Métodos de Geometría Algebraica en Teoría de Códigos Convolucionales

Gloria Serrano Sotelo

Memoria presentada para optar al Grado de Doctora en Matemáticas

bajo la dirección de los

Profesores Drs. D. J.M. Muñoz Porras y D. Francisco Plaza Martín

20 de Enero de 2014

Índice general

Introducción

La teoría de códigos juega un papel muy importante en los sistemas de comunicación a través de un canal con ruido. La codificación consiste en añadir información extra (redundancia) a los mensajes que se quieren transmitir a través del canal con el objetivo de minimizar los efectos del ruido, controlando los errores que éste produce, es decir, consiguiendo un sistema fiable de transmisión.

El sistema debe ser también eficiente en el sentido de que manteniendo una probabilidad de error baja se consiga una mayor velocidad, una menor potencia de transmisión, se necesite menor ancho de banda, etc., que repecto de la información sin codificar o de la información con otros codificadores. De hecho Shannon demostró en 1948 [32] que con una codificación apropiada se pueden reducir los errores producidos por el canal, sin sacrificar ni la tasa de transmisión, ni la potencia, ni el ancho de banda.

Los mejores códigos conocidos para la comunicación sobre canales con ruido son los códigos lineales de bloques, los códigos convolucionales y los códigos basados en ellos.

Los códigos convolucionales surgen después de los códigos de bloques y no requieren codificadores muy complicados. Estos códigos fueron introducidos por Elias en 1955 [8].

Su creciente aplicación fue debida en parte a los métodos de decodificación, puesto que se pasó de algoritmos que eran independientes de la memoria del código al algoritmo de Viterbi [34], cuya complejidad crece exponencialmente con la memoria, pero que es mucho más fiable como método de de-

codificación, puesto que no borra datos como los algoritmos secuenciales y además el tiempo de decodificación es fijo.

Uno de las principales aplicaciones de los códigos convolucionales es la transmisión de información en el espacio exterior (deep-space). Las transmisiones a través del espacio exterior están muy limitadas en potencia, pero no generalmente en ancho de banda. Si hay una disminución de SNR, con la misma potencia se cubren distancias mayores. Los sistemas de comunicación en las naves espaciales transmiten informaciones telemétricas (datos científicos con o sin imágenes, datos GSE, etc.), órdenes de la estación terrestre a la nave y "tracking" (seguimiento de la velocidad, posición y otros datos de la nave a través de los datos que ésta envía a tierra). En el canal telemétrico, donde la razón del código (proporción entre información y redundancia más información) es relativamente alta, se utilizan códigos convolucionales y de bloques.

En las misiones espaciales Pionner 10 y 11 a Júpiter y Saturno en 1972-73 se utilizó un código convolucional de razón 1/2 y memoria 31.

Es a partir del algoritmo de Viterbi cuando el estándar planetario se convierte en un código convolucional de memoria menor, memoria 6 y razón 1/2. Éste código se utilizó por primera vez en la misión Voyager 1 (1980-81) concatenado con un código lineal Reed-Solomon y después en las misiones Galileo (1986) y Voyager 2 (1989) concatenando el estándar con otros códigos convolucionales y de bloques.

Los códigos convolucionales se utilizan también en la construcción de los turbo códigos, que fueron introducidos en 1983 por Berrou, Glavieux y Thitimajshima en [2].

Massey y Sain [23] establecieron relaciones básicas entre la teoría de códigos convolucionales y la teoría algebraica de sistemas lineales de la que los trabajos de Kalman [21, 20] y posteriormente de Kailath [19] merecen mención especial.

En 1970 Forney desarrolla la teoría algebraica de los códigos convolucionales en su trabajo "Convolutional Codes I: Algebraic Structure" [11], que es una referencia principal desde entonces; trabajo que recoge Piret en su libro [29] y McEliece reelabora y ampla en el artículo de 1998 "The algebraic theory of convolutional codes", incluido en el libro "Handbook of coding theory" [24].

En este trabajo se presenta un nuevo tipo de códigos convolucionales que generalizan los códigos algebraicos de Goppa y que nos permiten construir importantes familias de códigos con buenas prestaciones en cuanto a su im-

plementación, con alfabeto pequeño, y a su capacidad de corregir errores, es decir, con la mayor distancia posible entre sus palabras. Los resultados más importantes, que ya han sido publicados [6, 26, 17, 30], se describen a continuación exponiéndolos divididos en los cinco capítulos de que se compone esta memoria.

En el **Capítulo 1**, se desarrolla la teoría general de códigos convolucionales:

Se parte de la interpretación de los codificadores convolucionales como dispositivos físicos (circuitos secuenciales lineales) para, a través de la teoría de sistemas lineales, dar su interpretación como morfismos lineales inyectivos, $\mathbb{F}_q(z)^k \xhookrightarrow{\mathbf{G}} \mathbb{F}_q(z)^n$, siguiendo las restricciones precisas de la teoría de control en comunicaciones, y tomando como equivalentes aquellos que tienen la misma imagen, obteniendo así el código convolucional como el subespacio imagen. Se estudian, desde el punto de vista de la teoría de control en comunicaciones, los codificadores que deben ser evitados y los que son óptimos en términos de una realización minimal del sistema lineal asociado y de su distancia. Se hace especial énfasis en su interpretación como módulos sobre un dominio de ideales principales, pues es esa estructura la que permite caracterizar los codificadores *básicos* y el *grado* y la *memoria* del código.

La teoría de Forney [11] y su posterior desarrollo por McEliece [24] son las referencias fundamentales. Las técnicas de Álgebra empleadas pueden encontrarse en manuales de Álgebra como [1, 3].

Por último, obtenemos un resultado nuevo para los códigos convolucionales de dimensión 1, el *Teorema* 1.43, recogido también en el preprint [7], que nos permite decidir cuándo un código convolucional de dimensión 1 es MDS en función de subcódigos lineales asociados. Utilizaremos este teorema en el Capítulo 3 para construir familias de códigos convolucionales que son óptimos o MDS, resultados que hemos publicado recientemente como parte del artículo [30].

El **Capítulo 2** está dedicado a los códigos convolucionales de Goppa definidos sobre curvas algebraicas.

En él definimos la noción de código convolucional de Goppa, como un código algebro-geométrico obtenido por evaluación de una serie lineal $\Gamma \subseteq L(G)$ en puntos racionales p_i de una curva algebraica sobre el cuerpo $\mathbb{F}_q(z)$ de las funciones racionales de una variable con coeficientes en el cuerpo finito $\mathbb{F}_q$, y calculamos (*Teorema* 2.2) su longitud y dimensión en función de los divisores sobre la curva G y $D = p_1 + \cdots + p_n$ asociados. Damos la corres-

pondiente noción de código convolucional dual como su subespacio ortogonal respecto de la métrica natural en $\mathbb{F}_q(z)^n$ y demostramos (*Teorema* 2.4) que también es un código convolucional de Goppa.

De este modo se generaliza la teoría de Goppa de códigos en curvas algebraicas sobre un cuerpo finito $\mathbb{F}_q$ [13, 14, 15] a un cuerpo (infinito) $\mathbb{F}_q(z)$. Es por ello que a estos nuevos códigos los denominamos códigos convolucionales de Goppa (CGC) o de tipo Goppa.

El capítulo termina ilustrando esta construcción general con algunos ejemplos de códigos convolucionales de Goppa sobre curvas de género cero y uno que son MDS.

Parte de este capítulo está basado en los artículos [6, 26].

Los métodos de Geometría algebraica utilizados se encuentran en [16].

El **Capítulo 3** se dedica a los códigos convolucionales de Goppa sobre la recta proyectiva $\mathbb{P}^1_{\mathbb{F}_q(z)}$.

La sencillez de las curvas de género cero aconsejó dedicar inicialmente nuestro estudio a los códigos convolucionales de Goppa sobre la recta proyectiva $\mathbb{P}^1_{\mathbb{F}_q(z)}$. Los buenos resultados obtenidos nos han permitido considerar el caso de $\mathbb{P}^1_{\mathbb{F}_q(z)}$ particularmente interesante y por eso le dedicamos un capítulo especial. Por una parte, podemos construir numerosos ejemplos generales de códigos convolucionales de Goppa sobre la recta proyectiva, que engloban resultados de otros autores [12], y construir y clasificar familias de códigos de este tipo que son óptimos o MDS, es decir, con la máxima distancia posible entre sus palabras; lo conseguimos, además, sobre alfabeto $\mathbb{F}_q$ pequeño, mientras que hasta entonces sólo había sido posible hacerlo sobre alfabeto grande [18, 31]. Por otro lado, recientemente hemos demostrado [5] que todo código convolucional puede ser construido como un código convolucional de Goppa sobre la recta proyectiva.

Este capítulo contiene los resultados más importantes de la memoria y está basado en los artículos [6, 26, 30]. Son resultados que permiten encontrar de forma constructiva códigos convolucionales de Goppa y describir explícitamente tanto sus matrices generadoras como sus matrices de control (*Teoremas* 3.2 y 3.4). Muchos de ellos son MDS, es decir, su distancia libre alcanza la cota de Singleton generalizada.

Para el caso de los códigos convolucionales de Goppa de dimensión 1, construimos familias de códigos dependientes de un conjunto de parámetros, que son MDS (*Teoremas* 3.10 y 3.13, *Corolarios* 3.11, 3.14 y 3.15).

Una primera familia de códigos convolucionales de Goppa de dimensión

1 sobre $\mathbb{P}^1_{\mathbb{F}_q(z)}$ está dada por la restricción a la serie lineal $\Gamma = \langle \lambda_s t^s + \cdots + \lambda_r t^r \rangle \subseteq L(G)\,, \lambda_i \in \mathbb{F}_q(z)$ del morfismo de evaluación asociado a los divisores $D = p_1 + \cdots + p_n$ y $G = rp_\infty - sp_0$, $0 \leq s \leq r < n$.

En el *Teorema* 3.10, cuando $s = r$, y eligiendo las coordenadas de los puntos $p_i = a_i z + b_i$ de forma que $b_i = c^{i-1} a_i$, siendo $c \in \mathbb{F}_q$ un elemento de orden $\geq n$, construimos una familia de códigos MDS determinados por una matriz generadora canónica. En particular, cuando se toma $a_i = 1$, y siempre que los coeficientes binómicos $\{\binom{m}{j}\ ,\ 0 \leq j \leq m\}$ sean no nulos, se obtiene una familia uniparamétrica de códigos convolucionales de Goppa de dimensión 1 que son MDS y se determina un representante canónico (*Corolario* 3.11).

En característica 2, esta teoría nos permite construir códigos convolucionales de longitud n y dimensión $k = 1$ que son MDS, haciendo variar su memoria m para que los coeficientes binómicos se mantegan no nulos. Así si $m = 1$ podemos construir códigos convolucionales MDS de grado $m = 1$, dimensión $k = 1$, longitudes $n = 2, 3$ sobre $\mathbb{F}_4(z)$, si $m = 3$ se obtienen de longitudes $n = 4, 5, 6, 7$ sobre $\mathbb{F}_8(z)$, si $m = 7$ se construyen de longitudes $n = 8, 9, 10, \ldots, 15$ sobre $\mathbb{F}_{16}(z)$, y así sucesivamente.

En el *Teorema* 3.13, cuando $s = 0$ y las coordenadas de los puntos p_i son de la forma $p_i = a_i z + b$, damos la condición necesaria y suficiente para que un código de la familia C_λ definida por la serie lineal $\Gamma = \langle \lambda_0 + \lambda_1 t \cdots + \lambda_r t^r \rangle$ y el divisor de puntos $D = p_1 + \cdots + p_n$ sea MDS. En particular, demostramos que el código C_λ, con todos los $\lambda_i \neq 0$ y $b = 0$ es MDS (*Corolario* 3.14). Hay que señalar que los códigos convolucionales MDS construidos por H. Gluesing-Luerssen y B. Langfeld [12] son de este tipo, como reseñamos en el *Corolario* 3.15.

Incluimos también un resultado de clasificación de códigos convolucionales de Goppa de dimensión 1 sobre $\mathbb{P}^1_{\mathbb{F}_q(z)}$. En el *Teorema* 3.16 demostramos que el conjunto de los códigos convolucionales de Goppa definidos por $\Gamma = \langle \lambda_0 + \lambda_1 t \cdots + \lambda_r t^r \rangle$ con $\lambda_i \in \mathbb{F}_q$ y el divisor de puntos $\{a_i z + b\}_{0 \leq i \leq n}$, $a_i \neq a_j \neq 0$ que son MDS, es un abierto no vacío de $\mathbb{P}^r_{\mathbb{F}_q}$ dando explícimante su complemetario, es decir, las ecuaciones de los códigos de la familia que no son MDS. Terminamos con algunos ejemplos que ponen de manifiesto la ventaja de la teoría desarrollada en la elección de códigos convolucionales MDS sobre alfabeto pequeño.

En el **Capítulo 4**, de carácer fundamentalmente técnico, se generaliza la construcción de los códigos convolucionales de Goppa sobre curvas del Capítulo 2 a variedades algebraicas proyectivas de dimensión superior.

Los códigos convolucionales de Goppa están ahora asociados a una pareja (D, G), donde $D = p_1 \cup \cdots \cup p_n$ es el subesquema de dimensión cero asociado a n puntos racionales diferentes y G es un divisor cuyo soporte no pasa por esos puntos. El código convolucional de Goppa $\mathcal{C}(D, G)$ es la imagen del morfismo de evaluación: $H^0(X, \mathcal{O}_X(G)) \to H^0(X, \mathcal{O}_D) \simeq \mathbb{F}_q(z)^n$. Análogamente, dado un subespacio $\Gamma \subseteq H^0(X, \mathcal{O}_X(G))$, se define el código convolucional de Goppa $\mathcal{C}(D, \Gamma)$ como la imagen de la restricción a Γ de dicho morfismo. En el *Teorema* 4.2 determinamos la longitud y la dimensión de estos códigos.

Detallamos esta construcción en dos casos interesantes. El primero es el del plano proyectivo $\mathbb{P}^2_{\mathbb{F}_q(z)}$ y el segundo es de la superficie reglada trivial $\mathbb{P}^1_{\mathbb{F}_q(z)} \times \mathbb{P}^1_{\mathbb{F}_q(z)}$.

En el caso del plano proyectivo, en el *Teorema* 4.3 determinamos de forma explícita una base del código $\mathcal{C}(D, \Gamma)$, siendo $\Gamma \subseteq H^0(X, \mathcal{O}(r))$ cuando $\Gamma \cap H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}(r)) = \{0\}$ (aquí $\mathcal{I}_D$ es el haz de ideales del subesquema D); obtenemos también una cota para el grado δ del código. Ello nos permite dar numerosos ejemplos de códigos de dimensiones 1 y 2 sobre el plano proyectivo que son MDS, utilizando alfabeto pequeño $\mathbb{F}_8$, con los que ilustramos de nuevo la potencia de esta teoría.

Análogamente, para la reglada trivial, en el *Teorema* 4.8 explicitamos el morfismo de evaluación y damos cotas para la dimensión del código y su memoria. Construimos asimismo diversos ejemplos de códigos convolucionales de Goppa que son MDS.

El **Capítulo 5** está dedicado a los códigos convolucionales de Goppa sobre familias de variedades algebraicas, generalizando los asociados a familias de curvas desarrollados en [6], proponiendo como aplicaciones: una interpretación geométrica de la distancia libre del código y un estudio de los códigos 2D introducidos por Fornasini y Valcher [9, 33] y continuado recientemente por otros autores Climent, Napp, Perea y Pinto [28, 4].

Por razón de su interés, nos restringimos a las fibraciones $\pi : X \to \mathbb{A}^1$ de variedades algebraicas parametrizadas por la recta afín $\mathbb{A}^1 = \operatorname{Spec} \mathbb{F}_q[z]$. Las definiciones se generalizan de manera directa a este caso, y los códigos convolucionales de Goppa asociados a la fibración se definen por evaluación de las secciones de un haz de línea en n secciones de la fibración.

Estos códigos definen, entonces, códigos lineales en las fibras sobre los puntos cerrados, que son variedades algebraicas sobre $\mathbb{F}_q$, y un código convolucional de Goppa en la fibra sobre el punto genérico, que es una variedad algebraica sobre $\mathbb{F}_q(z)$, una vez que se haya fijado una trivialización

$H^0(X, \mathcal{O}_D) \simeq \mathbb{F}_q[z]^n$. En este sentido, los códigos convolucionales de Goppa asociados a la fibración son familias de códigos lineales, obtenidos todos ellos por especialización de un código convolucional de Goppa sobre la fibra genérica.

Consideramos en primer lugar el caso de los códigos convolucionales de Goppa sobre las fibraciones de curvas, determinando la dimensión y las condiciones para que la matriz generadora asociada a una trivialización sea una matriz básica (*Proposiciones* 5.5 y 5.7, *Corolario* 5.6). Se especializan los resultados al caso de la fibración trivial $\mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{\pi} \mathbb{A}^1$. Al final se incluye un apartado en el que se propone una interpretación geométrica de la distancia libre del código como aplicación de esta teoría.

Por último estudiamos los códigos definidos sobre la fibración $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$. Utilizando nuestros códigos convolucionales de Goppa definidos sobre las fibraciones triviales $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ y $\mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ construimos códigos $2D$, lo que proporciona otro elemento de aplicación del estudio de los códigos convolucionales de Goppa sobre fibraciones de variedades al estudio de las propiedades de los códigos $2D$ así obtenidos a partir de ellos.

Este capítulo está basado en los artículos [6, 26, 17].

Agradecimientos

En primer lugar agradezco a los directores del trabajo, J.M. Muñoz Porras y Francisco Plaza Martín por su ayuda, apoyo e interés, y por sus ideas y sugerencias. Agradezco también a J.A. Domínguez Pérez, J. I. Iglesias Curto y Ángel Muñoz Castañeda por su trabajo y colaboración en la elaboración de nuestros artículos, así como a Esteban Gómez González, Daniel Hernández Serrano y a todos los que han participado en algunas reuniones del seminario de teoría de códigos que con sus indicaciones y observaciones han ayudado al desarrollo de esta memoria.

Capítulo 1

Códigos Convolucionales

1.1. Codificador convolucional como dispositivo físico

Si $\mathbb{F}_q$ representa el alfabeto o cuerpo finito de símbolos, comenzaremos recordando la definición de código lineal de bloques sobre $\mathbb{F}_q$ de razón k/n con $k < n$,

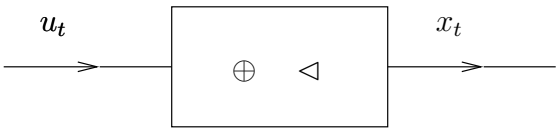
Definición 1.1. Un (n, k)-código lineal de bloques sobre $\mathbb{F}_q$ es un subespacio $\mathcal{C}$ de $\mathbb{F}_q^n$ de dimensión k.

Las aplicaciones lineales inyectivas $\mathbb{F}_q^k \overset{\mathbf{G}}{\hookrightarrow} \mathbb{F}_q^n$ de imagen el código, $\mathcal{C} = \operatorname{Im} \mathbf{G}$, se llaman *codificadores* y su representación en coordenadas son las *matrices generadoras* $\mathbf{G}$. Un codificador $\mathbf{G}$ asocia a cada *palabra de información* $u \in \mathbb{F}_q^k$ la *palabra código* $x \in \mathbb{F}_q^n$ por la regla $x = u \cdot \mathbf{G}$.

En muchos casos, un codificador se utiliza para codificar no una sino una secuencia de palabras de información, es decir, una función discreta del tiempo; de modo que *se puede interpretar el codificador* $\mathbf{G}$ *como una aplicación lineal que transforma la sucesión de palabras de información* k*-dimensionales* $(u_{t_0}, u_{t_0+1}, \dots)_{t_0 \in \mathbb{Z}}$ *en la sucesión de palabras código* n*-dimensionales* $(x_{t_0}, x_{t_0+1}, \dots)_{t_0 \in \mathbb{Z}}$ por la regla $x_t = u_t \mathbf{G}$ para $t \geq t_0$, que expresa en cada instante t la palabra código x_t como una función lineal de la palabra de información u_t en ese instante.

Si ahora pensamos el codificador lineal $\mathbf{G}$ como un dispositivo físico en el que se realizan operaciones lineales, sumadores ($\oplus$) y multiplicadores ($\triangleleft$)

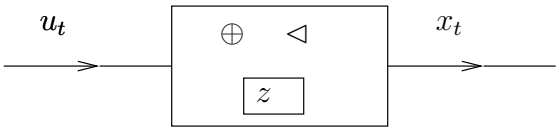
en $\mathbb{F}_q$, en cada instante de tiempo t la palabra código x_t sólo depende, y linealmente, de la palabra de información u_t introducida en ese instante.



En este sentido, podemos dar la siguiente

Definición 1.2. *Un codificador es convolucional* si la palabra código x_t en el instante t depende linealmente no sólo de la palabra de información u_t en ese instante, sino también de las palabras de información $u_{t-1}, u_{t-2}, \ldots$ en instantes anteriores a t.

Los dispositivos físicos que realizan estos codificadores tienen, además de los operadores lineales $\oplus$ y $\lhd$, retardadores de señal en el tiempo $zu_t = u_{t-1}$, $z^2u_t = u_{t-2}$



z es *el operador "delay"*.

Si en el instante t la palabra código x_t depende de un número finito m de muestras anteriores en el tiempo, u_{t-i} con $1 \leq i \leq m$, se dice que *el codificador convolucional tiene memoria* m. Los codificadores lineales de bloques son pues codificadores convolucionales de memoria cero.

Aunque en teoría pueden existir codificadores convolucionales de memoria infinita, en la práctica no es posible pues el número de *elementos con delay* o *elementos de memoria* que puede utilizar un dispositivo físico *tiene que ser finito*, en otro caso la realización material no sería posible.

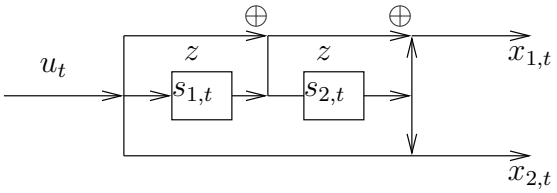
Se llama *grado del codificador* al número de elementos de memoria; el contenido de éstos informa en cada instante sobre el estado físico del codificador.

Los dispositivos físicos que realizan estos codificadores se llaman *circuitos secuenciales lineales* y las ecuaciones que los describen *sistemas lineales*

invariantes respecto del tiempo y *con un número finito de variables de estado* (igual al grado del codificador).

Sobre alfabeto binario $\mathbb{F}_q = \mathbb{Z}/2\mathbb{Z}$, veremos dos ejemplos de codificador convolucional definido por un circuito secuencial lineal y descrito por sus ecuaciones o bien por su matriz codificadora.

Ejemplo 1.3. Circuito secuencial lineal con dos elementos de memoria.



En cada instante $t \geq t_0$ se produce una entrada u_t y dos salidas $x_{1,t}$, $x_{2,t}$ y el estado físico viene dado por $(s_{1,t}, s_{2,t})$, donde $(s_{1,t_0}, s_{2,t_0}) = (0, 0)$.

- Sus ecuaciones son

$$\begin{aligned} s_{1,t+1} &= u_t & \qquad s_{2,t+1} &= s_{1,t} \\ x_{1,t} &= u_{1,t} + s_{1,t} + s_{2,t} & \qquad x_{2,t} &= u_t + s_{2,t} \end{aligned}$$

de donde

$$\begin{pmatrix} s_{1,t+1} & s_{2,t+1} \end{pmatrix} = \begin{pmatrix} s_{1,t} & s_{2,t} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + u_t(1,0)$$

$$\begin{pmatrix} x_{1,t} & x_{2,t} \end{pmatrix} = \begin{pmatrix} s_{1,t} & s_{2,t} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + u_t(1,1)$$

que expresa la relación entre el vector de salida $x_t = (x_{1,t}, x_{2,t})$ y el de entrada u_t en función del vector de estados $s_t = (s_{1,t}, s_{2,t})$ mediante el *sistema lineal*

$$\begin{cases} s_{t+1} = s_t A + u_t B \\ x_t = s_t C + u_t D \end{cases}$$

realizado por las matrices escalares

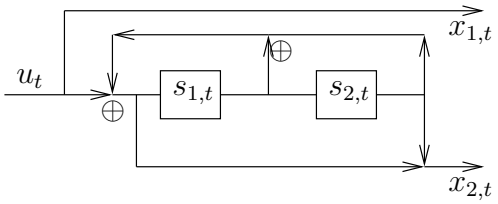
$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \end{pmatrix},\ C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ D = \begin{pmatrix} 1 & 1 \end{pmatrix}$$

- Utilizando el operador z podemos escribir directamente:

$$\left.\begin{array}{l} x_{1,t} = u_t + zu_t + z^2u_t \\ x_{2,t} = u_t + z^2u_t \end{array}\right\} \quad x_t = u_t \begin{pmatrix} 1+z+z^2 & 1+z^2 \end{pmatrix}$$

La matriz $\mathbf{G} = \begin{pmatrix} 1+z+z^2 & 1+z^2 \end{pmatrix}$ se llama *matriz codificadora*.

