{C}_k \equiv \operatorname{Img} G \subset \mathbb{F}_q^n$.

De este modo, la *codificación* es la transformación de una "palabra de información" $u \in \mathbb{F}_q^k$ en una "palabras del código" $x = u \cdot G \in \mathbb{F}_q^n$, mediante el producto por una "matriz codificadora" G de k filas y n columnas.

Si lo que se considera es una sucesión finita de palabras de información $u(1), u(2), \ldots, u(r)$, se obtiene a su vez una sucesión finita de palabras del código $x(1), x(2), \ldots, x(r)$, donde

$$x(t) = u(t) \cdot G\,, \tag{1}$$

de modo que $x(t)$ es una función lineal de $u(t)$.

Entendiendo $u(t)$ como una *palabra de información en el instante de tiempo* t, la idea de la codificación convolucional es hacer que $x(t)$ sea

una función lineal de $u(t)$ y de un número fijo de palabras de información anteriores $u(t), u(t-1), \ldots, u(t-m)$, donde m es un entero positivo denominado "memoria" del codificador (en particular, los códigos lineales son códigos convolucionales sin memoria, $m = 0$).

Este concepto de *codificador convolucional* fue introducido por P. Elias [1] en 1955, y desde el punto de vista algebraico fue desarrollado por G.D. Forney Jr. [2] en una serie de papeles clásicos en la década de 1970, y posteriormente reformulado por R. McEliece [3] en 1998. Más recientemente se han introducido técnicas de Geometría Algebraica en la teoría de códigos convolucionales con los trabajos de J. Rosenthal y R. Smarandache [4] y V. Lomadze [5], así como los publicados por los autores en colaboración con G. Serrano Sotelo y J.I. Iglesias Curto [6], [7], en cuyos resultados está basada esta exposición.

Para dar una definicón concreta de *código convolucional*, reexpresamos la fórmula (1) como un sumatorio formal (dependiente del tiempo t) introduciendo un *operador de retardo* D,

$$\sum_{t\geq 0} x(t)D^t = \sum_{t\geq 0} u(t)D^t \cdot G\,, \tag{2}$$

donde $D\left(\sum_{t\geq 0} u(t)D^t\right) = \sum_{t\geq 0} u(t)D^{t+1} = \sum_{t\geq 1} u(t-1)$. Si se denota

$$x(D) \equiv \sum_{t\geq 0} u(t)D^t \in \mathbb{F}_q[D]^n$$

$$u(D) \equiv \sum_{t\geq 0} u(t)D^t \in \mathbb{F}_q[D]^k$$

la expresión (2) se puede reescribir como

$$x(D) = u(D) \cdot G\,, \tag{3}$$

ecuación que resume el proceso de codificación lineal respecto a la matriz codificadora G. La codificación convolucional consiste entonces en hacer que la matriz codificadora que aparece en (3) dependa también del operador de retardo

$$x(D) = u(D) \cdot G(D)\,.$$

De este modo se obtiene una de las posibles definiciones de código convolucional, para la que utilizaremos una notación polinómica, reemplazando D por la variable z.

Definición 1.1. *Un $[n,k]$-codificador convolucional (polinómico) es un homomorfismo inyectivo de $\mathbb{F}_q[z]$-módulos*

$$\begin{aligned} G(z)\colon \mathbb{F}_q[z]^k &\hookrightarrow \mathbb{F}_q[z]^n \\ u(z) &\mapsto x(z) = u(z)\cdot G(z)\,. \end{aligned}$$

