XX Congreso de Ecuaciones Diferenciales y Aplicaciones
X Congreso de Matemática Aplicada
Sevilla, 24-28 septiembre 2007
(pp. 1–8)

Las matrices de Toeplitz en la construcción de códigos convolucionales perforados

V. Herranz[1], C. Perea[1],

[1] *Dpto. Estadística, Matemáticas e Informática, Universidad Miguel Hernández, Avda. Universidad, s/n E-03202 Elche. E-mails:* mavi.herranz@umh.es, perea@umh.es.

Palabras clave: Código convolucional, código perforado, código convolucional fuertemente MDS, representación entrada-estado-salida.

Resumen

En este trabajo presentamos la modelización de la técnica de perforación de códigos convolucionales introducida por McEliece desde el punto de vista de sistemas. Aplicando esta técnica a un $(2, 1, 1)$-código convolucional óptimo y teniendo en cuenta las propiedades de las matrices de Toeplitz, construimos un nuevo $(3, 2, 1)$-código óptimo.

1. Introducción

Los códigos convolucionales se emplean en muchas ocasiones para transferencia de datos con alta exigencia en la velocidad. Para ello, se requieren códigos potentes de tasas elevadas. Ahora bien, la complejidad de decodificación de códigos convolucionales con tasa elevada empleando una decodificación de máxima verosimilitud (en inglés, *Maximum Likehood Decoding*, MLD), o un algoritmo de decodificación (como por ejemplo, el algoritmo de Viterbi) o bien una decodificación a posteriori (en inglés, *Maximum A-Posteriori Probability*, MAP), crece exponencialmente con la tasa del código. La técnica de perforación de un código convolucional introducida por Cain, Clark y Geist [1] en 1979, soluciona este problema. En general, la técnica de perforación consiste en eliminar periódicamente dígitos codificados de las palabras código. De este modo, se consigue reducir el número de dígitos codificados correspondientes a dígitos de entrada, es decir, se aumenta la tasa del código. Este método ha sido muy empleado, ya que los mejores códigos construidos por perforación son más potentes que otros códigos con los mismos parámetros, y son considerablemente más fáciles de implementar que los códigos no perforados. En este trabajo, utilizamos la técnica de perforación introducida por McEliece [3], que describimos en la sección siguiente, junto con conceptos y avances recientes relacionados con la representación de códigos

convolucionales desde el punto de vista de sistemas. En la sección 3, introducimos la representación entrada-estado-salida del código obtenido por descomposición en bloques, como paso previo a la perforación. Finalmente, en la sección 4 presentamos, a partir de un código original óptimo, la construcción de un código perforado también óptimo empleando propiedades de las matrices de Toeplitz.

2. Resultados preliminares

Sea $\mathbb{F} = GF(q)$ el cuerpo de Galois de q elementos y $\mathbb{F}[z]$ el anillo de polinomios en la variable z con coeficientes en $\mathbb{F}$. Consideremos las matrices $A \in \mathbb{F}^{\delta\times\delta}$, $B \in \mathbb{F}^{\delta\times k}$, $C \in \mathbb{F}^{(n-k)\times\delta}$ y $D \in \mathbb{F}^{(n-k)\times k}$. Un *código convolucional* de tasa k/n y *complejidad* δ puede ser descrito por el sistema lineal gobernado por las ecuaciones

$$\begin{aligned} x_{t+1} &= Ax_t + Bu_t, \\ y_t &= Cx_t + Du_t, \\ v_t &= \begin{pmatrix} y_t \\ u_t \end{pmatrix}, \quad x_0 = 0, \end{aligned} \tag{1}$$

siendo $x_t \in \mathbb{F}^\delta$ *vector de estados*, $u_t \in \mathbb{F}^k$ el *vector información*, $y_t \in \mathbb{F}^{n-k}$ el *vector de paridad* y $v_t \in \mathbb{F}^n$ el *vector código* o *palabra código*, para cada instante t. Esta representación es conocida como la *representación entrada-estado-salida*.