Ejemplo 1.4. Circuito lineal con una entrada y dos salidas, dos elementos de memoria y con "feed-back".



- En términos de sistemas lineales

$$\begin{array}{ll} s_{1,t+1} = s_{1,t} + s_{2,t} + u_t & s_{2,t+1} = s_{1,t} \\ x_{1,t} = u_t & x_{2,t} = (u_t + s_{1,t} + s_{2,t}) + s_{2,t} = u_t + s_{1,t} \end{array}$$

Se obtiene el *sistema lineal*

$$\begin{cases} s_{t+1} = s_tA + u_tB \\ x_t = s_tC + u_tD \end{cases}$$

con

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \end{pmatrix},\ C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ D = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

- En términos del operador z:

$z^{-1}s_{1,t} = s_{1,t} + s_{2,t} + u_t$ y $z^{-1}u_{2,t} = u_{1,t}$ implican que $s_{1,t} = zs_{1,t} + z^2s_{1,t} + zu_t$ luego $s_{1,t} = \frac{z}{1+z+z^2}u_t$, de donde:

$$\begin{pmatrix} x_{1,t} & x_{2,t} \end{pmatrix} = \begin{pmatrix} u_t & u_t + \frac{z}{1+z+z^2}u_t \end{pmatrix} = u_t \begin{pmatrix} 1 & \frac{1+z^2}{1+z+z^2} \end{pmatrix}$$

La matriz codificadora es

$$\mathbf{G} = \begin{pmatrix} 1 & \frac{1+z^2}{1+z+z^2} \end{pmatrix},$$

y sus coeficientes son funciones racionales sin polos en el origen.

A partir de este ejemplo veremos qué relación existe entre la descripción del codificador por medio de la teoría de sistemas lineales y la descripción por la matriz codificadora $\mathbf{G}$ utilizando el operador z; lo que utilizaremos también para decidir *en qué dominios se deben elegir los coeficientes de* $\mathbf{G}$ *para que el codificador convolucional asociado se pueda realizar físicamente.*

Ahora podemos dar una primera aproximación a la definición de un (n, k) codificador convolucional (k entradas y n salidas en cada instante):

Dar un (n, k) *codificador convolucional* es dar una matriz $\mathbf{G}$ de orden $k \times n$ con coeficientes en el cuerpo de fracciones $\mathbb{F}_q(z)$ del anillo de polinomios $\mathbb{F}_q[z]$, $\mathbf{G} \in M(n \times k, \mathbb{F}_q(z))$. *Para que este codificador sea realizable, los coeficientes de* $\mathbf{G}$ *deben ser funciones racionales sin polos en el origen.*

Para cada una de estas matrices $\mathbf{G}$ no existe una única realización física (A, B, C, D); es la teoría de sistemas lineales la que estudia cuál elegir en función de las necesidades del problema planteado. Una restricción clara para que una realización física sea mas sencilla es diminuir el número de variables de estado o elementos de memoria (el grado del codificador); la que tiene el menor número de ellas se llama en teoría de sistemas lineales una *realización minimal.*

Es en el contexto de la *teoría de control* en comunicaciones a través de canales ruidosos, donde las restricciones sobre la matriz codificadora deben ser "más precisas" en términos de una "buena" decodificación. No sólo se plantea el problema de averiguar cuándo un codificador es físicamente realizable sino también de *buscar propiedades de la matriz codificadora para que el proceso de decodificación se pueda controlar de modo eficaz y con el menor coste algorítmico.*

En los primeros tiempos de la teoría de los codificadores convolucionales, la restricción sobre el número de variables de estado no era muy fuerte, pues los algoritmos de decodificación no dependían de los elementos de memoria. Sin embargo, a partir de la utilización del algoritmo de Viterbi [10, 25] se debe exigir la minimalidad de la realización, pues la complejidad de este algoritmo decodificador crece exponencialmente con el número de variables de estado.

1.2. Del sistema lineal al código convolucional

En este apartado se desarrolla, utilizando la teoría de sistemas lineales (volveremos a ella al final del capítulo), la definición general de un (n, k) codificador convolucional, en términos de lo descrito en el apartado anterior, para llegar a la definición de código convolucional de dimensión k y longitud n

Definición 1.5. Un (n, k) codificador convolucional sobre $\mathbb{F}_q$ es una aplicación lineal del espacio de sucesiones de palabras de información

$$\{u_t = (u_{1,t}, \ldots, u_{k,t}) \in \mathbb{F}_q^k\}_{t\in\mathbb{Z}, t\geq t_0}$$

en el espacio de sucesiones de palabras código

$$\{x_t = (x_{1,t}, \ldots, x_{n,t}) \in \mathbb{F}_q^n\}_{t\in\mathbb{Z}, t\geq t_0}$$

que en cada instante de tiempo t está representada por el sistema lineal de ecuaciones

$$\begin{cases} s_{t+1} = s_t A + u_t B \\ x_t = s_t C + u_t D \quad \text{para } t \geq t_0 \text{ y } s_{t_0} = 0 \end{cases} \tag{1.2.1}$$

donde $s_t = (s_{1,t}, \ldots, s_{\delta,t}) \in \mathbb{F}_q^\delta$ es el vector de estados y A, B, C y D son matrices con coeficientes en $\mathbb{F}_q$ de órdenes respectivos $\delta \times \delta$, $k \times \delta$, $\delta \times n$ y $k \times n$. El número δ es el *grado del codificador*.

Si $\mathbb{F}_q((z))$ representa el conjunto de la series de Laurent $\sum_{t\geq t_0} a_t z^t$, podemos identificar la sucesión $\{u_t = (u_{1,t}, \ldots, u_{k,t})\}$ con el *vector de información*

$$u(z) = \left(\sum_{t\geq t_0} u_{1,t} z^t, \ldots, \sum_{t\geq t_0} u_{k,t} z^t \right) \in \mathbb{F}_q((z))^k .$$

Análogamente, identificamos la sucesión $\{x_t = (x_{1,t}, \ldots, x_{n,t})\}_{t\in\mathbb{Z}, t\geq t_0}$ con el *vector código*

$$x(z) = \left(\sum_{t\geq t_0} x_{1,t} z^t, \ldots, \sum_{t\geq t_0} x_{n,t} z^t \right) \in \mathbb{F}_q((z))^n$$

y la sucesión $\{s_t = (s_{1,t}, \ldots, s_{\delta,t})\}_{t\in\mathbb{Z}, t\geq t_0}$ con el *vector de estados*

$$s(z) = \left(\sum_{t\geq t_0} s_{1,t} z^t, \ldots, \sum_{t\geq t_0} s_{\delta,t} z^t \right) \in \mathbb{F}_q((z))^\delta \,.$$

Con esta notación, multiplicando en el sistema (1.2.1) por z^t y sumando en t con $t \geq t_0$, teniendo en cuenta que s_t, u_t y x_t son cero para $t < t_0$, resulta la *nueva expresión del sistema lineal* (1.2.1) :

$$\begin{cases} z^{-1}s(z) = s(z)A + u(z)B \\ \quad x(z) = s(z)C + u(z)D \end{cases} \tag{1.2.2}$$

Resolviendo (1.2.2) para calcular $s(z)$ y $x(z)$ en función de $u(z)$ se obtiene

$$s(z) = u(z)B(z^{-1}I - A)^{-1}\,, \quad x(z) = u(z)[B(z^{-1}I - A)^{-1}C + D]$$

que define una matriz $\mathbf{G} = B(z^{-1}I - A)^{-1}C + D$ de orden $k \times n$ *cuyos coeficientes son funciones racionales* $g_{ij}(z) \in \mathbb{F}_q(z)$ *sin polos en el origen*, pues de $(z^{-1}I - A)^{-1} = z + Az^2 + A^2z^3 + \ldots$ se sigue

$$\mathbf{G} = \sum_{n\geq 0} z^{n+1}(B \cdot A^n \cdot C) + D\,,$$

esto es, $g_{ij}(z) = \sum_{n\geq 0} z^{n+1}(B \cdot A^n \cdot C)_{ij} + D_{ij}$.

Además $\mathbf{G}$ es *la matriz codificadora*, puesto que $x(z) = u(z)\mathbf{G}$.

Definición 1.6. Un (n, k) codificador convolucional es una aplicación $\mathbb{F}_q((z))$-lineal

$$\mathbb{F}_q((z))^k \xrightarrow{\mathbf{G}} \mathbb{F}_q((z))^n$$

cuyo subespacio imagen está formado por las palabras código $x(z) = u(z)\mathbf{G}$.

Como los coeficientes de $\mathbf{G}$ están en $\mathbb{F}_q(z)$ y sus filas son los generadores del subespacio de palabras código, podemos sin pérdida de generalidad restringirnos a $\mathbb{F}_q(z)$ y redefinir:

Definición 1.7. Un (n, k) *codificador convolucional* es una aplicación $\mathbb{F}_q(z)$-lineal

$$\mathbb{F}_q(z)^k \xrightarrow{\mathbf{G}} \mathbb{F}_q(z)^n$$

cuya imagen es el subespacio de $\mathbb{F}_q(z)^n$ formado por las palabras código $x(z) = u(z)\mathbf{G}$.

En el contexto de un sistema de comunicaciones, lo primero que *hay que exigir a estos morfismos codificadores es que sean inyectivos*, pues en caso contrario existiría alguna palabra código $x(z)$ producida por dos palabras de información $u_1(t)$ y $u_2(t)$ diferentes y entonces por linealidad, cualquier otra palabra código $\bar{x}(z)$ tendría por lo menos dos palabras de información diferentes asociadas, si $\bar{x}(z) = \bar{u}(z)\mathbf{G}$ también es $\bar{x}(z) = (\bar{u}(z) + u_1(z) - u_2(z))\mathbf{G}$, con lo que la probabilidad de cometer un error al decodificar sería igual o mayor que $1/2$.

Redefinimos de nuevo:

Definición 1.8. Un (n, k) *codificador convolucional* sobre $\mathbb{F}_q$ es un morfismo $\mathbb{F}_q(z)$-lineal inyectivo $\mathbb{F}_q(z)^k \overset{\mathbf{G}}{\hookrightarrow} \mathbb{F}_q(z)^n$.

El subespacio $\operatorname{Im}\mathbf{G}$ de las palabras código es un subespacio de dimensión k de $\mathbb{F}_q(z)^n$, lo que sugiere la siguiente:

Definición 1.9. Un (n, k) *código convolucional* $\mathcal{C}$ sobre $\mathbb{F}_q$ es un subespacio k dimensional de $\mathbb{F}_q(z)^n$.

Por analogía con los códigos lineales de bloques se dice que la razón del código es k/n.

Si $\{g_1, \ldots, g_k\}$ es una base de $\mathcal{C}$, la matriz codificadora $\mathbf{G} = (g_1, \ldots, g_k)^t$ se llama también, por razones obvias, *matriz generadora de* $\mathcal{C}$.

Proposición 1.10. *Todo (n, k)-código convolucional sobre $\mathbb{F}_q$ admite un representante polinómico.*

Demostración. Sea $\mathbf{G} = (g_1, \ldots, g_k)^t$ una matriz generadora del código $\mathcal{C}$. Si μ es el mínimo común múltiplo de los denominadores de los coeficientes de $\mathbf{G}$, la matriz $\mu\mathbf{G}$ genera también el código $\mathcal{C}$. □

Definición 1.11. Si $\mathbf{G}\colon \mathbb{F}_q[z]^k \hookrightarrow \mathbb{F}_q[z]^n$ es un representante polinómico de $\mathcal{C}$, el *grado del codificador* $\mathbf{G}$ es la suma de los grados de sus filas $g_1, \ldots, g_k$, donde se entiende por grado de la fila i-ésima el mayor de los grados de sus componentes polinómicas $g_{ij}(z) \in \mathbb{F}_q[z]$, esto es,

$$\operatorname{gr}\mathbf{G} = \sum_{i=1}^{k} \operatorname*{máx}_{1\le j\le n} (\operatorname{gr} g_{ij}(z))$$

La *memoria de* $\mathbf{G}$ es el grado m de la fila de mayor grado, $m = \operatorname{máx}_{ij}(\operatorname{gr}(g_{ij}))$.

La matriz $\mathbf{G}$ se puede expresar como

$$\mathbf{G} = \mathbf{G}_0 + \mathbf{G}_1 z + \cdots + \mathbf{G}_m z^m$$

cuyas representación escalar asociada es la matriz semi-infinita

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}_0 & \mathbf{G}_1 & \mathbf{G}_2 & \dots & \mathbf{G}_m & & & \dots & & \dots \\ & \mathbf{G}_0 & \mathbf{G}_1 & \dots & \mathbf{G}_{m-1} & \mathbf{G}_m & & \dots & & \dots \\ & & \mathbf{G}_0 & \dots & \mathbf{G}_{m-2} & \mathbf{G}_{m-1} & \mathbf{G}_m & \dots & & \dots \\ & & & \ddots & & & & \ddots & & \\ & & & & \mathbf{G}_0 & & & \dots & \mathbf{G}_m & \dots \\ & & & & \ddots & & & & & \ddots \end{pmatrix}$$

Para cada $\ell \geq m$ la matriz escalar de orden $k\ell \times (m+\ell)n$

$$\mathbf{G}_\ell = \begin{pmatrix} \mathbf{G}_0 & \mathbf{G}_1 & \dots & \mathbf{G}_m & & & & \\ & \mathbf{G}_0 & \dots & \mathbf{G}_{m-1} & \mathbf{G}_m & & & \\ & & \ddots & & & \ddots & & \\ & & & & & & \mathbf{G}_0 & \dots & \mathbf{G}_m \end{pmatrix}$$

define un código lineal de bloques de razón $\frac{k\ell}{(m+\ell)n}$

Ejemplo 1.12. Los codificadores convolucionales de los ejemplos 1.3 y 1.4 generan el mismo código convolucional de razón $1/2$,

$$\mathbf{G} = \begin{pmatrix} 1+z+z^2 & 1+z^2 \end{pmatrix}, \quad \mathbf{G}' = \begin{pmatrix} 1 & \frac{1+z^2}{1+z+z^2} \end{pmatrix}$$

pues $\mathbf{G} = (1+z+z^2)\mathbf{G}'$. La representación polinómica de $\mathbf{G}$ es

$$\mathbf{G} = \mathbf{G}_0 + z\mathbf{G}_1 + z^2\mathbf{G}_2\,,$$

con $\mathbf{G}_0 = \begin{pmatrix} 1 & 1 \end{pmatrix}$, $\mathbf{G}_1 = \begin{pmatrix} 1 & 0 \end{pmatrix}$ y $\mathbf{G}_2 = \begin{pmatrix} 1 & 1 \end{pmatrix}$.

Ejemplo 1.13. *Standard Planetario de la NASA*: Código convolucional de razón $1/2$ con matriz generadora en sistema octal $\mathbf{G} = (133, 171)$ y en sistema binario

$$\mathbf{G} = \begin{pmatrix} 1+z+z^2+z^3+z^4+z^6 & 1+z^3+z^4+z^5+z^6 \end{pmatrix},$$

que es un codificador de memoria y grado 6 y matriz escalar

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}_0 & \mathbf{G}_1 & \dots & \mathbf{G}_6 & & \dots & & \dots \\ & \mathbf{G}_0 & \dots & & \mathbf{G}_6 & \dots & & \dots \\ & & \ddots & & & \ddots & & \\ & & & \mathbf{G}_0 & & \dots & \mathbf{G}_6 & \dots \\ & & & \ddots & & & & \ddots \end{pmatrix}$$

con $\mathbf{G}_0 = \begin{pmatrix} 1 & 1 \end{pmatrix}$, $\mathbf{G}_1 = \begin{pmatrix} 1 & 0 \end{pmatrix}$, $\mathbf{G}_2 = \begin{pmatrix} 0 & 0 \end{pmatrix}$, $\mathbf{G}_3 = \begin{pmatrix} 1 & 1 \end{pmatrix}$, $\mathbf{G}_4 = \begin{pmatrix} 1 & 1 \end{pmatrix}$, $\mathbf{G}_5 = \begin{pmatrix} 0 & 1 \end{pmatrix}$ y $\mathbf{G}_6 = \begin{pmatrix} 1 & 1 \end{pmatrix}$.

1.3. Codificadores catastróficos

En este apartado veremos qué tipo de codificadores deben ser siempre evitados y los caracterizaremos para que ello sea posible.

Si para un cierto codificador convolucional $\mathbf{G}$ *existe una palabra código* $x(z)$ *de longitud finita que proviene de una palabra de información* $u(z)$ *de longitud infinita*, $x(z) = u(z)\mathbf{G}$, habrá una probabilidad no nula de que ocurra un error de longitud finita $e(z)$ en el proceso de control de trasmisión a través de un canal ruidoso. Este error conducirá a un error de información de longitud infinita, $e_u(z)$. Así, la palabra decodificada $\widehat{u(z)} = e_u(z) + u(z)$, diferirá de la palabra de información $u(z)$ emitida en un número infinito de lugares. Massey llamó a este tipo de errores *errores de propagación catastróficos* y *codificadores catastróficos* a los que producen estos errores.

En general una palabra código $x(z) \in \mathbb{F}_q[z]^n$ no puede provenir de ninguna palabra de información $u(z)$ de longitud infinita si existe una matriz $\mathbf{G}^{-1}$ de orden $n \times k$ con coeficientes funciones racionales de la forma $p(z)/z^n$, $n \geq 0$ y $p(z) \in \mathbb{F}_q[z]$, tal que $\mathbf{G} \cdot \mathbf{G}^{-1} = I_k$.

Veamos cual es el significado algebraico de esta condición. Consideremos para ello el anillo localizado

$$\mathbb{F}_q[z]_S = \left\{ \frac{p(z)}{z^n} \in \mathbb{F}_q(z) \,|\, n \geq 0 \right\}$$

de $\mathbb{F}_q[z]$ por el sistema multiplicativo $S = \{z^n, z \geq 0\}$. La existencia de $\mathbf{G}^{-1}$ equivale a que la localización del morfismo codificador

$$0 \to \mathbb{F}_q[z]_S^k \xrightarrow{\mathbf{G}} \mathbb{F}_q[z]_S^n \to \mathbb{F}_q[z]_S^n / \operatorname{Im}(\mathbf{G}) \to 0$$

admita un retracto $\mathbf{G}^{-1}\colon \mathbb{F}_q[z]_S^n \to \mathbb{F}_q[z]_S^k$ ($\mathbf{G}\cdot\mathbf{G}^{-1} = I_k$), y el retracto existe si y sólo si el módulo cociente $\mathbb{F}_q[z]_S^n/\operatorname{Im}(\mathbf{G})$ no tiene torsión.

La teoría de los factores invariantes sirve para determinar fácilmente cuando $\mathbb{F}_q[z]_S^n/\operatorname{Im}(\mathbf{G})$ no tiene torsión, pues nos dice que existen elementos $(\gamma_1,\ldots,\gamma_k)$ en $\mathbb{F}_q[z]_S$ de forma que $\gamma_i|\gamma_{i+1}$ y que

$$\mathbb{F}_q[z]_S^n/\operatorname{Im}(\mathbf{G}) \simeq L \oplus \mathbb{F}_q[z]_S/\langle\gamma_1\rangle \oplus \cdots \oplus \mathbb{F}_q[z]_S/\langle\gamma_k\rangle$$

siendo L un $\mathbb{F}_q[z]_S$-módulo libre finito-generado. Por tanto $\mathbb{F}_q[z]_S^n/\operatorname{Im}(\mathbf{G})$ no tiene torsión exactamente si todos los factores invariantes son invertibles en el anillo $\mathbb{F}_q[z]_S$, es decir, como polinomios en z son de la forma z^{m_i}.

Puesto que los factores invariantes γ_i de $\mathbb{F}_q[z]^n/\operatorname{Im}(\mathbf{G})$ (a los que también nos referiremos como factores invariantes de la matriz $\mathbf{G}$) están determinados (salvo unidades) por la fórmula

$$\gamma_i = \frac{\text{m. c. d.(menores de orden } i \text{ de } \mathbf{G})}{\text{m. c. d.(menores de orden } i-1 \text{ de } \mathbf{G})}$$

podemos caracterizar los codificadores no catastróficos (no producen errores de propagación catastróficos):

Proposición 1.14. *Un codificador polinómico* $\mathbf{G}\colon \mathbb{F}_q[z]^k \hookrightarrow \mathbb{F}_q[z]^n$ *es no catastrófico si y sólo si*

$$\text{m. c. d.(menores de orden } k \text{ de } \mathbf{G}) = z^r$$

para algún $r \geq 0$.

La extensión al cuerpo de fracciones $\mathbb{F}_q(z)$ es inmediata:

Definición 1.15. Un codificador $\mathbf{G}\colon \mathbb{F}_q(z)^k \hookrightarrow \mathbb{F}_q(z)^n$ es no catastrófico si

$$\frac{\text{m. c. d.(menores de orden } k \text{ de } \mu\mathbf{G})}{\mu} = z^r$$

para algún $r \geq 0$, siendo μ el mínimo común múltiplo de los denominadores de los coeficientes de $\mathbf{G}$.

Ejemplo 1.16. El codificador convolucional de razón 2/3 sobre $\mathbb{F}_2$ dado por

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & \frac{1}{1+z} \\ 0 & 1 & \frac{z}{1+z} \end{pmatrix}$$

es *no catastrófico*, pues $\mu = 1 + z$ y los menores de orden 2 de $\mu\mathbf{G}_1$ son $(1+z)^2$, $z(1+z)$ y $1+z$, luego

$$\frac{\text{m. c. d.}((1+z)^2, z(1+z), 1+z)}{1+z} = \frac{1+z}{1+z} = 1 = z^0$$

El codificador polinómico

$$\mathbf{G}_2 = \begin{pmatrix} 1+z & 0 & 1 \\ z & 1+z+z^2 & z^2 \end{pmatrix}$$

es *catastrófico*, pues el máximo común divisor de los menores de orden 2 de $\mathbf{G}_2$ es $1 + z + z^2$.

Los codificadores $\mathbf{G}_1$ y $\mathbf{G}_2$ definen el mismo código pues

$$\mathbf{G}_2 = \begin{pmatrix} 1+z & 0 \\ z & 1+z+z^2 \end{pmatrix} \cdot \mathbf{G}_1 \,.$$

En este caso, es el representante polinómico $\mathbf{G}_2$ del código convolucional el que se debe evitar.

1.4. Codificadores básicos. Códigos convolucionales como submódulos.

Si $\mathbf{G}$ es un (n, k) codificador convolucional polinómico, considerando $\mathbf{G}$ como un morfismo de $\mathbb{F}_q[z]$-módulos $\mathbf{G}\colon \mathbb{F}_q[z]^k \hookrightarrow \mathbb{F}_q[z]^n$, *el módulo libre* $L_{\mathbf{G}} = \text{Im}_{\mathbb{F}_q[z]}\, \mathbf{G}$ *es un submódulo de rango* k *de* $\mathbb{F}_q[z]^n$ *y* $\mathcal{C} = L_{\mathbf{G}} \otimes_{\mathbb{F}_q[z]} \mathbb{F}_q(z)$ *es el código convolucional de razón* k/n *que define.*

Si $\mathbf{G}'\colon \mathbb{F}_q[z]^k \hookrightarrow \mathbb{F}_q[z]^n$ es otro representante polinómico del código $\mathcal{C}$ se verifica

$$L_{\mathbf{G}} \otimes_{\mathbb{F}_q[z]} \mathbb{F}_q(z) = \mathcal{C} = L_{\mathbf{G}'} \otimes_{\mathbb{F}_q[z]} \mathbb{F}_q(z)$$

Definición 1.17. Un codificador polinómico $\mathbf{G}\colon \mathbb{F}_q[z]^k \hookrightarrow \mathbb{F}_q[z]^n$ es básico si el módulo cociente $\mathbb{F}_q[z]^n / L_{\mathbf{G}}$ es libre.