La imagen de este homomorfismo define (las palabras de) el $[n,k]$-código convolucional

$$\mathcal{C}_k \equiv \operatorname{Img} G(z)\,.$$

Dado un $[n,k]$-codificador convolucional $G(z)$, se tiene una sucesión exacta

$$0 \to \mathbb{F}_q[z]^k \xrightarrow{G(z)} \mathbb{F}_q[z]^n \to M \to 0\,,$$

donde M es un $\mathbb{F}_q[z]$-módulo de rango $n-k$. Tomando entonces duales como $\mathbb{F}_q[z]$-módulos, resulta otra sucesión exacta

$$0 \to \widehat{M} \to \widehat{\mathbb{F}_q[z]^n} \xrightarrow{G(z)^t} \widehat{\mathcal{C}}_k \to \widehat{\mathcal{C}}_k/\operatorname{Img} G(z)^t \to 0\,,$$

donde $\widehat{\mathcal{C}}_k/\operatorname{Img} G(z)^t$ es un $\mathbb{F}_q[z]$-módulo de torsión, cuyo anulador es precisamente

$$\operatorname{Ann}\left(\widehat{\mathcal{C}}_k/\operatorname{Img} G(z)^t\right) = \langle\{\text{menores } k\times k \text{ de } G(z)\}\rangle\,.$$

La aplicación $G(z)^t$ permite distinguir diversos tipos de codificadores, e introducir una noción de "grado interno" del codificador

$$\operatorname{Gr}_{in}(G(z)) \equiv \text{ máximo grado de los menores } k\times k \text{ de } G(z)\,,$$

en contraste con la noción de "grado externo",

$$\operatorname{Gr}_{ex}(G(z)) \equiv \sum_{i=1}^{k} \text{ máximo grado de la fila } i\text{-ésima de } G(z)\,.$$

Este grado externo se identifica con la idea de "memoria" que motivó la introducción de los codificadores convolucionales, por lo que denotaremos indistintamente

$$m_G \equiv \operatorname{Gr}_{ex}(G(z))\,.$$

Definición 1.2. *Un codificador convolucional $G(z)$ se dice*

- *básico* $\Leftrightarrow$ *$G(z)^t$ es epiyectiva.*
- *reducido* $\Leftrightarrow \operatorname{Gr}_{in}(G(z)) = \operatorname{Gr}_{ex}(G(z))$.

- *canónico* $\Leftrightarrow \mathrm{Gr}_{ex}(G(z))$ *es mínimo entre todos los codificadores polinómicos que definen el mismo código* $\mathcal{C}_k = \mathrm{Img}\, G(z)$.

A su vez, los conceptos de "grado" y "memoria" pueden aplicarse al propio código convolucional $\mathcal{C}_k$: considerando el conjunto de los codificadores polinómicos $G(z)$ tales que $\mathcal{C}_k = \mathrm{Img}\, G(z)$, el grado del código convolucional es

$$\begin{aligned}\delta(\mathcal{C}_k) &\equiv \text{mínimo } \mathrm{Gr}_{ex} \text{ de sus codificadores polinómicos} \equiv \\ &\equiv \text{memoria total de } \mathcal{C}_k \ .\end{aligned}$$

Observación 1.3. *Los códigos convolucionales se pueden definir a partir de codificadores más generales, considerando el cuerpo (infinito)* $\mathbb{F}_q(z)$ *de funciones racionales en una variable: un* $[n,k]$*-codificador convolucional es un homomorfismo inyectivo de* $\mathbb{F}_q(z)$*-espacios vectoriales* $G(z)\colon \mathbb{F}_q(z)^k \hookrightarrow \mathbb{F}_q(z)^n$ *y su imagen define el* $[n,k]$*-código convolucional* $\mathcal{C}_k \equiv \mathrm{Img}\, G(z)$.

2. Realización física de un codificador convolucional

Los codificadores convolucionales pueden realizarse físicamente mediante *circuitos secuenciales lineales*, equivalentes a *sistemas lineales invariantes respecto del tiempo y con un número finito de variables de estado.*

Para ello, si $G(z)$ es un $[n,k]$-codificador convolucional de memoria m, la ecuación

$$x(z) = u(z) \cdot G(z)$$

puede expresarse como un sistema lineal de ecuaciones, introduciendo las "variables de estado" $s(t)$, con $s(0) = 0$,

$$\begin{cases} s(t+1) = s(t) \cdot A + u(t) \cdot B \\ x(t) = s(t) \cdot C + u(t) \cdot G \end{cases}$$

donde $s(t)$, $u(t)$ y $x(t)$ son vectores de dimensiones m, k y n, respectivamente, mientras que A, B, C y D son matrices con coeficientes en $\mathbb{F}$ de dimensiones $m \times m$, $k \times m$, $m \times n$ y $k \times n$, respectivamente.