El conjunto de todas las palabras código de peso finito generado por las matrices (A, B, C, D) tiene una estructura de módulo sobre el anillo de polinomios $\mathbb{F}[z]$, que denotaremos por $\mathcal{C}(A, B, C, D)$. Como $\mathbb{F}[z]$ es un dominio de ideales principales, $\mathcal{C}(A, B, C, D)$ es un módulo libre de rango k, y, por tanto, existe una matriz polinómica $G(z)$ de tamaño $n \times k$ tal que

$$\mathcal{C}(A, B, C, D) = \{v(z) \in \mathbb{F}^n[z] \mid v(z) = G(z)u(z) \quad \text{con} \quad u(z) \in \mathbb{F}^k[z]\}.$$

Decimos entonces que $G(z)$ es una *matriz generadora* del código convolucional $\mathcal{C}(A, B, C, D)$. En lo que sigue, adoptamos la notación introducida por McEliece [3] y nos referiremos a un código convolucional de tasa k/n y complejidad δ como un (n, k, δ)-código.

Decimos que el código $\mathcal{C}$ es *observable* [5] si una y, por tanto, cualquier otra matriz generadora, es prima por la derecha, es decir, sus menores de tamaño $k \times k$ son no nulos y tienen factores comunes no triviales (considerando los factores de la forma z^s, con $s \in \mathbb{N}$, como triviales).

Si denotamos por $\mathrm{wt}(v)$ el peso de Hamming del vector v, tenemos la caracterización siguiente de la j-ésima *distancia columna* del código convolucional $\mathcal{C}(A, B, C, D)$, que denotamos por $d_j^c(\mathcal{C})$, en términos de la representación entrada-estado-salida

$$d_j^c(\mathcal{C}) = \min_{u_0 \neq 0} \left(\sum_{t=0}^{j} \mathrm{wt}(u_t) + \sum_{t=0}^{j} \mathrm{wt}(y_t) \right) \qquad \text{para } j = 0, 1, 2 \ldots \tag{2}$$

Definimos la *distancia libre* del código convolucional $\mathcal{C}(A, B, C, D)$, denotada por $d_{free}(\mathcal{C})$, como

$$d_{free}(\mathcal{C}) = \lim_{j\to\infty} d_j^c(\mathcal{C}) \tag{3}$$

Rosenthal y Smarandache [6] proporcionan una cota superior para la distancia libre, denominada *cota Singleton generalizada*. Si $\mathcal{C}$ es un (n,k,δ)-código sobre un cuerpo cualquiera $\mathbb{F}$, entonces

$$d_{free}(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{4}$$

Con estos preliminares, podemos dar las siguientes definiciones.

Definición 1 (Definición 1.8 de [2]) *Sea $\mathcal{C}$ un (n,k,δ)-código.*

1. *$\mathcal{C}$ es un código convolucional MDS (Maximum Distance Separable) si su distancia libre $d_{free}(\mathcal{C})$ alcanza la cota Singleton generalizada (4).*

2. *$\mathcal{C}$ es un código convolucional fuertemente MDS si*

$$d_M^c = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1 \quad \textit{para } M = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lceil \frac{\delta}{n-k} \right\rceil \tag{5}$$

Tenemos la siguiente caracterización de un (n,k,δ)-código fuertemente MDS en términos de la representación entrada-estado-salida, para el caso particular en que $n-k$ divida a δ .

Teorema 1 (Corolario 2.5 de [2]) *Sean n, k y δ tales que $n-k$ divide a δ. Entonces, las matrices (A,B,C,D) generan un (n,k,δ)-código fuertemente MDS si y sólo si la matriz de Toeplitz por bloques*

$$\mathcal{T}_M = \begin{pmatrix} D & O & \cdots & O & O \\ CB & D & \cdots & O & O \\ CAB & CB & \cdots & O & O \\ \vdots & \vdots & & \vdots & \vdots \\ CA^{L-1}B & CA^{L-2}B & \cdots & CB & D \end{pmatrix} \tag{6}$$

tiene la propiedad de que todo menor no trivialmente nulo, es no nulo.

