

# Universidad Miguel Hernández

Departamento de Estadística, Matemáticas e  
Informática



Estudio y construcción de códigos convolucionales:  
códigos perforados, códigos concatenados desde el  
punto de vista de sistemas

TESIS DOCTORAL

Presentada por:

María Victoria Herranz Cuadrado

Codirigida por:

Joan Josep Climent Coloma

María del Carmen Perea Marco



Universidad Miguel Hernández

Departamento de Estadística, Matemáticas e  
Informática

Estudio y construcción de códigos convolucionales:  
códigos perforados, códigos concatenados desde el  
punto de vista de sistemas



Memoria presentada para optar al grado de  
Doctora por MARÍA VICTORIA HERRANZ  
CUADRADO.

Elche, febrero de 2007.



D. JOAN JOSEP CLIMENT COLOMA, Catedrático de Universidad del Departamento de Ciencia de la Computación e Inteligencia Artificial de la Universidad de Alicante y Dña. MARÍA DEL CARMEN PEREA MARCO, Profesora Titular de Escuela Universitaria del Departamento de Estadística, Matemáticas e Informática de la Universidad Miguel Hernández de Elche

CERTIFICAN:

Que la presente memoria *Estudio y construcción de códigos convolucionales: códigos perforados, códigos concatenados desde el punto de vista de sistemas*, ha sido realizada bajo su dirección, en el Departamento de Estadística, Matemáticas e Informática de la Universidad Miguel Hernández de Elche, por la licenciada Dña. MARÍA VICTORIA HERRANZ CUADRADO, y constituye su tesis para optar al grado de Doctora.

Para que conste, en cumplimiento de la legislación vigente, autorizan la presentación de la referida tesis doctoral ante la comisión de Doctorado de la Universidad Miguel Hernández, firmando el presente certificado.

Elche, 10 de Enero de 2007

Joan Josep Climent Coloma

María del Carmen Perea Marco



D. JOSÉ LUIS RUIZ GÓMEZ, Profesor Titular de Universidad y director del Departamento de Estadística, Matemáticas e Informática de la Universidad Miguel Hernández

CERTIFICA:

Que la presente memoria *Estudio y construcción de códigos convolucionales: códigos perforados, códigos concatenados desde el punto de vista de sistemas*, realizada bajo la dirección de Joan Josep Climent Coloma y María del Carmen Perea Marco, en el Departamento de Estadística, Matemáticas e Informática de la Universidad Miguel Hernández de Elche, por la licenciada Dña. MARÍA VICTORIA HERRANZ CUADRADO, constituye su tesis para optar al grado de Doctora.

Para que conste, en cumplimiento de la legislación vigente, se ratifica en la autorización de la presentación de la referida tesis doctoral ante la comisión de Doctorado de la Universidad Miguel Hernández, firmando el presente certificado.

Elche, 10 de Enero de 2007

José Luis Ruiz Gómez



*A Vicente,*

*A mis padres, Aurelio y Pepita,*

*A la memoria de mi abuela.*





*Cerca está de agradecido quien se conoce deudor*

–Calderón, *El gran teatro del mundo*

Esta tesis está escrita en gran parte en primera persona del plural (nosotros). No es por mero accidente o por razones de estilo que esto es así. Con toda seguridad, no podría haber realizado todo el trabajo que ella me ha supuesto sin la ayuda de tantos amigos y compañeros que me han apoyado, comenzando por los directores de esta memoria, Joan Josep Climent y M<sup>a</sup> Carmen Perea, por la confianza que en mí depositaron, por compartir conmigo sus conocimientos e ideas y por su apoyo y trabajo a lo largo de esta memoria.

Mi gratitud también a todos y cada uno de los profesores del Departamento de Estadística, Matemáticas e Informática de la Universidad Miguel Hernández, por creer firmemente en el futuro que engendra el quehacer matemático. En especial, mi gratitud a Nati, Lola, Manolo, Joaquín, Marc, Asun, Javi, Álex, Yolanda y Mercedes, con los que he compartido muy buenos momentos.

Quiero agradecer al profesor Joachim Rosenthal por su gran hospitalidad durante mi estancia en la Universidad de Notre Dame (Indiana) y por introducirme en los códigos convolucionales. Es tremendamente satisfactorio compartir tiempo con alguien a quien admiras y de quien quieres aprender.

En el plano personal, el primer agradecimiento va por supuesto para mi familia y para la que se ha convertido en mi familia desde hace cuatro años. Empezando por los más cercanos y hasta los más lejanos todos han ayudado, desde los imprudentes que insistían en enterarse del tema de la tesis, hasta los que preguntaban que cuándo estaría terminada.

Gracias también a tantos amigos que me han apoyado y animado a lo largo de este proyecto: M<sup>a</sup> José, Natalia, Eli, Boria, Ana, Cristina, Irene, José Manuel... Gracias de todo corazón a Xaro y a M<sup>a</sup> Eugenia por estar a mi lado, por su apoyo desinteresado, por los buenos momentos de risas compartidos y, sobre todo, por creer en mí.

Gracias a mi “hermana” Mari Carmen, la hermana que siempre quise tener, por su apoyo en momentos decisivos, por su comprensión y por recordarme que la vida es

mucho más que matemáticas.

Sin lugar a dudas, las personas a las que estoy más agradecida son mis padres, Pepita y Aurelio, y a mi marido, Vicente, a quienes he dedicado el fruto de este esfuerzo. Mis padres, siempre preocupados por mi felicidad, alentadores y reconfortantes en los momentos bajos, han estado a mi lado en todo momento. Su empuje, ayuda incondicional y confianza en mí han sido decisivas. Vicente ha sido uno de los artífices en el empuje para la realización de esta tesis, sin su ilusión no hubiera sido posible. Él es mi mejor amigo y quien mejor me conoce y sabe lo gratificante que ha sido para mí el llevar a cabo este proyecto. Muchas de las horas aquí invertidas se las he robado a él y, a pesar de ello, me ha prestado siempre el apoyo y cariño necesarios que sólo una gran persona puede dar. Vicente, perdón por las ausencias y por los malos humores que esta tesis me ha generado. Esta tesis es también, en parte, de ellos tres. Nadie va a vivir este momento de ver mi tesis acabada con mayor felicidad que ellos. ¡Va por vosotros!







# Índice

---

Prólogo	xv
<b>1 Preliminares</b>	<b>1</b>
1.1 Introducción . . . . .	1
1.2 Códigos bloque . . . . .	3
1.3 Códigos convolucionales . . . . .	5
1.3.1 Propiedades estructurales . . . . .	6
1.3.2 Códigos convolucionales basados en la construcción de Justesen	11
1.3.3 Códigos convolucionales perforados . . . . .	12
1.4 Sistemas lineales invariantes en el tiempo . . . . .	15
1.5 Sistemas lineales y códigos convolucionales . . . . .	18
1.6 Códigos <i>woven</i> . . . . .	25
1.6.1 Producto de Kronecker . . . . .	28
1.6.2 Propiedades estructurales del warp . . . . .	30
1.6.3 Propiedades estructurales del <i>twill</i> . . . . .	34
<b>2 Códigos perforados basados en la construcción de Justesen</b>	<b>37</b>
2.1 Introducción . . . . .	37
2.2 Clasificación de códigos convolucionales basados en la construcción de Justesen . . . . .	39
2.3 Propiedades de los códigos convolucionales de Justesen . . . . .	43
2.4 Códigos convolucionales de Justesen perforados . . . . .	50

2.4.1	Estudio de la compacidad del código obtenido por descomposición en bloques de un código convolucional arbitrario . . . . .	50
2.4.2	Código obtenido por descomposición en bloques de un código convolucional de Justesen . . . . .	52
2.4.3	Códigos convolucionales de Justesen perforados . . . . .	57
2.5	Conclusiones . . . . .	61
<b>3</b>	<b>Concatenación en serie de códigos convolucionales</b>	<b>63</b>
3.1	Introducción . . . . .	63
3.2	Concatenación en serie sistemática . . . . .	65
3.2.1	Representación entrada-estado-salida . . . . .	66
3.2.2	Controlabilidad . . . . .	71
3.2.3	Observabilidad . . . . .	83
3.2.4	Distancias columnas y distancias libres . . . . .	99
3.2.5	Ejemplos . . . . .	102
3.3	Concatenación en serie no sistemática . . . . .	107
3.3.1	Representación entrada-estado-salida . . . . .	108
3.3.2	Controlabilidad . . . . .	113
3.3.3	Observabilidad . . . . .	126
3.3.4	Distancias columnas y distancias libres . . . . .	135
3.3.5	Ejemplos . . . . .	138
3.4	Conclusiones . . . . .	141
<b>4</b>	<b>Concatenación de un código bloque y un código convolucional</b>	<b>143</b>
4.1	Introducción . . . . .	143
4.2	Modelos de concatenación de un código bloque y un código convolucional . . . . .	145
4.3	Controlabilidad y observabilidad . . . . .	152
4.4	Distancias columnas y distancia libre . . . . .	156
4.4.1	Distancias columnas de $\mathcal{BC}^{(1)}$ y $\mathcal{BC}_{\text{sys}}^{(1)}$ . . . . .	156
4.4.2	Distancias columnas y distancia libre de $\mathcal{BC}^{(2)}$ y $\mathcal{BC}_{\text{sys}}^{(2)}$ . . . . .	159

4.5	Códigos concatenados con perfil de distancia máxima y fuertemente MDS . . . . .	165
4.6	Relaciones entre los diferentes modelos . . . . .	171
4.6.1	Ejemplos en $\mathbb{F} = GF(4)$ . . . . .	171
4.6.2	Ejemplos en $\mathbb{F} = GF(8)$ . . . . .	179
4.7	Conclusiones . . . . .	186
<b>5</b>	<b>Concatenación en paralelo de códigos convolucionales</b>	<b>189</b>
5.1	Introducción . . . . .	189
5.2	Modelos de concatenación en paralelo . . . . .	191
5.2.1	Representación entrada-estado-salida . . . . .	192
5.2.2	Controlabilidad . . . . .	197
5.2.3	Observabilidad . . . . .	198
5.2.4	Distancias columnas y distancias libres . . . . .	202
5.3	Concatenación en paralelo por bloques . . . . .	205
5.3.1	Propiedades estructurales de $\mathcal{PC}^{(3)}$ . . . . .	206
5.3.2	Representación entrada-estado-salida de $\mathcal{PC}^{(3)}$ . . . . .	208
5.4	Códigos convolucionales <i>woven</i> desde el punto de vista de sistemas lineales . . . . .	211
5.4.1	<i>Warp</i> formado por códigos convolucionales idénticos . . . . .	212
5.4.2	<i>Warp</i> formado por códigos convolucionales distintos . . . . .	214
5.5	Conclusiones . . . . .	218
<b>A</b>	<b>Líneas futuras</b>	<b>219</b>
	<b>Bibliografía</b>	<b>221</b>



# Prólogo

---

El origen de los códigos correctores de errores se remonta a finales de 1940 cuando los trabajos germinales de Shannon sobre la teoría de la información dieron paso a numerosos estudios cuyas implementaciones en el ámbito de las comunicaciones son considerables. De hecho, se suele tomar como fecha de nacimiento de la teoría de la codificación de la información la de la publicación, en 1948, del artículo *A mathematical Theory of Communication* [98], con el que se abrió una importante línea de investigación en la construcción de códigos y algoritmos de decodificación. En estos comienzos, la teoría de los códigos tenía un enfoque esencialmente probabilístico. Sin embargo, pasó posteriormente a un enfoque más algebraico, surgiendo entonces muchos ejemplos prácticos (aún en uso hoy en día) como los códigos de Golay y de Hamming, los códigos cíclicos y BCH, o los códigos de Reed-Solomon y de Reed-Muller.

Hamming introdujo en el año 1950 el primer código de corrección de errores, conocido posteriormente como el código de Hamming, aplicado aún en la actualidad. Su método permite identificar y corregir un bit erróneo en una palabra codificada. Este código había sido ya descubierto de forma independiente por Golay, en el año 1949. Los códigos de Hamming son utilizados actualmente, por ejemplo, en el proceso de lectura y escritura de la memoria RAM de un ordenador. Además, Golay diseñó los códigos que llevan su nombre, que permiten corregir hasta tres errores. Elias introdujo en 1955 los códigos convolucionales [39], que presentan en la actualidad multitud de aplicaciones: comunicaciones wireless (GSM, IMT-2000), comunicación digital terrestre y satélite, etc.

En 1960, Bose y Chaudhuri propusieron una clase de códigos correctores de errores múltiples que curiosamente fueron descubiertos independientemente por Hocqenghem en 1959. Estos códigos correctores son conocidos como códigos BCH (por las iniciales de los autores). También en 1960, Reed y Solomon publicaron un esquema de codificación que usa todo el potencial de los códigos bloque [84]. Los códigos Reed-Solomon han

sido muy utilizados por la NASA, para transmisión de información en las misiones al espacio Galileo, Magellan y Ulises, y en la actualidad se usan muy frecuentemente, desde los lectores de CD hasta los discos duros de los ordenadores. En 1966, Forney [41] discutió por primera vez la posibilidad de usar códigos concatenados (combinación de dos códigos) para incrementar la eficiencia, evitando hacer los dispositivos y componentes demasiado complejos. En 1967, Viterbi [113] diseñó un algoritmo decodificador utilizando el principio de máxima verosimilitud para códigos convolucionales y lidera, por su gran eficiencia en el consumo de recursos, el desarrollo actual de los esquemas para códigos correctores de errores en comunicaciones digitales.

El carácter innovador de estas investigaciones sobre los códigos correctores superaban las posibilidades técnicas de la época y, por ello, no fue posible una aplicación práctica inmediata. El desarrollo de los dispositivos para la corrección de errores solamente se dio hasta mediados de los años 70. En 1974, Blokh y Zyablov [14] y Zinov'ev [119] introdujeron una importante clase de códigos concatenados, que eran capaces de corregir tanto errores aleatorios como ráfagas de errores. La introducción, también en los años 70, por parte de Goppa [46] de una nueva construcción de códigos lineales a partir de curvas algebraicas lisas (llamados códigos geométricos de Goppa o códigos algebraico-geométricos) cambió por completo el panorama de investigación en el terreno de la teoría de códigos correctores de errores; por un lado, la codificación de dichos códigos parecía sencilla, y por otro sus parámetros podían ser fácilmente controlables a partir de fórmulas clásicas de la geometría algebraica (tales como el teorema de Riemann-Roch). Además, dicha teoría permitió la construcción explícita de familias de códigos cuyos parámetros sobrepasan asintóticamente la cota de Varshamov-Gilbert y, en consecuencia, dar una solución efectiva (y con complejidad polinómica) al problema principal de la teoría de códigos, que fue considerado por Shannon en términos puramente probabilísticos pero sin ninguna idea constructiva. Sin embargo, a pesar del interés que suscitó el estudio de los códigos geométricos de Goppa desde su origen, no pudieron encontrarse algoritmos eficientes para su decodificación hasta finales de los años 80 del siglo pasado, gracias a sucesivos trabajos de Justesen, Larsen, Jensen, Havemose y Hoholdt [67], Skorobogatov y Vladut [99] y Porter [83].

Se puede considerar que hasta mediados de los años 90, los códigos concatenados eran la mejor opción para la corrección de errores. Sin embargo, éstos fueron mejorados por la aparición de los denominados turbo códigos, que tratan de alcanzar las máximas tasas de transmisión posibles derivadas de la teoría de Shannon. Estos códigos fueron introducidos por Berrou, Glavieux y Thitimajshima [13] y la primera descripción, uti-

lizando argumentos probabilísticos, fue presentada en 1993. Estos códigos están siendo utilizados actualmente en canales de comunicación digital y en la telefonía de tercera generación.