Ejemplo 2.1. *Sea* $G(z) = (1 + z + z^2\ ,\ 1 + z^2)$. *En este caso,* $k = 1$, $n = 2$ *y* $m = 2$, *y la codificación puede expresarse*

$$(x_1(t), x_2(t)) = (u_1(t)) \cdot (1 + t + t^2\ ,\ 1 + t^2)\,,$$

o equivalentemente

$$(x_1(t), x_2(t)) = (u_1(t) + u_1(t-1) + u_1(t-2), u_1(t) + u_1(t-2))\,.$$

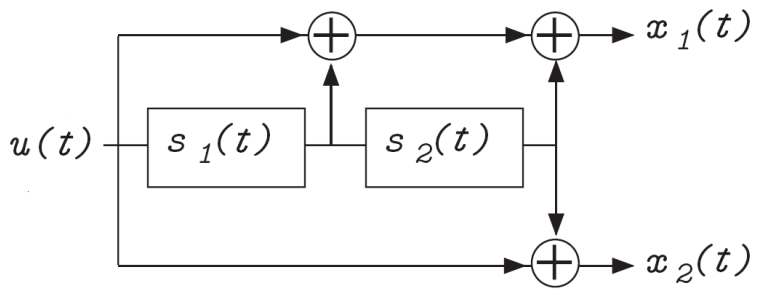
Introduciendo entonces las variables de estado,

$$\begin{cases} (s_1(t+1), s_2(t+1)) = (u_1(t), s_1(t)) \\ (x_1(t), x_2(t)) = (u_1(t) + s_1(t) + s_2(t), u_1(t) + s_2(t)) \end{cases}$$

resulta que la codificación es el sistema de ecuaciones lineales

$$\begin{cases} (s_1(t+1), s_2(t+1)) = (s_1(t), s_2(t)) \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + (u_1(t)) \cdot \begin{pmatrix} 1 & 0 \end{pmatrix} \\ (x_1(t), x_2(t)) = (s_1(t), s_2(t)) \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + (u_1(t)) \cdot \begin{pmatrix} 1 & 1 \end{pmatrix} \end{cases}$$

cuya realización física es el circuito



3. Codificadores polinómicos y haces sobre la recta proyectiva

Consideremos $\mathbb{P}^1 = \operatorname{Proj} \mathbb{F}_q[x_0, x_1]$ la recta proyectiva sobre el cuerpo $\mathbb{F}_q$, donde (x_0, x_1) son las coordenadas proyectivas, y su abierto afín $U = \mathbb{P}^1 - \{P_\infty\}$, con $P_\infty \equiv \{x_0 = 0\}$ el punto del infinito de modo que la variable $z = \frac{x_1}{x_0}$ sea la coordenada afín de esta recta proyectiva.

Dado entonces un codificador polinómico $G(z)$, es posible realizar su "homegenización" $G(x_0, x_1)$, haciendo un cambio de variable a las coordenadas proyectivas.