La descripción (A,B,C,D) dada por la expresión (1) no es única en general. Si $\mathcal{C}$ tiene complejidad δ, entonces es posible elegir las matrices A, B, C y D de tamaños $\delta \times \delta$, $\delta \times k$, $(n-k) \times \delta$ y $(n-k) \times k$, respectivamente. Una representación que tenga estos tamaños se llama *representación minimal* y está caracterizada algebraicamente a través de la condición de que (A,B) forma un par de matrices *controlable*, esto es,

$$\operatorname{rg}\begin{pmatrix} B & AB & \ldots & A^{\delta-1}B \end{pmatrix} = \delta. \tag{7}$$

Un código es *catastrófico* (véase [3]) si existe un vector información $\{u_t\}_{t\geq 0}$ con infinitas componentes no nulas, $\sum_{t=0}^{\infty} \operatorname{wt}(u_t) = \infty$, tal que proporciona una palabra código $\{v_t\}_{t\geq 0}$ con un número finito de componentes no nulas, $\sum_{t=0}^{\infty} \operatorname{wt}(v_t) < \infty$. Es decir, un código convolucional catastrófico causa al codificar un número infinito de errores cuando sólo un número finito de errores es recibido. Si $\mathcal{C}$ es un código observable, entonces es no

catastrófico. Tal y como se muestra en [4], el código convolucional $\mathcal{C}(A, B, C, D)$ definido por (1) representa un código observable si y sólo si el par de matrices (A, C) forma un par observable, esto es,

$$\operatorname{rg} \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{\delta-1} \end{pmatrix} = \delta. \tag{8}$$

La técnica de perforación que empleamos es la introducida por McEliece [3]. Partiendo de un (n, k, δ)-código $\mathcal{C}$, podemos describir el proceso de codificación de la siguiente forma: en el i-ésimo "tick" de un reloj imaginario, el código acepta un vector información u_i, y produce un vector código de n componentes v_i. Si consideramos ahora un reloj cuya velocidad es $1/M$ veces la del anterior, entonces el nuevo código acepta en el i-ésimo "tick" M vectores información y produce M vectores código de n componentes cada uno. Es decir, obtenemos un (nM, kM, δ)-código, al que denominamos *código convolucional obtenido al descomponer $\mathcal{C}$ en bloques de profundidad M*, y denotamos por $\mathcal{C}^{[M]}$. McEliece prueba que no sólo la complejidad es la misma para los códigos $\mathcal{C}$ y $\mathcal{C}^{[M]}$, sino que también tienen la misma distancia libre. Ahora, si borramos P componentes de la palabra código de $\mathcal{C}^{[M]}$, siendo $kM < nM - P$, obtenemos un nuevo código convolucional $\mathcal{C}_P$ de tasa $kM/(nM - P)$, al que llamamos *código perforado*.

3. Representación entrada-estado-salida del código $\mathcal{C}^{[M]}$

En esta sección, estudiamos y caracterizamos el código $\mathcal{C}^{[M]}$, obtenido al descomponer el código original $\mathcal{C}$ en bloques de profundidad M, desde el punto de vista de sistemas lineales. Denotamos por x_t, u_t, y_t y v_t el vector de estados, el vector información, el vector de paridad y la palabra código de $\mathcal{C}$, respectivamente, para cada instante t; del mismo modo, denotamos por $x_t^{[M]}$, $u_t^{[M]}$, $y_t^{[M]}$ y $v_t^{[M]}$, el vector de estados, el vector información, el vector de paridad y la palabra código de $\mathcal{C}^{[M]}$, respectivamente, para cada instante t.