Los códigos detectores y correctores de errores se dividen en dos categorías: los códigos bloque y los códigos convolucionales. Los códigos bloque han sido ampliamente estudiados y se ha demostrado que tienen muy buenas propiedades para corregir errores. Además, su estructura algebraica ha dado lugar al desarrollo de algoritmos de decodificación algebraicos que son fáciles de implementar. Los códigos convolucionales generalizan los códigos bloque de manera natural y han sido muy empleados desde su descubrimiento, por ejemplo, en comunicaciones vía satélite, discos de lectura óptica (CD-ROM), sistemas de audio y vídeo (sonido digital, CD, vídeo digital, DVD). Sin embargo, la teoría algebraica de los códigos convolucionales no ha avanzado tanto como la teoría algebraica de los códigos bloque. De hecho, en un principio, la mayor parte de los códigos convolucionales implementados fueron descubiertos por medio de cálculos computacionales. Posteriormente, se introdujeron construcciones basadas en la relación de las matrices generadoras de un código convolucional con las matrices generadoras de ciertos códigos bloque cíclicos o quasi-cíclicos [68, 75, 77, 107]. Abdel-Ghaffar [1] y Justesen [69] proponen técnicas efectivas para la construcción de códigos convolucionales de tasa  $1/n$ . Otra forma de construir códigos convolucionales con distancia libre elevada es restringirnos a la subclase de códigos convolucionales que tienen un grupo de automorfismos no trivial [82]. Rosenthal, Smarandache y Gluesing-Luerssen [101] proponen una construcción de códigos convolucionales MDS, esto es, cuya distancia libre es la mayor posible, basada en la construcción introducida por Justesen [69].

Los códigos convolucionales pueden considerarse como sistemas lineales discretos e invariantes en el tiempo sobre un cuerpo finito. En los últimos años ha aumentado el interés entre esta conexión. Rosenthal, York y Schumacher introducen la descripción de un código convolucional en teoría de sistemas mediante la llamada representación entrada-estado-salida [91]. Empleando herramientas básicas de sistemas, construyen códigos convolucionales de tipo Reed-Solomon y de tipo BCH. Posteriormente, Rosenthal y York [95] demuestran que la estructura algebraica de estos códigos puede emplearse para su decodificación algebraica. Además, Rosenthal y Smarandache [92] construyen códigos convolucionales de tipo alternante y también códigos convolucionales con distancia libre excelente empleando representaciones de primer orden. Con respecto a la decodificación, Rosenthal [88] introduce un algoritmo iterativo de decodificación que se aplica para decodificar códigos convolucionales con cierta estructura algebraica.

Otro tipo de construcciones de códigos convolucionales son las algebraico-geométricas. Domínguez, Muñoz, Iglesias y Serrano [36, 37] definen los códigos convolucionales Goppa sobre curvas algebraicas y construyen también los códigos duales correspondientes. Además, obtienen códigos convolucionales MDS. Como comentábamos anteriormente, Forney introdujo la construcción de códigos convolucionales basada en la técnica de concatenación. Esta técnica ha sido muy explotada, sobre todo desde la aparición de los turbo códigos. Otra técnica de construcción de códigos convolucionales es la técnica de perforación, aplicada con la finalidad de obtener códigos potentes de manera que la decodificación de Viterbi se simplifica considerablemente.

En esta memoria empleamos la técnica de perforación para construir códigos convolucionales obtenidos a partir de códigos bloque Reed-Solomon, así como la técnica de la concatenación para construir nuevos códigos convolucionales a partir de la concatenación en serie o en paralelo de códigos convolucionales y a partir de la concatenación en serie de un código bloque y un código convolucional. En el capítulo 1 introducimos los conceptos y resultados básicos sobre códigos bloque, códigos convolucionales y sistemas lineales, necesarios para un completo entendimiento de la memoria.

Los restantes capítulos corresponden a la parte fundamental de la memoria. En el capítulo 2, proporcionamos una clasificación que describe los códigos convolucionales basados en la construcción de Justesen. Además, aplicamos la técnica de perforación a estos códigos, obteniendo condiciones para que la matriz generadora del código perforado sea minimal. En los capítulos 3 y 4, caracterizamos diferentes tipos de concatenación en serie de dos códigos convolucionales así como de concatenación en serie de un código bloque con un código convolucional empleando la teoría de sistemas lineales. Proporcionamos condiciones para que la representación entrada-estado-salida que describe la concatenación sea minimal y de manera que el código concatenado sea no catastrófica. Asimismo, obtenemos cotas inferiores de las distancias libres de los códigos concatenados en función de las distancias de los códigos constituyentes. Finalmente, en el capítulo 5, estudiamos diferentes tipos de concatenación en paralelo de códigos convolucionales empleando la descripción de un código convolucional como un sistema lineal.

La memoria termina con un apéndice, en el que se recogen las líneas futuras de trabajo dentro de los problemas planteados, y con las referencias bibliográficas utilizadas para su elaboración.

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.

- Construcción 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.





---

# Capítulo 1

## Preliminares

---

*I was confident I was correct, not only in an intuitive way but in a rigorous way.  
I knew exactly what I was doing, and it all came out exactly right.*

–Claude Shannon

*Information is the resolution of uncertainty.*

–Claude Shannon

### 1.1 Introducción

En el proceso de comunicación de la información es frecuente la utilización de canales con perturbaciones, en los que la información (expresada correctamente en origen) puede sufrir alteraciones durante la transmisión, debido al ruido. Se hace, por tanto, necesario el uso de herramientas que garanticen la detección y corrección de los errores que se puedan generar en la comunicación. Los códigos detectores y correctores de errores se perfilan como el instrumento más apropiado para este fin; estos códigos añaden información redundante a la información, de modo que dos mensajes codificados cualesquiera son substancialmente diferentes; de esta manera, un número relativamente pequeño de errores no puede transformar un mensaje codificado en otro y, en consecuencia, se pueden detectar los errores e incluso corregirlos en algunos casos.

Los códigos detectores y correctores de errores utilizados en la práctica pueden clasificarse, con muy pocas excepciones, en dos grandes grupos. Los códigos bloque, que dividen los datos en bloques de longitud fija y transforman cada uno de ellos de forma independiente mediante un algoritmo de codificación fijo y los códigos convolucionales, que tratan los datos como un flujo y trabajan sobre bloques de longitud fija, pero hay

solapamiento entre los bloques. La mayoría de los códigos en bloque utilizados en la práctica en los últimos años son los códigos Reed-Solomon, o códigos estrechamente relacionados con ellos, utilizando generalmente el algoritmo de Berlekamp-Massey para la decodificación [61, 80]. En contraste con los códigos bloque cuya estructura algebraica ha sido estudiada con profundidad utilizando distintas herramientas, se sabe muy poco de la estructura algebraica de los códigos convolucionales. Los códigos convolucionales se utilizan en la transmisión de datos mediante líneas telefónicas, en sistemas de comunicación por radio o telefonía móvil y en la transmisión de imágenes desde sondas espaciales y satélites. La codificación convolucional es la técnica dominante en la corrección de errores en aplicaciones de transmisión de datos debido a la facilidad de implementación y a un rendimiento excepcional en canales de error aleatorios [105].

Desde finales de los años sesenta se sabe que los códigos convolucionales y los sistemas lineales discretos e invariantes con coeficientes en un cuerpo finito, son esencialmente los mismos objetos [78]. Recientemente ha aumentado el interés por la conexión entre la teoría de sistemas lineales y la teoría de códigos convolucionales. Concretamente, Rosenthal, Schumacher y York [91] introducen la representación entrada-estado-salida y establecen condiciones necesarias y suficientes para que dichas representaciones den lugar a buenos códigos. Posteriormente, Rosenthal y Smarandache [93] introducen construcciones de códigos óptimos a partir de la representación entrada-estado-salida, probando que para cualquier tasa de transmisión  $k/n$  y cualquier grado existen códigos convolucionales MDS para cuerpos de tamaño suficientemente grande. Se trata de un resultado de existencia obtenido a partir de condiciones algebraico-geométricas, pero no se dispone de un algoritmo para su construcción.

Más recientemente, con el propósito de obtener códigos con gran capacidad correctora de errores, Höst, Johannesson y Zyablov [59] introducen nuevos códigos convolucionales obtenidos como una concatenación en serie en la que el código interno, o el externo, o ambos son a su vez obtenidos mediante una particular combinación en paralelo de varios códigos convolucionales. Dichos códigos son conocidos como códigos convolucionales *woven* debido a que recuerda la estructura entrelazada de un tejido.

En este capítulo presentamos, de la forma más clara y escueta posible, los conceptos y resultados necesarios para el completo entendimiento del desarrollo de esta memoria. Haremos uso de los resultados más generales y elementales, en muchas ocasiones, sin mención explícita de ellos. A lo largo de la memoria, consideramos  $q = p^s$ , con  $p$  un número primo y  $\mathbb{F} = GF(q)$  el cuerpo de Galois de  $q$  elementos, de manera que:

- Si  $q = 2^2$ , entonces  $\alpha$  denota un elemento primitivo de  $\mathbb{F} = GF(4)$ , con

$$\alpha^2 + \alpha + 1 = 0.$$

- Si  $q = 2^3$ , entonces  $\alpha$  denota un elemento primitivo de  $\mathbb{F} = GF(8)$ , con  $\alpha^3 + \alpha + 1 = 0$ .
- Si  $q = 3^2$ , entonces  $\alpha$  denota un elemento primitivo de  $\mathbb{F} = GF(9)$ , con  $\alpha^2 + \alpha + 2 = 0$ .

## 1.2 Códigos bloque

**Definición 1.1:** Decimos que  $\mathcal{C}$  es un **código bloque lineal** de longitud  $N$  y dimensión  $K$  sobre  $\mathbb{F}$  si  $\mathcal{C}$  es un subespacio vectorial de  $\mathbb{F}^N$  de dimensión  $K$ . Decimos que una matriz  $G$  de tamaño  $N \times K$  es una **matriz generadora** de  $\mathcal{C}$  si sus columnas forman una base de  $\mathcal{C}$ . En este caso, el código  $\mathcal{C}$  está descrito por

$$\mathcal{C} = \{v \in \mathbb{F}^N \mid v = Gu \text{ con } u \in \mathbb{F}^K\}.$$

Nos referimos a  $\mathcal{C}$  como un  $[N, K]$ -código bloque, o simplemente  $[N, K]$ -código. Si la matriz generadora  $G$  del  $[N, K]$ -código  $\mathcal{C}$  viene dada como

$$G = \begin{pmatrix} I_K \\ P \end{pmatrix}$$

decimos que  $G$  es una **matriz generadora sistemática**. Decimos que  $u$  es el **vector de información** y  $v$  es el correspondiente vector código o **palabra código**. El **código dual** de  $\mathcal{C}$ , denotado por  $\mathcal{C}^\perp$ , es el  $[N, N - K]$ -código dado por

$$\mathcal{C}^\perp = \{v \in \mathbb{F}^N \mid G^T v = 0\}.$$

Llamamos **matriz de control de paridad** de  $\mathcal{C}$  a una matriz generadora de  $\mathcal{C}^\perp$ .

Los códigos bloque lineales son importantes porque su estructura algebraica hace sencilla su implementación. Ejemplos de códigos bloque se pueden encontrar, por ejemplo, en [61, 76, 87].

El parámetro más importante de un código bloque  $\mathcal{C}$  es la **distancia mínima**, denotada por  $d_{\min}(\mathcal{C})$ , ya que determina la capacidad del código de detectar y corregir errores. Si definimos el **peso de Hamming** de un vector  $v \in \mathbb{F}^N$ , denotado por  $\text{wt}(v)$ , como el número de sus componentes no nulas, la distancia mínima de  $\mathcal{C}$  se define

entonces como

$$d_{\min}(\mathcal{C}) = \min\{\text{wt}(v) \mid v \in \mathcal{C} \text{ con } v \neq 0\}.$$

Un código bloque  $\mathcal{C}$  con distancia mínima  $d_{\min}(\mathcal{C})$  puede detectar hasta  $d_{\min}(\mathcal{C}) - 1$  errores y puede corregir hasta  $\lfloor \frac{d_{\min}(\mathcal{C})-1}{2} \rfloor$  errores. Un buen código debe ser capaz de corregir el mayor número de errores como sea posible, por tanto, el objetivo principal en teoría de códigos bloque es la construcción de códigos con distancia mínima elevada. Singleton establece la siguiente cota superior para la distancia mínima del código bloque  $\mathcal{C}$ .

**Teorema 1.1 (Cota de Singleton):** *Sea  $\mathcal{C}$  un  $[N, K]$ -código lineal sobre un cuerpo cualquiera  $\mathbb{F}$ , entonces*

$$d_{\min}(\mathcal{C}) \leq N - K + 1. \quad (1.1)$$

Si un código bloque  $\mathcal{C}$  de tasa  $K/N$  alcanza esta cota, tiene la capacidad máxima de corregir errores, de entre todos los códigos bloque de tasa  $K/N$ . Decimos entonces que  $\mathcal{C}$  es un **código MDS** (*Maximum Distance Separable*), que viene caracterizado, en términos de su matriz generadora sistemática, como vemos en el resultado siguiente.

**Teorema 1.2 (Teorema 5.3.7 de [87]):** *Sea  $\mathcal{C}$  un  $[N, K]$ -código sobre  $\mathbb{F}$ , entonces las siguientes condiciones son equivalentes:*

- (a)  $\mathcal{C}$  es un código bloque MDS.
- (b) Si  $G = \begin{pmatrix} I_K \\ P \end{pmatrix}$  es una matriz generadora sistemática de  $\mathcal{C}$ , entonces toda submatriz de  $P$  es no singular.

Un ejemplo de código bloque MDS es el código Reed-Solomon, introducido por Reed y Solomon (de ahí su nombre) en el año 1960. Los códigos Reed-Solomon son códigos cíclicos no binarios y son, de hecho, un caso particular de otros códigos más generales, los códigos BCH, descubiertos paralelamente y de modo independiente por Hocquenghem en 1959 y Bose y Chaudhuri conjuntamente en 1960, como comentamos en el prólogo. Los códigos Reed-Solomon pueden ser descritos, como cualquier código cíclico, por un polinomio generador  $g(x)$ , de manera que todas las palabras código son múltiplos de dicho polinomio generador. Sea  $\alpha \in \mathbb{F}$  un elemento primitivo de  $\mathbb{F}$  y  $N = q - 1$ ; entonces un  $[N, K]$ -código Reed-Solomon, está generado por la matriz de

tamaño  $N \times K$  cuyas primeras filas y columnas son

$$G = \begin{pmatrix} g_0 & 0 & 0 & \cdots \\ g_1 & g_0 & 0 & \cdots \\ g_2 & g_1 & g_0 & \cdots \\ \vdots & \vdots & \vdots & \\ g_{N-K} & g_{N-K-1} & g_{N-K-2} & \cdots \\ 0 & g_{N-K} & g_{N-K-1} & \cdots \\ 0 & 0 & g_{N-K} & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix}$$

donde  $g_0, g_1, \dots, g_{N-K}$  son los coeficientes del polinomio generador de  $\mathcal{C}$ , cuyas raíces son potencias consecutivas de  $\alpha$ , es decir,

$$g(x) = g_0 + g_1x + \cdots + g_{N-K}x^{N-K} = (x - \alpha^b)(x - \alpha^{b+1}) \cdots (x - \alpha^{b+N-K-1})$$

con  $b$  un entero no negativo.