Ejemplo 3.1.

$$G(z) = (1 + z + z^2\ ,\ 1 + z^2)\colon \mathbb{F}_2[z] \hookrightarrow \mathbb{F}_2[z]^2$$
$$G(x_0, x_1) = (x_0^2 + x_0x_1 + x_1^2\ ,\ x_0^2 + x_1^2)\colon \mathbb{F}_2[x_0, x_1] \hookrightarrow \mathbb{F}_2[x_0, x_1]^2$$

El estudio de los codificadores polinómicos puede entonces plantearse en términos del haz de anillos sobre U

$$\mathcal{O}_U \equiv \widetilde{\mathbb{F}[z]}\,,$$

teniendo en cuenta las identificaciones:

$$\begin{aligned}
\mathrm{Hom}_{\mathbb{F}[z]}\left(\mathbb{F}[z]^k, \mathbb{F}[z]^n\right) =& \mathrm{Hom}_{\mathcal{O}_U}\left(\mathcal{O}_U^k, \mathcal{O}_U^n\right) = \\
=& H^0\left(U, \mathcal{H}om_{\mathcal{O}_{\mathbb{P}}}\left(\mathcal{O}_{\mathbb{P}}^k, \mathcal{O}_{\mathbb{P}}^n\right)\right) = \\
=& \varinjlim_m H^0\left(\mathbb{P}^1, \mathcal{H}om_{\mathcal{O}_{\mathbb{P}}}\left(\mathcal{O}_{\mathbb{P}}^k, \mathcal{O}_{\mathbb{P}}^n\right) \otimes \mathcal{O}_{\mathbb{P}}(mP_\infty)\right) = \\
=& \varinjlim_m H^0\left(\mathbb{P}^1, \mathcal{H}om_{\mathcal{O}_{\mathbb{P}}}\left(\mathcal{O}_{\mathbb{P}}^k, \mathcal{O}_{\mathbb{P}}^n(mP_\infty)\right)\right) = \\
=& \varinjlim_m \mathrm{Hom}\left(\mathcal{O}_{\mathbb{P}}^k, \mathcal{O}_{\mathbb{P}}(mP_\infty)^n\right) = \\
=& \varinjlim_m \mathrm{Hom}_{\mathbb{F}}\left(\mathbb{F}^k, H^0\left(\mathcal{O}_{\mathbb{P}}(mP_\infty)^n\right)\right)\ .
\end{aligned}$$

Siguiendo esta idea, los autores están trabajando conjuntamente con J.I. Iglesias Curto en la clasificación de los códigos convolucionales, en términos de esquemas Quot.

4. La noción de distancia para códigos convolucionales

Dado un vector polinómico $x(z) = (x_1(z), \ldots, x_n(z)) \in \mathbb{F}[z]^n$, es posible definir su *peso de Hamming* como

$$hwt(x(z)) = \#\{i \mid x_i(z) \neq 0\}\,.$$

Sin embargo, este peso no sirve para medir los errores de transmisión si se utiliza la codificación convolucional. En la teoría de códigos convolucionales, la noción natural de peso se obtiene considerando los vectores polinómicos $x(z) \in \mathbb{F}[z]^n$ como $x(z) = \sum_t x(t)z^t$, con

$x(t) = (x_1(t), \ldots, x_n(t)) \in \mathbb{F}^n$, de modo que el *peso* de $x(t)$ es

$$wt(x(z)) = \sum_t hwt(x(t)) \,, \quad \text{donde } hwt(x(t)) = \#\{i \mid x_i(t) \neq 0\} \,.$$

De este modo, el concepto de *distancia libre* de un $[n,k]$-código convolucional $\mathcal{C}_k \subseteq \mathbb{F}[z]^n$ es

$$d_{free}\,(\mathcal{C}_k) = \text{mín}\,\{wt(x(z)) \mid x(z) \in \mathcal{C}_k\,,\ x(z) \neq 0\}\ .$$

Teorema 4.1. (véase [4]) *Dado un $[n,k]$-código convolucional de grado δ, su distancia libre d_{free} verifica la* cota de Singleton generalizada

$$d_{free} \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1 \,.$$

Un código convolucional cuya distancia libre alcanza el valor máximo de esta cota se denomina *MDS (Maximum Distance Separable).*

La cuestión clave es entonces la construcción de códigos convolucionales MDS, para lo cual es posible introducir técnicas algebraicas, similares a las utilizadas en la teoría de códigos algebraico-geométricos de Goppa.