Teorema 1.18. *Sea* $\mathbf{G}\colon \mathbb{F}_q[z]^k \hookrightarrow \mathbb{F}_q[z]^n$ *un codificador básico. Las siguientes proposiciones son equivalentes:*

1. $\mathbf{G}$ *admite una inversa polinómica por la derecha, esto es, existe* $\mathbf{G}^{-1} \in M(n \times k, \mathbb{F}_q[z])$ *tal que* $\mathbf{G} \cdot \mathbf{G}^{-1} = I_k$.

2. *Los factores invariantes de* $\mathbf{G}$ *son todos iguales a 1.*

3. *El máximo común divisor de los menores de orden* k *de* $\mathbf{G}$ *es 1.*

4. $\operatorname{rg}\mathbf{G} = k$ *en cualquier extensión de* $\mathbb{F}_q$.

En particular, todo codificador básico es no catastrófico.

Demostración. Si $\gamma_1, \ldots, \gamma_k$ son los factores invariantes de $\mathbf{G}$, se tiene que $\mathbb{F}_q[z]^n/L_{\mathbf{G}}$ es libre si y sólo si es libre de torsión. Eso equivale a que $\mathbb{F}_q[z]/\langle\gamma_1\rangle \oplus \cdots \oplus \mathbb{F}_q[z]/\langle\gamma_k\rangle = 0$ es decir, a que $\gamma_1 = \cdots = \gamma_k = 1$, o sea, a que el máximo común divisor de los menores de orden k de $\mathbf{G}$ es 1.

Por otra parte, $\mathbb{F}_q[z]^n/L_{\mathbf{G}}$ es libre si y sólo si la sucesión exacta de $\mathbb{F}_q[z]$-módulos

$$0 \to L_{\mathbf{G}} \xrightarrow{\mathbf{G}} \mathbb{F}_q[z]^n \to \mathbb{F}_q[z]^n/L_{\mathbf{G}} \to 0$$

rompe, es decir, si y sólo si $\mathbf{G}$ admite un retracto $\mathbf{G}^{-1}$. □

Ejemplo 1.19. El codificador binario

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

es básico pues el máximo común divisor de los menores de orden 2 de $\mathbf{G}$ es 1

Probaremos ahora de modo constructivo siguiendo a Forney [11] la existencia de codificadores básicos para cualquier código convolucional.

Teorema 1.20. *Todo* (n, k) *código convolucional admite un representante básico.*

Demostración. Sean $\mathbf{G}$ un representante polinómico del código y $\gamma_1, \ldots, \gamma_k$ sus factores invariantes respecto de $\mathbb{F}_q[z]$. Consideremos la matriz

$$\Gamma = \left(\begin{array}{ccc|c} \gamma_1 & & & \\ & \ddots & & 0_{k\times(n-k)} \\ & & \gamma_k & \end{array}\right)$$

Se tiene $\mathbf{G} = A \cdot \Gamma \cdot B$ para ciertas matrices $A \in \operatorname{Aut}_{\mathbb{F}_q[z]} \mathbb{F}_q[z]^k$ y $B \in \operatorname{Aut}_{\mathbb{F}_q[z]} \mathbb{F}_q[z]^n$.

La matriz $\mathbf{G}_0$ construida con las primeras k filas de B define el codificador básico buscado. En efecto, si $\{b_1, \ldots, b_k, \ldots, b_n\}$ son las filas de B y $\{c_1, \ldots, c_k, \ldots, c_n\}$ son las columnas de su inversa B^{-1}, se tiene:

1. $\mathbf{G}_0 = (b_1, \ldots, b_k)^t$ tiene una inversa polinómica $\mathbf{G}_0^{-1} = (c_1, \ldots, c_k)$.

2. $\mathbf{G}$ y $\mathbf{G}_0$ generan el mismo código: Si $x \in \mathrm{Im}_{\mathbb{F}_q[z]} \mathbf{G}$ se tiene

$$x = u\mathbf{G} = (uA)\Gamma B = u_{\sigma(1)}\gamma_1 b_1 + \cdots + u_{\sigma(k)}\gamma_k b_k \in \mathrm{Im}_{\mathbb{F}_q[z]} \mathbf{G}_0$$

La tercera igualdad se debe a que como $A \in \mathrm{Aut}_{\mathbb{F}_q[z]} \mathbb{F}_q[z]^k$, uA consiste sólo en permutar las componentes $(u_1, \ldots, u_k)$ de u; σ representa tal permutación. Se sigue que $\mathrm{Im}_{\mathbb{F}_q[z]} \mathbf{G} \subseteq \mathrm{Im}_{\mathbb{F}_q[z]} \mathbf{G}_0$ y como son subespacios de $\mathbb{F}_q(z)^n$ de la misma dimensión, coinciden.

□

Nota 1.21. El algoritmo de cálculo de los factores invariantes de una matriz y el teorema anterior permiten construir *un algoritmo programable para calcular un representante básico* a partir de un representante polinómico cualquiera del código convolucional.

Demostraremos a continuación que los codificadores básicos *son invariantes por la acción del grupo unimodular* $GL(k, \mathbb{F}_q[z]) = \mathrm{Aut}_{\mathbb{F}_q[z]} \mathbb{F}_q[z]^k$ y que *son los elementos maximales de la clase de codificadores polinómicos de un código convolucional*, lo que utilizaremos para definir el *grado del código convolucional* y para buscar una *clase canónica* de representantes polinómicos, en el sentido de la minimalidad de la realización física trivial del código.

Teorema 1.22. *Sean* $\mathbf{G}$ *y* $\mathbf{G}'$ *dos codificadores polinómicos que definen el mismo* (n, k) *código convolucional* $\mathcal{C}$ *y sean* $L_{\mathbf{G}}$ *y* $L_{\mathbf{G}'}$ *los submódulos libres de rango* k *asociados. Se verifica*

1. *Si* $\mathbf{G}$ *es básico y* $L_{\mathbf{G}} \subseteq L_{\mathbf{G}'}$*, entonces* $L_{\mathbf{G}} = L_{\mathbf{G}'}$.

2. *Si* $\mathbf{G}$ *y* $\mathbf{G}'$ *son ambos básicos,* $L_{\mathbf{G}} = L_{\mathbf{G}'}$.

Demostración. (1) Componiendo las sucesiones exactas de $\mathbb{F}_q[z]$-módulos asociadas a $\mathbf{G}$ y $\mathbf{G}'$,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L_{\mathbf{G}} & \xrightarrow{\mathbf{G}} & \mathbb{F}_q[z]^n & \longrightarrow & \mathbb{F}_q[z]^n/L_{\mathbf{G}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \| & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L_{\mathbf{G}'} & \xrightarrow{\mathbf{G}'} & \mathbb{F}_q[z]^n & \longrightarrow & \mathbb{F}_q[z]^n/L_{\mathbf{G}'} & \longrightarrow & 0 \end{array}$$

se tiene que $\ker h = \operatorname{coker} f$. Como f es inyectiva, $\operatorname{coker} f = L_{\mathbf{G}'}/L_{\mathbf{G}}$ y como $\mathbf{G}$ es básico $\mathbb{F}_q[z]^n/L_{\mathbf{G}}$ es libre, luego $\ker h$ no tiene torsión y por tanto $L_{\mathbf{G}'}/L_{\mathbf{G}} = 0$.

(2) El submódulo $L_{\mathbf{G}} + L_{\mathbf{G}'}$ genera el mismo código $\mathcal{C}$ y contiene a $L_{\mathbf{G}}$ y a $L_{\mathbf{G}'}$, luego por (1) es $L_{\mathbf{G}} = L_{\mathbf{G}} + L_{\mathbf{G}'} = L_{\mathbf{G}'}$. □

Corolario 1.23. *Si* $\mathbf{G}$ *y* $\mathbf{G}'$ *son dos representantes básicos de un* (n, k) *código convolucional, se verifica*

$$\mathbf{G}' = A \cdot \mathbf{G} \quad \textit{con } A \in \operatorname{Aut}_{\mathbb{F}_q[z]} \mathbb{F}_q[z]^k (= GL(k, \mathbb{F}_q[z])) .$$

□

Corolario 1.24. *Los codificadores básicos son los elementos maximales de la clase de los codificadores polinómicos de un código convolucional.* □

Sea $\mathbf{G}$ un *codificador polinómico* de un (n, k) código convolucional $\mathcal{C}$. Representemos por $\delta_{\mathbf{G}}$ el *máximo grado de los menores de orden* k *de* $\mathbf{G}$ (grado interno de $\mathbf{G}$ según McEliece [24]).

Teorema 1.25. *Si* $\mathbf{G}$ *es un* (n, k) *codificador básico se verifica que* $\delta_{\mathbf{G}} \leq \delta_{\mathbf{G}'}$ *para todo codificador polinómico* $\mathbf{G}'$ *que genera el mismo código convolucional.*

Demostración. Como generan el mismo código, existe $A \in GL(k, \mathbb{F}_q(z))$ tal que $\mathbf{G}' = A \cdot \mathbf{G}$; pero A es polinómica pues por ser $\mathbf{G}$ básico es $L_{\mathbf{G}'} \subseteq L_{\mathbf{G}}$.

$$\begin{array}{ccc} \mathbb{F}_q[z]^k & \xrightarrow[\simeq]{\mathbf{G}} & L_{\mathbf{G}} \\ {\scriptstyle A}\uparrow & & \uparrow \\ \mathbb{F}_q[z]^k & \xrightarrow[\simeq]{\mathbf{G}'} & L_{\mathbf{G}'} \end{array}$$

Luego como los menores de orden k de $\mathbf{G}'$ se obtienen multiplicando por el determinante de A los menores de orden k de $\mathbf{G}$, resulta que $\delta_{\mathbf{G}'} \geq \delta_{\mathbf{G}}$. □

Corolario 1.26. *Si* $\mathbf{G}$ *y* $\mathbf{G}'$ *son codificadores básicos que definen el mismo código convolucional, se verifica que* $\delta_{\mathbf{G}} = \delta_{\mathbf{G}'}$. □

Y podemos definir ahora un invariante del código, *el grado de un código convolucional*:

Definición 1.27. El grado δ de un código convolucional de dimensión k es

$\delta = \delta_{\mathbf{G}} =$ *máximo grado de los menores de orden* k *de un representante básico* $\mathbf{G}$

Y así podemos abordar la teoría de códigos convolucionales desde el punto de vista de los módulos, sin más que identificar *los* (n, k) *códigos convolucionales con la clase de los submódulos básicos de rango* k *de* $\mathbb{F}_q[z]$.

1.5. Codificadores básicos minimales. Codificadores canónicos

Nos interesan *aquellos codificadores polinómicos en los que el grado del código coincide con el grado del codificador y éste último es el menor posible entre todos los representantes polinómicos del código.* En sentido de Forney, estos codificadores forman una *clase canónica de codificadores básicos*, los codificadores minimales respecto de los que la realización física trivial requiere el menor número de elementos de memoria.

Forney [11] definió los codificadores minimales:

Definición 1.28. Un codificador básico $\mathbf{G}$ es *minimal* si su grado $\mathrm{gr}(\mathbf{G})$ coincide con el grado δ del código, esto es

$$\mathrm{gr}(\mathbf{G}) = \sum_{i=1}^{k} \nu_i = \delta \,,$$

con $\nu_i = \mathrm{gr}\, g_i$ y $\mathbf{G} = \begin{pmatrix} g_1 & \dots & g_k \end{pmatrix}^t$.

Los números $\nu_1, \dots, \nu_k$ se llaman *índices de Forney* y son invariantes del código.

Forney [11] demostró la existencia de tales codificadores: *Entre todos los codificadores básicos que definen el mismo código convolucional existe por lo menos uno que es minimal.*

McEliece calcula en [22] el número de codificadores básicos minimales en forma estándar $(\nu_1 \leq \nu_2 \leq \cdots \leq \nu_k)$ que tiene un código convolucional.

McEliece [24] llama *canónicos* a estos codificadores básicos minimales de Forney y para ello utiliza los *codificadores polinómicos reducidos*. Las definiciones son las siguientes:

Definición 1.29. Un codificador polinómico $\mathbf{G}$ es *reducido* si $\delta_{\mathbf{G}} = \operatorname{gr} \mathbf{G}$.

Definición 1.30. Un codificador polinómico $\mathbf{G}$ es *canónico* si es a la vez básico y reducido.

Así, el grado δ de un código convolucional coincide con el grado de cualquier codificador canónico $\mathbf{G}$ que represente al código, $\delta = \operatorname{gr}(\mathbf{G})$, y su memoria m es el grado de la fila de mayor grado de $\mathbf{G}$, que coincide con el índice de Forney ν_k si $\mathbf{G}$ está en forma estándar.

1.6. Codificadores convolucionales sistemáticos

Un codificador es sistemático si las palabras código que produce contienen los mensajes originales.

Definición 1.31. Un (n, k) codificador convolucional $\mathbf{G}$ es sistemático si

$$\mathbf{G} = (I_k | R)\,, \quad \text{con } R \in M(k \times (n-k), \mathbb{F}_q(z))\,.$$

Teorema 1.32. [11, Forney] *Todo (n, k) código convolucional tiene un representante sistemático realizable.*

Demostración. Sea $\mathbf{G}_0$ un representante básico del código. $\mathbf{G}_0$ contiene al menos una submatriz polinómica de orden k, $A \in M(k \times k, \mathbb{F}_q[z])$, con $\det A$ no nulo y no divisible por z, pues $\mathbf{G}_0$ es de rango k y el máximo común divisor de los menores de orden k de $\mathbf{G}_0$ es 1 por ser $\mathbf{G}_0$ básico. Luego A posee una inversa con coeficientes funciones racionales sin polos en el origen, $A^{-1} = \frac{A^t}{\det A}$, y la matriz $\mathbf{G} = A^{-1} \cdot \mathbf{G}_0 = (I_k | R)$ define un codificador sistemático realizable. □

Ejemplo 1.33. El codificador $\mathbf{G} = \begin{pmatrix} 1 & 0 & \frac{1}{1+z} \\ 0 & 1 & \frac{z}{1+z} \end{pmatrix}$ es sistemático y realizable con feed-back.

Los codificadores sistemáticos realizables con feed-back forman una clase muy importante entre todos los representantes de un código convolucional (sólo hay uno por cada código). Este tipo de codificadores se utiliza en la construcción de los *turbo códigos* (1983, [2]).

1.7. Código dual. Matriz de control

Sea $\mathcal{C}$ un (n,k) código convolucional.

Definición 1.34. El código convolucional dual de $\mathcal{C}$ es el $\mathbb{F}_q(z)$-subespacio $\mathcal{C}^\perp$ de $\mathbb{F}_q(z)^n$ dado por

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

respecto de la métrica $\langle x, y\rangle = \sum_i x_i y_i$ con $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ en $\mathbb{F}(z)^n$.

Teorema 1.35. *$\mathcal{C}^\perp$ es un $(n-k,k)$ código convolucional de grado igual al de $\mathcal{C}$.*

Demostración. Sea $\mathbf{G}$ un representante básico de $\mathcal{C}$ y $L_{\mathbf{G}}$ el submódulo de $\mathbb{F}_q[z]^n$ asociado. Como $\mathbf{G}$ es básico, el módulo cociente $\mathbb{F}_q[z]^n/L_{\mathbf{G}}$ es libre, luego la sucesión exacta

$$0 \to L_{\mathbf{G}} \xrightarrow{\mathbf{G}} \mathbb{F}_q[z]^n \xrightarrow{\mathbf{H}^t} \mathbb{F}_q[z]^n/L_{\mathbf{G}} \to 0$$

induce una sucesión exacta de $\mathbb{F}_q[z]$-módulos libres

$$0 \to (\mathbb{F}_q[z]^n/L_{\mathbf{G}})^* \xrightarrow{\mathbf{H}} \mathbb{F}_q[z]^n \xrightarrow{\mathbf{G}^t} L_{\mathbf{G}}^* \to 0$$

donde $(\mathbb{F}_q[z]^n/L_{\mathbf{G}})^* = \mathrm{Hom}_{\mathbb{F}_q[z]}(\mathbb{F}_q[z]^n/L_{\mathbf{G}}), \mathbb{F}_q)$ y $L_{\mathbf{G}}^* = \mathrm{Hom}_{\mathbb{F}_q[z]}(L_{\mathbf{G}}, \mathbb{F}_q)$ son los duales como $\mathbb{F}_q[z]$-módulo, lo que prueba que el código dual $\mathcal{C}^\perp$ es isomorfo a $(\mathbb{F}_q[z]^n/L_{\mathbf{G}})^*$ como $\mathbb{F}_q[z]$-módulo, que $\mathbf{H}$ es un representante básico y que $\delta_{\mathbf{G}} = \delta_{\mathbf{H}} = \delta$. □

Como en los códigos lineales de bloques, a partir de un representante sistemático del código se puede construir un representante sistemático del código dual.

Proposición 1.36. *Si $\mathbf{G} = (I_k|R)$ es un codificador sistemático realizable del código convolucional $\mathcal{C}$, $\mathbf{H} = (-R^t|I_{n-k})$ es un representante sistemático realizable del código dual $\mathcal{C}^\perp$.*

Demostración. De la sucesión exacta de $\mathbb{F}_q(z)$-espacios vectoriales

$$0 \to \mathbb{F}_q(z)^k \xrightarrow{\mathbf{G}} \mathbb{F}_q(z)^n \xrightarrow{\mathbf{H}^t} \mathbb{F}_q(z)^{n-k} \to 0$$

se sigue, tomando duales, la sucesión exacta

$$0 \to \mathbb{F}_q(z)^{n-k} \xrightarrow{\mathbf{H}} \mathbb{F}_q(z)^n \xrightarrow{\mathbf{G}^t} \mathbb{F}_q(z)^n/\mathbb{F}_q(z)^k \to 0$$

y de $\mathbf{H} \cdot \mathbf{G}^t = 0$ resulta $\mathbf{H} = (-R^t | I_{n-k})$. □

Veremos ahora un método debido a Forney [11] para construir a la vez un código convolucional y su dual mediante representantes básicos. Este método puede resultar útil cuando se decodifica mediante síndromes.

Proposición 1.37. *Construcción de un (n, k) código convolucional y su dual con generadores básicos.*

Demostración. Sea $\mathbf{G}_P$ un representante polinómico del código y $\mathbf{G}_P = A\Gamma B$ la descomposición por factores invariantes (Teorema 1.20).

Si $\{b_1, \ldots, b_k, \ldots, b_n\}$ son las filas de la matriz unimodular B y denotamos por $\{c_1, \ldots, c_k, \ldots, c_n\}$ las columnas de su inversa B^{-1}, se tiene

- $\mathbf{G} = \begin{pmatrix} b_1 & \ldots & b_k \end{pmatrix}^t$ es un representante básico del código, de hecho su inversa por la derecha es $\mathbf{G}^{-1} = \begin{pmatrix} c_1 & \ldots & c_k \end{pmatrix}$.
- $\mathbf{H} = \begin{pmatrix} c_{k+1} & \ldots & c_n \end{pmatrix}^t$ es un representante básico del código dual; su inversa por la derecha es $\mathbf{H}^{-1} = \begin{pmatrix} b_{k+1} & \ldots & b_n \end{pmatrix}$.

□

Nota 1.38. De $B^{-1} = \begin{pmatrix} \mathbf{G}^{-1} & \mathbf{H}^t \end{pmatrix}$ se sigue que si u es el vector de información, x la palabra codificada, R la palabra recibida y e el vector de error, $R = x + e$, se tiene

$$RB^{-1} = \begin{pmatrix} R\mathbf{G}^{-1} & R\mathbf{H}^t \end{pmatrix} = \begin{pmatrix} u + e\mathbf{G}^{-1} & e\mathbf{H}^t \end{pmatrix}$$

siendo $e\mathbf{H}^t$ el síndrome de la palabra recibida y $u + e\mathbf{G}^{-1}$ la estimación del ruido.

1.8. Distancia libre

Dado un vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, se define su peso $w(x)$ como el número de componentes no nulas:

$$w(x) = \#\{i \mid x_i \neq 0\}$$

En el caso de los códigos convolucionales, se necesita una definición análoga para el peso de un vector con componentes polinómicas, $x(z) \in \mathbb{F}_q[z]^n$. Teniendo en cuenta que el peso de un polinomio es el número de sus coeficientes no nulos, podemos dar las siguientes definiciones para el *peso* y la *distancia*(*libre*) en teoría de códigos convolucionales:

Definición 1.39. El *peso* de $x(z) = (x_1(z), \ldots, x_n(z)) \in \mathbb{F}_q[z]^n$ es la suma de los pesos de sus componentes polinómicas:

$$w(x(z)) = \sum_{i=1}^{n} w(x_i(z)) \,.$$

Definición 1.40. La *distancia libre* de un código convolucional $\mathcal{C} \subseteq \mathbb{F}_q(z)^n$ es el menor de los pesos de las palabras código no nulas,

$$d_{free}(\mathcal{C}) = \text{mín}\{w(x(z)) \mid x(z) \in \mathcal{C} \cap \mathbb{F}_q[z]^n \,,\ x(z) \neq 0\} \,.$$

En particular, si el grado del código es cero, $\mathcal{C}$ es un código lineal y su distancia (libre) coincide con su distancia mínima (Hamming) como código lineal.

Como para los códigos lineales, se buscan cotas para la distancia libre de los códigos convolucionales utilizando subcódigos polinómicos como hace McEliece en [24, Theor. 4.4].

Recordemos que una buena cota para la distancia de un (n, k) código lineal es la Cota de Singleton $n-k+1$ y que aquellos códigos que la alcanzan, es decir, cumplen que su distancia de Hamming es $n-k+1$, se llaman códigos lineales óptimos o MDS (maximum distance separable).

Rosenthal y Smarandache demuestran en [31] que para cada (n, k) código convolucional de grado δ existe una cota para su distancia libre:

$$d_{free}(\mathcal{C}) \leq (n-k)\big(\lfloor \frac{\delta}{k} \rfloor + 1\big) + \delta + 1 \,,$$

que coincide cuando $\delta = 0$ con la Cota de Singleton de un (n, k) código lineal. Por esta razón se llama *Cota de Singleton generalizada* y conduce a la siguiente definición:

Definición 1.41. Un código convolucional $\mathcal{C}$ es *óptimo* o MDS si su distancia libre alcanza la Cota de Singleton generalizada, esto es si:

$$d_{free}(\mathcal{C}) = (n-k)(\lfloor \delta/k \rfloor + 1) + \delta + 1 \,,$$

donde n, k and δ son respectivamente la longitud, la dimensión y el grado del código.

1.9. Sistemas lineales asociados a un código convolucional

Sea $\mathcal{C}$ un (n,k) código convolucional sobre $\mathbb{F}_q$ de memoria m, índices de Forney $\nu_1 \leq \nu_2 \leq \ldots \nu_k = m$ y grado $\delta = \nu_1 + \cdots + \nu_k$.

Al código le podemos asociar una matriz polinómica E y dos matrices escalares $A \in \mathcal{M}(\delta \times \delta, \mathbb{F}_q)$ y $B \in \mathcal{M}(k \times \delta, \mathbb{F}_q)$ en la forma:

- *Morfismo de estados*, es la aplicación $\mathbb{F}_q[z]$-lineal

$$\begin{aligned} \mathbb{F}_q[z]^k &\xrightarrow{E} \mathbb{F}_q[z]^\delta \\ u(z) &\to u(z)E = s(z)\,, \end{aligned}$$

  donde $s(z)$ es el estado de la palabra emitida $u(z)$.