Teniendo en cuenta la construcción del código $\mathcal{C}^{[M]}$, tenemos que el vector de estados, el vector información, el vector de paridad y la palabra código de $\mathcal{C}^{[M]}$, vienen dados por

$$x_t^{[M]} = x_{t+M-1}, \quad u_t^{[M]} = \begin{pmatrix} u_t \\ u_{t+1} \\ \vdots \\ u_{t+M-1} \end{pmatrix}, \quad y_t^{[M]} = \begin{pmatrix} y_t \\ y_{t+1} \\ \vdots \\ y_{t+M-1} \end{pmatrix}, \quad v_t^{[M]} = \begin{pmatrix} y_t \\ y_{t+1} \\ \vdots \\ y_{t+M-1} \\ u_t \\ u_{t+1} \\ \vdots \\ u_{t+M-1} \end{pmatrix}. \tag{9}$$

El teorema siguiente proporciona la representación entrada-estado salida para el código $\mathcal{C}^{[M]}$, en función de la representación entrada-estado-salida del código original $\mathcal{C}$.

Teorema 2 *Si $\mathcal{C}(A, B, C, D)$ es un (n, k, δ)-código y $\mathcal{C}^{[M]}(A_M, B_M, C_M, D_M)$ es el (nM, kM, δ)-código obtenido al descomponer $\mathcal{C}$ en bloques de profundidad M, entonces*

una representación entrada-estado-salida para $\mathcal{C}^{[M]}$ viene dada por el sistema lineal (1), donde

$$A_M = A^M, \qquad B_M = \begin{pmatrix} A^{M-1}B & A^{M-2}B & \cdots & AB & B \end{pmatrix},$$
$$C_M = \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{M-1} \end{pmatrix}, \qquad D_M = \begin{pmatrix} D & O & \cdots & O & O \\ CB & D & \cdots & O & O \\ \vdots & \vdots & & \vdots & \vdots \\ CA^{M-2}B & CA^{M-1}B & \cdots & CB & D \end{pmatrix}. \tag{10}$$

Demostración. De la expresión (1), tenemos, para el código original $\mathcal{C}$,

$$\begin{aligned} x_{t+1} &= Ax_t + Bu_t, \\ y_t &= Cx_t + Du_t, \\ v_t &= \begin{pmatrix} y_t \\ u_t \end{pmatrix}, \quad x_0 = 0. \end{aligned} \tag{11}$$

Iterando las ecuaciones que definen el sistema (11) hasta el instante $t = M$, obtenemos que

$$\begin{aligned} x_{t+1}^{[M]} = x_{t+M} &= A^M x_{t+M-1} + \begin{pmatrix} A^{M-1}B & A^{M-2}B & \cdots & AB & B \end{pmatrix} \begin{pmatrix} u_t \\ u_{t+1} \\ \vdots \\ u_{t+M-2} \\ u_{t+M-1} \end{pmatrix} \\ y_{t+M-1} &= CA^{M-1}x_t + \begin{pmatrix} CA^{M-2}B & CA^{M-3}B & \cdots & CB & D \end{pmatrix} \begin{pmatrix} u_t \\ u_{t+1} \\ \vdots \\ u_{t+M-2} \\ u_{t+M-1} \end{pmatrix}. \end{aligned} \tag{12}$$

Ahora bien, teniendo en cuenta las expresiones (9) y (12), una representación entrada-estado-salida del código $\mathcal{C}^{[M]}$ viene dada por

$$\begin{aligned} x_{t+1}^{[M]} &= A^M x_t^{[M]} + \begin{pmatrix} A^{M-1}B & A^{M-2}B & \cdots & AB & B \end{pmatrix} u_t^{[M]} \\ y_t^{[M]} &= \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{M-1} \end{pmatrix} x_t^{[M]} + \begin{pmatrix} D & O & \cdots & O & O \\ CB & D & \cdots & O & O \\ \vdots & \vdots & & \vdots & \vdots \\ CA^{M-2}B & CA^{M-1}B & \cdots & CB & D \end{pmatrix} u_t^{[M]}. \end{aligned} \tag{13}$$