5. Códigos de Goppa convolucionales

Sea $\mathbb{F}_q(z)$ el cuerpo (infinito) de funciones racionales en una variable, y X una curva proyectiva lisa sobre $\mathbb{F}_q(z)$. Consideremos $D = P_1 + \cdots + P_n$ un divisor de n puntos $\mathbb{F}_q(z)$-racionales distintos de X y G otro divisor con soporte disjunto a D, tal que

$$2g - 2 < \text{Gr}(G) < n \,.$$

Sobre el $\mathbb{F}_q(z)$-espacio de secciones globales $L(G)$ se tiene una aplicación $\mathbb{F}_q(z)$-lineal inyectiva

$$\begin{aligned} \alpha\colon L(G) &\to \mathbb{F}_q(z) \times \overset{n}{\cdots} \times \mathbb{F}_q(z) \\ f &\mapsto (f(P_1), \ldots, f(P_n)) \end{aligned}$$

Definición 5.1. (véase [6] o [7]) *El código de Goppa convolucional de longitud n y dimensión $k = \text{Gr}(G) + 1 - g$ asociado al par (D,G) es*

$$\mathcal{C}(D,G) \equiv \text{Img}\,\alpha \subset \mathbb{F}_q(z)^n \,.$$

Considerando sobre el $\mathbb{F}_q(z)$-espacio vectorial $\mathbb{F}_q(z)^n$ el producto escalar $\langle\ ,\ \rangle$

$$\begin{aligned}\mathbb{F}_q(z)^n \times \mathbb{F}_q(z)^n &\to \mathbb{F}_q(z)\\ (x(z), y(z)) &\mapsto \langle x(z), x(z)\rangle = \sum_{i=1}^{n} x_i(z)y_i(z)\,,\end{aligned}$$

es posible construir el correspondiente *código de Goppa convolucional dual*,

$$\mathcal{C}(D,G)^{\perp} \equiv \{y(z) \in \mathbb{F}_q(z)^n \mid \langle x(z), y(z)\rangle = 0 \text{ para todo } x(z) \in \mathcal{C}(D,G)\}\,.$$

Teorema 5.2. (véase [6] o [7]) *$\mathcal{C}^{\perp}(D,G)$ es también un código de Goppa convolucional: si K es el divisor canónico de formas diferenciales racionales sobre X, entonces $\mathcal{C}^{\perp}(D,G)$ es la imagen de la aplicación $\mathbb{F}_q(z)$-lineal $\beta\colon L(K+D-G) \to \mathbb{F}_q(z)^n$, dada por*

$$\beta(\eta) = (\mathrm{Res}_{p_1}(\eta), \ldots, \mathrm{Res}_{p_n}(\eta))\,.$$

6. Códigos de Goppa convolucionales sobre la recta proyectiva

Consideremos $X = \mathbb{P}^1_{\mathbb{F}_q(z)} = \operatorname{Proj} \mathbb{F}_q(z)[u_0, u_1]$ la recta proyectiva sobre el cuerpo $\mathbb{F}_q(z)$, donde $w = u_1/u_0$ es la coordenada afín, $P_0 = (1,0)$ es el punto origen, y $P_\infty = (0,1)$ el punto del infinito. Sean $P_1, \ldots, P_n$ un conjunto de n puntos racionales distintos, $P_i = (1, \alpha_i) \neq P_0, P_\infty$.