  Matriz de estados

$$E = \begin{pmatrix} z & \ldots & z^{\nu_1} & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & 0 & z & \ldots & z^{\nu_2} & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & z & \ldots & z^{\nu_k} \end{pmatrix}$$

- Sea A la forma canónica del *endomorfismo nilpotente* $\mathbb{F}_q^\delta \xrightarrow{A} \mathbb{F}_q^\delta$ de índices $\nu_1 \leq \nu_2 \leq \ldots \nu_k = m$, ν_i es la dimensión del monógeno de anulador x^{ν_i} y $\nu_k = m$ es el índice de nilpotencia:

$$A = \begin{pmatrix} A_{\nu_1} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & A_{\nu_k} \end{pmatrix}, \quad A_{\nu_i} = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}$$

  Es inmediato comprobar que

$$E \cdot A = z^{-1}E - z^{-1}E_{|z=0}$$

  De modo que si representamos por B la matriz escalar $z^{-1}E_{|z=0}$ se tiene la ecuación matricial $z^{-1}E = E \cdot A + B$, que vectorialmente se escribe

$z^{-1}u(z)E = u(z)E \cdot A + u(z)B$, de donde se obtiene la *ecuación que describe la evolución del estado en función del tiempo de emisión*:

$$z^{-1}s(z) = s(z)A + u(z)B \tag{1.9.1}$$

Observemos que A y B no dependen de ningún codificador, tan sólo de los invariantes del código dados por los índices de Forney.

Para construir las matrices C y D elegimos un representante canónico $\mathbf{G}$ del código, cuyas filas $1, \ldots, k$ tengan grados $\nu_1, \ldots, \nu_k = m$ respectivamente.

Sea $\mathbf{G} = \mathbf{G}_0 + \mathbf{G}_1 z + \cdots + \mathbf{G}_m z^m$ su descomposición polinómica, y representemos por $\mathbf{G}_{ij}$ la fila j no nula de la matriz escalar $\mathbf{G}_i$.

- La matriz $C \in \mathcal{M}(\delta \times n, \mathbb{F}_q)$ definida por:

$$C = \begin{pmatrix} \mathbf{G}_{11} \\ \vdots \\ \mathbf{G}_{\nu_1 1} \\ \mathbf{G}_{12} \\ \vdots \\ \mathbf{G}_{\nu_2 2} \\ \vdots\vdots \\ \mathbf{G}_{1\nu_k} \\ \vdots \\ \mathbf{G}_{\nu_k \nu_k} \end{pmatrix}, \quad \text{verifica } E \cdot C = \mathbf{G} - \mathbf{G}_0.$$

- *La ecuación* matricial $\mathbf{G} = E \cdot C + D$ con $D = \mathbf{G}_0$ *describe la palabra código* $x(z) = u(z)\mathbf{G}(z)$ *en función de la palabra emitida* $u(z)$ *y su estado* $s(z) = u(z)E$, esto es

$$x(z) = s(z)C + u(z)D \tag{1.9.2}$$

Se obtiene así el *sistema lineal asociado a la matriz canónica* $\mathbf{G}$:

$$\left.\begin{aligned} z^{-1}s(z) &= s(z)A + u(z)B \\ x(z) &= s(z)C + u(z)D \end{aligned}\right\}, \tag{1.9.3}$$

que se corresponde en el contexto de la Teoría de Sistemas con el sistema lineal de ecuaciones

$$\begin{cases} s_{t+1} = s_t A + u_t B \\ x_t = s_t C + u_t D \quad \text{para } t \geq t_0 \text{ y } s_{t_0} = 0 \end{cases} \tag{1.9.4}$$

donde

$$u_t = (u_{1,t}, \ldots, u_{k,t}) \in \mathbb{F}_q^k,\ s_t = (s_{1,t}, \ldots, s_{\delta,t}) \in \mathbb{F}_q^\delta,\ x_t = (x_{1,t}, \ldots, x_{n,t}) \in \mathbb{F}_q^n$$

representan los vectores de entrada, estados y salida, respectivamente.

Tiene por matriz de transferencia $R(s) = B \cdot (sI - A)^{-1} \cdot C$, siendo $s = z^-1$ y $R(s) = \mathbf{G} - D$, que es una matriz racional propia e invariante por cambios de base en el espacio de estados $\mathbb{F}_q^\delta$, $(A, B, C) \to (\tau A \tau^{-1}, B\tau^{-1}, \tau C)$ para cada $\tau \in \operatorname{Aut} \mathbb{F}_q^\delta$.

El sistema tiene el mínimo número de variables de estado, es decir la terna (A, B, C) es una *realización minimal* con grado de McMillan δ.

1.10. Ejemplo de cálculo de la distancia libre y del sistema lineal asociados a un código convolucional

Para el cálculo de la distancia libre de un (n, k) código convolucional $\mathcal{C}$ de grado δ e índices de Forney $\nu_1, \ldots, \nu_k$, utilizaremos el siguiente procedimiento:

- Si $\mathbf{G}$ es u n representante canónico del código en forma estándar ($\nu_1 \leq \cdots \leq \nu_k$), escribimos $\mathbf{G} = \begin{pmatrix} A & B \end{pmatrix}$ con A una matriz invertible de orden k. Una matriz de control es $\mathbf{H} = \begin{pmatrix} -B^t \cdot \operatorname{Adj}(A) & \det(A) \cdot I \end{pmatrix}$, pues $\mathbf{H}\mathbf{G}^t = 0$ (ecuaciones del código).

- Las descomposiciones polinómicas de $\mathbf{G}$ y $\mathbf{H}$ son

  $$\mathbf{G} = \mathbf{G}_0 + \mathbf{G}_1 z + \cdots + \mathbf{G}_m z^m \quad y \qquad \mathbf{H} = \mathbf{H}_0 + \mathbf{H}_1 z + \cdots + \mathbf{H}_\delta z^\delta$$

  siendo $m = \nu_k$ la memoria de $\mathcal{C}$ y δ su grado.

Las matrices escalares

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_0 & & & & & & \\ \mathbf{H}_1 & \mathbf{H}_0 & & & & & \\ \vdots & \vdots & & & & & \\ \mathbf{H}_\delta & \mathbf{H}_{\delta-1} & \dots & \dots & \dots & \mathbf{H}_0 & \\ 0 & \mathbf{H}_\delta & \dots & \dots & \dots & \mathbf{H}_1 & \mathbf{H}_0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & \mathbf{H}_\delta & \dots & \mathbf{H}_m & \mathbf{H}_{m-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \mathbf{H}_\delta & \mathbf{H}_{\delta-1} \\ 0 & \dots & 0 & 0 & \dots & 0 & \mathbf{H}_\delta \end{pmatrix} \quad y \quad \begin{pmatrix} \mathbf{G}_0^t \\ \mathbf{G}_1^t \\ \vdots \\ \mathbf{G}_m^t \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

determinan las ecuaciones $\mathbf{H}\mathbf{G}^t = 0$ del código.

- Como para los códigos lineales, el estudio de la independencia lineal de las columnas de $\mathbf{H}$ determina la distancia, la distancia es d si en $\mathbf{H}$ hay d columnas linealmente dependientes pero no $d-1$.

Veamos un ejemplo de código convolucional definido por un representante canónico en forma estándar y calcularemos su distancia libre y un sistema lineal asociado.

Ejemplo 1.42. Cuerpo $\mathbb{F}_5$.

$$\mathbf{G} = \begin{pmatrix} 1+z & 3+2z & 4+4z & 2+3z \\ 1+2z+z^2 & 4+2z+4z^2 & 1+2z+z^2 & 4+2z+4z^2 \end{pmatrix} = \begin{pmatrix} A & B \end{pmatrix}$$

es un representante canónico en forma estándar del $(4,2)$ código convolucional de memoria $m=2$ y grado $\delta=3$.

La *matriz de control* $\mathbf{H} = \begin{pmatrix} -B^t \operatorname{Adj}(A) & \det(A)\cdot I \end{pmatrix}$ es

$$\begin{pmatrix} 2+4z+3z^2+z^3 & 3+4z+4z^2+3z^3 & 1+3z+4z^2+2z^3 & 0 \\ 4+3z+2z^2+z^3 & 3+z+2z^2+4z^3 & 0 & 1+3z+4z^2+2z^3 \end{pmatrix}$$

y la descomposición polinómica de $\mathbf{H}$ es

$$\mathbf{H} = \mathbf{H}_0 + \mathbf{H}_1 z + \mathbf{H}_2 z^2 + \mathbf{H}_3 z^3$$

con

$$\mathbf{H}_0 = \begin{pmatrix} 2 & 3 & 1 & 0 \\ 4 & 3 & 0 & 1 \end{pmatrix}, \mathbf{H}_1 = \begin{pmatrix} 4 & 4 & 3 & 0 \\ 3 & 1 & 0 & 3 \end{pmatrix}$$
$$\mathbf{H}_2 = \begin{pmatrix} 3 & 4 & 4 & 0 \\ 2 & 2 & 0 & 4 \end{pmatrix}, \mathbf{H}_3 = \begin{pmatrix} 1 & 3 & 2 & 0 \\ 1 & 4 & 0 & 2 \end{pmatrix}$$

en este caso la matriz $\mathbf{H}$ es

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_0 & & & & \\ \mathbf{H}_1 & \mathbf{H}_0 & & & \\ \mathbf{H}_2 & \mathbf{H}_1 & \mathbf{H}_0 & & \\ \mathbf{H}_3 & \mathbf{H}_2 & \mathbf{H}_1 & \mathbf{H}_0 & \\ & \mathbf{H}_3 & \mathbf{H}_2 & \mathbf{H}_1 & \mathbf{H}_0 \\ & & \mathbf{H}_3 & \mathbf{H}_2 & \mathbf{H}_1 \\ & & & \mathbf{H}_3 & \mathbf{H}_2 \\ & & & & \mathbf{H}_3 \end{pmatrix}$$

Se comprueba que cualesquiera 7 columnas de $\mathbf{H}$ son linealmente independientes y hay 8 linealmente dependientes, por ejemplo las 8 primeras. Por tanto la distancia del código es 8. El código es óptimo o MDS pues la cota de Singleton generalizada es también 8.

Calculemos ahora las matrices A, B, C y D del **sistema lineal asociado**,

$$\begin{cases} z^{-1}s = sA + uB \\ u\mathbf{G} = sC + uD \end{cases}, \quad \text{siendo } \mathbf{G} = B(z^{-1}I - A)^{-1}C + D$$

- Morfismo de estados

$$\mathbb{F}[z]^2 \to \mathbb{F}[z]^3$$
$$u \mapsto u \cdot E \qquad \text{con } E = \begin{pmatrix} z & 0 & 0 \\ 0 & z & z^2 \end{pmatrix}$$

- Como para $z = 0$ es $s = 0$, resulta

$$D = \mathbf{G}_0 = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \end{pmatrix}$$

- $$B = z^{-1}E_{|z=0} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

- $$C = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 2 & 2 & 2 \\ 1 & 4 & 1 & 4 \end{pmatrix}$$

  como se sigue de

  $$E \cdot C = \mathbf{G} - D = z\mathbf{G}_1 + z^2\mathbf{G}_2 = \begin{pmatrix} z & 0 & 0 \\ 0 & z & z^2 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{G}_1 \\ \mathbf{G}_2^* \end{pmatrix}$$

  siendo $\mathbf{G}_2^*$ la matriz $\mathbf{G}_2$ sin la fila de ceros.

- De $E \cdot A = z^{-1}E - B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & z \end{pmatrix}$ se obtiene

  $$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

1.11. Códigos convolucionales unidimensionales

Por último, obtendremos un resultado para los códigos convolucionales de dimensión 1 que utilizaremos en el capítulo 3 para construir familias de códigos convolucionales de Goppa que son MDS.

Si $\mathcal{C}$ es un código convolucional de dimensión 1, un representante polinómico $\mathbf{G}$ de grado m es básico si y sólo si $\mathbf{G} = \mathbf{G}_0 + z\mathbf{G}_1 + \cdots + z^m\mathbf{G}_m$ es no nulo para todo z en cualquier extensión de $\mathbb{F}_q$ (Teorema 1.18). En particular, $\mathbf{G}$ es básico si $\mathrm{rg}(\mathbf{G}_0, \mathbf{G}_1, \ldots \mathbf{G}_m)^t = m+1$. Además, su grado coincide con el grado del código (Definición 1.27), es decir, todo codificador básico es canónico.

Teorema 1.43. *Sea $\mathcal{C}$ un código convolucional de dimensión 1 y longitud n y $\mathbf{G} = \mathbf{G}_0 + \mathbf{G}_1 z + \cdots + \mathbf{G}_\delta z^\delta$ la descomposición polinómica de una matriz*

generadora $\mathbf{G}$. *Si los códigos lineales* $\{\mathbf{G}_j\}_{0\leq j\leq \delta}$ *son MDS y* $\begin{pmatrix}\mathbf{G}_j\\ \vdots \\ \mathbf{G}_0\end{pmatrix}$, $\begin{pmatrix}\mathbf{G}_\delta\\ \vdots \\ \mathbf{G}_{\delta-j}\end{pmatrix}$ *son* $(n, j+1)$ *códigos lineales MDS para todo* $0 \leq j \leq \delta$, *entonces* $\mathcal{C}$ *es un código convolucional MDS de grado* δ *y* $\mathbf{G}$ *es una matriz generadora canónica.*

Demostración.

$\mathbf{G}$ es básica, pues $\mathbf{G}_{z=a} \neq 0$ para todo $a \in \mathbb{F}_q$ ya que $\begin{pmatrix}\mathbf{G}_\delta\\ \vdots \\ \mathbf{G}_0\end{pmatrix}$ tiene rango $\delta + 1$. Luego el grado de $\mathcal{C}$ es δ, con $\delta < n$.

Las palabras código polinómicas de $\mathcal{C}$ son de la forma $p_j(z)\mathbf{G}$, siendo$p_j(z) \in \mathbb{F}_q[z]$ un polinomio de grado j.

Sea $p_j(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_j z^j$, con $a_j \neq 0$; podemos suponer que $a_0 \neq 0$ pues el peso de una palabra código no cambia al multiplicar por z.

Los coeficientes de la palabra código $p_j(z)\mathbf{G}$ son palabras código de los códigos lineales del enunciado; por tanto, una cota inferior I_j para su peso $w(p_j(z)\mathbf{G})$ está dada por la suma de las distancias mínimas de esos códigos. Se tiene:

$$I_0 = n(\delta+1)$$
$$I_j = 2n + 2(n-1) + 2(n-2) + \cdots + 2(n-j+1) + (n-j)(\delta-j+1),\ j \leq \delta$$
$$I_{\delta+i} = I_\delta + i(n-\delta)\,,\ i \geq 0\,,$$

de lo que se deduce:

$$I_j = (j+1)n + (n-j)\delta\,,\ \text{para todo } j \geq 0\,.$$

Finalmente, como $I_{j+1} - I_j = n - \delta > 0$, para $j \geq 0$, la distancia libre del código $\mathcal{C}$ es

$$d_{free}(\mathcal{C}) = I_0 = n(\delta+1)\,.$$

□

Capítulo 2

Códigos Convolucionales de Goppa sobre curvas algebraicas

En este capítulo se definen los Códigos Convolucionales de Goppa como códigos de evaluación asociados a curvas algebraicas sobre el cuerpo $\mathbb{F}_q(z)$ de las funciones racionales de una variable y se construyen los correspondientes códigos duales. Se generaliza así la teoría de Goppa de códigos en curvas algebraicas sobre un cuerpo finito $\mathbb{F}_q$ a un cuerpo (infinito) $\mathbb{F}_q(z)$.

2.1. Código convolucional de Goppa

Sea $(X, \mathcal{O}_X)$ una curva proyectiva no singular de género g sobre $\mathbb{F}_q(z)$ y Σ_X su cuerpo de funciones racionales. Supondremos que $\mathbb{F}_q(z)$ es algebraicamente cerrado en Σ_X.

Para cada punto $p \in X$ denotamos por $\mathcal{O}_p$ el anillo local de X en p y por $\mathfrak{m}_p$ su ideal maximal. El cuerpo residual en p es el cociente $\mathcal{O}_p/\mathfrak{m}_p$ y se tiene una extensión finita de cuerpos $\mathbb{F}_q(z) \hookrightarrow \mathcal{O}_p/\mathfrak{m}_p$. El grado de p, $\mathrm{gr}(p)$, es la dimensión de esta extensión. El punto p es *racional* si $\mathbb{F}_q(z) \simeq \mathcal{O}_p/\mathfrak{m}_p$, es decir, si $\mathrm{gr}(p) = 1$.

Un divisor D sobre X es una suma formal $D = \sum_{p \in X} n_p p$ donde casi todos los $n_p \in \mathbb{Z}$ son nulos. Se define el grado del divisor D por $\mathrm{gr}(D) = \sum_{p \in X} n_p \,\mathrm{gr}(p)$.

Dada una función racional $f \in \Sigma_X$, (f) representa el divisor definido por $(f) = \sum_i n_i c_i - \sum_j m_j p_i$, donde $n_i, m_j \in \mathbb{Z}^+$ son las multiplicidades de los ceros $c_i \in X$ y los polos $p_j \in X$ de la función f.

Sea $\mathcal{O}_X(D)$ el haz de línea asociado al divisor D sobre X y dado por:

$$\mathcal{O}_X(D)(U) = \{f \in \Sigma_X \,|\, ((f) + D)_{|U} \geq 0\,,\ U \text{ abierto de } X\}\,,$$

sus secciones globales definen la *serie lineal completa* asociada a D:

$$L(D) = H^0(X, \mathcal{O}_X(D)) = \{f \in \Sigma_X \,|\, (f) + D \text{ es un divisor positivo en X}\}\,. \tag{2.1.1}$$

Si $p_1, \ldots, p_n$ son n puntos racionales distintos de X y $D = p_1 + \cdots + p_n$ es el divisor que definen, se tiene la sucesión exacta de haces:

$$0 \to \mathcal{O}_X(-D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0 \tag{2.1.2}$$

donde el cociente $\mathcal{O}_D$ es un haz acíclico con soporte en los puntos p_i. Localmente, en cada punto p_i, esta sucesión se escribe:

$$\begin{array}{c} 0 \to \mathfrak{m}_{p_i} \to \mathcal{O}_{p_i} \to \mathcal{O}_{p_i}/\mathfrak{m}_{p_i} \simeq \mathbb{F}_q(z) \to 0\,. \\ f \mapsto f(p_i) \end{array} \tag{2.1.3}$$

Para cada divisor G sobre X con soporte disjunto de D, tensorializando la sucesión exacta (2.1.2) por el haz de línea asociado $\mathcal{O}_X(G)$ se obtiene

$$0 \to \mathcal{O}_X(G - D) \to \mathcal{O}_X(G) \to \mathcal{O}_D \to 0 \tag{2.1.4}$$

donde el isomorfismo

$$\mathcal{O}_X(G) \otimes \mathcal{O}_D \simeq \mathcal{O}_D$$

viene dado en cada punto $p \in D$ por $f \otimes 1 \mapsto f(p)$, ya que $\mathcal{O}_X(G)$ es un subhaz del haz constante Σ_X y los divisores G y D tienen soporte disjunto.

Tomando secciones globales en (2.1.4)

$$\begin{array}{c} 0 \to L(G - D) \to L(G) \xrightarrow{\alpha} \mathbb{F}_q(z) \times \overset{n}{\ldots} \times \mathbb{F}_q(z) \to \ldots \\ f \mapsto (f(p_1), \ldots, f(p_n)) \end{array} \tag{2.1.5}$$

donde $L(G-D)$ y $L(G)$ representan las series lineales asociadas a los divisores $G - D$ y G como en (2.1.1).

Definición 2.1. El código convolucional de Goppa $\mathcal{C}(D, G)$ asociado al par de divisores (D, G) es la imagen del morfismo $\mathbb{F}_q(z)$-lineal

$$\begin{array}{l} L(G) \xrightarrow{\alpha} \mathbb{F}_q(z)^n \\ \quad f \mapsto (f(p_1), \ldots, f(p_n))\,. \end{array}$$

Análogamente, dado un subespacio $\Gamma \subseteq L(G)$, se define el código convolucional de Goppa $\mathcal{C}(D, \Gamma)$ como la imagen del morfismo $\alpha_{|\Gamma}$.

Teorema 2.2. *El código convolucional de Goppa* $\mathcal{C}(D,G)$ *tiene longitud* $n = \operatorname{gr} D$ *y dimensión* $k = \dim_{\mathbb{F}_q(z)} L(G) - \dim_{\mathbb{F}_q(z)} L(G-D)$.

Si $2g-2 < \operatorname{gr} G < \operatorname{gr} D$ *su dimensión es* $k = 1-g+gr(G)$.

Demostración.

Como $\mathcal{C}(D,G) = \operatorname{Im}\left(L(G) \xrightarrow{\alpha} \mathbb{F}_q(z)^n\right)$ es un subespacio de $\mathbb{F}_q(z)^n$ su longitud es n y su dimensión k viene dada por:

$$k = \dim_{\mathbb{F}_q(z)} L(G) - \dim_{\mathbb{F}_q(z)} \ker\alpha = \dim_{\mathbb{F}_q(z)} L(G) - \dim_{\mathbb{F}_q(z)} L(G-D)\,.$$

Sea K un divisor canónico sobre X, es decir el divisor de una diferencial meromorfa sobre X, $\operatorname{gr} K = 2g-2$.

Si $2g-2 < \operatorname{gr} G < \operatorname{gr} D$ se tiene que $L(K-G) = 0$, $L(G-D) = 0$, y utilizando el teorema de Riemann-Roch,

$$\dim L(G) - \dim L(K-G) = 1-g+\operatorname{gr}(G)\,,$$

resulta:

$$k = \dim L(G) = 1-g+\operatorname{gr}(G)$$

□

2.2. Código convolucional de Goppa dual

Consideremos la métrica sobre $\mathbb{F}_q(z)^n$ definida por

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

donde $x = (x_1,\ldots,x_n)$, $y = (y_1,\ldots,y_n) \in \mathbb{F}_q(z)^n$.

Definición 2.3. El código convolucional dual del código $\mathcal{C}(D,G)$ es el $\mathbb{F}_q(z)$-subespacio $\mathcal{C}^{\perp}(D,G)$ de $\mathbb{F}_q(z)^n$ dado por

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

Su longitud es $n = \operatorname{gr}(D)$ y su dimensión $n - \dim \mathcal{C}(D,G)$.

Teorema 2.4. *El código convolucional dual $\mathcal{C}^{\perp}(D,G)$ es el código convolucional de Goppa $\mathcal{C}(D,K+D-G)$ asociado al par de divisores $(D,K+D-G)$.*

Demostración. Tensorializando la sucesión exacta de haces (2.1.2) por el haz de línea $\mathcal{O}_X(K+D-G)$ se tiene

$$0 \to \mathcal{O}_X(K-G) \to \mathcal{O}_X(K+D-G) \to \mathcal{O}_D \to 0 \tag{2.2.1}$$

Como $\mathcal{O}_X(K)$ es el haz ω_X de las diferenciales, $\mathcal{O}_X(K-G)$ se identifica con el haz $\omega_X(-G)$ de las diferenciales sin polos y con ceros en G y $\mathcal{O}_X(K+D-G)$ con el haz $\omega_X(D-G)$ de las diferenciales con ceros en G y polos a lo sumo de orden uno en los puntos de D.

Por tanto, localmente en cada $p_i \in D$, un generador local de $\mathcal{O}_X(K+D-G)$ es $\dfrac{1}{t_i}dt_i$ y el isomorfismo $\mathcal{O}_X(K+D-G)\otimes\mathcal{O}_D \simeq \mathcal{O}_D$ está dado por $f\dfrac{1}{t_i}dt_i \otimes 1 \mapsto f(p_i) := \operatorname{Res}_{p_i}(f\dfrac{1}{t_i}dt_i)$. Así, tomando secciones globales en la sucesión anterior se obtiene:

$$\begin{aligned} 0 \to L(K-G) \to L(K+D-G) &\xrightarrow{\beta} \mathbb{F}_q(z)^n \to \dots \\ \eta &\mapsto (\operatorname{Res}_{p_1}\eta, \dots, \operatorname{Res}_{p_n}\eta) \end{aligned} \tag{2.2.2}$$

Por definición de código convolucional de Goppa asociado al par de divisores $(D, K+D-G)$ es $\operatorname{Im}\beta = \mathcal{C}(D,K+D-G)$.