Los códigos Reed-Solomon son códigos bloque muy buenos debido a su estructura cíclica y a su capacidad correctora de errores; además, tienen un algoritmo algebraico de decodificación eficiente. Son códigos MDS y encuentran actualmente aplicación en áreas como la grabación de CD, telefonía móvil y sondas espaciales (la sonda Galileo a Júpiter en 1989, la sonda Magallanes a Venus ese mismo año o la sonda Ulises al Sol en 1990, por citar algunos ejemplos). La NASA utiliza una concatenación de un [255, 223]-código Reed-Solomon externo con un código convolucional interno de tasa  $1/2$  y un entrelazado de grado 4 entre los códigos externo e interno [105]. También es de destacar el empleo del código Reed-Solomon en las comunicaciones por satélite *Digital Video Broadcasting* (DVB), así como en los sistemas xDSL de comunicación por cable [85, 105]. Este tipo de código pertenece a la categoría FEC (*Forward Error Correction*), es decir, corrige los datos alterados en el receptor y para ello utiliza unos bits adicionales que permiten esta recuperación a posteriori.

## 1.3 Códigos convolucionales

En esta sección, introducimos en primer lugar el concepto de código convolucional y sus principales propiedades relacionadas con su matriz generadora, que empleamos

únicamente en el capítulo 2, ya que el resto de la memoria se centra en la construcción de códigos convolucionales empleando herramientas de la teoría de sistemas. También describimos en esta sección la construcción de códigos convolucionales introducida por Justesen [68], así como la técnica de perforación de códigos convolucionales que empleamos en el capítulo 2. A lo largo de la memoria, denotamos por  $\deg g(z)$  el grado del polinomio  $g(z)$ .

### 1.3.1 Propiedades estructurales

Si en vez de considerar matrices generadoras con elementos en  $\mathbb{F}$ , permitimos que éstos sean elementos de  $\mathbb{F}[z]$ , entonces obtenemos el concepto de código convolucional. Un **código convolucional**  $\mathcal{C}$  de **tasa**  $k/n$  es un submódulo de  $\mathbb{F}^n[z]$  (véase [91, 95, 118]). Como  $\mathbb{F}[z]$  es un dominio de ideales principales y  $\mathcal{C}$  es un submódulo del módulo libre  $\mathbb{F}^n[z]$ , el código  $\mathcal{C}$  es libre. Sea  $k$  el rango de  $\mathcal{C}$  y  $\{g_1(z), \dots, g_k(z)\} \subset \mathbb{F}^n[z]$  una base del módulo libre  $\mathcal{C}$ . Entonces, una matriz  $G(z)$  de tamaño  $n \times k$  cuya  $i$ -ésima columna es el vector polinómico  $g_i(z)$ , para  $i = 1, 2, \dots, k$ , es una **matriz generadora** o **codificador** de  $\mathcal{C}$ . El código convolucional  $\mathcal{C}$  está descrito entonces por

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

siendo  $u(z)$  el **vector información** y  $v(z)$  el vector código o **palabra código**.

Si  $v(z) = v_0 + v_1z + \dots + v_lz^l \in \mathbb{F}^n[z]$  (con  $l \geq 0$ ), definimos el **peso** de  $v(z)$ , denotado por  $\text{wt}(v(z))$ , como la suma de los pesos de Hamming de todos sus coeficientes, es decir,

$$\text{wt}(v(z)) = \sum_{i=0}^l \text{wt}(v_i).$$

Si  $\mathcal{C}$  es un código convolucional de tasa  $k/n$  generado por la matriz

$$G(z) = \begin{pmatrix} g_{11}(z) & g_{12}(z) & \cdots & g_{1k}(z) \\ g_{21}(z) & g_{22}(z) & \cdots & g_{2k}(z) \\ \vdots & \vdots & & \vdots \\ g_{n1}(z) & g_{n2}(z) & \cdots & g_{nk}(z) \end{pmatrix}, \quad (1.2)$$

entonces los grados de las columnas (que abreviaremos como grados columna) de la matriz generadora  $G(z)$  son los números naturales  $\nu_1, \nu_2, \dots, \nu_k$ , siendo

$$\nu_j = \max\{\deg(g_{ij}(z)) \mid 1 \leq i \leq n\}, \quad \text{para } j = 1, 2, \dots, k. \quad (1.3)$$

Tras permutar las columnas de  $G(z)$  si es necesario, asumimos que

$$\nu_1 \leq \nu_2 \leq \dots \leq \nu_k.$$

La **memoria** de la matriz generadora  $G(z)$  es  $\nu_k$ . El **grado**, **complejidad** o bien **longitud restrictiva** (en inglés, *constraint length* [32]) de  $G(z)$ , denotado por  $\delta_{G(z)}$ , viene dado por

$$\delta_{G(z)} = \sum_{i=1}^k \nu_i.$$

Dos matrices  $G_1(z)$  y  $G_2(z)$  generan el mismo código convolucional  $\mathcal{C}$  si y sólo si existe una matriz unimodular  $U(z) \in \mathbb{F}^{k \times k}[z]$  (es decir, el determinante de  $U(z)$  es un elemento no nulo de  $\mathbb{F}$ ) tal que  $G_1(z) = G_2(z)U(z)$ , y decimos que  $G_1(z)$  y  $G_2(z)$  son **matrices generadoras equivalentes**. Notemos que si trabajamos con módulos, la equivalencia entre matrices generadoras de un código convolucional es más restrictiva que si trabajamos en el marco de los espacios vectoriales, en los que dos matrices generadoras son equivalentes cuando están relacionadas por una matriz no singular [89].

La equivalencia en el marco de módulos entre dos matrices generadoras del código convolucional  $\mathcal{C}$ , permite definir la **complejidad** o **grado** de  $\mathcal{C}$ , denotado por  $\delta$ , como el grado máximo de todos los menores de tamaño  $k \times k$  de una matriz generadora  $G(z)$ . Notemos que, dado que trabajamos en módulos, este concepto es independiente de la elección de  $G(z)$ .

Para códigos convolucionales, la elección de la matriz generadora es de suma importancia. Una matriz generadora de un código convolucional es **catastrófica** [64] si existe un vector de información  $u(z)$  con infinitas componentes no nulas,  $\text{wt}(u(z)) = \infty$ , tal que proporciona una palabra código  $v(z)$  con un número finito de componentes no nulas,  $\text{wt}(v(z)) < \infty$ . Es decir, si  $G(z)$  es una matriz generadora no catastrófica, entonces las palabras código de peso finito sólo pueden ser obtenidas a partir de vectores de información con peso finito.

En el marco de espacios vectoriales, hay muchos tipos de matrices generadoras de un código convolucional, tales como matriz básica (es decir, matriz generadora polinómica que tiene inversa polinómica), matriz minimal y matriz minimal-básica. Ahora bien, si trabajamos en módulos, como es nuestro caso, el concepto de matriz básica carece de sentido. Únicamente tenemos el concepto de matriz generadora minimal (pueden encontrarse más detalles en [45, 63, 64, 79, 90]).

**Definición 1.2:** Sea  $\mathcal{C}$  un código convolucional de grado  $\delta$  y  $G(z)$  una matriz generadora de  $\mathcal{C}$  con grado  $\delta_{G(z)}$ . Decimos que  $G(z)$  es una **matriz minimal** de  $\mathcal{C}$  si y sólo si

$$\delta_{G(z)} = \delta.$$

Los **índices de Forney** [79] del código convolucional  $\mathcal{C}$  son los grados columna de cualquier matriz generadora minimal de  $\mathcal{C}$ . Notemos que los índices de Forney de un código son únicos, ya que si  $G_1(z)$  y  $G_2(z)$  son dos matrices generadoras minimales de  $\mathcal{C}$ , entonces tienen los mismos grados columnas (véase, por ejemplo, [118]).

Forney introdujo una caracterización muy útil de matriz generadora minimal. Con objeto de presentar dicha caracterización, introducimos la siguiente notación. Sea  $G(z)$  la matriz generadora del código convolucional  $\mathcal{C}$  dada por la expresión (1.2), sea  $\deg(g_{ij}) = s_{ij}$ , para  $i = 1, 2, \dots, n$  y  $j = 1, 2, \dots, k$  y consideremos

$$g_{ij}(z) = a_0^{(ij)} + a_1^{(ij)}z + a_2^{(ij)}z^2 + \dots + a_{s_{ij}}^{(ij)}z^{s_{ij}}$$

Entonces, denotamos por  $[G(z)]_h = \left( g_{ij}^{(h)} \right)$  la matriz de tamaño  $n \times k$ , siendo

$$g_{ij}^{(h)} = \begin{cases} a_{s_{ij}}^{(ij)} & \text{si } s_{ij} = \nu_j, \\ a_{s_{ij}}^{(ij)} & \text{si } s_{ij} < \nu_j, \end{cases}$$

para  $i = 1, 2, \dots, n$ ,  $j = 1, 2, \dots, k$ , con  $\nu_j$  el número definido por la expresión (1.3). La matriz  $[G(z)]_h$  se conoce como la **matriz de coeficientes principales** (en inglés, *leading coefficient matrix*). Tenemos entonces la siguiente caracterización de matriz minimal, obtenida al considerar el teorema 6 de [64] en el marco de módulos.

**Teorema 1.3:** Sea  $G(z)$  una matriz generadora del código convolucional  $\mathcal{C}$ . Las condiciones siguientes son equivalentes:

- (a)  $G(z)$  es una matriz minimal.
- (b) La matriz  $[G(z)]_h$  tiene rango completo.

Decimos que el código  $\mathcal{C}$  es **observable** si una matriz generadora, y por tanto cualquier otra matriz generadora, es prima por la derecha (en inglés, *right-prime*), 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  $G(z)$

es una matriz generadora de un código convolucional observable, entonces  $G(z)$  es no catastrófica.

A lo largo de la memoria, adoptaremos la notación introducida por McEliece [79] y nos referiremos a un código convolucional de tasa  $k/n$  y grado  $\delta$  como un  $(n, k, \delta)$ -código. Observemos que un código bloque es, en particular, un código convolucional con grado  $\delta = 0$ .

También emplearemos, en el capítulo 2, el concepto de código compacto (véase [79]).

**Definición 1.3:** Un  $(n, k, \delta)$ -código  $\mathcal{C}$  es **compacto** si tiene  $\delta \bmod k$  índices de Forney iguales a  $\lceil \frac{\delta}{k} \rceil$  y  $k - (\delta \bmod k)$  índices de Forney iguales a  $\lfloor \frac{\delta}{k} \rfloor$ .

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

$$d_{free}(\mathcal{C}) = \min\{\text{wt}(v(z)) \mid v(z) \in \mathcal{C} \text{ con } v(z) \neq 0\}. \quad (1.4)$$

Rosenthal y Smarandache [93] generalizaron la cota Singleton para códigos convolucionales. Si  $\mathcal{C}$  es un  $(n, k, \delta)$ -código sobre un cuerpo cualquiera  $\mathbb{F}$ , entonces

$$d_{free}(\mathcal{C}) \leq (n - k) \left( \left\lceil \frac{\delta}{k} \right\rceil + 1 \right) + \delta + 1.$$

Dicha cota se conoce como **cota Singleton generalizada**. Observemos que si  $\mathcal{C}$  es un código bloque, es decir,  $\delta = 0$ , la cota Singleton generalizada no es más que la cota Singleton existente para códigos bloque (véase la expresión (1.1)). De forma análoga a como definíamos un código bloque MDS, decimos que un  $(n, k, \delta)$ -código es **MDS** si su distancia libre alcanza la cota Singleton generalizada. Notemos que un código convolucional MDS es, en particular, un código compacto.

A continuación, analizamos la relación entre la distancia libre y el concepto de distancia columna conocido en la teoría de códigos [63]. Supongamos que

$$G(z) = G_0 + G_1 z + G_2 z^2 + \cdots + G_{\nu_k} z^{\nu_k}$$

es una matriz generadora de  $\mathcal{C}$  con grados columna  $\nu_1 \leq \nu_2 \leq \dots \leq \nu_k$ . Denotamos

entonces por

$$G = \begin{pmatrix} G_0 & O & O & \cdots \\ G_1 & G_0 & O & \cdots \\ G_2 & G_1 & G_0 & \cdots \\ \vdots & \vdots & \vdots & \\ G_{\nu_1} & G_{\nu_1-1} & G_{\nu_1-2} & \cdots \\ G_{\nu_1+1} & G_{\nu_1} & G_{\nu_1-1} & \cdots \\ \vdots & \vdots & \vdots & \\ G_{\nu_k} & G_{\nu_k-1} & G_{\nu_k-2} & \cdots \\ O & G_{\nu_k} & G_{\nu_k-1} & \cdots \\ O & O & G_{\nu_k} & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix}$$

la llamada **matriz generadora semi-infinita corregida** (en inglés, *semi-infinite sliding generator matrix*). En tal caso, podemos definir el código convolucional  $\mathcal{C}$  como

$$\mathcal{C} = \{G(u_0, u_1, \dots) \mid u_j \in \mathbb{F}^k \text{ para } j = 0, 1, \dots\}.$$

Siguiendo [63, 65], definimos la  $j$ -ésima **distancia columna** de  $\mathcal{C}$ , denotada por  $d_j^c(\mathcal{C})$ , como

$$d_j^c(\mathcal{C}) = \min_{u_0 \neq 0} \text{wt}(G_j^c u_{[0,j]}),$$

siendo  $G_j^c$  la submatriz formada por las  $n(j+1)$  primeras filas y las  $k(j+1)$  primeras columnas de la matriz semi-infinita  $G$ . Además, se verifica que

$$d_{free}(\mathcal{C}) = \lim_{j \rightarrow \infty} d_j^c(\mathcal{C}). \quad (1.5)$$

Gluesing-Luerssen, Rosenthal y Smarandache [44] prueban que la menor distancia columna del código  $\mathcal{C}$  que puede alcanzar la cota Singleton generalizada es  $d_M^c$ , siendo  $M = \lfloor \frac{\delta}{k} \rfloor + \lceil \frac{\delta}{n-k} \rceil$ , e introducen las definiciones siguientes.

**Definición 1.4 (Definición 1.8 de [62]):** Sea  $\mathcal{C}$  un  $(n, k, \delta)$ -código con distancias columnas  $d_j^c(\mathcal{C})$  y distancia libre  $d_{free}(\mathcal{C})$ .

(a)  $\mathcal{C}$  tiene **perfil de distancia máxima** si

$$d_j^c(\mathcal{C}) = (n - k)(j + 1) + 1 \quad \text{para } j = 0, 1, \dots, L$$

siendo

$$L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor. \quad (1.6)$$

(b)  $\mathcal{C}$  es un código **fuertemente MDS** si

$$d_M^c = (n-k) \left( \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) + \delta + 1.$$

**Observación 1.1:** Notemos que si  $n-k$  divide a  $\delta$ , entonces un  $(n, k, \delta)$ -código tiene perfil de distancia máxima si y sólo si es fuertemente MDS, ya que en este caso, tenemos que  $M = L$ . ■

El teorema siguiente proporciona la caracterización de códigos con perfil de distancia máxima en función de la matriz generadora.

**Teorema 1.4 (Teorema 2.12 de [44]):** Sea  $G(z) = \sum_{j=0}^{\nu_k} G_j z^j$  la matriz generadora de un  $(n, k, \delta)$ -código  $\mathcal{C}$  y consideremos la matriz

$$G_L^c = \begin{pmatrix} G_0 & G_1 & \cdots & G_L \\ O & G_0 & \cdots & G_{L-1} \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & G_0 \end{pmatrix} \in \mathbb{F}^{(L+1)n \times (L+1)k}.$$

Entonces  $\mathcal{C}$  es un código con perfil de distancia máxima si y sólo si todo menor de tamaño  $(L+1)k \times (L+1)k$  obtenido de las filas con índices  $1 \leq i_1 < \dots < i_{(L+1)k}$ , donde  $i_{sk+1} > sn$ , para  $s = 1, \dots, L$ , es no nulo.