□

Tal y como describimos en la sección 2, la controlabilidad del par (A, B) está relacionado con el de minimalidad de la representación entrada-estado-salida (A, B, C, D) y la observabilidad del par (A, C), con el hecho de que el código convolucional sea no catastrófico. Así pues, nuestro objetivo a continuación es analizar las condiciones que deben

cumplir las matrices A, B, C y D que describen el código original $\mathcal{C}$ para que el código obtenido por la descomposición en bloques de profundidad M sea no catastrófico y tenga una representación minimal.

El resultado siguiente pone de manifiesto que el código $\mathcal{C}^{[M]}$ obtenido por la descomposición de $\mathcal{C}$ en bloques de profundidad M, hereda las propiedades de controlabilidad y observabilidad del código original $\mathcal{C}$.

Teorema 3 *Sean $\mathcal{C}(A,B,C,D)$ un (n,k,δ)-código y $\mathcal{C}^{[M]}(A_M,B_M,C_M,D_M)$ el (nM,kM,δ)-código obtenido al descomponer $\mathcal{C}$ en bloques de profundidad M.*

1. *Si (A,B) es controlable, entonces (A_M,B_M) es controlable.*
2. *Si (A,C) es observable, entonces (A_M,C_M) es observable.*

Demostración. 1. Como (A,B) es controlable,

$$\operatorname{rg}\begin{pmatrix} B & AB & \dots & A^{\delta-1}B \end{pmatrix} = \delta. \tag{14}$$

Ahora bien, teniendo en cuenta la expresión de las matrices A_M y B_M dada en (10), así como la relación (14), tenemos que

$$\begin{aligned} \delta &\geq \operatorname{rg}\begin{pmatrix} B_M & A_MB_M & \dots & A_M^{\delta-1}B_M \end{pmatrix} \\ &= \operatorname{rg}\begin{pmatrix} A^{M-1}B & A^{M-2}B & \dots & A^{(\delta-1)M+1}B & A^{(\delta-1)M}B \end{pmatrix} \\ &\geq \operatorname{rg}\begin{pmatrix} B & AB & \dots & A^{\delta-1}B \end{pmatrix} = \delta. \end{aligned} \tag{15}$$

Por tanto, el par (A_M,B_M) es controlable.

2. La condición de observabilidad del par (A_M,C_M) se obtiene a partir de las expresiones (8) y (10), siguiendo un argumento análogo al apartado anterior. □

4. Códigos perforados fuertemente MDS

El objetivo de esta sección es obtener condiciones para que, partiendo de códigos convolucionales fuertemente MDS, el código perforado sea también fuertemente MDS. El ejemplo siguiente muestra que el hecho de que el código original sea fuertemente MDS, no implica que el código perforado obtenido a partir de él también lo sea.

Ejemplo 1 *Sea α un elemento primitivo de $GF(8)$, con $\alpha^3+\alpha+1=0$. Consideremos el $(2,1,1)$-código fuertemente MDS $\mathcal{C}(A,B,C,D)$ (véase [8]) descrito por las matrices*

$$A=\begin{pmatrix}\alpha\end{pmatrix}, \qquad B=\begin{pmatrix}1\end{pmatrix}, \qquad C=\begin{pmatrix}\alpha^4\end{pmatrix} \quad y \quad D=\begin{pmatrix}1\end{pmatrix} \tag{16}$$

Sea $\mathcal{C}^{[3]}(A_3,B_3,C_3,D_3)$ el $(6,3,1)$-código obtenido al descomponer $\mathcal{C}(A,B,C,D)$ en bloques de profunidad $M=3$, descrito por las matrices

$$A_3=\begin{pmatrix}\alpha^3\end{pmatrix}, \qquad B_3=\begin{pmatrix}\alpha^2 & \alpha & 1\end{pmatrix}, \qquad C_3=\begin{pmatrix}\alpha^4\\ \alpha^5\\ \alpha^6\end{pmatrix} \quad y \quad D_3=\begin{pmatrix}1 & 0 & 0\\ \alpha^4 & 1 & 0\\ \alpha^5 & \alpha^4 & 1\end{pmatrix} \tag{17}$$