El Teorema de los residuos permite demostrar que este código está contenido en el código dual $\mathcal{C}^{\perp}(D,G)$. En efecto, para cada $\eta \in L(K+D-G)$ y cada $f \in L(G)$ se verifica:

$$\langle \beta(\eta), \alpha(f)\rangle = \sum_{i=1}^{n} f(p_i)\operatorname{Res}_{p_i}\eta = \sum_{i=1}^{n}\operatorname{Res}_{p_i}(f\eta) = 0$$

donde

$$\begin{aligned} L(G) &\xrightarrow{\alpha} \mathbb{F}_q(z)^n \\ f &\mapsto (f(p_1), \dots, f(p_n)), \qquad \operatorname{Im}\alpha = \mathcal{C}(D,G) \end{aligned}$$

Lo que prueba que $\beta(\eta) \in \mathcal{C}^{\perp}(D,G)$, es decir, $\mathcal{C}(D,K+D-G) \subseteq \mathcal{C}^{\perp}(D,G)$.

Finalmente, el Teorema de Riemman-Roch permite demostrar que ambos códigos tienen la misma dimensión:

$$\begin{aligned}&\dim \mathcal{C}(D, K+D-G) + \dim \mathcal{C}(D,G) = \\ &= \dim L(K+D-G) - \dim L(K-G) + \dim L(G) - \dim L(G-D) \\ &= \dim L(K+D-G) - \dim L(G-D) + \dim L(G) - \dim L(K-G) \\ &= 1-g+\mathrm{gr}(K+D-G) + 1 - g + \mathrm{gr}(G) = \mathrm{gr}(D) = n\,.\end{aligned}$$

Se concluye que:

$$\mathcal{C}^{\perp}(D,G) = \mathcal{C}(D, K+D-G)\,.$$

En particular, si $2g-2 < \mathrm{gr}\, G < \mathrm{gr}\, D$ el morfismo β es inyectivo, pues $L(K-G) = 0$, y la dimensión del código dual es $n - (1 - g + gr(G))$, como se sigue del teorema 2.2. □

2.3. Ejemplos de construcción sobre curvas de géneros 0 y 1

Ejemplo 2.5.

Sea $X = \mathbb{P}^1_{\mathbb{F}_8(z)}$ la recta proyectiva sobre el cuerpo $\mathbb{F}_8(z)$. Representemos por $\{x_0, x_1\}$ sus coordenadas homogéneas, por $t = x_1/x_0$ su coordenada afín y por $p_\infty = (0,1)$ el punto del infinito.

Consideremos el divisor de puntos

$$D = p_1 + p_2 + p_3 + p_4\,,$$

siendo $p_i = z + \alpha^{i-1}$ la coordenada afín de p_i y α un elemento primitivo de $\mathbb{F}_8$ tal que $\alpha^3 + \alpha^2 + 1 = 0$, esto es, $\mathbb{F}_8 = \mathbb{F}_2[x]/x^3 + x^2 + 1$.

Sea $G = 3p_\infty$ y Γ el subespacio de $L(G) = \langle 1, t, t^2, t^3\rangle$ generado por t^3, $\Gamma = \langle t^3\rangle$.

El código convolucional de Goppa , $\mathcal{C}(D,\Gamma)$, asociado a D y Γ tiene longitud $n = 4 = \mathrm{gr}\, D$, dimensión $k = 1 = \dim \Gamma$, grado $\delta = 3$ y matriz generadora:

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

Es claro que $\mathbf{G}$ es canónica y su descomposición polinómica es:

$$\mathbf{G} = G_0 + G_1 z + G_2 z^2 + G_3 z^3 \,,$$

siendo

$$\begin{aligned} G_3 &= \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \\ G_2 &= \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \end{pmatrix} \\ G_1 &= \begin{pmatrix} 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{pmatrix} \\ G_0 &= \begin{pmatrix} 1 & \alpha^3 & \alpha^6 & \alpha^9 \end{pmatrix} \end{aligned}$$

Los códigos $\{G_j\}_{0 \le j \le \delta}$ y $\begin{pmatrix} G_j \\ \vdots \\ G_0 \end{pmatrix}$, $\begin{pmatrix} G_\delta \\ \vdots \\ G_{\delta - j} \end{pmatrix}$ son códigos lineales de Goppa, luego MDS para todo $0 \le j \le \delta$. Por el Teorema 1.43 el código convolucional de matriz generadora $\mathbf{G}$ es también MDS.

Ejemplo 2.6.

Sea $X = \mathbb{P}^1_{\mathbb{F}_8(z)}$, como en el ejemplo anterior.

Divisor de puntos $D = p_1 + p_2 + p_3 + p_4$, con $p_1 = z+1, p_2 = \alpha z + \alpha^3, p_2 = \alpha^2 z + \alpha^6, p_2 = \alpha^3 z + \alpha^2$.

Divisor $G = 2p_\infty$, subespacio $\Gamma = \langle t, t^2 \rangle \subset L(G)$.

El código $\mathcal{C}(D, \Gamma)$ tiene longitud $n = 4 = \operatorname{gr} D$, dimensión $k = 2 = \dim \Gamma$, grado $\delta = 3$ y matriz generadora canónica:

$$\mathbf{G} = \begin{pmatrix} z+1 & \alpha z + \alpha^3 & \alpha^2 z + \alpha^6 & \alpha^3 z + \alpha^2 \\ z^2+1 & \alpha^2 z^2 + \alpha^6 & \alpha^4 z^2 + \alpha^5 & \alpha^6 z^2 + \alpha^4 \end{pmatrix}$$

Su distancia es $d_{free} = 8$, y coincide con la cota de Singleton generalizada, es decir, el código es MDS.

Ejemplo 2.7.

Sea $\mathbb{P}^2_{\mathbb{F}_2(z)} = \operatorname{Proj} \mathbb{F}_2(z)[x_0, x_1, x_2]$ el plano proyectivo sobre $\mathbb{F}_2(z)$ y sean $x = x_1/x_0$, $y = x_2/x_0$ las coordenadas afines.

La *curva elíptica* X definida sobre $\mathbb{F}_2(z)$ por la ecuación:

$$y^2 + xy + zy = x^3 + zx^2 + x$$

tiene un punto de inflexión en $p_\infty = (0,0,1)$ y pasa por los puntos

$$p_1 = (1,z)\,, \quad p_2 = (0,z)\,, \quad p_3 = (z+1,z)$$

Elegimos los siguientes divisores en X:

$$D = p_1 + p_2 + p_3\,, \quad G = 6p_\infty\,,$$

y tomamos el subespacio $\Gamma = \langle x+y^2\rangle$ de la serie lineal $L(G) = \langle 1, x, y, xy, x^2, y^2\rangle$.

El código convolucional de Goppa asociado $\mathcal{C}(D,\Gamma)$ tiene longitud $n = 3$, dimensión $k = 1$, grado $\delta = 2$ y matriz generadora canónica:

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

Su distancia libre es 6, luego este código también es MDS.

Ejemplo 2.8. Con la misma curva y los mismos divisores del ejemplo anterior podemos construir códigos asociados a subespacios $\Gamma \subset L(G)$ de dimensión 2, pero con peores prestaciones, pues ni los representantes que se obtienen son básicos ni sus distancias alcanzan la cota de Singleton generalizada. Es el caso, por ejemplo, de $\Gamma = \langle x, y\rangle$, en el que la matriz generadora asociada $\begin{pmatrix} 1 & 0 & 1+z \\ z & z & z \end{pmatrix}$ no es básica; un representante básico es $\begin{pmatrix} 1 & 0 & 1+z \\ 0 & 1 & z \end{pmatrix}$, el grado es 1 y la distancia libre 2, siendo la cota de Singleton 3.

Ejemplo 2.9.

Sea X una *curva elíptica* de la familia de cúbicas no singulares con punto de inflexión en $p_\infty = (0,0,1)$ definida por la ecuación

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5\,, \quad a_i \in \mathbb{F}_8(z)$$

y que pasa por los puntos no alineados

$$p_1 = (\alpha^2 z + \alpha, \alpha^4 z + \alpha^2)\,,\ p_2 = (\alpha^4 z + \alpha^2, \alpha z + \alpha^4)\,,\ p_3 = (\alpha z + \alpha^4, \alpha^2 z + \alpha)\,,$$

siendo α un elemento primitivo de $\mathbb{F}_8 = \mathbb{F}_2[x]/x^3 + x^2 + 1$.

El código $\mathcal{C}(D,\Gamma)$ asociado a los divisores $D = p_1 + p_2 + p_3\,,\ G = 6p_\infty$ y al subespacio $\Gamma = \langle x, y^2\rangle$ tiene longitud $n = 3$, dimensión $k = 2$, grado $\delta = 2$ y distancia libre $d_{libre} = 6 =$ Cota de Singleton. Una matriz generadora canónica es:

$$\mathbf{G} = \begin{pmatrix} \alpha^2 z + \alpha & \alpha^4 z + \alpha^2 & \alpha z + \alpha^4 \\ \alpha^4 z^2 + \alpha^2 & \alpha z^2 + \alpha^4 & \alpha^2 z^2 + \alpha \end{pmatrix}$$

Capítulo 3

Códigos convolucionales de Goppa sobre $\mathbb{P}^1$

3.1. Códigos convolucionales de Goppa sobre $\mathbb{P}^1$

Sea X la recta proyectiva sobre $\mathbb{F}_q(z)$, $X = \mathbb{P}^1_{\mathbb{F}_q(z)} = \operatorname{Proj} \mathbb{F}_q(z)[x_0, x_1]$, y sean $t = x_1/x_0$ la coordenada afín, $p_0 = (1, 0)$ el origen y $p_\infty = (0, 1)$ el punto del infinito.

Sean $p_1, \ldots, p_n$ puntos racionales diferentes de $\mathbb{P}^1_{\mathbb{F}_q(z)}$ con $p_i \neq p_0$ y $p_i \neq p_\infty$ y $n \leq q - 1$.

Consideremos los divisores $D = p_1 + \cdots + p_n$ y $G = rp_\infty - sp_0$ con $r \neq 0$ y $0 \leq s \leq r < n < q$.

Lema 3.1. *$L(G)$ es un $\mathbb{F}_q(z)$-espacio vectorial de dimensión $1 + r - s$ y una base es $\{t^s, \ldots, t^r\}$.*

Demostración. Por Riemann-Roch, $\dim L(G) = \dim L(K - G) + 1 - g + \operatorname{gr}(G) = 1 + r - s$ pues $g = 0$. Para cada $s \leq i \leq r$, se tiene que $t^i \in L(G)$, pues tiene un polo de orden $i \leq r$ en p_∞ y un cero de orden $i \geq s$ en p_0, luego $\langle t^s, \ldots, t^r \rangle = L(G)$. □

Teorema 3.2. *El morfismo de evaluación*

$$\begin{aligned} L(G) &\xrightarrow{\alpha} \mathbb{F}_q(z)^n \\ f &\mapsto (f(p_1), \ldots, f(p_n)) \end{aligned}$$

es inyectivo y su imagen define un código convolucional de Goppa $\mathcal{C}(D,G)$ de longitud n y dimensión $1+r-s$.

Respecto de la base $\{t^s,\dots,t^r\}$ de $L(G)$ una matriz generadora del código es

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

donde $\alpha_i\in\mathbb{F}_q(z)$ es la coordenada local del punto $p_i\in\mathbb{P}^1_{\mathbb{F}_q(z)}$, $1\le i\le n$.

En particular, dado un subespacio $\Gamma\subseteq L(G)$ la imagen del morfismo $\alpha_{|\Gamma}$ define un código convolucional de Goppa $\mathcal{C}(D,\Gamma)$ de longitud n y dimensión $\le 1+r-s$.

Demostración.

Como $gr(G-D)=r-s-n<0$, es $L(G-D)=0$, luego α es inyectivo y $\dim \mathrm{Im}(\alpha)=\dim L(G)=1+r-s$.

Por otra parte, para cada $s\le i\le r$ la fila i-ésima de la matriz de la aplicación $\mathbb{F}_q(z)$-lineal α respecto de la base $\{t^s,\dots,t^r\}$ de $L(G)$ y la estándar de $\mathbb{F}_q(z)^n$ es $\alpha(t^i)=(t^i(p_1),\dots,t^i(p_n))=(\alpha_1^i,\dots,\alpha_n^i)$, luego una matriz codificadora es

$$\mathbf{G}=\begin{pmatrix}\alpha(t^s)\\ \vdots\\ \alpha(t^r)\end{pmatrix}$$

□

Construiremos ahora una base del código dual $\mathcal{C}^\perp(D,G)$ y por tanto una matriz de control $\mathbf{H}$.

Lema 3.3. *$L(K+D-G)$ es un $\mathbb{F}_q(z)$-espacio vectorial de dimensión $n-(1+r-s)$ y*

$$\left\{\frac{1}{t^s\prod_{i=1}^n(t-\alpha_i)},\frac{t}{t^s\prod_{i=1}^n(t-\alpha_i)},\dots,\frac{t^{n-r+s-2}}{t^s\prod_{i=1}^n(t-\alpha_i)}\right\}$$

es una base.

Demostración. Por Riemann-Roch,

$$\dim L(K+D-G) = \dim L(G-D) + 1 - g + \mathrm{gr}(K+D-G) = n-(1+r-s)$$

pues $L(G-D)=0$ y $g=0$.

Pongamos

$$f_k = \frac{t^k}{t^s \prod_{i=1}^{n}(t-\alpha_i)}\,,\ \text{para } k=0,\ldots,n-(1+r-s)-1.$$

Se tiene

$$f_k = \frac{x_0^{n+s-k}}{x_1^{s-k}\prod_{i=1}^{n}(x_1-\alpha_i x_0)}$$

luego f_k es una función racional con un cero de orden $\geq r+2$ en p_∞, un polo de orden 1 en cada p_i $(1\leq i\leq n)$ y un polo de orden $\leq s$ en p_0, y por tanto $f_k \in L(K+D-G) = L(sp_0-(r+2)p_\infty+D)$. Así se concluye que las $n-(1+r-s)$ funciones $\{f_k\}$ forman una base de $L(K+D-G)$. □

Teorema 3.4. *El morfismo de evaluación*

$$\begin{aligned} L(K+D-G) &\xrightarrow{\beta} \mathbb{F}_q(z)^n \\ \eta &\mapsto (\mathrm{Res}_{p_1}\eta,\ldots,\mathrm{Res}_{p_n}\eta) \end{aligned}$$

es inyectivo y su imagen define un código convolucional de Goppa , que es el código dual $\mathcal{C}^\perp(D,G)$. Además, respecto de la base de $L(K+D-G)$ del Lema 3.3, una matriz generadora del código $\mathcal{C}^\perp(D,G)$ es

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

con

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

H *es una matriz de control del código $\mathcal{C}(D,G)$.*

Demostración.

El haz $\mathcal{O}_X(K-G)$ no tiene secciones globales pues $\mathrm{gr}(K-G) = -2-(r-s) < 0$, luego β es inyectivo e $\mathrm{Im}(\beta)$ es un código convolucional de Goppa de longitud n y dimensión $n-(1+r-s)$.

Sea $t_j = t - \alpha_j$, $1 \leq j \leq n$, y evaluemos β respecto de la base del Lema 3.3,

$$\mathrm{Res}_{p_{ij}}(t_j^{-1} f_k(t_j) dt_j) = f_k(\alpha_j) = \frac{\alpha_j^k}{\alpha_j^s \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\alpha_j - \alpha_i)}$$

para $k = 0, \ldots, n-r+s-2$ y $j = 1, \ldots, n$.

Si escribimos $h_j = \dfrac{1}{\alpha_j^s \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\alpha_j - \alpha_i)}$, la matriz de β es

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

que por construcción verifica $\mathbf{H} \cdot \mathbf{G}^t = 0$ siendo $\mathbf{G}$ la matriz generadora del código $\mathcal{C}(D,G)$ (Teorema 3.2). □

3.2. Aplicación y ejemplos

Para aplicar esta teoría comencemos por un caso muy simple, la coordenada local $\alpha_i \in \mathbb{F}_q(z)$ del punto racional p_i es de la forma

$$\alpha_i = a^{i-1} z + b^{i-1}\,, \quad \text{con } a, b \in \mathbb{F}_q\,,\ a \neq b \neq 0\,,$$

y una matriz generadora canónica de la forma:

$$\mathbf{G} = \begin{pmatrix} (z+1)^s & (az+b)^s & \ldots & (a^{n-1}z + b^{n-1})^s \\ (z+1)^{s+1} & (az+b)^{s+1} & \ldots & (a^{n-1}z + b^{n-1})^{s+1} \\ \vdots & \ddots & \vdots & \\ (z+1)^r & (az+b)^r & \ldots & (a^{n-1}z + b^{n-1})^r \end{pmatrix},\ \text{con } 1 \leq s \leq r \leq n\,,$$

que da un código convolucional de Goppa $\mathcal{C}(D,G)$ con:

- Longitud n y dimensión $k = r - s + 1$.
- Memoria $m = r$ y grado $\delta = \dfrac{(r-s+1)(s+r)}{2}$.
- Distancia libre $d_{free} \leq d_{Singleton} = (n-k)(\lfloor \delta/k \rfloor + 1) + \delta + 1$

Veamos algunos ejemplos de códigos de este tipo que son MDS, es decir que alcanzan la cota de Singleton generalizada $d_{Singleton}$.

Ejemplo 3.5. Cuerpo $\mathbb{F}_3(z)$, $\mathbb{F}_3 = \{0, 1, 2\}$.

- $n = 2$, $s = r = 1$, $k = 1$; $a = 1$, $b = 2$, $\alpha_1 = z + 1$, $\alpha_2 = z + 2$.
- Matriz generadora canónica $\mathbf{G} = \begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} z+1 & z+2 \end{pmatrix}$.
- Matriz de control $\mathbf{H} = \begin{pmatrix} \frac{1}{\alpha_1(\alpha_1-\alpha_2)} & \frac{1}{\alpha_2(\alpha_2-\alpha_1)} \end{pmatrix} = \begin{pmatrix} \frac{1}{2(z+1)} & \frac{1}{z+2} \end{pmatrix}$.
- $\delta = 1$, $d_{free} = 4$, $d_{Singleton} = 4$.
- Realización minimal (A, B, C, D)del sistema lineal asociado:

$$A = \begin{pmatrix} 0 \end{pmatrix} \ , \ B = \begin{pmatrix} 1 \end{pmatrix}$$
$$C = \begin{pmatrix} 1 & 1 \end{pmatrix} \ , \ D = \begin{pmatrix} 1 & 2 \end{pmatrix}$$

Ejemplo 3.6. Cuerpo $\mathbb{F}_4(z)$, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ con $1 + \alpha + \alpha^2 = 0$.

- $n = 3$, $s = 0$, $r = 1$, $k = 2$; $a = \alpha$, $b = \alpha^2$, $\alpha_1 = z + 1$, $\alpha_2 = \alpha z + \alpha^2$, $\alpha_3 = \alpha^2 z + \alpha$.
- Matriz generadora canónica $\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 \\ z+1 & \alpha z + \alpha^2 & \alpha^2 z + \alpha \end{pmatrix}$.
- Matriz de control

  $\mathbf{H} = \begin{pmatrix} \frac{1}{\alpha_3\alpha_2} & \frac{1}{\alpha_3\alpha_1} & \frac{1}{\alpha_2\alpha_1} \end{pmatrix} = \begin{pmatrix} \frac{1}{(\alpha^2 z+\alpha)(\alpha z+\alpha^2)} & \frac{1}{(\alpha^2 z+\alpha)(z+1)} & \frac{1}{(\alpha z+\alpha^2)(z+1)} \end{pmatrix}$.

- $\delta = 1$, $d_{free} = 3$, $d_{Singleton} = 3$.

- Realización minimal (A, B, C, D) del sistema lineal asociado:

$$A = \begin{pmatrix} 0 \end{pmatrix} \ , \ B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$C = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix} \ , \ D = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix}$$

Ejemplo 3.7. Cuerpo $\mathbb{F}_4(z)$, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ con $1 + \alpha + \alpha^2 = 0$.

- $n = 3$, $s = r = 1$, $k = 1$; $a = 1$, $b = \alpha$, $\alpha_1 = z + 1$, $\alpha_2 = z + \alpha$, $\alpha_3 = z + \alpha^2$.
- Matriz generadora canónica

$$\mathbf{G} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} z+1 & z+\alpha & z+\alpha^2 \end{pmatrix} .$$

- Matriz de control

$$\mathbf{H} = \begin{pmatrix} \frac{1}{\alpha_1} & \frac{1}{\alpha^2\alpha_1} & \frac{1}{\alpha\alpha_3} \\ 1 & \frac{1}{\alpha^2} & \frac{1}{\alpha} \end{pmatrix} = \begin{pmatrix} \frac{1}{z+1} & \frac{\alpha}{z+\alpha} & \frac{\alpha^2}{z+\alpha^2} \\ 1 & \alpha & \alpha^2 \end{pmatrix} .$$

- $\delta = 1$, $d_{free} = 6$, $d_{Singleton} = 6$.
- Realización minimal (A, B, C, D) del sistema lineal asociado:

$$A = \begin{pmatrix} 0 \end{pmatrix} \ , \ B = \begin{pmatrix} 1 \end{pmatrix}$$
$$C = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \ , \ D = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}$$

Ejemplo 3.8. Cuerpo $\mathbb{F}_5(z)$, $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.

- $n = 3$, $s = r = 2$, $k = 1$; $a = 1$, $b = 2$, $\alpha_1 = z+1$, $\alpha_2 = z+2$, $\alpha_3 = z+4$.
- Matriz generadora canónica

$$\mathbf{G} = \begin{pmatrix} \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix} = \begin{pmatrix} (z+1)^2 & (z+2)^2 & (z+4)^2 \end{pmatrix} .$$

- Matriz de control

$$\mathbf{H} = \begin{pmatrix} h_1 & h_2 & h_3 \\ \alpha_1 h_1 & \alpha_2 h_2 & \alpha_3 h_3 \end{pmatrix} = \begin{pmatrix} \frac{2}{(z+1)^2} & \frac{2}{(z+2)^2} & \frac{1}{(z+4)^2} \\ \frac{2}{z+1} & \frac{2}{z+2} & \frac{1}{z+4} \end{pmatrix}.$$

  pues $h_j = \frac{1}{\alpha_j^2 \prod_{i,j=1, i\neq j}^{3} (\alpha_j - \alpha_i)}$, $1 \leq j \leq 3$.

- $\delta = 2$, $d_{free} = 9$, $d_{Singleton} = 9$.

- Realización minimal (A, B, C, D) del sistema lineal asociado:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 0 \end{pmatrix}$$
$$C = \begin{pmatrix} 2 & 4 & 3 \\ 1 & 1 & 1 \end{pmatrix}, \; D = \begin{pmatrix} 1 & 4 & 1 \end{pmatrix}$$

Ejemplo 3.9. Cuerpo $\mathbb{F}_5(z)$, $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.

- $n = 4$, $s = 1$, $r = 2$, $k = 2$; $a = 2$, $b = 3$, $\alpha_1 = z + 1$, $\alpha_2 = 2z + 3$, $\alpha_3 = 4z + 4$, $\alpha_4 = 3z + 2$.

- Matriz generadora canónica

$$\mathbf{G} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 \end{pmatrix} = \begin{pmatrix} z+1 & 2z+3 & 4z+4 & 3z+2 \\ (z+1)^2 & (2z+3)^2 & (4z+4)^2 & (3z+2)^2 \end{pmatrix}$$
$$= \begin{pmatrix} z+1 & 2(z+4) & 4(z+1) & 3(z+4) \\ (z+1)^2 & 4(z+4)^2 & (z+1)^2 & 4(z+4)^2 \end{pmatrix}.$$

- Matriz de control

$$\mathbf{H} = \begin{pmatrix} h_1 & h_2 & h_3 & h_4 \\ \alpha_1 h_1 & \alpha_2 h_2 & \alpha_3 h_3 & \alpha_4 h_4 \end{pmatrix}$$
$$= \begin{pmatrix} \frac{4}{(z+1)^2(z+2)(z+3)} & \frac{4}{(z+2)(z+3)(z+4)^2} & \frac{4}{(z+1)^2(z+2)(z+3)} & \frac{4}{(z+2)(z+3)(z+4)^2} \\ \frac{4}{(z+1)(z+2)(z+3)} & \frac{3}{(z+2)(z+3)(Z+4)} & \frac{1}{(z+1)(z+2)(z+3)} & \frac{2}{(z+2)(z+3)(z+4)} \end{pmatrix}.$$

  con $h_j = \frac{1}{\alpha_j^2 \prod_{i,j=1, i\neq j}^{3} (\alpha_j - \alpha_i)}$, $1 \leq j \leq 3$.