### 1.3.2 Códigos convolucionales basados en la construcción de Justesen

Justesen [68] muestra que los polinomios generadores de ciertos códigos cíclicos definen códigos convolucionales no catastróficos cuyas distancias libres están acotadas inferiormente por las distancias mínimas de los códigos cíclicos. Empleando este resultado, construye códigos convolucionales con buena distancia libre a partir de códigos Reed-Solomon.

Sea  $N = p^s - 1$  la longitud de un código Reed-Solomon sobre  $\mathbb{F} = GF(p^s)$  y supongamos que  $\nu$  divide  $N$  y  $\kappa$  divide  $K$ . Sea también

$$g(z) = g_0(z^\nu) + zg_1(z^\nu) + z^2g_2(z^\nu) + \cdots + z^{\nu-1}g_{\nu-1}(z^\nu)$$

el polinomio generador del código bloque Reed-Solomon de tasa  $K/N = \kappa/\nu$ . Entonces, decimos que un código convolucional  $\mathcal{C}$  **está generado por el polinomio**  $g(z)$  (véase [68]) si su matriz generadora es de la forma

$$G(z) = \begin{pmatrix} g_0(z) & zg_{\nu-1}(z) & \cdots & zg_{\nu-\kappa+1}(z) \\ g_1(z) & g_0(z) & \cdots & zg_{\nu-\kappa+2}(z) \\ \vdots & \vdots & & \vdots \\ g_{\nu-1}(z) & g_{\nu-2}(z) & \cdots & g_{\nu-\kappa}(z) \end{pmatrix}. \quad (1.7)$$

Obtenemos entonces que  $G(z)$  es una matriz minimal (véase por ejemplo [68, 101]). La distancia libre del código convolucional obtenido de esta construcción es  $N - K + 1$ , como prueba Justesen [68] en el teorema siguiente, que utilizaremos posteriormente en el capítulo 2.

**Teorema 1.5 (Teorema 4 de [68]):** Si  $g(z)$  es el polinomio generador de un código Reed-Solomon de tasa  $K/N = \kappa/\nu$  sobre  $\mathbb{F}$ , entonces el código convolucional de tasa  $\kappa/\nu$  generado por la matriz  $G(z)$  dada en (1.7) es no catastrófica y tiene distancia libre  $d_{free}(\mathcal{C}) = N - K + 1$ .

### 1.3.3 Códigos convolucionales perforados

En esta memoria, emplearemos la técnica de perforación de códigos convolucionales introducido por McEliece [79]. Según esta técnica, un paso previo a la obtención de dicho código es la construcción del código original por bloques de profundidad  $M$ , obteniendo entonces un  $(\nu M, \kappa M, \delta)$ -código. Por tanto, comenzamos describiendo este paso intermedio necesario para la perforación de un código convolucional.

**Definición 1.5 (Definición 8.1 de [79]):** Si  $f(z) = a_0 + a_1z + a_2z^2 + \cdots$  es una serie de potencias (o bien un polinomio) en la indeterminada  $z$ , entonces para cualquier entero  $M \geq 1$ , la  $M$ -ésima **descomposición polifásica** de  $f(z)$  es

$$(f_0(z), f_1(z), \dots, f_{M-1}(z))$$

en donde

$$f_j(z) = \sum_{h \geq 0} a_{hM+j} z^h \quad \text{para } j = 0, 1, \dots, M-1$$

se conoce como la  $(j, M)$ -ésima **componente polifásica** de  $f(z)$ .

Las componentes de la  $M$ -ésima descomposición polifásica se emplean para construir la llamada  $M$ -ésima matriz policíclica pseudocirculante (o abreviadamente, PCPC) asociada a  $f(z)$ .

**Definición 1.6 (Definición 8.2 de [79]):** Sea  $f(z) = a_0 + a_1z + a_2z^2 + \dots$  una serie de potencias (o bien un polinomio) en la indeterminada  $z$ . Supongamos que para cualquier  $M \geq 1$ ,  $(f_0(z), f_1(z), \dots, f_{M-1}(z))$  es la  $M$ -ésima descomposición polifásica de  $f(z)$ . Entonces, la  $M$ -ésima matriz **policíclica pseudocirculante (PCPC)** asociada a  $f(z)$  es la matriz polinómica de tamaño  $M \times M$  dada por

$$f^{[M]}(z) = \begin{pmatrix} f_0(z) & zf_{M-1}(z) & zf_{M-2}(z) & \cdots & zf_1(z) \\ f_1(z) & f_0(z) & zf_{M-1}(z) & \cdots & zf_2(z) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{M-1}(z) & f_{M-2}(z) & f_{M-3}(z) & \cdots & f_0(z) \end{pmatrix}.$$

El teorema siguiente proporciona una descripción algebraica de la matriz generadora  $G^{[M]}(z)$  del código de tasa  $\kappa M/\nu M$  obtenida de la descomposición del  $(\nu, \kappa, \delta)$ -código (con matriz generadora  $G(z)$ ) en bloques de profundidad  $M$ .

**Teorema 1.6 (Teorema 8.3 de [79]):** Sea  $\mathcal{C}$  un  $(\nu, \kappa, \delta)$ -código. Entonces, el código obtenido de la descomposición de  $\mathcal{C}$  en bloques de profundidad  $M$ , denotado por  $\mathcal{C}^{[M]}$ , es un código de tasa  $\kappa M/\nu M$ . Si  $G(z) = (g_{i,j}(z))$  es una matriz generadora polinómica de tamaño  $\nu \times \kappa$  del código original  $\mathcal{C}$ , entonces una matriz generadora de  $\mathcal{C}^{[M]}$ , denotada por  $G^{[M]}(z)$ , se obtiene de  $G(z)$  reemplazando cada entrada  $g_{i,j}(z)$  de  $G(z)$  por la correspondiente  $M$ -ésima matriz PCPC, intercalando entonces las columnas hasta la profundidad  $M$ .

Una consecuencia importante del teorema anterior es el resultado siguiente.

**Corolario 1.1 (Corolario 8.4 de [79]):** Sean  $(e_1, e_2, \dots, e_\kappa)$  los grados columna de la matriz generadora  $G(z)$ . Entonces, los grados columna de  $G^{[M]}(z)$  son

$$(\lfloor e_i/M \rfloor, \lfloor (e_i + 1)/M \rfloor, \dots, \lfloor (e_i + M - 1)/M \rfloor) \quad \text{para } i = 1, \dots, \kappa.$$

En otras palabras, cada grado columna  $e$  de  $G(z)$  es reemplazado por  $M$  grados columna en  $G^{[M]}(z)$ . Es más, si  $e = e'M + r$ , con  $0 \leq r < M$ , entonces  $M - r$  de estos grados son iguales a  $e'$  y  $r$  son iguales a  $e' + 1$ . Observemos que de hecho,  $e' = \lfloor e/M \rfloor$ . La suma de los grados columna de  $G^{[M]}(z)$ , es decir, el grado de  $G^{[M]}(z)$ , es entonces el mismo que el de  $G(z)$ .

La matriz generadora  $G^{[M]}(z)$  obtenida de la descomposición por bloques de profundidad  $M$  de la matriz generadora minimal  $G(z)$ , es también minimal, como pone de manifiesto el resultado siguiente.

**Teorema 1.7 (Teorema 8.5 de [79]):** Si  $G(z)$  es una matriz generadora minimal de  $\mathcal{C}$ , entonces  $G^{[M]}(z)$  es una matriz generadora minimal de  $\mathcal{C}^{[M]}$ . Por tanto, el grado del código obtenido por descomposición en bloques,  $\mathcal{C}^{[M]}$ , es el mismo que el del código original.

Observemos que no sólo el grado es el mismo para los códigos  $\mathcal{C}$  y  $\mathcal{C}^{[M]}$ ; el código original  $\mathcal{C}$  y todos los códigos por bloques obtenidos de él, tienen la misma distancia libre, ya que el conjunto de palabras código es el mismo para todos los valores de  $M$ .

Teniendo en cuenta ahora esta observación, junto con el teorema 1.6 y el corolario 1.1, tenemos una relación entre los índices de Forney del código  $\mathcal{C}^{[M]}$  y del código  $\mathcal{C}$ , como muestra el resultado siguiente.

**Corolario 1.2 (Corolario 8.6 de [79]):** Si  $\mathcal{C}^{[M]}$  es el código por bloques de profundidad  $M$  obtenido de un  $(\nu, \kappa, \delta)$ -código  $\mathcal{C}$  con distancia libre  $d_{free}(\mathcal{C})$ , entonces  $\mathcal{C}^{[M]}$  es un  $(\nu M, \kappa M, \delta)$ -código con la misma distancia libre,  $d_{free}(\mathcal{C}^{[M]}) = d_{free}(\mathcal{C})$ . Si los índices de Forney del código original son  $(e_1, e_2, \dots, e_\kappa)$ , entonces los índices de Forney de  $\mathcal{C}^{[M]}$  son

$$(\lfloor e_i/M \rfloor, \lfloor (e_i + 1)/M \rfloor, \dots, \lfloor (e_i + M - 1)/M \rfloor) \quad \text{para } i = 1, 2, \dots, \kappa.$$

La técnica de perforación de códigos convolucionales que empleamos en la memoria se describe entonces como sigue. Comenzamos con un  $(\nu, \kappa, \delta)$ -código y lo descomponemos en bloques de profundidad  $M$ , es decir, agrupamos la sucesión de entradas en bloques de  $M$  componentes cada una. El resultado es un  $(\nu M, \kappa M, \delta)$ -código con la misma distancia libre que el código patrón. A continuación, consideramos la matriz de perforación  $P$ , es decir, una matriz de tamaño  $\nu \times M$  cuyos elementos son 0 y 1 de manera que el número de unos es  $\tilde{N}$  y el número de ceros es  $\nu M - \tilde{N}$  (con  $\tilde{N} < \nu M$  y  $N > \kappa M$ ). Entonces, si borramos o perforamos  $\nu M - \tilde{N}$  componentes de cada salida empleando la matriz  $P$  como patrón, el resultado es un  $(\tilde{N}, \kappa M, \tilde{\delta})$ -código convolucional que llamamos código convolucional perforado, verificándose que  $\tilde{\delta} \leq \delta$ .

**Definición 1.7 (Definición 8.9 de [79]):** Si  $G(z)$  es una matriz polinómica de tamaño  $\nu \times \kappa$  y  $P$  es una matriz de tamaño  $\nu \times M$  compuesta por ceros y unos, las  $\nu M$  filas de la matriz  $G^{[M]}(z)$  están en correspondencia biunívoca con las  $\nu M$  entradas de  $P$  y la matriz  $G_P(z)$  es la matriz obtenida de  $G^{[M]}(z)$  al borrar aquellas filas que corresponden con las entradas 0 en  $P$ . El código definido por la matriz generadora  $G_P(z)$  se llama **código convolucional perforado** obtenido de  $\mathcal{C}$  según  $P$ .

## 1.4 Sistemas lineales invariantes en el tiempo

Con objeto de estudiar los códigos convolucionales desde el punto de vista de sistemas lineales, describimos en esta sección los conceptos y resultados de teoría de sistemas discretos invariantes en el tiempo necesarios para dicho estudio. Las demostraciones de los teoremas que se presentan en esta sección pueden encontrarse en [30, 70].

Consideremos las matrices  $\mathcal{A} \in \mathbb{F}^{\delta \times \delta}$ ,  $\mathcal{B} \in \mathbb{F}^{\delta \times k}$ ,  $\mathcal{C} \in \mathbb{F}^{n \times \delta}$  y  $\mathcal{D} \in \mathbb{F}^{n \times k}$ . Estas matrices definen un **sistema lineal invariante en el tiempo** a través de las ecuaciones siguientes:

$$\begin{aligned} x_{t+1} &= \mathcal{A}x_t + \mathcal{B}u_t, & x_0 &= 0, \\ v_t &= \mathcal{C}x_t + \mathcal{D}u_t. \end{aligned} \tag{1.8}$$

Decimos entonces que la cuádrupla de matrices  $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  es una **realización** para el sistema lineal (1.8), siendo  $x_t \in \mathbb{F}^{\delta}$  el **vector de estados**,  $u_t \in \mathbb{F}^k$  el **vector**

**información** o **vector de entradas** y  $v_t \in \mathbb{F}^{n-k}$  el **vector de salidas**. En sistemas lineales, la representación anterior se conoce como la **representación espacio-estado**.

Esta representación, tiene asociada una matriz racional, llamada **función de transferencia**, que relaciona la salida del sistema y la entrada y viene dada por

$$T(z) = \mathcal{C}(zI - \mathcal{A})^{-1} \mathcal{B} + \mathcal{D}. \quad (1.9)$$

Recordemos que una función racional  $\frac{p(z)}{q(z)} \in \mathbb{F}(z)$  es **propia** si  $\deg q(z) > \deg p(z)$ . De este modo, una matriz  $R(z)$  con entradas en  $\mathbb{F}(z)$  es una **función de transferencia propia** si cada entrada de  $R(z)$  es una función racional propia.

Kalman [71] introdujo los conceptos de controlabilidad (con una elección adecuada de entradas, se puede llevar un vector de estados dado a cualquier otro vector de estados en tiempo finito). y de observabilidad (si se observan las entrada y salidas de un sistema en un período suficiente de tiempo, entonces se puede determinar exactamente el estado interno del sistema). Consideremos una realización  $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  para un sistema lineal dado en representación espacio-estado. Para cada un entero positivo  $j$  consideremos las matrices

$$\Phi_j(\mathcal{A}, \mathcal{B}) = \begin{pmatrix} \mathcal{B} & \mathcal{A}\mathcal{B} & \cdots & \mathcal{A}^{j-2}\mathcal{B} & \mathcal{A}^{j-1}\mathcal{B} \end{pmatrix} \quad \text{y} \quad \Omega_j(\mathcal{A}, \mathcal{C}) = \begin{pmatrix} \mathcal{C} \\ \mathcal{C}\mathcal{A} \\ \mathcal{C}\mathcal{A}^2 \\ \vdots \\ \mathcal{C}\mathcal{A}^{j-1} \end{pmatrix}.$$

**Definición 1.8:** Sean  $\mathcal{A}$  y  $\mathcal{B}$  matrices de tamaños  $\delta \times \delta$  y  $\delta \times k$ , respectivamente. Entonces, el par  $(\mathcal{A}, \mathcal{B})$  es **controlable** si

$$\text{rg } \Phi_\delta(\mathcal{A}, \mathcal{B}) = \delta.$$

Si  $(\mathcal{A}, \mathcal{B})$  es un par controlable, entonces el menor entero  $\kappa$  con la propiedad de que  $\text{rg } \Phi_\kappa(\mathcal{A}, \mathcal{B}) = \delta$  es el **índice de controlabilidad** de  $(\mathcal{A}, \mathcal{B})$ .

Ahora bien, por el llamado test de Popov-Belevitch-Hautus, **test PBH**, (véase [53], o [70, Teorema 6.2-6]), el par  $(\mathcal{A}, \mathcal{B})$  es controlable si y sólo si

$$\text{rg} \begin{pmatrix} zI - \mathcal{A} & \mathcal{B} \end{pmatrix} = \delta, \quad \text{para todo } z \in \overline{\mathbb{F}}.$$

Observemos además, por ser la matriz  $\mathcal{A}$  de tamaño  $\delta \times \delta$ , que

$$\operatorname{rg} \begin{pmatrix} zI - \mathcal{A} & \mathcal{B} \end{pmatrix} = \delta \quad \text{para todo } z \in \overline{\mathbb{F}}$$

si y sólo si

$$\operatorname{rg} \begin{pmatrix} zI - \mathcal{A} & \mathcal{B} \end{pmatrix} = \delta \quad \text{para todo } z \text{ valor propio de } \mathcal{A}.$$

De manera similar, definimos el concepto de par observable.