Ahora, si borramos las dos primeras filas de las matrices C_3 y D_3, obtenemos el código perforado de tasa $3/4$ y complejidad $\delta = 1$ descrito por las matrices

$$A_P = \begin{pmatrix} \alpha^3 \end{pmatrix}, \qquad B_P = \begin{pmatrix} \alpha^2 & \alpha & 1 \end{pmatrix}, \qquad C_P = \begin{pmatrix} \alpha^6 \end{pmatrix} \quad y \quad D_P = \begin{pmatrix} \alpha^5 & \alpha^4 & 1 \end{pmatrix}. \tag{18}$$

Obtenemos entonces que $d_1(\mathcal{C}_P) = 2$, y, por tanto, $\mathcal{C}_P$ no es fuertemente MDS. Es más, $d_{free}(\mathcal{C}_P) = 2$, siendo 3 la cota Singleton generalizada para un $(4, 3, 1)$-código. Por tanto, el código perforado $\mathcal{C}_P$ tampoco es MDS.

El resultado siguiente proporciona las condiciones bajo las cuales el código perforado obtenido a partir de un $(2, 1, 1)$-código fuertemente MDS, es también fuertemente MDS.

Teorema 4 *Sean $\mathcal{C}(A, B, C, D)$ un $(2, 1, 1)$-código convolucional fuertemente MDS, $\mathcal{C}^{[M]}(A_M, B_M, C_M, D_M)$ el $(2M, M, 1)$-código obtenido al descomponer $\mathcal{C}$ en bloques de profunidad M y $\mathcal{C}_P(A_P, B_P, C_P, D_P)$ el código perforado de tasa $M/(M + 1)$ obtenido al eliminar las $M - 1$ primeras filas de C_M y D_M.*

1. *Si $M = 2$, entonces $\mathcal{C}_P$ es un código fuertemente MDS.*
2. *Si $M > 2$, entonces $\mathcal{C}_P$ no es un código fuertemente MDS.*

Demostración. Supongamos que partimos de una representación minimal del código observable $\mathcal{C}(A, B, C, D)$.

1. Si $M = 2$, entonces teniendo en cuenta la expresión (10), el código perforado está generado por las matrices

$$A_P = \begin{pmatrix} A^2 \end{pmatrix}, \qquad B_P = \begin{pmatrix} AB & B \end{pmatrix}, \qquad C_P = \begin{pmatrix} CA \end{pmatrix} \quad \text{y} \quad D_P = \begin{pmatrix} CB & D \end{pmatrix}. \tag{19}$$

Como $\mathcal{C}(A, B, C, D)$ es un $(2, 1, 1)$-código, las matrices A, B y C son escalares. Por tanto, dado que (A, B) es controlable y (A, C) es observable, tenemos que el par (A_P, B_P) es controlable y el par (A_P, C_P) es observable, de donde obtenemos que la complejidad del código perforado es $\delta_P = 1$. Ahora, teniendo en cuenta que el código $\mathcal{C}(A, B, C, D)$ es fuertemente MDS y aplicando el teorema 1, tenemos que la matriz

$$\mathcal{T}_1 = \begin{pmatrix} CB & D & 0 & 0 \\ CA^2B & CAB & CB & D \end{pmatrix} \tag{20}$$

tiene la propiedad de que todo menor no trivialmente nulo, es no nulo. Por tanto, el código perforado $\mathcal{C}_P(A_P, B_P, C_P, D_P)$ es fuertemente MDS, ya que $M = 1$ en este caso.