- $\delta = 3$, $d_{free} = 8$, $d_{Singleton} = 8$.

- Realización minimal (A, B, C, D) del sistema lineal asociado:

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \ , \ B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 2 & 2 & 2 \\ 1 & 4 & 1 & 4 \end{pmatrix} \ , \ D = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \end{pmatrix}$$

3.3. El caso particular de los códigos convolucionales de Goppa de dimensión 1 sobre $\mathbb{P}^1_{\mathbb{F}_q(z)}$

Por construcción, los códigos convolucionales de Goppa de dimensión 1 y longitud n sobre $\mathbb{P}^1_{\mathbb{F}_q(z)}$ asociados a la pareja de divisores $D = p_1 + \cdots + p_n$ y $G = rp_\infty - sp_0$ son los subespacios de $\mathbb{F}_q(z)^n$ definidos por la imagen del morfismo de evaluación en los puntos $p_1, \ldots, p_n$ de las series lineales $\Gamma = \langle \lambda_s t^s + \cdots + \lambda_r t^r \rangle \subseteq L(G)$, con $\lambda_i \in \mathbb{F}_q(z)$ para $s \leq i \leq r$.

Construiremos códigos convolucionales de Goppa de tipo $(n, 1)$ sobre $\mathbb{P}^1_{\mathbb{F}_q(z)}$ que son MDS, es decir, cuya distancia libre alcanza la cota de Singleton generalizada, que coincide con $n(\delta + 1)$ siendo δ el grado del código.

Sea $L(G) = \langle t^s, t^{s+1}, \ldots, t^r \rangle \xrightarrow{\alpha} \mathbb{F}_q(z)^n$ el morfismo de evaluación asociado a los divisores $D = p_1 + \cdots + p_n$ y $G = rp_\infty - sp_0$, $0 \leq s \leq r < n$, como en la Sección 3. Y para cada $1 \leq i \leq n$ sea $a_i z + b_i$, con $a_i \neq 0$, $b_i \in \mathbb{F}_q$ la coordenada local del punto racional $p_i \in \mathbb{P}^1_{\mathbb{F}_q(z)}$.

El código convolucional de Goppa definido por la restricción de α al subespacio

$$\Gamma = \langle \lambda_s t^s + \cdots + \lambda_r t^r \rangle \subseteq L(G) \, , \lambda_i \in \mathbb{F}_q(z)$$

admite como representante la siguiente matriz generadora:

$$\mathbf{G} = \left(\sum_{i=s}^{r} \lambda_i (a_1 z + b_1)^i \quad \sum_{i=s}^{r} \lambda_i (a_2 z + b_2)^i \quad \ldots \quad \sum_{i=s}^{r} \lambda_i (a_n z + b_n)^i \right) \quad (3.3.1)$$

Describiremos estos códigos y probaremos que algunos de ellos son MDS.

Teorema 3.10. *Si* $s = r$*, es* $\Gamma = \langle t^r \rangle$ *y una matriz generadora del código es:*

$$\begin{pmatrix} (a_1 z + b_1)^r & (a_2 z + b_2)^r & \dots & (a_n z + b_n)^r \end{pmatrix} .$$

Si elegimos a_i, b_i *para cada* $1 \leq i \leq n$*, tal que* $\dfrac{b_i}{a_i} = c^{i-1}$*, donde* c *es un elemento de* $\mathbb{F}_q$ *de orden* $\geq n$*, una matriz generadora del código es:*

$$\mathbf{G} = \begin{pmatrix} a_1^r (z+1)^r & a_2^r (z+c)^r & a_3^r (z+c^2)^r & \dots & a_n^r (z+c^{n-1})^r \end{pmatrix} .$$

La matriz $\mathbf{G}$ *es canónica, el grado del código es* r *y, si* $\binom{r}{j} \neq 0$ *para todo* $j \leq r$*, su distancia libre es* $n(r+1)$*, es decir, el código es MDS.*

Demostración. $\mathbf{G}$ es básica, pues $\operatorname{mcd}(a_1^r(z+1)^r, \dots, a_1^r(z+c^{n-1})^r) = 1$, luego canónica. La memoria y el grado son iguales a r y la cota de Singleton generalizada es $n(r+1)$.

Es claro que, si todos los coeficientes binómicos $\binom{r}{j}$ son no nulos, el peso mínimo de una palabra del código es $n(r+1)$, luego la distancia libre del código es $n(r+1)$ y éste es MDS. □

Corolario 3.11. *Los códigos del tipo anterior, con* $a_i = 1$*,* $b_i = b^{i-1}$ *y* $order(b) \geq n$*, son MDS y con matriz generadora canónica*

$$\mathbf{G} = \begin{pmatrix} (z+1)^m & (z+b)^m & (z+b^2)^m & \dots & (z+b^{n-1})^m \end{pmatrix}$$

siempre que los coeficientes binómicos $\left\{ \binom{m}{j} \ , \ 0 \leq j \leq m \right\}$ *sean no nulos.*

Observación 3.12. En característica 2, esta teoría permite construir códigos convolucionales de longitud n y dimensión $k = 1$ que son MDS, haciendo variar su memoria m para que los coeficientes binómicos se mantegan no nulos, pues como se debe cumplir $m < n < q = 2^-$, se tiene:

- Si $m = 1$ es $1 < 2 < 2^2$, luego podemos construir códigos convolucionales MDS de grado $m = 1$, dimensión $k = 1$, longitudes $n = 2, 3$ sobre $\mathbb{F}_4(z)$.
- Si $m = 3$, $3 < 4 < 2^3$, se obtienen de longitudes $n = 4, 5, 6, 7$ sobre $\mathbb{F}_8(z)$.

- $m = 7\,, \quad 7 < 8 < 2^4$, se construyen de longitudes $n = 8, 9, 10, \ldots, 15$ sobre $\mathbb{F}_{16}(z)$.
- $m = 15\,, \quad 15 < 16 < 2^5$, se construyen de longitudes $n = 16, 17, \ldots 31$ sobre $\mathbb{F}_{32}(z)$.
- $m = 31\,, \quad 31 < 32 < 2^6$, se obtienen de longitudes $n = 32, 33, \ldots 63$ sobre $\mathbb{F}_{64}(z)$.

  Análogamente se puede continuar.

Supongamos ahora que $s = 0$, esto es, $L(G) = \langle 1, t, \ldots, t^r \rangle$, y consideremos los códigos convolucionales de Goppa de longitud n, dimensión 1 y grado $\leq r$ definidos valorando el subespacio $\Gamma = \langle \lambda_0 + \lambda_1 t \cdots + \lambda_r t^r \rangle$ con $\lambda_i \in \mathbb{F}_q$, $0 \leq i \leq r$, en los puntos p_i con todos los b_i iguales, $p_i = \{a_i z + b\}_{0 \leq i \leq n}$.

Si $\mathbf{G} = G_0 + G_1 z + \cdots + G_r z^r$ es la descomposición polinómica de la matriz generadora definida en (3.3.1), se tiene:

$$G_j = \left(\sum_{m=j}^{r} \lambda_m \binom{m}{j} a_1^j b_1^{m-j} \quad \ldots \quad \sum_{m=j}^{r} \lambda_m \binom{m}{j} a_n^j b_n^{m-j} \right) , \quad 0 \leq j \leq r\,.$$

De modo que si definimos funciones $\mathbb{F}_q^{r+1} \times \mathbb{F}_q \xrightarrow{\phi^{(j)}} \mathbb{F}_q$ por

$$\phi_\lambda^{(j)}(t) = \sum_{m=j}^{r} \binom{m}{j} \lambda_m t^{m-j}\,, \quad 0 \leq j \leq r\,,\ \lambda = (\lambda_0, \ldots, \lambda_r)\,,$$

podemos escribir

$$G_j = \left(a_1^j \phi_\lambda^{(j)}(b) \quad \ldots \quad a_n^j \phi_\lambda^{(j)}(b) \right) , \quad 0 \leq j \leq r\,. \tag{3.3.2}$$

pues $b_i = b$ para todo $1 \leq i \leq n$.

Representemos por C_λ el código convolucional de Goppa de longitud n y dimensión 1 asociado a $\Gamma = \langle \lambda_0 + \lambda_1 t \cdots + \lambda_r t^r \rangle$, con $\lambda_i \in \mathbb{F}_q$ y al divisor $D = p_1 + \cdots + p_n$, con $p_i = a_i z + b$.

Teorema 3.13. *Sea C_λ el código convolucional de Goppa de longitud n y dimensión 1 asociado a $\Gamma = \langle \lambda_0 + \lambda_1 t \cdots + \lambda_r t^r \rangle$, con $\lambda_i \in \mathbb{F}_q$ y al divisor $D = p_1 + \cdots + p_n$, con $p_i = a_i z + b$.*

C_λ es un código convolucional MDS con matriz generadora canónica $\mathbf{G}$ si y sólo si $\phi_\lambda^{(j)}(b) \neq 0$ para todo $0 \leq j \leq r$.

Demostración. Recordemos primero que un código lineal de dimensión 1 y longitud n es MDS si el peso mínimo de una palabra código es n, lo que equivale a que los coeficientes de cualquier matriz generadora sean no nulos. Por tanto, la expresión (3.3.2) garantiza que los códigos lineales $G_j \in \mathcal{M}_{\mathbb{F}_q}(1 \times n)$ son MDS si y sólo si $\phi_\lambda^{(j)}(b) \neq 0$, ya que $a_i \neq 0$ para todo $1 \leq i \leq n$.

Si C_λ es MDS, cada matriz escalar G_j de la descomposición polinómica $\mathbf{G} = G_0 + G_1 z + \cdots + G_r z^r$ define un código lineal G_j que tiene que ser MDS, pues si alguno de estos G_j no fuera MDS existiría una palabra polinómica del código C_λ de peso menor que $n(r+1)$, lo que contradice que la distancia libre de C_λ sea $n(r+1)$.

Recíprocamente, si $\phi_\lambda^{(j)}(b) \neq 0$, con $0 \leq j \leq r$, todos los códigos lineales $\begin{pmatrix} G_s \\ \vdots \\ G_p \end{pmatrix}$ son MDS, pues todos sus menores de orden máximo son de la forma

$$\begin{vmatrix} a_i^s & \dots & a_m^s \\ & \ddots & \\ a_i^p & \dots & a_m^p \end{vmatrix} \phi_\lambda^{(s)}(b) \cdot \dots \cdot \phi_\lambda^{(p)}(b)\,,$$

luego no nulos, ya que $a_i \neq a_j \neq 0$ for $i \neq j$.

En particular, la matriz generadora $\mathbf{G} = G_0 + G_1 z + \cdots + G_r z^r$ es canónica y por el teorema (1.43) el código convolucional C_λ es MDS. □

Corolario 3.14. *El código C_λ, con todos los $\lambda_i \neq 0$ y $b = 0$ es MDS.*

Demostración. Si $b = 0$, las ecuaciones de los códigos C_λ no MDS son $\lambda_i = 0$ para todo $0 \leq i \leq r$. Por tanto, el código correspondiente a $\lambda = (\lambda_1, \dots, (\lambda_n)$ es MDS, y con matriz generadora canónica:

$$\mathbf{G} = \begin{pmatrix} \sum_{i=0}^{r} a_1^i z^i & \dots & \sum_{i=0}^{r} a_n^i z^i \end{pmatrix}.$$

□

La clase de códigos convolucionales MDS de tipo $(n, 1, r)$ construidos por H. Gluesing-Luerssen y B. Langfeld [12] son de este tipo:

Corolario 3.15. *El código* C_λ*, con* $\lambda = (1, \ldots, 1)$*,* $b = 0$*,* $a_i = a^{i-1}$ *y* $order(a) \geq n$*, es MDS y con matriz generadora canónica:*

$$\mathbf{G} = \sum_{i=0}^{r} z^i \begin{pmatrix} 1 & a^i & a^{2i} \ldots & a^{(n-1)i} \end{pmatrix}$$

Teorema 3.16. *El conjunto de los códigos convolucionales de Goppa definidos por* $\Gamma = \langle \lambda_0 + \lambda_1 t \cdots + \lambda_r t^r \rangle$ *con* $\lambda_i \in \mathbb{F}_q$ *y el divisor de puntos* $\{a_i z + b\}_{0 \leq i \leq n}$*,* $a_i \neq a_j \neq 0$ *que son MDS es un abierto no vacío de* $\mathbb{P}^r_{\mathbb{F}_q}$*, su complementario es la unión de los hiperplanos* $\phi^{(j)}_\lambda(b) = 0$*,* $0 \leq j \leq r$*.*

Demostración. Se tiene:

$$\{\lambda \in \mathbb{P}^r_{\mathbb{F}_q} \,|\, C_\lambda \text{ es MDS}\} = \{\lambda \in \mathbb{P}^r_{\mathbb{F}_q} \,|\, \phi^{(j)}_\lambda(b) \neq 0\,, \text{ para todo } 0 \leq j \leq r\}$$

Este conjunto no es vacío como se sigue de los Corolarios anteriores. □

Veamos ahora algunos ejemplos que nos muestren la ventaja de esta teoría en la elección de códigos óptimos sobre alfabeto pequeño.

Ejemplo 3.17.

Con alfabeto $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, siendo $1 + \alpha + \alpha^2 = 0$ y $\alpha^3 = 1$.

Consideremos la familia de códigos convolucionales de Goppa de longitud 3 y dimensión 1, C_λ, con $\lambda = (\lambda_0, \lambda_1, \lambda_2)$, asociados a $\Gamma = \langle \lambda_0 + \lambda_1 t + \lambda_2 t^2 \rangle$, con $\lambda_i \in \mathbb{F}_4$, y al divisor $D = p_1 + p_2 + p_3$, con $p_1 = z + b$, $p_2 = \alpha z + b$ y $p_3 = \alpha^2 z + b$.

Las ecuaciones de los C_λ que no son MDS son:

$$\phi^{(0)}_\lambda(b) = \lambda_0 + \lambda_1 b + \lambda_2 b^2 = 0$$
$$\phi^{(1)}_\lambda(b) = \lambda_1 = 0$$
$$\phi^{(2)}_\lambda(b) = \lambda_2 = 0$$

Si $\lambda = (1, 1, 1)$, la condición para que sea MDS es $1 + b + b^2 \neq 0$, que se cumple para $b = 0$ y $b = 1$. Obsérvese que el caso $b = 0$ ya ha sido estudiado en el Corolario 3.14.

Por ejemplo también, si $\lambda = (1, \alpha, \alpha)$, la condición para que C_λ sea MDS es $1 + \alpha b + \alpha b^2 \neq 0$, que se verifica para cualquier $b \in \mathbb{F}_4$.

Ejemplo 3.18.

Alfabeto $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.

Divisor de puntos: $D = p_1 + p_2 + p_3 + p_4$, con $p_i = \alpha^{i-1}z + b \in \mathbb{F}_5(z)$ siendo α un elemento primitivo de $\mathbb{F}_5$ ($\alpha = 2$ ó 3).

Serie lineal y morfismo de evaluación:

$$\Gamma = \langle \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \lambda_3 t^3 \rangle \hookrightarrow \mathbb{F}_5(z)^4$$

Las condiciones para que el código C_λ asociado a D y a Γ sea MDS son en este caso:

$$\begin{aligned} &\lambda_0 + \lambda_1 b + \lambda_2 b^2 + \lambda_3 b^3 \neq 0 \\ &\lambda_1 + 2\lambda_2 b + 3\lambda_3 b^2 \neq 0 \\ &\lambda_2 + 3\lambda_3 b \neq 0 \\ &\lambda_3 \neq 0 \end{aligned}$$

Para $\lambda = (1, 1, 1, 1)$ los valores de b que satisfacen esas condiciones son $b = 0, 1$. Estos valores de b también valen para $\lambda = (1, \alpha, \alpha, \alpha)$, por ejemplo.

Ejemplo 3.19.

Alfabeto $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$, siendo $1 + \alpha^2 + \alpha^3 = 0$ y $\alpha^7 = 1$.

Consideremos el código C_λ definido por los puntos $\{p_i = \alpha^{i-1}z + b \in \mathbb{F}_8(z)\}_{1 \leq i \leq 4}$ y la serie lineal $\Gamma = \langle \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \lambda_3 t^3$.

C_λ coincide con el del ejemplo anterior sobre alfabeto $\mathbb{F}_8$ y observemos como al ampliar el alfabeto el número de códigos MDS que podemos construir aumenta:

Si $\lambda = (1, 1, 1, 1)$ las condiciones para que C_λ sea MDS son en este caso:

$$\begin{aligned} &1 + b + b^2 + b^3 \neq 0 \\ &1 + b^2 \neq 0 \\ &1 + b \neq 0\,, \end{aligned}$$

que se cumplen para cualquier valor de $b \in \mathbb{F}_8$ distinto de 1.

3.3.1. Clasificación de los códigos convolucionales de Goppa de dimensión 1 sobre $\mathbb{P}^1_{\mathbb{F}_q(z)}$

En el Teorema 3.16 hemos demostrado que la familia de códigos convolucionales de Goppa asociados a $\Gamma = \langle \lambda_0 + \lambda_1 t \cdots + \lambda_r t^r \rangle$ con $\lambda_i \in \mathbb{F}_q$ que son MDS, $\{\lambda \in \mathbb{P}^r_{\mathbb{F}_q} \,|\, C_\lambda \text{ es MDS}\}$, es un abierto no vacío del espacio proyectivo $\mathbb{P}^r_{\mathbb{F}_q}$ dando explícitamente las ecuaciones del cerrado complementario.

Ahora bien, todo código convolucional de Goppa de dimensión uno sobre $\mathbb{P}^1_{\mathbb{F}_q(z)}$ está asociado a una serie lineal de la forma $\Gamma = \langle \lambda_0 + \lambda_1 t \cdots + \lambda_r t^r \rangle$ donde no todos los λ_i son escalares sino funciones racionales, es decir, $\lambda_i \in \mathbb{F}_q(z)$. De acuerdo con los resultados demostrados en [27] el espacio de móduli de estos códigos es una unión de espacios proyectivos; dado que la condición de ser MDS para un código convolucional cualquiera es una condición abierta [31, 17], para clasificar estos códigos queda por determinar explícitamente las condiciones que deben cumplir los parámetros λ_i para que un código sea MDS, es decir, calcular las ecuaciones de los que no son MDS. Ello requerirá fijar el grado del código y será objeto de trabajo futuro.

Capítulo 4

Códigos convolucionales de Goppa sobre una variedad

Sea $(X, \mathcal{O}_X)$ una variedad proyectiva no singular sobre $\mathbb{F}_q(z)$ y Σ_X su cuerpo de funciones racionales, que suponemos algebraicamente cerrado sobre $\mathbb{F}_q(z)$, así $H^0(X, \mathcal{O}_X) = \mathbb{F}_q(z)$.

Sean $p_1, \ldots, p_n$ puntos racionales distintos de X y $D = p_1 \cup \cdots \cup p_n$ el subesquema de dimensión cero asociado.

Denotemos por $\mathcal{O}_D$ el haz concentrado en los puntos de D, esto es, $\mathcal{O}_{D|p_i} \simeq \mathcal{O}_{p_i}/\mathfrak{m}_{p_i} \simeq \mathbb{F}_q(z)$ y $\mathcal{O}_{D|p} = 0$ para todo $p \neq p_i$, y por $\mathcal{I}_D$ el haz de ideales de las funciones de $\mathcal{O}_X$ que se anulan en los puntos de D, de modo que para cada abierto U:

$$\mathcal{I}_D(U) = \{f \in \mathcal{O}_X(U) : f(p) = 0, \forall p \in D \cap U\}.$$

Se tiene la sucesión exacta de haces

$$0 \to \mathcal{I}_D \to \mathcal{O}_X \to \mathcal{O}_D \to 0\,. \tag{4.0.1}$$

Sea G un divisor de X que no pasa por los puntos de D y tensorialicemos la sucesión exacta anterior (4.0.1) por el haz de línea $\mathcal{O}_X(G)$:

$$0 \to \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(G) \to \mathcal{O}_X(G) \to \mathcal{O}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(G) \simeq \mathcal{O}_D \to 0 \tag{4.0.2}$$

Tomando cohomología en (4.0.2) se obtiene la sucesión exacta:

$$\begin{aligned} 0 \to H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(G)) \to H^0(X, \mathcal{O}_X(G)) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \simeq \mathbb{F}_q(z)^n \to \\ \to H^1(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(G)) \to H^1(X, \mathcal{O}_X(G)) \to 0 \end{aligned} \tag{4.0.3}$$

pues $\mathcal{O}_D$ está concentrado en puntos, luego sus grupos de cohomología superiores son 0.

Definición 4.1. El código convolucional de Goppa $\mathcal{C}(Z, G)$ asociado al subesquema D y al divisor G es la imagen del morfismo α (4.0.3) explícitamente dado por:

$$\begin{aligned} H^0(X, \mathcal{O}_X(G)) &\xrightarrow{\alpha} \mathbb{F}_q(z)^n \\ f &\mapsto (f(p_1), \ldots, f(p_n)) \end{aligned}$$

Análogamente, dado un subespacio $\Gamma \subseteq H^0(X, \mathcal{O}_X(G))$, se define el código convolucional de Goppa $\mathcal{C}(D, \Gamma)$ como la imagen del morfismo $\alpha_{|\Gamma}$.

Teorema 4.2. *Los códigos convolucionales de Goppa $\mathcal{C}(D, G)$ y $\mathcal{C}(D, \Gamma)$ tienen longitud n igual a la longitud de D y dimensión*

$$\begin{aligned} \dim_{\mathbb{F}_q(z)} \mathcal{C}(D, G) &= h^0(\mathcal{O}_X(G)) - h^0(\mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(G)) = \\ &= n - h^1(\mathcal{I}_Z \otimes_{\mathcal{O}_X} \mathcal{O}_X(G)) + h^1(\mathcal{O}_X(G)) \end{aligned}$$

$$\dim_{\mathbb{F}_q(z)} \mathcal{C}(D, \Gamma) = \dim_{\mathbb{F}_q(z)} \Gamma - \dim_{\mathbb{F}_q(z)}(\Gamma \cap H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(G)))$$

Demostración. La longitud se deduce de $H^0(X, \mathcal{O}_D) \simeq \mathbb{F}_q(z)^n$.

La primera de las dimensiones se sigue de la definición y la sucesión exacta de cohomología (4.0.3).

En cuanto a la segunda, se obtiene de $\ker \alpha_{|\Gamma} = \Gamma \cap H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(G))$. □

4.1. Códigos convolucionales de Goppa sobre $\mathbb{P}^2$

Sea X el plano proyectivo sobre $\mathbb{F}_q(z)$, $X = \mathbb{P}^2_{\mathbb{F}_q(z)} = \operatorname{Proj} \mathbb{F}_q(z)[x_0, x_1, x_2]$, y sea H_∞ la recta del infinito de ecuación $x_0 = 0$. Denotamos por $t = x_1/x_0$, $s = x_2/x_0$ las coordenadas afines.

Todo divisor G es linealmente equivalente a rH_∞, siendo $r \in \mathbb{Z}$, de forma que el haz de línea $\mathcal{O}_X(G)$ es isomorfo a $\mathcal{O}(r)$ y se verifica:

Para $r \geq 0$, $\dim_{\mathbb{F}_q(z)} H^0(X, \mathcal{O}(r)) = \binom{r+2}{2}$ y los grupos de cohomología superiores son nulos, mientras que $\mathcal{O}(-r)$, $(r > 0)$, no tiene secciones ni H^1 y $\dim_{\mathbb{F}_q(z)} H^2(X, \mathcal{O}(-r)) = \binom{r+2}{2}$ ([16], Thm.III.5.1).

Además, si $r \geq 0$, $H^0(X, \mathcal{O}(r))$ está formado por los polinomios homogéneos de grado menor o igual a r en x_0, x_1, x_2, y podemos escribir:

$$H^0(X, \mathcal{O}(r)) = L(rH_\infty) = \langle 1, t, s, \ldots, t^r, t^{r-1}s, \ldots, ts^{r-1}, s^r \rangle$$

Consideremos los n puntos racionales $p_1, \ldots, p_n \in \mathbb{P}^2_{\mathbb{F}_q(z)}$ de coordenadas afines $(a_{i1}z + b_{i1}, a_{i2}z + b_{i2})$, con $a_{ij}, b_{ij} \in \mathbb{F}_q$ y sea $D = p_1 \cup \cdots \cup p_n$ el subesquema de dimensión cero asociado.