Tomando los divisores $D = P_1 + \cdots + P_n$ y $G = rP_\infty - sP_0$, con $0 \leq s \leq r < n$, el $\mathbb{F}_q(z)$-espacio vectorial $L(G)$ tiene como base

$$L(G) = \langle w^s, w^{s+1}, \ldots, w^r\rangle$$

y el código de Goppa convolucional $\mathcal{C}(D,G)$ es la imagen de la aplicación

$$\begin{aligned}\alpha\colon L(G) &\to \mathbb{F}_q(z) \times \overset{n}{\cdots} \times \mathbb{F}_q(z)\\ w^i &\mapsto (\alpha_1^i, \ldots, \alpha_n^i)\end{aligned}$$

Se obtiene de este modo un código convolucional $\mathcal{C}(D,G)$ de longitud n y dimensión $k = r - s + 1$, cuya matriz generadora es

$$G = \begin{pmatrix} \alpha_1^s & \alpha_2^s & \dots & \alpha_n^s \\ \alpha_1^{s+1} & \alpha_2^{s+1} & \dots & \alpha_n^{s+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^r & \alpha_2^r & \dots & \alpha_n^r \end{pmatrix}.$$

En cuanto al código dual, como

$$\Omega(G-D) = \left\langle \frac{dw}{w^s \prod_{i=1}^n (w-\alpha_i)}, \frac{w\, dw}{w^s \prod_{i=1}^n (w-\alpha_i)}, \dots, \frac{w^{n-r+s-2} dw}{w^s \prod_{i=1}^n (w-\alpha_i)} \right\rangle$$

y calculando los residuos

$$\mathrm{Res}_{P_j}\left(\frac{w^m dw}{w^s \prod_{i=1}^n (w-\alpha_i)} \right) = \frac{\alpha_j^m dw}{\alpha_j^s \prod_{\substack{i=1 \\ i\neq j}}^n (\alpha_j - \alpha_i)}$$

resulta que $\mathcal{C}(D,G)^*$ es un código convolucional de longitud n y dimensión $n-k = n-r+s-1$ que tiene como matriz generadora (= matriz de control de $\mathcal{C}(D,G)$)

$$H = \begin{pmatrix} h_1 & h_2 & \dots & h_n \\ h_1\alpha_1 & h_2\alpha_2 & \dots & h_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ h_1\alpha_1^{n-r+s-2} & h_2\alpha_2^{n-r+s-2} & \dots & h_n\alpha_n^{n-r+s-2} \end{pmatrix},$$

donde $h_j = \frac{1}{\alpha_j^s \prod_{\substack{i=1 \\ i\neq j}}^n (\alpha_j - \alpha_i)}$.

Obsérvese que esa matriz generadora H de $\mathcal{C}(D,G)^\perp$ tiene la forma de un "codificador alternante" sobre $\mathbb{F}_q(z)$, lo que sugiere la posibilidad de emplear en este contexto convolucional los algoritmos algebraicos de decodificación conocidos para los códigos lineales alternantes.

Como casos particulares, vamos a calcular las matrices G y H en el caso de puntos $\mathbb{F}_q(z)$-racionales $P_i = (1, \alpha_i)$ cuando

$$\alpha_i = a^{i-1} z + b^{i-1}, \quad i = 1, \dots, n, \quad n < q,$$

comprobando además que en estos casos resultan códigos convolucionales MDS.

• Cuerpo $\mathbb{F}_3(z) = \{0, 1, 2\}$

Caso $a = 1, b = 2, G = P_\infty - P_0$.

$$G = \begin{pmatrix} z+1 & z+2 \end{pmatrix}$$

$$H = \begin{pmatrix} \frac{1}{2(z+1)} & \frac{1}{z+2} \end{pmatrix}$$

$$(n, k, \delta, d) = (2, 1, 1, 4)$$

• Cuerpo $\mathbb{F}_4(z) = \{0, 1, \xi, \xi^2\}$, con $\xi^2 + \xi + 1 = 0$

Caso $a = \xi, b = \xi^2, G = P_\infty$

$$G = \begin{pmatrix} 1 & 1 & 1 \\ z+1 & \xi z+\xi^2 & \xi^2 z+\xi \end{pmatrix}$$

$$H = \begin{pmatrix} \frac{1}{(\xi^2 z+\xi)(\xi z+\xi^2)} & \frac{1}{(\xi^2 z+\xi)(z+1)} & \frac{1}{(\xi z+\xi^2)(z+1)} \end{pmatrix}$$