**Definición 1.9:** Sea  $\mathcal{A}$  una matriz de tamaño  $\delta \times \delta$  y sea  $\mathcal{C}$  una matriz de tamaño  $n \times \delta$ . Entonces, el par  $(\mathcal{A}, \mathcal{C})$  es **observable** si

$$\operatorname{rg} \Omega_\delta(\mathcal{A}, \mathcal{C}) = \delta,$$

Si  $(\mathcal{A}, \mathcal{C})$  es observable, entonces el menor entero  $\nu$  con la propiedad de que  $\operatorname{rg} \Omega_\nu(\mathcal{A}, \mathcal{C}) = \delta$  es el **índice de observabilidad** de  $(\mathcal{A}, \mathcal{C})$ .

De nuevo, por el llamado test PBH, el par  $(\mathcal{A}, \mathcal{C})$  es observable si y sólo si

$$\operatorname{rg} \begin{pmatrix} zI - \mathcal{A} \\ \mathcal{C} \end{pmatrix} = \delta, \quad \text{para todo } z \in \overline{\mathbb{F}},$$

siendo esta condición equivalente, a su vez, a

$$\operatorname{rg} \begin{pmatrix} zI - \mathcal{A} \\ \mathcal{C} \end{pmatrix} = \delta \quad \text{para todo } z \text{ valor propio de } \mathcal{A}.$$

Hay múltiples realizaciones  $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  para un sistema lineal dado. En particular,  $\delta$ , el tamaño de la matriz  $\mathcal{A}$  no es constante en el conjunto de todas las realizaciones. Como  $\delta$  siempre es un entero positivo, debe alcanzar un valor mínimo para cierta realización. Dicho valor mínimo de  $\delta$  se llama **el grado de McMillan** del sistema. Una realización  $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  para la cual  $\delta$  es igual al grado de McMillan, decimos que es una **representación minimal**. La propiedad de minimalidad de una realización está relacionada con los conceptos de controlabilidad y observabilidad (véase por ejemplo, [18, 70]).

**Teorema 1.8 (Teorema 3.9 de [4]):** *La realización  $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  de un sistema lineal es minimal si y sólo si  $(\mathcal{A}, \mathcal{B})$  es un par controlable y  $(\mathcal{A}, \mathcal{C})$  es un par observable.*

Dada una realización  $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  no minimal de un sistema lineal, Kalman [71] establece que dicho sistema contiene un “subsistema” controlable. De forma más precisa, tenemos el resultado siguiente.

**Teorema 1.9:** *Con la notación anterior, supongamos que la matriz de controlabilidad  $\Phi_\delta(\mathcal{A}, \mathcal{B})$  tiene rango  $r < \delta$ . Entonces, existe una matriz invertible  $S$  de tamaño  $\delta \times \delta$  tal que*

$$SAS^{-1} = \begin{pmatrix} \mathcal{A}_1 & \mathcal{A}_2 \\ O & \mathcal{A}_3 \end{pmatrix}, \quad S\mathcal{B} = \begin{pmatrix} \mathcal{B}_1 \\ O \end{pmatrix} \quad y \quad \mathcal{C}S^{-1} = \begin{pmatrix} \mathcal{C}_1 & \mathcal{C}_2 \end{pmatrix} \quad (1.10)$$

siendo  $\mathcal{A}_1 \in \mathbb{F}^{r \times r}$ ,  $\mathcal{B}_1 \in \mathbb{F}^{r \times k}$  y  $\mathcal{C}_1 \in \mathbb{F}^{n \times r}$ . Además,

- (a) el par  $(\mathcal{A}_1, \mathcal{B}_1)$  es controlable.
- (b)  $\mathcal{C}(zI - \mathcal{A})^{-1}\mathcal{B} = \mathcal{C}_1(zI - \mathcal{A}_1)^{-1}\mathcal{B}_1$ .

## 1.5 Sistemas lineales y códigos convolucionales

A lo largo de esta memoria consideramos básicamente, excepto en el capítulo 2, una representación de códigos convolucionales en teoría de sistemas lineales, conocida como la representación entrada-estado-salida o representación  $(A, B, C, D)$ , introducida por Rosenthal, Schumacher y York [91]. Dicha representación ha sido empleada en los últimos años en el análisis y construcción de códigos convolucionales; véase, por ejemplo, [3, 62, 89, 91, 92, 94, 95, 102, 118]. Así pues, describimos a continuación los códigos convolucionales desde el punto de vista de la teoría de sistemas lineales. En la sección anterior hemos analizado la representación espacio-estado de un sistema lineal invariante en el tiempo. Sin embargo, aunque muchos autores emplean dicha representación, ésta no es la mejor para la construcción de códigos convolucionales, como veremos posteriormente. Consideremos ahora 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  $\mathcal{C}$  de tasa  $k/n$  y grado  $\delta$  puede ser descrito por el sistema lineal gobernado por las ecuaciones

$$\begin{aligned}
x_{t+1} &= Ax_t + Bu_t, \\
y_t &= Cx_t + Du_t, \\
v_t &= \begin{pmatrix} y_t \\ u_t \end{pmatrix}, \quad x_0 = 0,
\end{aligned} \tag{1.11}$$

siendo  $x_t \in \mathbb{F}^\delta$  el **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**. Esta representación es conocida como la **representación entrada-estado-salida**. Precisamente, el grado  $\delta$  del código convolucional coincide con el grado de McMillan del sistema lineal (1.11). El grado de McMillan es igual a la dimensión del espacio de estados  $\mathbb{F}^\delta$ .

Ahora bien, dicha representación es diferente a la representación espacio-estado,

$$\begin{aligned}
x_{t+1} &= \mathcal{A}x_t + \mathcal{B}u_t \\
y_t &= \mathcal{C}x_t + \mathcal{D}u_t
\end{aligned} \tag{1.12}$$

La representación (1.12) fue usada por Massey y Sain [78, Teorema 1] y se convirtió en la manera estándar en la que los códigos convolucionales eran presentados en términos de sistemas lineales (véase [79]). Observemos que en la representación entrada-estado-salida, la palabra código se particiona, estando compuesta por el vector de paridad y el vector información. De hecho, la diferencia entre (1.11) y (1.12) se ve claramente en el caso particular cuando  $\delta = 0$ , caso en el que el código convolucional no tiene memoria (es un código bloque). Para ello, denotemos por  $I_{n-k}$  la matriz identidad de tamaño  $(n-k) \times (n-k)$ . Las ecuaciones (1.11) se reducen entonces a la ecuación de paridad

$$\begin{pmatrix} I_{n-k} & -D \end{pmatrix} \begin{pmatrix} y_t \\ u_t \end{pmatrix} = 0. \tag{1.13}$$

Sin embargo, la expresión (1.12) se reduce a

$$\begin{pmatrix} y_t \\ u_t \end{pmatrix} = v_t = \mathcal{D}u_t.$$

Como vemos en esta sección, la representación entrada-estado-salida es la más adecuada para la construcción de códigos convolucionales. Los conceptos de controlabilidad y observabilidad empleados en la teoría de sistemas lineales, siguen siendo válidos para

esta representación, así como el teorema 1.9. Es importante señalar que mientras que en la teoría de sistemas lineales, una realización es minimal si y sólo si el par  $(A, B)$  es controlable y el par  $(A, C)$  es observable (véase el teorema 1.8), para la representación entrada-estado-salida no tenemos el mismo resultado. De hecho, basta con que el par  $(A, B)$  sea controlable para que dicha representación sea minimal.

En términos de la representación entrada-estado-salida, tenemos la siguiente caracterización de la distancia libre

$$d_{free}(\mathcal{C}) = \min \left\{ \sum_{t=0}^{\infty} \text{wt}(u_t) + \sum_{t=0}^{\infty} \text{wt}(y_t) \right\}, \quad (1.14)$$

en donde el mínimo se considera sobre todas las palabras código no nulas.

Debido a razones algebraicas, asumimos a lo largo de la memoria que las palabras código son de peso finito.

**Definición 1.10 (Definición 2.3 de [95]):** Una sucesión

$$\left\{ \begin{pmatrix} y_t \\ u_t \end{pmatrix} \in \mathbb{F}^n \mid t = 0, 1, 2, \dots \right\} \quad (1.15)$$

representa una **palabra de peso finito** si se satisfacen las dos condiciones siguientes

- (a) La ecuación (1.11) se satisface para todo  $t \in \mathbb{Z}_+$ , siendo  $\mathbb{Z}_+$  el conjunto de los enteros positivos.
- (b) Existe un entero  $\gamma$  tal que  $x_{\gamma+1} = 0$  y  $u_t = 0$  para todo  $t \geq \gamma + 1$ .

La definición anterior implica, en particular, que  $y_t = 0$ , para  $t \geq \gamma + 1$  y, por tanto, la sucesión de palabras código (1.15) tiene peso finito. Entonces, para una palabra código de peso finito, se requiere que tanto la sucesión de entradas como la sucesión de estados (y por consiguiente, la sucesión de salidas) tengan peso finito.

El conjunto de palabras código de peso finito puede ser caracterizada a través de una matriz de paridad, empleada en [95] para la construcción de códigos convolucionales. En este teorema, y en todo lo que sigue, denotamos por  $O$  la matriz nula del tamaño apropiado.

**Teorema 1.10 (Proposición 2.4 de [95]):** Sea  $\mathcal{T}_\gamma$  la matriz definida por

$$\mathcal{T}_\gamma = \begin{pmatrix} D & O & \cdots & O & O \\ CB & D & \cdots & O & O \\ CAB & CB & \cdots & O & O \\ \vdots & \vdots & & \vdots & \vdots \\ CA^{\gamma-1}B & CA^{\gamma-2}B & \cdots & CB & D \end{pmatrix}.$$

Entonces,  $\left\{ \begin{pmatrix} y_t \\ u_t \end{pmatrix} \in \mathbb{F}^n \mid t = 0, 1, \dots, \gamma \right\}$  representa una palabra de peso finito si y sólo si

$$\left( \begin{array}{c|cccc} O & A^\gamma B & A^{\gamma-1}B & \cdots & AB & B \\ \hline -I & & \mathcal{T}_\gamma & & & \end{array} \right) \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_j \\ u_0 \\ u_1 \\ \vdots \\ u_j \end{pmatrix} = 0. \quad (1.16)$$

El conjunto de palabras de peso finito tiene una estructura de módulo sobre el anillo de polinomios  $\mathbb{F}[z]$  (véase [95]). Haciendo un abuso de notación, denotamos este módulo por  $\mathcal{C}(A, B, C, D)$ , que denominamos **código convolucional de peso finito** generado por las matrices  $A, B, C, D$ .

En la teoría de códigos, es costumbre definir un código convolucional como un  $\mathcal{F}$ -subespacio lineal de  $\mathcal{F}^n$ , en donde  $\mathcal{F}$  denota el cuerpo de las funciones racionales  $\mathbb{F}(z)$  o bien el cuerpo de las series de Laurent  $\mathbb{F}((z))$  (véase [42, 64, 63, 79, 82]). Si  $G(z)$  es una matriz generadora del código  $\mathcal{C}(A, B, C, D)$ , entonces  $G(z)$  induce un código convolucional  $\widehat{\mathcal{C}}(A, B, C, D) \subset \mathcal{F}^n$  definido como el  $\mathcal{F}$ -espacio generado por las columnas de  $G(z)$ . Notemos que esta definición es independiente de la matriz generadora  $G(z)$  de  $\mathcal{C}(A, B, C, D)$ . La distancia libre del código convolucional  $\widehat{\mathcal{C}}$  se define por la expresión (1.14), donde el mínimo se considera sobre todas las posibles palabras código no nulas de  $\widehat{\mathcal{C}}$  (véase [63, 82]). El lema siguiente pone de manifiesto que para construcciones

de códigos convolucionales es suficiente con considerar el código convolucional de peso finito  $\mathcal{C}(A, B, C, D)$ .

**Lema 1.1 (Lema 2.13 de [95]):** Sea  $\widehat{\mathcal{C}}(A, B, C, D) \subset \mathcal{F}^n$  el código convolucional descrito por las matrices  $A$ ,  $B$ ,  $C$  y  $D$ . Supongamos que el par  $(A, C)$  es observable. Si en la expresión (1.14) consideramos el mínimo de entre todas las palabras código no nulas de  $\widehat{\mathcal{C}}$ , entonces el valor mínimo se alcanza en una palabra código del código convolucional de peso finito  $\mathcal{C}(A, B, C, D)$ .

Si el par  $(A, C)$  no es observable, entonces la minimización sobre las palabras código no nulas de  $\widehat{\mathcal{C}}(A, B, C, D)$  es, en general, más pequeña que la minimización sobre las palabras código no nulas de  $\mathcal{C}(A, B, C, D)$ . A lo largo de la memoria, suponemos que  $\mathcal{C}(A, B, C, D)$  es un código convolucional de peso finito.

A continuación, presentamos la conexión entre la teoría de sistemas y las representaciones con matrices polinómicas de códigos convolucionales. El lema siguiente proporciona cómo obtener una matriz generadora polinómica de  $\mathcal{C}(A, B, C, D)$ .

**Lema 1.2 (Lema 2.5 de [95]):** Sea  $\mathcal{C}(A, B, C, D)$  un código convolucional. Entonces existen matrices polinómicas  $X(z)$ ,  $Y(z)$  y  $U(z)$  de tamaños  $\delta \times k$ ,  $(n - k) \times k$  y  $k \times k$ , respectivamente, tales que

$$\ker_{\mathbb{F}[z]} \begin{pmatrix} zI - A & O & -B \\ -C & I & -D \end{pmatrix} = \text{Im}_{\mathbb{F}[z]} \begin{pmatrix} X(z) \\ Y(z) \\ U(z) \end{pmatrix}. \quad (1.17)$$

Es más, la matriz polinomial

$$G(z) = \begin{pmatrix} Y(z) \\ U(z) \end{pmatrix}$$

describe una matriz generadora polinomial para el  $(n, k, \delta)$ -código asociado al sistema lineal (1.11).

Como vimos en la sección 1.3, la elección de la matriz generadora es de suma importancia. A continuación, estamos interesados en establecer condiciones para las matrices  $A$ ,  $B$ ,  $C$  y  $D$  que garanticen que la matriz generadora polinómica  $G(z)$  que inducen sea no catastrófica. El resultado siguiente caracteriza los códigos observables.

**Teorema 1.11 (Lema 2.11 de [95]):** *Supongamos que el par  $(A, B)$  es controlable. El código convolucional  $\mathcal{C}(A, B, C, D)$  definido por (1.11) representa un código observable si y sólo si el par  $(A, C)$  es observable.*

Es importante recalcar que un resultado análogo al teorema 1.11 para la representación espacio-estado no existe, como ponemos de manifiesto en el ejemplo siguiente.

**Ejemplo 1.1 (Ejemplo 2.12 de [95]):** Sea  $\mathcal{C}$  el código convolucional de tasa  $1/2$  sobre  $\mathbb{F} = GF(2)$  con matriz generadora catastrófica

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

La representación espacio-estado para este sistema viene dada por

$$\begin{aligned} x_{t+1} &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} x_t + \begin{pmatrix} 1 \\ 0 \end{pmatrix} u_t, \\ y_t &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x_t + \begin{pmatrix} 1 \\ 1 \end{pmatrix} u_t. \end{aligned}$$

Aunque la matriz  $G(z)$  es catastrófica, tenemos que el par

$$\left( \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$$

es controlable y el par

$$\left( \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right)$$

es observable. ■

Es más, podemos demostrar que cualquier matriz generadora polinómica catastrófica  $G(z)$  tiene una representación espacio-estado  $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  dada por (1.12) de manera que  $(\mathcal{A}, \mathcal{B})$  y  $(\mathcal{A}, \mathcal{C})$  son controlables y observables, respectivamente. Así pues, la representación espacio-estado no es buena para la construcción de códigos convolucionales. Hay otra peculiaridad de la representación espacio-estado. Si  $G(z)$  es una matriz generadora polinómica, entonces la matriz  $\mathcal{A}$  de (1.12) necesariamente es nilpotente. Por

todas estas razones, es preferible trabajar con la representación entrada-estado-salida (1.11) de un código.