Teorema 4.3. *Sea $\mathcal{C}(D, \Gamma)$ el código convolucional de Goppa n dimensional asociado a $D = p_1 \cup \cdots \cup p_n$, con $p_i = (a_{i1}z + b_{i1}, a_{i2}z + b_{i2}) \in \mathbb{P}^2_{\mathbb{F}_q(z)}$, y $\Gamma \subseteq H^0(X, \mathcal{O}(r))$, y supongamos que $\Gamma \cap H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}(r)) = \{0\}$. Se verifica:*

1. *Una base de $\mathcal{C}(D, \Gamma)$ está generada por vectores de $\mathbb{F}_q(z)^n$ de la forma $\alpha_{|\Gamma}(t^i s^j) = ((a_{11}z + b_{11})^i (a_{12}z + b_{12})^j, \ldots, (a_{n1}z + b_{n1})^i (a_{n2}z + b_{n2})^j)$, con $i + j = r$.*

2. *La dimensión del código es $\dim_{\mathbb{F}_q(z)} \mathcal{C}(D, \Gamma) = \dim_{\mathbb{F}_q(z)} \Gamma \leq \binom{r+2}{2}$.*

3. *La memoria m y el grado δ están acotados por:*

$$m \leq r\,, \quad \delta \leq \sum_{0 \leq m \leq r} m(m+1)$$

Demostración. El morfismo de evaluación de la definición 4.1 es en este caso:

$$\begin{aligned} H^0(X, \mathcal{O}(r)) &\xrightarrow{\alpha} \mathbb{F}_q(z)^n \\ t^i s^j &\mapsto ((a_{11}z + b_{11})^i (a_{12}z + b_{12})^j, \ldots, (a_{n1}z + b_{n1})^i (a_{n2}z + b_{n2})^j)\,, \end{aligned} \tag{4.1.1}$$

y su restricción al subespacio Γ es inyectiva, pues $\ker \alpha_{|\Gamma} = \Gamma \cap H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}(r)) = \{0\}$. □

4.1.1. Ejemplos de códigos de dimensiones 1 y 2 sobre el plano proyectivo $\mathbb{P}^2$ que son MDS

Recordemos primero que un código convolucional de longitud n, dimensión k y grado δ es MDS si su distancia libre alcanza la cota Singleton generalizada:

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

Tomaremos como alfabeto $\mathbb{F}_8 = \mathbb{F}_2[x]/x^3+x^2+1$ y denotaremos por a cualquier generador de $\mathbb{F}_8^*$ (en $\mathbb{F}_8$ todo $a \neq 0, 1$ es primitivo).

Ejemplo 4.4. *Código convolucional de Goppa de longitud 3, dimensión 1, memoria y grado $m = \delta = 2$ y distancia 9.*

Elegimos los puntos

$$p_1 = (az + a^2, a^2z + a^4)\,,\ p_2 = (a^2z + a^4, a^4z + a)\,,\ p_3 = (a^4z + a, az + a^2)\,,$$

el divisor $G = 2H_\infty$ y el subespacio $\Gamma = \langle t+s^2\rangle \subset L(2H_\infty) = \langle 1, t, s, t^2, ts, s^2\rangle$.

La restricción a Γ del morfismo de evaluación

$$\begin{aligned} \Gamma = \langle t + s^2\rangle &\xrightarrow{\alpha_{|\Gamma}} \mathbb{F}_8(z)^3 \\ f &\mapsto (f(p_1), f(p_2), f(p_3)) \end{aligned}$$

es no nula y por tanto inyectiva.

Luego el código convolucional de Goppa definido por $D = p_1 \cup p_2 \cup p_3$ y $\Gamma = \langle t + s^2\rangle$ tiene longitud 3, dimensión 1 y matriz generadora

$$\mathbf{G} = \begin{pmatrix} a^4z^2 + az + a^6 & az^2 + a^2z + a^5 & a^2z^2 + a^4z + a^3 \end{pmatrix}$$

$\mathbf{G}$ es canónica, pues $mcd(a^4z^2+az+a^6, az^2+a^2z+a^5, a^2z^2+a^4z+a^3) = 1$, por tanto la memoria m y el grado δ son $m = \delta = 2$.

Utlizando la matriz de control

$$\mathbf{H} = \begin{pmatrix} az^2 + a^2z + a^5 & a^4z^2 + az + a^6 & 0 \\ a^2z^2 + a^4z + a^3 & 0 & a^4z^2 + az + a^6 \end{pmatrix}$$

calculamos su distancia libre, que coincide con la cota Singleton generalizada= 9, esto es, el código es MDS.

Ejemplo 4.5. *Código convolucional de Goppa de longitud 3, dimensión 2, memoria $m = 2$, grado $\delta = 3$ y distancia 6.*

Tomamos los mismos puntos y el mismo divisor $G = 2H_\infty$ del ejemplo anterior, y elegimos $\Gamma = \langle t, s^2 \rangle$.

La restricción del morfismo de evaluación a Γ viene dado por la matriz

$$\mathbf{G} = \begin{pmatrix} az + a^2 & a^2z + a^4 & a^4z + a \\ a^4z^2 + a & az^2 + a^2 & a^2z^2 + a^4 \end{pmatrix}$$

que es básica y reducida, luego define un $(n = 3, k = 2)$ código convolucional de memoria $m = 2$ y grado $\delta = 3$.

Una matriz de control es

$$\mathbf{H} = \begin{pmatrix} a^2z^3 + az^2 + a^4 & a^4z^3 + a^2z^2 + a & az^3 + a^4z^2 + a^2 \end{pmatrix},$$

y su distancia libre es 6, luego es MDS.

Ejemplo 4.6. *Código convolucional de Goppa de longitud 4, dimensión 1, memoria y grado $m = \delta = 2$ y distancia 12.*

Tomamos los siguientes puntos de $\mathbb{P}^2_{\mathbb{F}_8(z)}$:

$$p_1 = (a^3z + a, z + a^2),\ p_2 = (a^6z + a^2, z + a^4)$$
$$p_3 = (a^2z + a^3, z + a^6),\ p_4 = (a^5z + a^4, z + a)$$

Elegimos el subespacio $\Gamma = \langle t + s^2 \rangle \subset L(2H_\infty) = \langle 1, t, s, t^2, ts, s^2 \rangle$.

Resulta de nuevo un código MDS con matrices generadora y de control:

$$\mathbf{G} = \begin{pmatrix} z^2 + a^3z + a^3 & z^2 + a^6z + a^6 & z^2 + a^2z + a^6 & z^2 + a^5z + a^5 \end{pmatrix}$$

$$\mathbf{H} = \begin{pmatrix} z^2 + a^6z + a^6 & z^2 + a^3z + a^3 & 0 & 0 \\ z^2 + a^2z + a^6 & 0 & z^2 + a^3z + a^3 & 0 \\ z^2 + a^5z + a^5 & 0 & 0 & z^2 + a^3z + a^3 \end{pmatrix}.$$

Ejemplo 4.7. *Código convolucional de Goppa de longitud 4, dimensión 2, memoria $m = 2$, grado $\delta = 3$ y distancia 8.*

Con los puntos p_1, p_2, p_3, p_4 del ejemplo anterior y el subespacio $\Gamma = \langle t, s^2 \rangle \subset L(2H_\infty) = \langle 1, t, s, t^2, ts, s^2 \rangle$, obtenemos otro código de Goppa convolutional de parámetros $(n = 4, k = 1, m = 2, \delta = 3)$ con matriz generadora canónica $\mathbf{G}$, asociada a la restricción a Γ del morfismo de evaluación,

$$\mathbf{G} = \begin{pmatrix} a^3z + a & a^6z + a^2 & a^2z + a^3 & a^5z + a^4 \\ z^2 + a^4 & z^2 + a & z^2 + a^5 & z^2 + a^2, \end{pmatrix},$$

y matriz de control

$$\mathbf{H} = \begin{pmatrix} az^3+z^2+az+a^6 & z^3+a^4z^2+a^3z+a^4 & a^5z^3+a^6z^2+az+a & 0 \\ a^3z^3+a^5z^2+a^2z+a^2 & a^6z^3+a^3z^2+a^4z+a^4 & 0 & a^5z^3+a^6z^2+az+a \end{pmatrix}.$$

Su distancia libre es 8, alcanza la cota de Singleton generaliza, es decir, es también MDS.

4.2. Códigos convolucionales de Goppa sobre una superficie reglada

Consideremos la superficie reglada trivial $X = \mathbb{P}^1_{\mathbb{F}_q(z)} \times \mathbb{P}^1_{\mathbb{F}_q(z)}$.

Sean $\mathbb{P}^1_{\mathbb{F}_q(z)} = \operatorname{Proj} \mathbb{F}_q(z)[x_0, x_1]$, $p_\infty = (0,1)$ el punto del infinito, t la coordenada afín en la primera copia de $\mathbb{P}^1_{\mathbb{F}_q(z)}$ y s la coordenada afín en la segunda copia de $\mathbb{P}^1_{\mathbb{F}_q(z)}$.

Para cada par de enteros positivos (r, l) podemos definir el divisor G sobre $X = \mathbb{P}^1_{\mathbb{F}_q(z)} \times \mathbb{P}^1_{\mathbb{F}_q(z)}$ dado por $G = rF_1 + lF_2$, siendo F_1 y F_2 las rectas definidas por las fibras de las proyecciones $\pi_1, \pi_2 \colon \mathbb{P}^1_{\mathbb{F}_q(z)} \times \mathbb{P}^1_{\mathbb{F}_q(z)} \to \mathbb{P}^1_{\mathbb{F}_q(z)}$ en el punto del infinito, $F_1 = \pi_1^{-1}(p_\infty)$ y $F_2 = \pi_2^{-1}(p_\infty)$. Se tiene:

$$\mathcal{O}_X(G) = \pi_1^* \mathcal{O}_{\mathbb{P}^1_{\mathbb{F}_q(z)}}(rp_\infty) \otimes_{\mathcal{O}_X} \pi_2^* \mathcal{O}_{\mathbb{P}^1_{\mathbb{F}_q(z)}}(lp_\infty)$$

$$H^0(X, G) = \langle t^i \otimes s^j, 0 \le i \le r, 0 \le j \le l \rangle$$

Elijamos n puntos racionales diferentes $p_1, \ldots, p_n \in \mathbb{P}^1_{\mathbb{F}_q(z)} \times \mathbb{P}^1_{\mathbb{F}_q(z)}$ de coordenadas afines $p_i = (a_{i1}z + b_{i1}, a_{i2}z + b_{i2})$, con $a_{ij}, b_{ij} \in \mathbb{F}_q$.

Sea $G = rF_1 + lF_2$ uno de tales divisores que no pase por esos puntos p_i y sea $D = p_1 \cup \cdots \cup p_n$. En este caso, resulta:

Teorema 4.8. *Para cada subespacio Γ de $H^0(X, G)$ tal que $\Gamma \cap H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(G)) = \{0\}$, el código convolucional de Goppa $\mathcal{C}(D, \Gamma)$ definido por la imagen del morfismo de evaluación*

$$H^0(X, \mathcal{O}_X(G)) \xrightarrow{\alpha} \mathbb{F}_q(z)^n \tag{4.2.1}$$

$$t^i \otimes s^j \mapsto ((a_{11}z + b_{11})^i (a_{12}z + b_{12})^j, \ldots, (a_{n1}z + b_{n1})^i (a_{n2}z + b_{n2})^j) \tag{4.2.2}$$

tiene longitud n, dimensión $k \le (r+1)(l+1)$ y memoria $m \le r + l$. □

Veamos algunos ejemplos de Códigos convolucionales de Goppa que son óptimos:

Ejemplo 4.9. *Código convolucional de Goppa sobre* $\mathbb{F}_8 = \mathbb{F}_2[x]/x^3 + x^2 + 1$ *de longitud 3, dimensión 1, memoria y grado* $m = \delta = 3$ *y distancia 12.*

Tomemos el divisor $G = 2F_1 + F_2$ y el esquema de puntos $D = p_1 \cup p_2 \cup p_3$ siendo:

$$p_1 = (az + a^2, a^2z + a^4)\,,\ p_2 = (a^2z + a^4, a^4z + a)\,,\ p_3 = (a^4z + a, az + a^2)\,,$$

Se tiene que $H^0(X, \mathcal{O}_X(G)) = \langle 1, t \otimes 1, t^2 \otimes 1, 1 \otimes s, t \otimes s, t^2 \otimes s \rangle$.

Si consideramos el subespacio $\Gamma = \langle t \otimes 1 + t^2 \otimes s \rangle \subset H^0(X, \mathcal{O}_X(G))$, resulta que $\Gamma \cap H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(G)) = \{0\}$, pues la restricción a Γ del morfismo de evaluación 4.2.1 es no nula.

El código convolucional de Goppa definido tiene longitud 3, dimensión 1 y matriz generadora canónica

$$\mathbf{G} = \begin{pmatrix} a^4z^3 + a^6z^2 + a^2z + a^6 & az^3 + a^5z^2 + a^4z + a^5 & a^2z^3 + a^3z^2 + a^4z + a^5 \end{pmatrix}.$$

Una matriz de control es:

$$\mathbf{H} = \begin{pmatrix} az^3 + a^5z^2 + a^4z + a^5 & a^4z^3 + a^6z^2 + a^2z + a^6 & 0 \\ a^2z^3 + a^3z^2 + a^4z + a^5 & 0 & a^4z^3 + a^6z^2 + a^2z + a^6 \end{pmatrix}$$

El grado del código es 3 y su distancia alcanza la cota de Singleton generalizada, $d_{free} = 12$, es decir, el código es MDS.

Ejemplo 4.10. *Código convolucional de Goppa MDS de longitud* $n = 4$*, dimensión* $k = 1$*, memoria y grado* $m = \delta = 3$*, alfabeto* $\mathbb{F}_8 = \mathbb{F}_2[x]/x^3 + x^2 + 1$ *y distancia 16.*

Consideremos, como en el ejemplo anterior, el divisor $G = 2F_1 + F_2$ y el subespacio $\Gamma = \langle t \otimes 1 + t^2 \otimes s \rangle \subset H^0(X, \mathcal{O}_X(G)) = \langle 1, t \otimes 1, t^2 \otimes 1, 1 \otimes s, t \otimes s, t^2 \otimes s \rangle$.

Y tomemos en este caso el esquema de puntos $D = p_1 \cup p_2 \cup p_3 \cup p_4$ asociado a:

$$p_1 = (a^3z + a, z + a^2)\,,\ p_2 = (a^6z + a^2, z + a^4)\,,$$
$$p_3 = (a^2z + a^3, z + a^6)\,,\ p_4 = (a^5z + a^4, z + a)$$

La restricción a Γ del morfismo de evaluación 4.2.1 es también inyectivo y el código convolucional de Goppa definido tiene longitud 4, dimensión 1 y matriz generadora canónica

$$\mathbf{G} = \begin{pmatrix} a^6z^3 + az^2 + z + a^3 & a^5z^3 + a^2z^2 + z + a^6 & a^4z^3 + a^3z^2 + az + a^6 & a^3z^3 + a^4z^2 + z + a^5 \end{pmatrix}$$

y matriz de control

$$\mathbf{H} = \begin{pmatrix} a^5z^3 + a^2z^2 + z + a^6 & a^6z^3 + az^2 + z + a^3 & 0 & 0 \\ a^4z^3 + a^3z^2 + az + a^6 & 0 & a^6z^3 + az^2 + z + a^3 & 0 \\ a^3z^3 + a^4z^2 + z + a^5 & 0 & 0 & a^6z^3 + az^2 + z + a^3 \end{pmatrix} 0$$

El grado del código es 3 y su distancia alcanza la cota de Singleton generalizada, $d_{free} = 16$, es decir, el código es MDS.

Capítulo 5

Códigos convolucionales de Goppa sobre fibraciones

Construiremos códigos convolucionales de Goppa asociados a familias de variedades algebraicas, generalizando así los asociados a familias de curvas que hemos desarrollado en el artículo [6] y que detallaremos incluyendo además un apartado en el que se propone una interpretación geométrica de la distancia libre del código. Estudiaremos también el caso de los Códigos convolucionales de Goppa sobre las fibraciones triviales en $\mathbb{P}^1$ y $\mathbb{P}^1 \times \mathbb{P}^1$ y su relación con los códigos 2D definidos en [9, 33].

5.1. Fibraciones de variedades

Dada una variedad algebraica S sobre $\mathbb{F}_q$, una familia de variedades algebraicas proyectivas parametrizadas por S es un morfismo proyectivo y plano de variedades algebraicas $\pi : X \to S$ cuyas fibras $X_s = \pi^{-1}(s)$ son variedades lisas y geométricamente irreducibles sobre $\mathbb{F}_q(s)$ (cuerpo residual de $s \in S$).

Consideremos la familia de variedades:

$$\pi : X \to \mathbb{A}^1$$

parametrizada por la recta afín $\mathbb{A}^1 = \operatorname{Spec} \mathbb{F}_q[z]$.

Elijamos n secciones diferentes de π:

$$p_i : \mathbb{A}^1 \to X\,, \quad 1 \leq i \leq n\,,$$

donde $p_i \circ \pi = Id$ y $p_i(\mathbb{A}^1) \subset X$ una curva isomorfa a $\mathbb{A}^1$ para cada $1 \leq i \leq n$.

Consideremos el subesquema $D \subset X$ que tales secciones determinan:

$$D = p_1(\mathbb{A}^1) \cup \cdots \cup p_n(\mathbb{A}^1)$$

Sean $\mathcal{O}_D$ su haz de anillos e $\mathcal{I}_D$ su haz de ideales, como hemos definido en el capítulo 4.

La restricción de π a D es un morfismo plano de grado n sobre $\mathbb{A}^1$ y por tanto $H^0(X, \mathcal{O}_D)$ es un $\mathbb{F}_q[z]$-módulo libre de rango n.

Observemos también que si η es el punto genérico de $\mathbb{A}^1$, la fibra $X_\eta = \pi^{-1}(\eta)$ es una variedad algebraica lisa sobre el cuerpo $\mathbb{F}_q(z)$ y $p_1(\eta), \ldots, p_n(\eta)$ son n puntos racionales diferentes de la variedad X_η, luego $H^0(X, \mathcal{O}_D)_\eta$ como $\mathbb{F}_q(z)$-álgebra es canónicamente isomorfa a $\mathbb{F}_q(z)^n$:

$$H^0(X, \mathcal{O}_D)_\eta \simeq \mathbb{F}_q(z)^n \,.$$

Para cada haz invertible $\mathcal{L}$, tensorializando la sucesión exacta

$$0 \to \mathcal{I}_D \to \mathcal{O}_X \to \mathcal{O}_D \to 0 \,. \tag{5.1.1}$$

se obtiene la sucesión exacta de haces sobre X

$$0 \to \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{L} \to \mathcal{L} \to \mathcal{L}_D = \mathcal{O}_D \otimes_{\mathcal{O}_X} \mathcal{L} \to 0 \,, \tag{5.1.2}$$

donde la restricción de $\mathcal{L}$ a D, $\mathcal{L}_D$, es trivial, esto es $\mathcal{L}_D \simeq \mathcal{O}_D$.

Y tomando cohomología en la sucesión 5.1.2 resulta la sucesión exacta larga de $\mathbb{F}_q[z]$-módulos:

$$\begin{aligned} 0 \to H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{L}) \to H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \to \\ \to H^1(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{L}) \to H^1(X, \mathcal{L}) \to 0 \,, \end{aligned} \tag{5.1.3}$$

que localizada en el punto genérico $\eta \in \mathbb{A}^1$ da la sucesión de $\mathbb{F}_q(z)$-espacios vectoriales:

$$\begin{aligned} 0 \to H^0(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{L})_\eta \to H^0(X, \mathcal{L})_\eta \xrightarrow{\alpha_\eta} H^0(X, \mathcal{O}_D)_\eta \to \\ \to H^1(X, \mathcal{I}_D \otimes_{\mathcal{O}_X} \mathcal{L})_\eta \to H^1(X, \mathcal{L})_\eta \to 0 \,, \end{aligned} \tag{5.1.4}$$

donde $H^0(X, \mathcal{O}_D)_\eta$ como $\mathbb{F}_q(z)$-álgebra es canónicamente isomorfa a $\mathbb{F}_q(z)^n$:

$$H^0(X, \mathcal{O}_D)_\eta \simeq \mathbb{F}_q(z)^n$$

Ahora podemos dar una primera definición de código convolucional de Goppa asociado a $\mathcal{L}$ y a D en términos de espacios vectoriales.

Definición 5.1. El código convolucional de Goppa asociado a $\mathcal{L}$ and D es la imagen del morfismo α_η

$$\mathcal{C}(\mathcal{L}, D) = \mathrm{Im}\left(H^0(X, \mathcal{L})_\eta \xrightarrow{\alpha_\eta} H^0(X, \mathcal{O}_D)_\eta \simeq \mathbb{F}_q(z)^n\right) .$$

Dado un submódulo libre $\Gamma \subseteq H^0(X, \mathcal{L})$, el código convolucional de Goppa asociado a Γ and D es la imagen del morfismo $\alpha_{\eta_{|\Gamma_\eta}}$

$$\mathcal{C}(\Gamma, D) = \mathrm{Im}\left(\Gamma_\eta \xrightarrow{\alpha_\eta} \mathbb{F}_q(z)^n\right) .$$

Cada matriz que representa a α_η (respectivamente $\alpha_{\eta_{|\Gamma_\eta}}$) es una matriz generadora de funciones racionales para el código $\mathcal{C}(\mathcal{L}, D)$ (resp. $\mathcal{C}(\Gamma, D)$).

Observación 5.2. Los códigos $\mathcal{C}(\mathcal{L}, D)$ y $\mathcal{C}(\Gamma, D)$ son Códigos convolucionales de Goppa sobre la fibra X_η, pero en general no todos los Códigos convolucionales de Goppa definidos sobre la variedad X_η (capítulo 4) proceden de uno de estos.

Observación 5.3. El isomorfismo canónico $H^0(X, \mathcal{O}_D)_\eta \simeq \mathbb{F}_q(z)^n$ como $\mathbb{F}_q(z)$-álgebras no extiende en general a un isomorfismo $H^0(X, \mathcal{O}_D) \simeq \mathbb{F}_q[z]^n$ como anillos; de hecho, extiende siempre que $p_1(\mathbb{A}^1), \dots p_n(\mathbb{A}^1)$ sean secciones disjuntas. No obstante, como $H^0(X, \mathcal{O}_D)$ es un módulo libre de rango n siempre existen trivializaciones $H^0(X, \mathcal{O}_D) \overset{\phi}{\xrightarrow{\sim}} \mathbb{F}_q[z]^n$, aunque no en general morfismos de anillos.

Teniendo en cuenta la observación 5.3, daremos una nueva defición de código convolucional asociado a una fibración de variedades en términos de submódulos.

Definición 5.4. Dada una trivialización $\phi\colon H^0(X, \mathcal{O}_D) \xrightarrow{\sim} \mathbb{F}_q[z]^n$ como $\mathbb{F}_q[z]$-módulos, se define el código convolucional de Goppa $\mathcal{C}(\mathcal{L}, D, \phi)$ como el submódulo imagen del morfismo $\phi \circ \alpha$

$$H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \overset{\phi}{\xrightarrow{\sim}} \mathbb{F}_q[z]^n .$$

Analogamente, se define el código convolucional de Goppa $\mathcal{C}(\Gamma, D, \phi)$ relativo al submódulo $\Gamma \subseteq H^0(X, \mathcal{L})$.

Cada matriz que representa a α (resp. $\alpha_{|\Gamma_\eta}$) es una matriz generadora de funciones polinómicas para el código $\mathcal{C}(\mathcal{L}, D, \phi)$ (resp. $\mathcal{C}(\Gamma, D, \phi)$).

5.2. Fibraciones de curvas

Consideremos una familia de curvas $\pi : X \to \mathbb{A}^1$ y n secciones diferentes $p_i : \mathbb{A}^1 \to X$.