$$(n, k, \delta, d) = (3, 2, 1, 3)\,.$$

Caso $a = 1, b = \xi, G = P_\infty - P_0$

$$G = \begin{pmatrix} z+1 & z+\xi & z+\xi^2 \end{pmatrix}$$

$$H = \begin{pmatrix} \frac{1}{z+1} & \frac{\xi}{z+\xi} & \frac{\xi^2}{z+\xi^2} \\ 1 & \xi & \xi^2 \end{pmatrix}$$

$$(n, k, \delta, d) = (3, 1, 1, 6)\,.$$

• Cuerpo $\mathbb{F}_5(z)$

Caso $a = 1, b = 2, G = 2P_\infty - 2P_0$

$$G = \begin{pmatrix} (z+1)^2 & (z+2)^2 & (z+4)^2 \end{pmatrix}$$

$$H = \begin{pmatrix} \frac{2}{(z+1)^2} & \frac{2}{(z+2)^2} & \frac{1}{(z+4)^2} \\ \frac{2}{z+1} & \frac{2}{z+2} & \frac{1}{z+4} \end{pmatrix}$$

$$(n, k, \delta, d) = (3, 1, 2, 9)\,.$$

Caso $a = 2, b = 3, G = 2P_\infty - P_0$

$$G = \begin{pmatrix} \frac{z+1}{(z+1)^2} & \frac{2z+3}{(2z+3)^2} & \frac{4z+4}{(4z+4)^2} & \frac{3z+2}{(3z+2)^2} \end{pmatrix}$$

$$H = \begin{pmatrix} \frac{4}{(z+1)^2(z+2)(z+3)} & \frac{4}{(z+2)(z+3)(z+4)^2} & \frac{4}{(z+1)^2(z+2)(z+3)} & \frac{4}{(z+2)(z+3)(z+4)^2} \\ \frac{4}{(z+1)(z+2)(z+3)} & \frac{3}{(z+2)(z+3)(z+4)} & \frac{1}{(z+1)(z+2)(z+3)} & \frac{2}{(z+2)(z+3)(z+4)} \end{pmatrix}$$

$(n, k, \delta, d_{free}) = (4, 2, 3, 8)$.

Agradecimientos. Los autores manifiestan su gratitud a sus colaboradores del grupo de investigación *Geometría Algebraica, Aritmética y Teoría de Códigos* del Departamento de Matemáticas de la Universidad de Salamanca, especialmente a Gloria Serrano Sotelo y J.I. Iglesias Curto.

Referencias

[1] P. Elias, Coding for noisy channels, *I.R.E. Nat. Conv. Record* **3**, 34–45, (1955).
[2] G.D. Forney Jr, Convolutional codes I: Algebraic structure, *IEEE Trans. Inform. Theory*, **16** (3), 720–738, (1970).
[3] R.J. McEliece, The algebraic theory of convolutional codes, in *Handbook of coding theory, Vol. I*, 1065–1138, North-Holland, Amsterdam, (1998).
[4] J. Rosenthal and R.Smarandache, Maximum distance separable convolutional codes, *Appl. Algebra Engrg. Comm. Comput.*, **10** (1), 15–32, (1999).
[5] V. Lomadze, Convolutional Codes and Coherent Sheaves, *Algebra Engrg. Comm. Comput.*, **12** (4), 273–326, (2001).
[6] J.A. Domínguez Pérez, J.M. Muñoz Porras and G. Serrano Sotelo, Convolutional Codes of Goppa type, *Algebra Engrg. Comm. Comput.*, **15** (1), 51–61, (2004).
[7] J.M. Muñoz Porras, J.A. Domínguez Pérez, J.I. Iglesias Curto and G. Serrano Sotelo, Convolutional Goppa Codes, *IEEE Trans. Inform. Theory*, **52** (1), 340–344, (2006).