Podemos obtener una matriz de transferencia del código  $\widehat{\mathcal{C}}(A, B, C, D)$  a partir de las matrices  $A, B, C$  y  $D$  que lo describen, como pone de manifiesto el resultado siguiente (notemos que la matriz de transferencia puede ser una matriz racional, por lo que debemos considerar el código  $\widehat{\mathcal{C}}(A, B, C, D)$ , definido sobre  $\mathcal{F}$ . Véanse los comentarios anteriores al lema 1.1).

**Teorema 1.12 (Lema 2.14 de [95]):** *Con la notación empleada en el lema 1.2. Las matrices  $A, B, C, D$  de (1.17) representan una realización de entrada-estado-salida de la función de transferencia  $Y(z)U(z)^{-1}$ , es decir, se tiene la siguiente relación:*

$$C(zI - A)^{-1}B + D = Y(z)U(z)^{-1}$$

En particular,

$$T(z) = Y(z)U(z)^{-1} = C(zI - A)^{-1}B + D \quad (1.18)$$

es una función de transferencia propia de  $\widehat{\mathcal{C}}(A, B, C, D)$ .

**Observación 1.2:** Si las matrices polinómicas  $U(z)$  y  $Y(z)$  son tales que  $Y(z)U(z)^{-1}$  es una función de transferencia propia, entonces siempre existen matrices  $A, B, C$  y  $D$  satisfaciendo (1.18). El sistema dinámico (1.11) se llama entonces una realización espacio-estado de la matriz de transferencia  $Y(z)U(z)^{-1}$ . Si  $U(z)$  no es invertible o bien  $Y(z)U(z)^{-1}$  no es propia, entonces se necesita una descripción espacio-estado más general, como la descripción  $(K, L, M)$  que podemos ver en [91, Teorema 3.1]. ■

Podemos ver la función de transferencia  $Y(z)U(z)^{-1}$  de dos maneras. En la teoría de códigos es costumbre considerar el código  $\widehat{\mathcal{C}}(A, B, C, D) \subset \mathcal{F}^n$ , como el  $\mathcal{F}$ -subespacio vectorial generado por las columnas de  $G(z)$ . Como matriz generadora sobre  $\mathcal{F}$ ,  $G(z)$  es equivalente a la matriz generadora sistemática

$$\begin{pmatrix} Y(z)U(z)^{-1} \\ I_k \end{pmatrix}$$

y podemos entonces considerar la codificación como una aplicación lineal

$$\begin{aligned} \phi &: \mathcal{F}^k &\rightarrow \mathcal{F}^{n-k} \\ u(z) &\mapsto y(z) = Y(z)U(z)^{-1}u(z) \end{aligned}$$

Bajo este punto de vista, no hay restricciones sobre  $u(z) \in \mathcal{F}^k$ . De manera alternativa,  $Y(z)U(z)^{-1}$  describe un homomorfismo de módulos entre el módulo generado por las columnas de  $U(z)$  y el módulo generado por las columnas de  $Y(z)$ . Desde este punto de vista, consideramos que el vector información  $u(z)$  pertenece al módulo generado por las columnas de  $U(z)$ . Esta restricción nos garantiza que la sucesión de vectores de estados  $x_0, x_1, x_2, \dots$  alcanza el estado cero en un tiempo finito.

En términos de la representación entrada-estado-salida, tenemos la siguiente caracterización de la  $j$ -ésima distancia columna del código convolucional  $\mathcal{C}$

$$d_j^c(\mathcal{C}) = \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\}, \quad \text{para } j = 0, 1, 2, \dots \quad (1.19)$$

Finalmente, tenemos la siguiente caracterización de código convolucional con perfil de distancia máxima, en términos de la representación entrada-estado-salida.

**Teorema 1.13 (Corolario 2.5 de [62]):** *Sea  $L = \lfloor \frac{\delta}{k} \rfloor + \lfloor \frac{\delta}{n-k} \rfloor$ . Entonces, las matrices  $(A, B, C, D)$  generan un  $(n, k, \delta)$ -código con perfil de distancia máxima si y sólo si la matriz*

$$\mathcal{T}_L = \begin{pmatrix} D & O & \dots & O & O \\ CB & D & \dots & O & O \\ CAB & CB & \dots & O & O \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ CA^{L-2}B & CA^{L-3}B & \dots & D & O \\ CA^{L-1}B & CA^{L-2}B & \dots & CB & D \end{pmatrix} \quad (1.20)$$

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

## 1.6 Códigos woven

En esta sección, presentamos la construcción de los códigos convolucionales llamados *woven*, que modelizamos desde el punto de vista de sistemas en el capítulo 5. Comenzamos en primer lugar describiendo las propiedades del producto de Kronecker de dos matrices, herramienta utilizada para la obtención de la matriz generadora así como para la representación entrada-estado-salida de un código *woven*.

Höst, Johannesson y Zyablov [59] desarrollaron la concatenación de códigos convo-

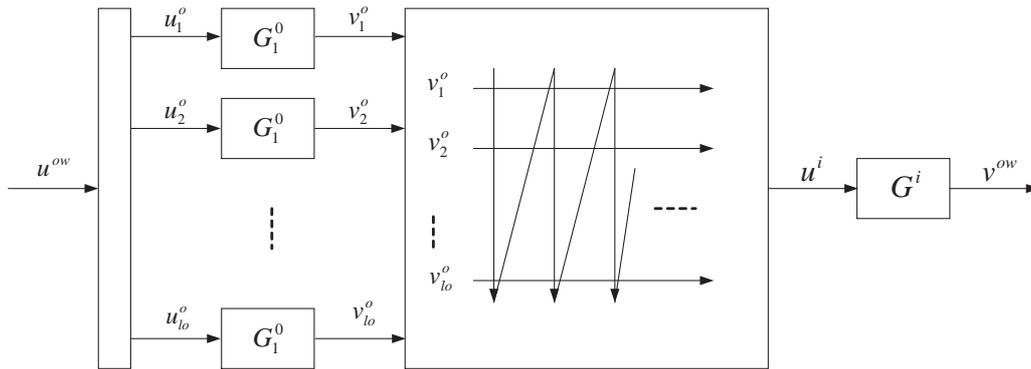


Figura 1.1: Código convolucional woven con warp externo

lucionales llamados **códigos convolucionales woven** (códigos convolucionales “entrelazados”), ya que recuerdan la estructura de un tejido. Consisten en la combinación de varios códigos convolucionales de manera que el código final es también un código convolucional. En la concatenación en serie usual de códigos, se serializa un código externo seguido de un código interno, a diferencia de los códigos *woven*, en los que se considera un conjunto de códigos convolucionales en paralelo en vez del código externo y el código interno. En esta sección describimos los tres tipos de códigos *woven*: códigos *woven* con **warp externo** (formados por varios códigos convolucionales externos), códigos *woven* con **warp interno** (formados por varios códigos convolucionales internos) y los códigos *woven* con **twill** (formado por varios códigos convolucionales externos e internos). Comenzamos describiendo la matriz generadora del *warp*, así como sus propiedades estructurales.

Consideramos en primer lugar  $l_o$  códigos convolucionales externos de tasas  $k_o/n_o$  con matrices generadoras  $G_j^o(z)$  en paralelo (véase la figura 1.1). El vector información se subdivide en subbloques de  $l_o k_o$  símbolos de información cada uno. Estos subbloques son entonces multiplexados a los  $l_o$  códigos externos en paralelo. Las  $n_o$  palabras de cada código se serializan y se escriben a trozos en filas en un buffer compuesto por  $l_o$  filas. Estos  $l_o$  códigos constituyen el **warp**. La sucesión código del *warp* es entonces leída a trozos por columnas desde el buffer y empleada como entrada para un código convolucional interno de tasa  $k_i/n_i$  con matriz generadora  $G^i(z)$  (el **weft**). Esta construcción se denomina **código convolucional woven con warp externo**, que tiene tasa  $k_{ow}/n_{ow}$ , siendo  $k_{ow} = K_{ow} l_o k_o$  y  $n_{ow} = K_{ow} l_o n_o n_i / k_i$ , donde  $K_{ow}$  es el menor entero tal que  $n_{ow}$  es un entero.

La segunda construcción es inversa comparada con la anterior. Empleamos un có-

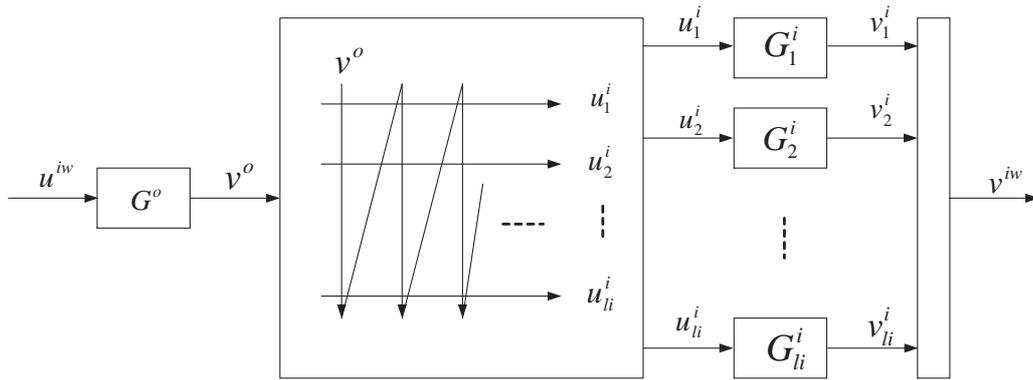


Figura 1.2: Código convolucional woven con warp interno

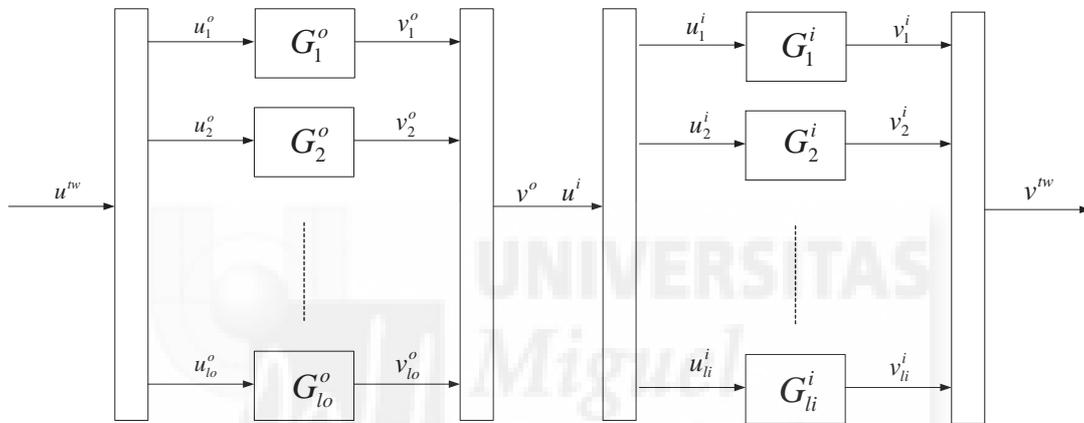


Figura 1.3: Código convolucional woven con twill

digo convolucional externo con matriz generadora  $G^o(z)$  como el *wef*t. La sucesión código se escribe a trozos en columnas en un buffer con  $l_i$  filas, considerando los símbolos de las filas como entradas para los  $l_i$  códigos convolucionales interno en paralelo con matrices generadoras  $G_j^i(z)$  (el *warp* de la construcción, véase la figura 1.2). Obtenemos entonces el llamado **código convolucional woven con warp interno**, que tiene tasa  $k_{iw}/n_{iw}$ , siendo  $k_{iw} = K_{iw}l_i k_i k_o/n_o$  y  $n_{iw} = K_{iw}l_i k_i$ , donde  $K_{iw}$  es el menor entero tal que  $k_{iw}$  es un entero.

Ambas construcciones pueden considerarse como casos especiales del *twill*, que tiene tanto *warp* externo como interno (véase la figura 1.3). El *warp* externo consiste en  $l_o$  códigos convolucionales externos de tasas  $k_o/n_o$  con matrices generadoras  $G_j^o(z)$ , para  $j = 1, 2, \dots, l_o$ ; el *warp* interno consiste en  $l_i$  códigos convolucionales internos de tasas  $k_i/n_i$  de tasas  $k_i/n_i$  con matrices generadoras  $G_j^i(z)$ , para  $j = 1, 2, \dots, l_i$ . El vector información se divide en subbloques de  $k_{tw} = l_o l_i k_o$  símbolos de información cada

uno. Estos subbloques se introducen en paralelo en los  $l_o$  códigos paralelos. Después de codificar y serializar, estas  $l_o$  sucesiones código constituyen el *warp* externo. Entonces, las  $l_i$  palabras código de cada sucesión del *warp* externo se leen a trozos por columnas y se emplean como entradas para los  $l_i$  códigos convolucionales internos. La tasa del *twill* es entonces  $k_{tw}/n_{tw}$ , siendo  $n_{tw} = K_{tw}l_o l_i n_o n_i / k_i$ , en donde  $K_{tw}$  es el menor entero tal que  $n_{tw}$  es un entero. Observemos que un código convolucional *woven* con *warp* externo, respectivamente, interno, es un *twill* con  $l_i = 1$ , respectivamente,  $l_o = 1$ .

### 1.6.1 Producto de Kronecker

La reordenación de las entradas y salidas que se efectúa en el *warp*, hace que la matriz generadora de este código esté descrita en términos de las matrices generadoras de los códigos constituyentes mediante el producto de Kronecker, como vemos a continuación. En esta subsección nos centramos en las propiedades fundamentales de esta operación.

El producto de Kronecker es una operación entre dos matrices de tamaños arbitrarios que da lugar a una matriz por bloques. Se trata de un caso especial del producto tensorial.

**Definición 1.11:** Si  $E = (e_{ij})$  es una matriz de tamaño  $m \times n$  y  $F$  es una una matriz de tamaño  $p \times q$ , entonces el **producto de Kronecker**, que denotaremos por  $E \otimes F$ , es la matriz por bloques de tamaño  $mp \times nq$  definida como

$$E \otimes F = \begin{pmatrix} e_{11}F & e_{12}F & \cdots & e_{1n}F \\ e_{21}F & e_{22}F & \cdots & e_{2n}F \\ \vdots & \vdots & & \vdots \\ e_{m1}F & e_{m2}F & \cdots & e_{mn}F \end{pmatrix}$$

Las principales propiedades del producto de Kronecker [47, 104, 112] que emplearemos en la memoria son las que se enuncian a continuación

(a) Asociatividad:

$$E \otimes (F \otimes H) = (E \otimes F) \otimes H.$$

(b) Distributividad respecto de la suma ordinaria de matrices:

$$(E + F) \otimes H = E \otimes H + F \otimes H \quad \text{y} \quad E \otimes (F + H) = E \otimes F + E \otimes H$$

(c) Compatibilidad con la multiplicación ordinaria de matrices

$$(E \otimes F)(H \otimes J) = (EH) \otimes (FJ).$$

(d) Compatibilidad con la traspuesta ordinaria de matrices

$$(E \otimes F)^T = E^T \otimes F^T.$$

(e) Compatibilidad con la inversa ordinaria de matrices

$$(E \otimes F)^{-1} = E^{-1} \otimes F^{-1}.$$

(f) Compatibilidad con el producto ordinario de un escalar por una matriz

$$a \otimes F = F \otimes a = aF, \quad \text{siendo } a \text{ un escalar.}$$

(g) Rango

$$\text{rg}(E \otimes F) = \text{rg}(E) \text{rg}(F)$$

(h) Para matrices por bloques,

$$(E_1, E_2) \otimes F = (E_1 \otimes F, E_2 \otimes F) \quad \text{y} \quad \begin{pmatrix} E_1 \\ E_2 \end{pmatrix} \otimes F = \begin{pmatrix} E_1 \otimes F \\ E_2 \otimes F \end{pmatrix}$$

pero  $E \otimes (F_1, F_2) \neq (E \otimes F_1, E \otimes F_2)$ .