En este caso, $D = p_1(\mathbb{A}^1) \cup \cdots \cup p_n(\mathbb{A}^1)$ es un divisor de Cartier sobre X, su haz de ideales es $\mathcal{I}_D = \mathcal{O}_X(D)$ y la sucesión exacta larga de $\mathbb{F}_q[z]$-módulos (5.1.3) se escribe:

$$0 \to H^0(X, \mathcal{L}(-D)) \to H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \to H^1(X, \mathcal{L}(-D)) \to \\ \to H^1(X, \mathcal{L}) \to 0\,. \tag{5.2.1}$$

Proposición 5.5. *Sea r el grado de $\mathcal{L}$ en cada fibra $X_u = \pi^{-1}(u)$, con $u \in \mathbb{A}^1$, y g el género de cada fibra, ambos independientes de la fibra. Se verifica:*

(a) Si $2g-2 < r$, se tiene que $H^1(X, \mathcal{L}) = 0$ y $H^0(X, \mathcal{L})$ es un $\mathbb{F}_q[z]$-módulo libre de rango $1 - g + r$.

(b) Si $r < n$, se cumple que $H^0(X, \mathcal{L}(-D) = 0$ y $H^1(X, \mathcal{L}(-D)$ es un $\mathbb{F}_q[z]$-módulo libre de rango $n - r + g - 1$.

(c) Si $2g - 2 < r < n$, se tiene la siguiente sucesión exacta de $\mathbb{F}_q[z]$-módulos:

$$0 \to H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \to H^1(X, \mathcal{L}(-D)) \to 0\,, \tag{5.2.2}$$

que sigue siendo exacta en cada fibra X_u.

Demostración.

(a) Si $2g - 2 < r$ es $H^1(X_u, \mathcal{L}_{X_u}) = 0$ para cada $u \in \mathbb{A}^1$, luego la función $u \to h^0(X_u, \mathcal{L}_{X_u}) = 1 - g + r$ es constante y aplicando el ([16] III Corollary 12.9) se concluye.

(b) Si $r < n$ es $H^0(X_u, \mathcal{L}(-D)_{X_u} = 0$ para cada $u \in \mathbb{A}^1$, por tanto $h^1(X_u, \mathcal{L}(-D)_{X_u}) = -1 + g + n - r$ es constante y de nuevo por ([16] III Corollary 12.9) se acaba.

(c) Se sigue de la sucesión exacta larga 5.2.1 y de los dos apartados anteriores.

□

Como consecuencia directa de la Proposición 5.5 y de la definición de matriz generadora básica de un código convolucional se obtiene:

Corolario 5.6. *Bajo las condiciones* $2g-2 < r < n$ *el código convolucional de Goppa* $\mathcal{C}(\mathcal{L}, D, \phi)$ *tiene dimensión* $k = r - g + 1$ *y longitud* n.
Cada matriz asociada al morfismo $\phi \circ \alpha$ *es una matriz generadora básica de* $\mathcal{C}(\mathcal{L}, D, \phi)$.

Por último, y en las hipótesis anteriores, veamos qué condición se debe cumplir para que sea básica una matriz generadora del código convolucional de Goppa $\mathcal{C}(\Gamma, D, \phi)$ definido por un submódulo $\Gamma \subseteq H^0(X, \mathcal{L})$ y una trivialización ϕ.

Proposición 5.7. *Cada matriz asociada a* $\phi \circ \alpha_{|_\Gamma}$ *es una matriz generadora básica del código convolucional de Goppa* $\mathcal{C}(\Gamma, D, \phi)$ *si y sólo si* $H^0(X, \mathcal{L})/\Gamma$ *es u* $\mathbb{F}_q[z]$*-módulo libre de torsión.*

Demostración. La sucesión (5.2.2) induce un diagrama

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \Gamma & \xrightarrow{\alpha_{|_\Gamma}} & H^0(X, \mathcal{O}_D) & \longrightarrow & H^1(X, \Gamma) & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow & & \\
0 & \longrightarrow & H^0(X, \mathcal{L}) & \longrightarrow & H^0(X, \mathcal{O}_D) & \longrightarrow & H^1(X, \mathcal{L}(-D)) & \longrightarrow & 0 \\
 & & \downarrow & & & & \downarrow & & \\
 & & H^0(X, \mathcal{L})/\Gamma & & & & 0 & &
\end{array}$$

Se deduce que el núcleo de $H^1(X, \Gamma) \to H^1(X, \mathcal{L}(-D))$ es isomorfo a $H^0(X, \mathcal{L})/\Gamma$ y $H^1(X, \mathcal{L}(-D))$ es libre. Luego los elementos de torsión de $H^1(X, \Gamma)$ están contenidos en $H^0(X, \mathcal{L})/\Gamma$, lo que permite concluir. □

5.2.1. Códigos asociados a fibraciones de rectas proyectivas

Sea $\mathbb{P}^1 = \operatorname{Proj} \mathbb{F}_q[x_0, x_1]$ la recta proyectiva sobre $\mathbb{F}_q$, $t = x_1/x_0$ su coordenada afín y p_∞ el punto del infinito.

Elijamos la fibración trivial:

$$X = \mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{\pi} \mathbb{A}^1$$

y n secciones diferentes de ella

$$p_i \colon \mathbb{A}^1 \to \mathbb{P}^1 \times \mathbb{A}^1$$

definidas en las coordenadas (t, z) por

$$p_i(z) = (\alpha_i z + \beta_i, z)\,,\ \alpha_i, \beta_i \in \mathbb{F}_q\,.$$

Consideremos el divisor D y el haz invertible $\mathcal{L}$ sobre X dados por:

$$D = p_1(\mathbb{A}^1) + \cdots + p_n(\mathbb{A}^1)\,, \quad \mathcal{L} = \pi_1^* \mathcal{O}_{\mathbb{P}^1}(r p_\infty) \otimes_{\mathbb{F}_q} \mathbb{F}_q[z]\,.$$

La sucesión exacta (5.2.2) es en este caso:

$$\begin{array}{ccccccc} 0 \to H^0(X, \mathcal{L}) & \xrightarrow{\quad\alpha\quad} & H^0(X, \mathcal{O}_D) & \longrightarrow & H^1(X, \mathcal{L}(-D)) & \longrightarrow & 0\,. \\ \| & & \| & & & & \\ H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(r p_\infty)) \otimes \mathbb{F}_q[z] & \xrightarrow{\alpha} & \mathbb{F}_q[z]^n & & & & \end{array}$$

Localizando en el punto genérico η, el morfismo α_η es el morfismo de evaluación en los puntos $p_1(\eta), \ldots, p_n(\eta)$:

$$H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(r p_\infty)) \otimes_{\mathbb{F}_q} \mathbb{F}_q(z) \xrightarrow{\alpha_\eta} \mathbb{F}_q(z)^n$$

dado por:

$$\alpha_\eta(t^j) = \big(t^j(p_1(\eta)), \ldots, t^j(p_n(\eta))\big) = \big((\alpha_1 z + \beta_1)^j, \ldots, (\alpha_n z + \beta_n)^j\big)\,,$$

siendo $\{1, t, \ldots, t^r\}$ la base de $H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(r p_\infty))$ respecto de la coordenada afín t de $\mathbb{P}^1$.

Si $\Gamma \subseteq H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(rp_\infty))$ es el subespacio generado por $\{t^s, \ldots, t^r\}$, el código convolucional de Goppa $\mathcal{C}(\Gamma, D)$ es la imagen del morfismo

$$\begin{aligned} \alpha_\eta \colon \Gamma \otimes_{\mathbb{F}_q} \mathbb{F}_q(z) &\to \mathbb{F}_q(z)^n \\ t^j &\longmapsto \alpha_\eta(t^j)\,, \quad \text{for } s \leq j \leq r\,. \end{aligned}$$

En este caso, $H^0(X, \mathcal{L})/\Gamma \simeq (H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(rp_\infty))/\Gamma) \otimes_{\mathbb{F}_q} \mathbb{F}_q[z]$ no tiene torsión, luego por la Proposición **??** cada matriz asociada a

$$\alpha \colon \Gamma \otimes_{\mathbb{F}_q} \mathbb{F}_q[z] \to H^0(X, \mathcal{O}_D)$$

es una matriz generadora básica del código.

5.2.2. Interpretación geométrica de la distancia libre

Consideremos el código convolucional de Goppa $\mathcal{C}(\mathcal{L}, D)$ definido sobre la fibración de curvas $\pi : X \to \mathbb{A}^1$ por n secciones diferentes $p_i : \mathbb{A}^1 \to X$ y un haz invertible muy amplio $\mathcal{L}$ sobre X.

Sea C_{p_i} la curva de la fibración definida por la imagen de la sección $p_i : \mathbb{A}^1 \to X$ y q_0 la intersección de C_p con la fibra en el origen, esto es, $q_0 = p_i(0)$.

Como $\mathcal{L}$ es muy amplio se tiene una inmersión cerrada:

$$\begin{aligned} X &\hookrightarrow \mathbb{P}H^0(X, \mathcal{L})^* = \mathbb{P}^{r-g} \times \mathbb{A}^1 \\ p &\to \langle \omega_p \rangle\,, \end{aligned}$$

donde ω_p viene definida por

$$\begin{aligned} H^0(X, \mathcal{L}) &\xrightarrow{\omega_p} \mathbb{F}_q[z] \\ f &\to f(p)\,. \end{aligned}$$

Si representamos por $\pi_r(q_0)$ el r-ésimo plano osculador de la curva C_p en el punto q_0, se tiene:

$$\pi_0(q_0) = q_0 \subset \pi_1(q_0) \subset \pi_2(q_0) \subset \cdots \subset \pi_s(q_0) \subset \cdots\,,$$

y para cada $f \in H^0(X, \mathcal{L})$ su evaluación en p, $f(p)$, viene dada por

$$f(p) = f_0 + f_1 z + \cdots + f_n z^n\,,$$

donde $f_0 = f(0)$ y f_s puede ser interpretado como el coeficiente s-ésimo del desarrollo de Taylor de f en el punto q_0.

De lo que se deduce que $f_s = 0$ si y solo si

$$H_f \cap \pi_s(q_0) \neq \emptyset \text{ and } H_f \cap \pi_{s-1}(q_0) \subsetneqq H_f \cap \pi_s(q_0)\,,$$

donde H_f es el hiperplano que la sección f define.

Por tanto, el problema de calcular el número de coeficientes no nulos de $f(p)$ y así la distancia libre del código se convierte en un problema de geometría enumerativa sobre un cuerpo finito.

5.3. Códigos definidos por fibraciones triviales de variedades

Sean t y s las respectivas coordenadas afines de las primera y segunda copias de $\mathbb{P}^1 = \mathbb{P}^1_{\mathbb{F}_q}$.

Consideremos la fibración trivial:

$$X = \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{\pi} \mathbb{A}^1$$

y las secciones

$$p_i \colon \mathbb{A}^1 \to \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{A}^1$$

definidas en las coordenadas (t, s, z) por

$$p_i(z) = (\alpha_{i,1} z + \beta_{i,1}, \alpha_{i,2} z + \beta_{i,2}, z)\,,\ \alpha_{i,j}, \beta_{i,j} \in \mathbb{F}_q\,,\ 1 \leq i \leq n\,,\ j = 1, 2$$

Para cada par de enteros positivos (r, l), sea $\mathcal{L}$ el haz invertible sobre X dado por

$$\mathcal{L} = \pi_1^* \mathcal{O}_{\mathbb{P}^1}(r p_\infty) \otimes_{\mathbb{F}_q} \pi_2^* \mathcal{O}_{\mathbb{P}^1}(l p_\infty) \otimes_{\mathbb{F}_q} \mathbb{F}_q[z]\,,$$

para sus secciones globales se tiene:

$$H^0(X, \mathcal{L}) = H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(r p_\infty)) \otimes H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(l p_\infty)) \otimes \mathbb{F}_q[z]\,.$$

Si $D = p_1(\mathbb{A}^1) + \cdots + p_n(\mathbb{A}^1)$ el morfismo α de la sucesión exacta (5.2.2) es en este segundo caso:

$$H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(r p_\infty)) \otimes H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(l p_\infty)) \otimes \mathbb{F}_q[z] \xrightarrow{\alpha} \mathbb{F}_q[z]^n\,.$$

Como antes, tomando fibras en el punto genérico, el morfismo de evaluación $H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(rp_\infty)) \otimes H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(lp_\infty)) \otimes \mathbb{F}_q(z) \xrightarrow{\alpha_\eta} \mathbb{F}_q(z)^n$ en los puntos $p_1(\eta), \ldots, p_n(\eta)$ es:

$$\alpha_\eta(t^i \otimes s^j) = \left((\alpha_{1,1}z + \beta_{1,1})^i(\alpha_{1,2}z + \beta_{1,2})^j, \ldots, (\alpha_{n,1}z + \beta_{n,1})^i(\alpha_{n,2}z + \beta_{n,2})^j\right) .$$

Análogamente, si Γ es un subespacio de $H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(rp_\infty)) \otimes H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(lp_\infty))$, el código convolucional de Goppa $\mathcal{C}(\Gamma, D)$ es la imagen del morfismo

$$\alpha_\eta \colon \Gamma \otimes_{\mathbb{F}_q} \mathbb{F}_q(z) \to \mathbb{F}_q(z)^n$$

Y también en este caso, $H^0(X, \mathcal{L})/\Gamma$ no tiene torsión, por tanto cada matriz asociada a

$$\alpha \colon \Gamma \otimes_{\mathbb{F}_q} \mathbb{F}_q[z] \to H^0(X, \mathcal{O}_D)$$

es una matriz generadora básica del código.

5.3.1. Códigos 2D

En el procesamiento de imágenes digitales se necesita codificar datos que dependen no sólo del tiempo sino también de otras variables independientes, como pueden ser la intensidad, brillo, saturación, etc. Es la teoría de sistemas lineales discretos multivariantes, cuyas matrices de transferencia tienen coeficientes en el anillo de polinomios $\mathbb{F}_q[z_1, z_2, \ldots, z_m]$ o en su cuerpo de fracciones $\mathbb{F}_q(z_1, z_2, \ldots, z_m)$, la que permite, en muchos casos, describir y estudiar este proceso.

Así como los códigos convolucionales que hemos estudiado se corresponden con los sistemas lineales discretos respecto del tiempo (una única variable), una generalización natural son los códigos convolucionales multivariantes o códigos mD asociados a los sistemas lineales multivariantes. En este sentido, nuestros códigos convolucionales son códigos $1D$ y, dado que éstos son subespacios de $\mathbb{F}_q(z)^n$, podemos definir un código mD como un subespacio de $\mathbb{F}_q(z_1, z_2, \ldots, z_m)^n$. Es claro que el estudio de estos nuevos códigos presenta mayor dificultad que el de los 1D pues las propiedades del anillo $\mathbb{F}_q[z_1, z_2, \ldots, z_m]$ no son las mismas que las de $\mathbb{F}_q[z]$; baste notar, por ejemplo, que todo submódulo de $\mathbb{F}_q[z_1, z_2, \ldots, z_m]$ es finito generado pero, en general, no es libre.

Fornasini y Valcher, siguiendo el desarrollo algebraico de Forney para los códigos convolucionales, definen y estudian los códigos $2D$ [9, 33].

Utilizaremos como definición de código $2D$ la siguiente:

Definición 5.8. Un *código* $2D$ con alfabeto $\mathbb{F}_q$ y longitud n es un subespacio de $\mathbb{F}_q(z,\bar{z})^n$; la dimensión del código es su dimensión como subespacio.

En términos de módulos, un código libre modular 2D de longitud n y dimensión k es un submódulo libre de $\mathbb{F}_q[z,\bar{z},z^{-1},\bar{z}^{-1}]^n$ de rango k (free modular code, Fornasini). Estos códigos 2D son un caso particular de los anteriores.

Desarrollamos a continuación un ejemplo de código $2D$ obtenido a partir de dos códigos convolucionales de Goppa definidos sobre fibraciones triviales.

Para ello, comenzamos factorizando la proyección $\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{A}^1 \xrightarrow{\pi} \mathbb{A}^1$ como composición de las proyecciones:

$$\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{A}^1 \xrightarrow{\pi_{23}} \mathbb{P}^1\times\mathbb{A}^1 \xrightarrow{\pi_2} \mathbb{A}^1\,.$$

Consideremos ahora las n secciones p_i de la proyección $\mathbb{P}^1\times\mathbb{A}^1 \xrightarrow{\pi_2} \mathbb{A}^1$ definidas en coordenadas por:

$$\mathbb{A}^1 \xrightarrow{p_i} \mathbb{P}^1\times\mathbb{A}^1\,,\quad p_i(z)=(\alpha_{i2}z+\beta_{i2},z)\,,\ \alpha_{i2},\beta_{i2}\in\mathbb{F}_q\,,\ 1\le i\le n\,,$$

y elijamos n secciones distintas q_i de $\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{A}^1 \xrightarrow{\pi_{23}} \mathbb{P}^1\times\mathbb{A}^1$ dadas por:

$$\begin{aligned} q_i\colon \mathbb{P}^1\times\mathbb{A}^1 &\to \mathbb{P}^1\times\mathbb{P}^1\times\mathbb{A}^1\\ (s,z) &\to (\alpha_{i1}z+\beta_{i1}+s,s,z)\,,\quad \alpha_{i1},\beta_{i1}\in\mathbb{F}_q\,,\ 1\le i\le n\,, \end{aligned}$$

siendo s la coordenada afín en la segunda copia de $\mathbb{P}^1$.

Componiendo obtenemos n secciones diferentes $\bar{p}_i = q_i\circ p_i$ de la proyección $\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{A}^1 \xrightarrow{\pi} \mathbb{A}^1$ definidas por:

$$\begin{aligned} \bar{p}_i\colon \mathbb{A}^1 &\to \mathbb{P}^1\times\mathbb{P}^1\times\mathbb{A}^1\\ z &\to (\alpha_{i,1}z+\beta_{i,1}+\alpha_{i,2}z+\beta_{i,2},\alpha_{i,2}z+\beta_{i,2},z)\\ &\quad \text{con } \alpha_{i,j},\beta_{i,j}\in\mathbb{F}_q\,,\ 1\le i\le n\,,\ j=1,2 \end{aligned}$$

La evaluación de $H^0(\mathbb{P}^1,\mathcal{O}_{\mathbb{P}^1}(rp_\infty)\otimes\mathbb{F}_q[s]\otimes\mathbb{F}_q[z]$ en las secciones $q_1,\dots,q_n$ está determinada por:

$$t^i(q_1,\dots,q_n)=\left((\alpha_{11}z+\beta_{11}+s)^i,\dots,(\alpha_{n1}z+\beta_{n1}+s)^i\right)\,,\ 0\le i\le r$$

y permite definir subespacios de $\mathbb{F}_q(s,z)^n$, es decir, códigos 2D de longitud n. Sin embargo, la evaluación en las secciones p_i y $\bar{p}_i$ definen códigos convolucionales de Goppa de los tipos (5.2.1) y (5.3).

Otro objetivo para un futuro trabajo es estudiar las propiedades de los códigos $2D$ así obtenidos a partir de nuestros códigos convolucionales de Goppa definidos sobre fibraciones.

Bibliografía

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] C. Berrou, A. Glavieux, and Thitimajshima, *Near shannon limit error-correcting coding and decoding: Turbo codes*, Proc. I.E.E.E., (1983), pp.–.

[3] N. Bourbaki, *Elements of mathematics. Commutative algebra*, Hermann, Paris, 1972. Translated from the French.

[4] J.-J. Climent, D. Napp, C. Perea, and R. Pinto, *A construction of MDS 2D convolutional codes of rate* $1/n$ *based on superregular matrices*, Linear Algebra Appl., 437 (2012), pp. 766–780.

[5] J. I. I. Curto, Á. L. M. Castañeda, J. M. M. Porras, and G. S. Sotelo, *Every convolutional code is a Goppa code*, IEEE Trans. Inform. Theory, 59 (2013), pp. 6628–6641.

[6] J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo, *Convolutional codes of Goppa type*, Appl. Algebra Engrg. Comm. Comput., 15 (2004), pp. 51–61.

[7] ——, *One dimensional convolutional Goppa codes over the projective line*, Preprint available at arXiv:1107.2059, (2011).

[8] P. Elias, *Coding for noisy channels*, I.R.E. Nat. Conv. Record, 3 (1955), pp. 34–45.

[9] E. Fornasini and M. E. Valcher, *Algebraic aspects of two-dimensional convolutional codes*, IEEE Trans. Inform. Theory, 40 (1994), pp. 1068–1082.

[10] G. D. Forney, Jr., *The Viterbi algorithm*, Proc. IEEE, 61 (1973), pp. 268–278.

[11] G. D. Forney Jr, *Convolutional codes I: Algebraic structure*, I.E.E.E. Trans. Inform. Theory, 16 (1970), pp. 720–738.

[12] H. Gluesing-Luerssen and B. Langfeld, *A class of one-dimensional MDS convolutional codes*, J. Algebra Appl., 5 (2006), pp. 505–520.

[13] V. D. Goppa, *Codes that are associated with divisors*, Problemy Peredači Informacii, 13 (1977), pp. 33–39.

[14] ——, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR, 259 (1981), pp. 1289–1290.

[15] ——, *Algebraic-geometric codes*, Izv. Akad. Nauk SSSR Ser. Mat., 46 (1982), pp. 762–781, 896.

[16] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.

[17] J. I. Iglesias Curto, J. M. Muñoz Porras, F. J. Plaza Martín, and G. Serrano Sotelo, *Convolutional Goppa codes defined on fibrations*, Appl. Algebra Engrg. Comm. Comput., 23 (2012), pp. 165–178.

[18] J. Justesen and L. R. Hughes, *On maximum-distance-separable convolutional codes*, IEEE Trans. Information Theory, IT-20 (1974), p. 288.

[19] T. Kailath, *Linear systems*, Prentice-Hall Inc., Englewood Cliffs, N.J., 1980. Prentice-Hall Information and System Sciences Series.

[20] R. E. Kalman, *Advanced theory of linear systems*, in Topics in Mathematical System Theory, McGraw-Hill, New York, 1969, pp. 237–339.

[21] R. E. Kalman, P. L. Falb, and M. A. Arbib, *Topics in mathematical system theory*, McGraw-Hill Book Co., New York, 1969.

[22] K. Lumbrad and R. J. McEliece, *Counting minimal generator matrices*. 1995.

[23] J. Massey and M. Sain, *Codes, automata, and continuous systems: Explicit interconnections*, IEEE Transactions on Automatic Control, AC-12 (1967), pp. 644–650.

[24] R. J. McEliece, *The algebraic theory of convolutional codes*, in Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1065–1138.

[25] R. J. McEliece, *The theory of information and coding*, vol. 86 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, second ed., 2002.

[26] J. M. Muñoz Porras, J. A. Domínguez Pérez, J. I. Iglesias Curto, and G. Serrano Sotelo, *Convolutional Goppa codes*, IEEE Trans. Inform. Theory, 52 (2006), pp. 340–344.

[27] J. M. Muñoz Porras and J. I. Iglesias Curto, *Classification of convolutional codes*, Linear Algebra Appl., 432 (2010), pp. 2701–2725.

[28] D. Napp, C. Perea, and R. Pinto, *Input-state-output representations and constructions of finite support 2D convolutional codes*, Adv. Math. Commun., 4 (2010), pp. 533–545.

[29] P. Piret, *Convolutional codes*, MIT Press, Cambridge, MA, 1988. An algebraic approach.

[30] F. J. Plaza-Martín, J. I. Iglesias-Curto, and G. Serrano-Sotelo, *On the construction of 1-D MDS convolutional Goppa codes*, IEEE Trans. Inform. Theory, 59 (2013), pp. 4615–4625.

[31] J. Rosenthal and R. Smarandache, *Maximum distance separable convolutional codes*, Appl. Algebra Engrg. Comm. Comput., 10 (1999), pp. 15–32.

[32] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J., 27 (1948), pp. 379–423, 623–656.

[33] M. E. Valcher and E. Fornasini, *On 2D finite support convolutional codes: an algebraic approach*, Multidimens. Systems Signal Process., 5 (1994), pp. 231–243.

[34] A. J. Viterbi, *Error bounds far convolutional codes and an asymptotically optimum decoding algorithm*, IEEE Trans. Information Theory, IT-13 (1967), pp. 260–269.