2. Supongamos ahora que $M > 2$. De nuevo por la expresión (10), el código perforado está generado por las matrices

$$\begin{array}{cc} A_P = \begin{pmatrix} A^M \end{pmatrix}, & B_P = \begin{pmatrix} A^{M-1}B & A^{M-2}B & \dots & AB & B \end{pmatrix} \\ C_P = \begin{pmatrix} CA^{M-1} \end{pmatrix}, & D_P = \begin{pmatrix} CA^{M-2}B & CA^{M-3}B & \dots & CB & D \end{pmatrix}. \end{array} \tag{21}$$

Siguiendo un razonamiento similar al hecho en el apartado anterior, el par (A_P, B_P) es controlable y el par (A_P, C_P) es observable. Por tanto, la complejidad el código perforado es $\delta_P = 1$. Ahora bien, en este caso, la matriz

$$\mathcal{T}_1 = \begin{pmatrix} CA^{M-2}B & CA^{M-3}B & \dots & D & 0 & 0 & \dots & 0 \\ CA^{2M-2}B & CA^{2M-3}B & \dots & CA^{M-1}B & CA^{M-2}B & CA^{M-3}B & \dots & D \end{pmatrix} \tag{22}$$

siempre contiene el menor de tamaño 2×2 no trivialmente nulo

$$\begin{vmatrix} CA^{M-2}B & CA^{M-3}B \\ CA^{2M-2}B & CA^{2M-3}B \end{vmatrix} = 0, \tag{23}$$

de donde obtenemos que $\mathcal{C}_P$ no es fuertemente MDS, ya que $M = 1$ en este caso.
□

Agradecimientos

Este trabajo ha sido parcialmente subvencionado por los siguientes proyectos:

- Construcción de códigos convolucionales. Algoritmos secuenciales y paralelos de decodificación (MTM2005-05759). Subvencionado por el Ministerio de Educación y Ciencia.
- Construccción geométrica de códigos convolucionales sobre curvas algebraicas (SA028A05). Subvencionado por la Junta de Castilla y León.
- Estudio y construcción de códigos convolucionales concatenados y paralelos (EGV06/078). Subvencionado por la Generalitat Valenciana.

Referencias

[1] J. B. Cain, G. C. Clark y J. M. Geist. *Punctured convolutional codes of rate* $(n-1)/n$ *and simplified maximum likelihood decoding*. IEEE Transactions on Information Theory. **25(1)** (1979), 97–100.

[2] R. Hutchinson, J. Rosenthal, y R. Smarandache. *Convolutional Codes with Maximum Distance Profile*. Systems and Control Letters, **4(1)** (2005), 53-63.

[3] R. J. McEliece. *The algebraic theory of convolutional codes* En V. Pless y W. C. Huffman, editores, " Handbook of Coding Theory", **Vol. I** 1065-1138. Elsevier Science Publishers, Amsterdam, The Netherlands, (1998).

[4] J. Rosenthal, J.M. Schumacher y E.V. York. *On behaviors and convolutional codes*. IEEE Transactions on Information Theory, **42(6)** (1996), 1881–1891.

[5] J. Rosenthal, y R. Smarandache. *Construction of Convolutional Codes using Methods from Linear Systems Theory*. Proceedings of the 35th Allerton Conference on Communication, Control and Computing, 953–960, Allerton House, Monticello, IL, Septiembre 1997.

[6] J. Rosenthal y R. Smarandache. *Maximum distance separable convolutional codes*. Applicable Algebra in Engineering, Communication and Computing, **10** (1999), 15–32.

[7] J. Rosenthal y E. V. York., *BCH convolutional codes*. IEEE Transactions on Information Theory **42(6)** (1996), 1881–1891.

[8] R. Smarandache y J. Rosenthal. *A state space approach for constructing MDS rate* $1/n$ *convolutional codes*. Proceedings of the 1998 IEEE Information Theory Workshop on Information Theory, 116–117, Killarney, Kerry, Ireland, Junio 1998.