De las propiedades anteriores, así como de la definición del producto de Kronecker, se deducen las siguientes propiedades adicionales. Sea  $l_w$  un número natural.

(i) Si denotamos por  $e_l$  el vector de  $l_w$  componentes que tiene un uno en la  $l$ -ésima componente y ceros en el resto de las componentes, entonces

$$\left( \sum_{l=1}^{l_w} P_l \otimes \text{diag}(e_l) \right) \left( \sum_{l=1}^{l_w} Q_l \otimes \text{diag}(e_l) \right) = \sum_{l=1}^{l_w} (P_l Q_l) \otimes \text{diag}(e_l)$$

siendo  $P_l$  y  $Q_l$  matrices de tamaños  $p \times s$  y  $s \times q$ , respectivamente.

(j) Si  $P_l$  una matriz invertible, entonces

$$\left( \sum_{l=1}^{l_w} P_l \otimes \text{diag}(e_l) \right)^{-1} = \sum_{l=1}^{l_w} P_l^{-1} \otimes \text{diag}(e_l).$$

(k) Para matrices por bloques,

$$\left( \sum_{l=1}^{l_w} P_l \otimes \text{diag}(e_l), \sum_{l=1}^{l_w} Q_l \otimes \text{diag}(e_l) \right) = \sum_{l=1}^{l_w} (P_l \otimes \text{diag}(e_l), Q_l \otimes \text{diag}(e_l)),$$

$$\begin{pmatrix} \sum_{l=1}^{l_w} P_l \otimes \text{diag}(e_l) \\ \sum_{l=1}^{l_w} Q_l \otimes \text{diag}(e_l) \end{pmatrix} = \sum_{l=1}^{l_w} \begin{pmatrix} P_l \otimes \text{diag}(e_l) \\ Q_l \otimes \text{diag}(e_l) \end{pmatrix}.$$

$$(1) \text{ rg} \left( \sum_{l=1}^{l_w} P_l \otimes \text{diag}(e_l) \right) = \sum_{l=1}^{l_w} \text{ rg}(P_l).$$

## 1.6.2 Propiedades estructurales del warp

El *warp* es el componente principal de los códigos woven. Consideramos  $l_w$  códigos convolucionales  $\mathcal{C}_j^o$ , para  $j = 1, 2, \dots, l_w$ , de tasas  $k/n$  en paralelo, con matrices generadoras  $G_j(z)$ . Estos  $l_w$  códigos constituyen el *warp*.

El vector información  $u^w(z)$  se subdivide en bloques de  $l_w k$  símbolos de información cada uno, esto es, se considera

$$u^w(z) = \left( u^{(1)}(z), u^{(2)}(z), \dots, u^{(k)}(z) \right)^T \quad (1.21)$$

siendo  $u^{(j)}(z) = \left( u_1^{(j)}(z), u_2^{(j)}(z), \dots, u_{l_w}^{(j)}(z) \right)^T$ , para  $j = 1, 2, \dots, k$ . Estos subbloques se multiplexan a los  $l_w$  códigos externos paralelos, siendo entonces

$$u_l^w(z) = \left( u_l^{(1)}(z), u_l^{(2)}(z), \dots, u_l^{(k)}(z) \right)^T, \quad \text{para } l = 1, 2, \dots, l_w$$

el vector información para el  $l$ -ésimo código.

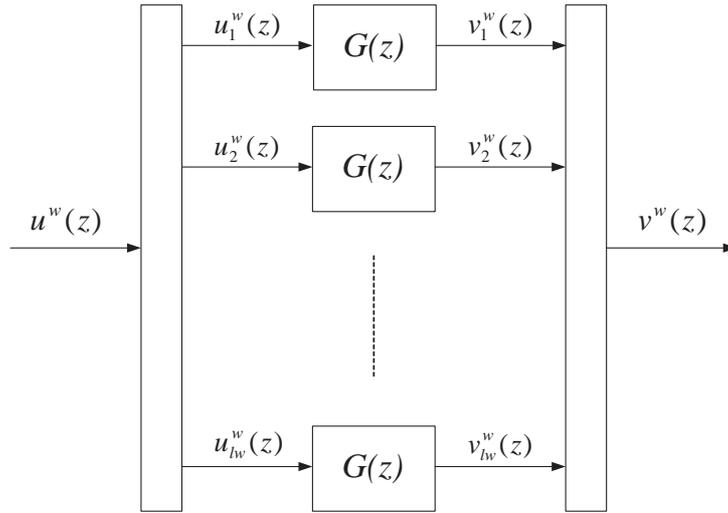


Figura 1.4: Warp formado por  $l_w$  códigos idénticos

### Warp con códigos constituyentes idénticos.

Supongamos en primer lugar que todos los códigos que forman el *warp* son idénticos (véase la figura 1.4), con matriz generadora

$$G(z) = \begin{pmatrix} g_{11}(z) & g_{12}(z) & \cdots & g_{1k}(z) \\ g_{21}(z) & g_{22}(z) & \cdots & g_{2k}(z) \\ \vdots & \vdots & & \vdots \\ g_{n1}(z) & g_{n2}(z) & \cdots & g_{nk}(z) \end{pmatrix} = \begin{pmatrix} g_1(z) \\ g_2(z) \\ \vdots \\ g_n(z) \end{pmatrix}$$

siendo  $g_i(z)$  la  $i$ -ésima fila de  $G(z)$ , para  $i = 1, 2, \dots, n$ . La palabra del  $l$ -ésimo código, para  $l = 1, 2, \dots, l_w$ , viene entonces dada por

$$v_l^w(z) = G(z)u_l^w(z) = \begin{pmatrix} g_1(z)u_l^w(z) \\ g_2(z)u_l^w(z) \\ \vdots \\ g_n(z)u_l^w(z) \end{pmatrix} = \begin{pmatrix} v_l^{(1)}(z) \\ v_l^{(2)}(z) \\ \vdots \\ v_l^{(n)}(z) \end{pmatrix}. \quad (1.22)$$

Cada una de estas  $l_w$  sucesiones código se serializan y se escriben a trozos en filas en un buffer compuesto por  $l_w$  filas. La palabra código  $v^w(z)$  del *warp* es leída a trozos

por columnas desde el buffer, obteniendo entonces

$$v^w(z) = \begin{pmatrix} v^{(1)}(z) \\ v^{(2)}(z) \\ \vdots \\ v^{(n)}(z) \end{pmatrix}, \quad (1.23)$$

siendo

$$v^{(i)}(z) = \begin{pmatrix} v_1^{(i)}(z) \\ v_2^{(i)}(z) \\ \vdots \\ v_{l_w}^{(i)}(z) \end{pmatrix} = \begin{pmatrix} g_i(z)u_1^w(z) \\ g_i(z)u_2^w(z) \\ \vdots \\ g_i(z)u_{l_w}^w(z) \end{pmatrix}, \quad \text{para } i = 1, 2, \dots, n.$$

Empleando el producto de Kronecker y teniendo en cuenta la expresión (1.22), la relación (1.23) se puede escribir como

$$\begin{aligned} v^w(z) &= \begin{pmatrix} g_{11}(z)u_1^{(1)}(z) + \cdots + g_{1k}(z)u_1^{(k)}(z) \\ \vdots \\ g_{11}(z)u_{l_w}^{(1)}(z) + \cdots + g_{1k}(z)u_{l_w}^{(k)}(z) \\ \vdots \\ g_{n1}(z)u_1^{(1)}(z) + \cdots + g_{nk}(z)u_1^{(k)}(z) \\ \vdots \\ g_{n1}(z)u_{l_w}^{(1)}(z) + \cdots + g_{nk}(z)u_{l_w}^{(k)}(z) \end{pmatrix} \\ &= \begin{pmatrix} g_{11}(z) & & & g_{1k}(z) \\ & \ddots & & \vdots \\ & & g_{11}(z) & & g_{1k}(z) \\ & & \vdots & & \vdots \\ g_{n1}(z) & & & g_{nk}(z) \\ & \ddots & & \vdots \\ & & g_{n1}(z) & & g_{nk}(z) \end{pmatrix} \begin{pmatrix} u_1^{(1)}(z) \\ \vdots \\ u_{l_w}^{(1)}(z) \\ \vdots \\ u_1^{(k)}(z) \\ \vdots \\ u_{l_w}^{(k)}(z) \end{pmatrix} \\ &= (G(z) \otimes I_{l_w})u^w(z) \end{aligned} \quad (1.24)$$

siendo  $u^w(z)$  el vector dado por la relación (1.21). Así, de la expresión (1.24), obtenemos que la matriz generadora  $G^w(z)$  (de tamaño  $nl_w \times kl_w$ ) para un *warp* con  $l_w$  códigos

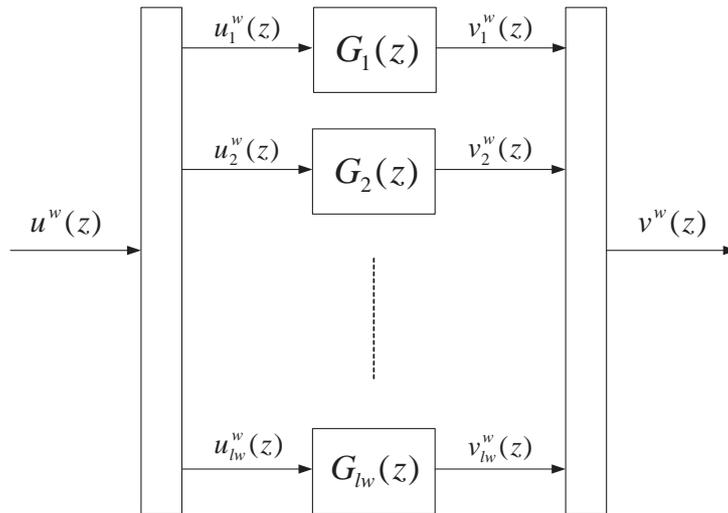


Figura 1.5: Warp formado por  $l_w$  códigos diferentes

constituyentes idénticos con matriz generadora  $G(z)$ , es

$$G^w(z) = G(z) \otimes I_{l_w}. \quad (1.25)$$

El resultado siguiente muestra que la matriz generadora del *warp* con códigos convolucionales constituyentes idénticos, hereda muchas de las propiedades de las matrices generadoras de dichos códigos.

**Teorema 1.14 (Teorema 2 de [60]):** *Sea  $G^w(z)$  la matriz generadora de un warp formado por  $l_w$  códigos idénticos con matriz generadora  $G(D)$ . Entonces,  $G^w(z)$  es minimal si y sólo si  $G(z)$  es minimal*

### Warp con códigos constituyentes diferentes.

Supongamos ahora que los  $l_w$  códigos del *warp* pueden ser diferentes pero con la misma tasa  $k/n$  y denotemos por  $G_l(z)$  la matriz generadora de  $\mathcal{C}_l$ , para  $l = 1, 2, \dots, l_w$  (véase la figura 1.5). Entonces, repitiendo los cálculos realizados para obtener la matriz generadora del warp formado por códigos idénticos, obtenemos que

$$\begin{aligned}
G^w(z) &= \begin{pmatrix} g_{11}^{(1)}(z) & & & g_{1k}^{(1)}(z) & & \\ & \ddots & & \dots & & \ddots \\ & & g_{11}^{(l_w)}(z) & & & g_{1k}^{(l_w)}(z) \\ & & \vdots & & & \vdots \\ g_{n1}^{(1)}(z) & & & g_{nk}^{(1)}(z) & & \\ & \ddots & & \dots & & \ddots \\ & & g_{n1}^{(l_w)}(z) & & & g_{nk}^{(l_w)}(z) \end{pmatrix} \\
&= \sum_{l=1}^{l_w} G_l(z) \otimes \text{diag}(e_l), \tag{1.26}
\end{aligned}$$

en donde  $e_l$  denota el vector que tiene un 1 en la  $l$ -ésima componente y 0 en el resto de las componentes, y  $\text{diag}(e_l)$  es una matriz diagonal con el vector  $e_l$  en su diagonal.

### 1.6.3 Propiedades estructurales del *twill*

Si el *twill* está formado por un *warp* externo con  $l_o$  códigos y un *warp* interno con  $l_i$  códigos, entonces la matriz generadora viene dada por (véase [60])

$$G^{tw}(z) = (G^o(z) \otimes I_{l_o})(G^i(z) \otimes I_{l_i}). \tag{1.27}$$

La matriz generadora de un código convolucional *woven* con *warp* externo formado por  $l_o$  códigos puede expresarse como

$$G^{ow}(z) = (G^o(z) \otimes I_{l_o})G^i(z), \tag{1.28}$$

y la matriz generadora de un código convolucional *woven* con *warp* interno formado por  $l_i$  códigos, como

$$G^{iw}(z) = G^o(z)(G^i(z) \otimes I_{l_i}). \tag{1.29}$$

En las relaciones (1.27), (1.28) y (1.29), hemos supuesto que el producto de matrices está definido. Ahora bien, el producto de las matrices generadoras de los *warps* no siempre está definido; si éste es el caso, entonces se consideran submatrices de tamaños más grandes (véase [60]).

Höst, Johannesson y Zyablov [60] introducen el concepto de código *woven* trabajando en espacios vectoriales. Así, demuestran que si partimos de matrices generadoras

básicas del *warp* externo y del *warp* interno, la matriz generadora del *twill* es también básica. Ahora bien, no tienen un resultado similar para la matrices minimales, que son aquellas cuyo grado coincide con la complejidad del código. Höst, Johannesson, Sidorenko, Zingangirov y Zyablov [58] muestran que si consideramos dos matrices generadoras minimales para el *warp* externo e interno, la matriz generadora del código *twill* no es necesariamente minimal. Esto significa, en particular, que desconocemos el grado del código *woven*.

Notemos que, debido a la estructura del *warp*, este código nunca puede ser MDS, ya que su distancia libre es el mínimo de las distancias libres de los códigos que lo forman.





# Códigos perforados basados en la construcción de Justesen

---

*Mathematics possesses not only truth, but also supreme beauty.*

–Bertrand Russell

*Omnia apud me mathematica fiunt. With me everything turns into mathematics.*

–René Descartes

## 2.1 Introducción

Para aplicaciones con alta exigencia en la velocidad de transferencia de datos, 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 Likelihood 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 [15] en 1979, soluciona este problema. Ellos obtuvieron códigos de tasas  $2/3$  y  $3/4$  a partir de la perforación de códigos de tasa  $1/2$ . Los códigos perforados obtenidos fueron casi tan buenos como el resto de los códigos conocidos de las mismas tasas, con la ventaja de que son más sencillos de decodificar. Posteriormente, Yasuda, Hirata, Nakamura y Otani [116] y Yasuda, Kashiki e Hirata [117], encontraron una familia de códigos de tasa  $(N - 1)/N$ , para  $N \leq 14$  obtenidos de la perforación de códigos de tasa  $1/2$ , y construyeron decodificadores de Viterbi empleando decodificación de decisión dura.

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. Además, la decodificación de Viterbi de códigos convolucionales de tasas grandes se simplifica considerablemente empleando códigos perforados. De hecho, los códigos convolucionales perforados son empleados generalmente en comunicaciones por satélite, por ejemplo, en el sistema INTELSAT y en la difusión de vídeo digital (*digital video broadcasting*) [31].

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. Existen varias técnicas de perforación de un código convolucional tales como las descritas por Hole [54, 55, 56, 57]. Hagenauer [50] define una clase de códigos convolucionales perforados compatibles en tasa (*rate-compatible punctured convolutional codes*, RCPC) obtenidos al añadir la restricción de compatibilidad en tasa a la regla de perforación. Estos códigos han sido empleados en un mecanismo híbrido de repetición automática (*hybrid Automatic Repeat Request*, hybrid-ARQ) [48, 49], así como en códigos obtenidos por concatenación paralela de códigos convolucionales [66, 96, 97] y en códigos obtenidos por concatenación en serie de códigos convolucionales [5, 17, 72].

En este capítulo, empleamos la técnica de perforación presentada por McEliece [79] y establecemos la clasificación de códigos convolucionales basados en la construcción de Justesen dada por Smarandache, Gluesing-Luerssen y Rosenthal [100] desde otro punto de vista. Partiendo de un código Reed-Solomon fijo de tasa  $K/N$ , analizamos en la sección 2.2 de qué tipo es el código convolucional de Justesen a partir de la relación entre los parámetros de ambos códigos. Una vez obtenida dicha clasificación, pasamos a analizar en la sección 2.3 cuándo un código de Justesen puede tener perfil de distancia máxima y cuándo puede ser fuertemente MDS. En la sección 2.4 damos los resultados principales de este capítulo, relacionados con códigos obtenidos de la perforación de códigos basados en la construcción de Justesen. Comenzamos con propiedades que hereda el código  $\mathcal{C}^{[M]}$  obtenido por la descomposición en bloques de profundidad  $M$  de un código convolucional arbitrario, para pasar posteriormente a la descripción de las matrices policíclicas pseudocirculantes asociadas a los polinomios que forman la matriz generadora del código obtenido por la descomposición en bloques de un código convolucional de Justesen. Éste será un paso previo a la perforación de códigos convolucionales de Justesen según la técnica descrita en la sección 1.3.3.

## 2.2 Clasificación de códigos convolucionales basados en la construcción de Justesen

Como hemos comentado en la introducción, Smarandache, Gluesing-Luerssen y Rosenthal [101] proporcionan una construcción de un  $(\nu, \kappa, \delta)$ -código MDS para cada tasa  $\kappa/\nu$  y cada grado  $\delta$ . En esta sección consideramos un  $[N, K]$ -código Reed-Solomon y proporcionamos una clasificación basada en los parámetros del código bloque Reed-Solomon y del código convolucional de Justesen obtenido a partir de él.

Para evitar confusiones entre los parámetros del código bloque y del código convolucional de Justesen, denotamos por  $K$  y  $N$  las dimensiones de la entrada y salida, respectivamente, del código bloque Reed-Solomon.

Sea  $g(z) = \sum_{i=0}^{N-K} a_i z^i$  (con  $a_{N-K} = 1$ ) el polinomio generador de un código Reed-Solomon de tasa  $K/N = \kappa/\nu$ . Sea  $r$  el resto de la división de  $N - K$  por  $\nu$ , entonces

$$N - K = \left\lfloor \frac{N - K}{\nu} \right\rfloor \nu + r, \quad \text{con } 0 \leq r < \nu. \quad (2.1)$$

Así,

$$g(z) = \sum_{i=0}^{\nu-1} z^i g_i(z^\nu)$$

siendo

$$g_i(z^\nu) = \begin{cases} a_i + a_{\nu+i} z^\nu + \cdots + a_{\lfloor \frac{N-K}{\nu} \rfloor \nu + i} z^{\lfloor \frac{N-K}{\nu} \rfloor \nu}, \\ \text{para } i = 0, 1, \dots, r \\ a_i + a_{\nu+i} z^\nu + \cdots + a_{(\lfloor \frac{N-K}{\nu} \rfloor - 1)\nu + i} z^{(\lfloor \frac{N-K}{\nu} \rfloor - 1)\nu}, \\ \text{para } i = r + 1, \dots, \nu - 1 \end{cases}$$

Observemos que de la relación (2.1), se deduce que el sumando  $z^r g_r(z^\nu)$  alcanza el grado  $N - K$  del polinomio  $g(z)$ .

Tal y como indicamos en la sección 1.3.2, podemos construir la matriz generadora polinómica  $G(z)$  del código convolucional de Justesen  $\mathcal{C}$  dada por la relación (1.7) a partir de los polinomios

$$g_i(z) = \begin{cases} a_i + a_{\nu+i} z + \cdots + a_{\lfloor \frac{N-K}{\nu} \rfloor \nu + i} z^{\lfloor \frac{N-K}{\nu} \rfloor}, \\ \text{para } i = 0, 1, \dots, r \\ a_i + a_{\nu+i} z + \cdots + a_{(\lfloor \frac{N-K}{\nu} \rfloor - 1)\nu + i} z^{\lfloor \frac{N-K}{\nu} \rfloor - 1}, \\ \text{para } i = r + 1, \dots, \nu - 1 \end{cases} \quad (2.2)$$

Además,  $G(z)$  es una matriz minimal de  $\mathcal{C}$  (véase la sección 1.3.2). De este modo, obtenemos la clasificación siguiente de  $\mathcal{C}$  basada en el parámetro  $r$ .

**Teorema 2.1:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$ ,  $\mathcal{C}$  el código convolucional de Justesen generado por el polinomio  $g(z)$  y  $r$  el parámetro definido en (2.1).

- (a) Si  $K = \kappa$  (y por tanto  $N = \nu$ ) o  $N = \nu$  (y por tanto  $K = \kappa$ ), entonces  $\mathcal{C}$  es el código Reed-Solomon original, y por tanto,  $\mathcal{C}$  es un código bloque MDS.
- (b) Supongamos que  $K = \lambda\kappa$  y  $N = \lambda\nu$ , con  $\lambda > 1$ ,
- (1) Si  $0 \leq r \leq \nu - \kappa$ , entonces  $\mathcal{C}$  es un código convolucional con grado  $\delta = \kappa \lfloor \frac{N-K}{\nu} \rfloor$ . Es más,  $\mathcal{C}$  es un código convolucional MDS si y sólo si  $r = \nu - \kappa$ .
- (2) Si  $\nu - \kappa + 1 \leq r < \nu$ , entonces  $\mathcal{C}$  es un código convolucional MDS con grado  $\delta = \kappa \lfloor \frac{N-K}{\nu} \rfloor + \kappa - \nu + r$ .

DEMOSTRACIÓN: (a) En este caso, la matriz  $G(D)$  es exactamente la matriz generadora del código Reed-Solomon original de tasa  $K/N$  que, de forma trivial, es un código bloque MDS.

(b) Del teorema 1.5 y de la definición de código convolucional MDS dada en la sección 1.3.1 tenemos que  $\mathcal{C}$  es un código convolucional MDS si y sólo si

$$N - K + 1 = (\nu - \kappa) \left( \left\lfloor \frac{\delta}{\kappa} \right\rfloor + 1 \right) + \delta + 1. \quad (2.3)$$

Para el caso (1), todos los grados columna tienen el mismo valor,  $\nu_j = \lfloor \frac{N-K}{\nu} \rfloor$  para  $j = 1, 2, \dots, \kappa$ . Teniendo en cuenta que  $G(z)$  es una matriz minimal, el grado de  $\mathcal{C}$  es  $\delta = \kappa \lfloor \frac{N-K}{\nu} \rfloor$  y, por tanto, tenemos la igualdad (2.3) si y sólo si  $r = \nu - \kappa$ .

Para el caso (2), obtenemos que

$$\nu_j = \begin{cases} \left\lfloor \frac{N-K}{\nu} \right\rfloor, & \text{para } j = 1, 2, \dots, \nu - r \\ \left\lfloor \frac{N-K}{\nu} \right\rfloor + 1, & \text{para } j = \nu - r + 1, \nu - r + 2, \dots, \kappa \end{cases}$$

y, por tanto, el grado de  $\mathcal{C}$  es

$$\delta = (\nu - r) \left\lfloor \frac{N-K}{\nu} \right\rfloor + (\kappa - \nu + r) \left( \left\lfloor \frac{N-K}{\nu} \right\rfloor + 1 \right)$$

$$= \kappa \left\lfloor \frac{N-K}{\nu} \right\rfloor + \kappa - \nu + r.$$

Ahora bien, como  $\nu - \kappa + 1 \leq r < \nu$ , entonces  $0 \leq \frac{1}{\kappa} \leq \frac{r+\kappa-\nu}{\kappa} < 1$  y así,

$$\left\lfloor \frac{\delta}{\kappa} \right\rfloor = \left\lfloor \frac{N-K}{\nu} \right\rfloor, \quad (2.4)$$

de donde obtenemos la igualdad (2.3).

Como consecuencia del teorema anterior, tenemos que si  $K/N = \kappa/\nu$  y  $\nu$  divide a  $N - K$ , entonces  $r = 0$  y, por tanto, el código convolucional  $\mathcal{C}$  de Justesen es un código convolucional no MDS. Además, si la fracción  $N/K$  es irreducible, aplicando el apartado (a), deducimos que el código convolucional de Justesen es precisamente el código Reed-Solomon original. Por tanto, el mínimo valor del parámetro  $N$  para obtener un código convolucional propio (es decir, que no sea un código bloque) basado en la construcción de Justesen, es  $N = 3^2 - 1$ .

Hay otro caso en el que el código convolucional obtenido de la construcción de Justesen es en realidad el código bloque Reed-Solomon original, como muestra el resultado siguiente.

**Teorema 2.2:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$  y  $\mathcal{C}$  el código convolucional de Justesen generado por el polinomio  $g(z)$ . Sea  $r$  el parámetro definido en (2.1) y supongamos que  $0 < r \leq \nu - \kappa$  y  $\nu > K$ . Entonces  $\mathcal{C}$  es el código Reed-Solomon original.

DEMOSTRACIÓN: Como  $0 < r \leq \nu - \kappa$ , aplicando el teorema 2.1, el grado de  $\mathcal{C}$  es  $\delta = \kappa \left\lfloor \frac{N-K}{\nu} \right\rfloor$ . Además, por ser  $\nu > K$ , entonces  $0 < \frac{K}{\nu} < 1$  y, por tanto,

$$\lambda - 1 < \lambda - \frac{K}{\nu} < \lambda,$$

de donde  $\left\lfloor \lambda - \frac{K}{\nu} \right\rfloor = \lambda - 1$  y

$$\left\lfloor \frac{N-K}{\nu} \right\rfloor = \left\lfloor \frac{\lambda(\nu - \kappa)}{\nu} \right\rfloor = \left\lfloor \lambda - \frac{\lambda\kappa}{\nu} \right\rfloor = \left\lfloor \lambda - \frac{K}{\nu} \right\rfloor = \lambda - 1. \quad (2.5)$$

Pero, de nuevo, por ser  $\nu > K$ ,

$$0 \leq \frac{\delta}{\nu - \kappa} = \frac{\kappa}{\nu - \kappa} \left\lfloor \frac{N-K}{\nu} \right\rfloor = \frac{\kappa}{\nu - \kappa} (\lambda - 1) = \frac{K - \kappa}{\nu - \kappa} < \frac{\nu - \kappa}{\nu - \kappa} = 1$$

con lo que necesariamente  $K = \kappa$ ,  $N = \nu$  y  $\delta = 0$ . Así, por el apartado (a) del teorema 2.1,  $\mathcal{C}$  es el código Reed-Solomon original.  $\square$

Como consecuencia del teorema 2.1 y de los corolarios anteriores, obtenemos que el código convolucional obtenido de la construcción de Justesen es un código MDS si y sólo si  $\nu - \kappa \leq r < \nu$ , como muestra el resultado siguiente.

**Corolario 2.1:** *Sea  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$  y sea  $\mathcal{C}$  el código convolucional de Justesen generado por el polinomio  $g(z)$ . Entonces,  $\mathcal{C}$  es un código MDS si y sólo si  $\nu - \kappa \leq r < \nu$ .*

*Es más, en tal caso, el grado de  $\mathcal{C}$  es  $\delta = \kappa \left\lfloor \frac{N-K}{\nu} \right\rfloor + \kappa - \nu + r$ .*

DEMOSTRACIÓN: Si  $\mathcal{C}$  un código convolucional propio (es decir,  $\lambda > 1$ ), entonces, aplicando el teorema 2.1, tenemos el resultado. Si  $\mathcal{C}$  es un código bloque (es decir,  $\lambda = 1$ ), entonces  $K = \kappa$ ,  $N = \nu$ , y por tanto

$$\left\lfloor \frac{N-K}{\nu} \right\rfloor = \left\lfloor \frac{\nu - \kappa}{\nu} \right\rfloor = 0.$$

Además, de la expresión (2.1), tenemos que

$$\nu - \kappa = N - K = r \quad \text{y} \quad \kappa \left\lfloor \frac{N-K}{\nu} \right\rfloor + \kappa - \nu + r = 0 = \delta$$

por tanto, aplicando teorema 2.1, obtenemos que  $\mathcal{C}$  es un código bloque MDS, con complejidad  $\delta = 0$ .  $\square$

Aplicando el teorema 2.1 y el corolario 2.1, tenemos que el código convolucional  $\mathcal{C}$  obtenido de la construcción de Justesen es un código compacto, como ponemos de manifiesto en el resultado siguiente.

**Corolario 2.2:** *Sea  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$  y sea  $\mathcal{C}$  el código convolucional de Justesen generado por el polinomio  $g(z)$ . Entonces,  $\mathcal{C}$  es un código compacto.*

DEMOSTRACIÓN: Si  $\nu - \kappa \leq r \leq \nu - 1$ , aplicando el corolario 2.1,  $\mathcal{C}$  es un código convolucional MDS y, en particular,  $\mathcal{C}$  es un código compacto.

Si  $0 \leq r < \nu - \kappa$ , por el teorema 2.1, todos los índices de Forney tienen el mismo valor,  $\left\lfloor \frac{N-K}{\nu} \right\rfloor = \frac{\delta}{\kappa}$ . Por tanto,  $\mathcal{C}$  tiene exactamente  $\kappa$  índices de Forney iguales a  $\frac{\delta}{\kappa}$  y, en consecuencia,  $\mathcal{C}$  es un código compacto.  $\square$

$N$	$K$	$\nu$	$\kappa$	$r$	$\delta$
15	3	5	1	2	2
15	5	3	1	1	3
15	9	5	3	1	3

**Tabla 2.1:** Parámetros de los códigos convolucionales del ejemplo 2.1 correspondientes al caso (1) del teorema 2.1

$N$	$K$	$\nu$	$\kappa$	$r$	$\delta$
15	6	5	2	4	3
15	10	3	2	2	3
15	12	5	4	3	2

**Tabla 2.2:** Parámetros de los códigos convolucionales del ejemplo 2.1 correspondientes al caso (2) del teorema 2.1

## 2.3 Propiedades de los códigos convolucionales de Justesen

Una vez obtenida la clasificación de los códigos convolucionales de Justesen en función del parámetro  $r$  dada en el teorema 2.1, nos planteamos las condiciones para que estos códigos puedan tener perfil de distancia máxima.

Los ejemplos siguientes, obtenidos aplicando el teorema 1.4 mediante un software de cálculo algebraico, sugieren que los códigos convolucionales de Justesen no tienen perfil de distancia máxima.

**Ejemplo 2.1:** Si trabajamos en el cuerpo  $\mathbb{F} = GF(2^4)$ , obtenemos los resultados mostrados en las tablas 2.1 y 2.2, que corresponden a los casos (1) y (2), respectivamente, del teorema 2.1. Por tanto, los códigos cuyos parámetros aparecen en la tabla 2.1 no son MDS mientras que los de la tabla 2.2 sí lo son. Estos códigos no tienen perfil de distancia máxima. ■

**Ejemplo 2.2:** Para los cuerpos  $\mathbb{F} = GF(2^6)$  y  $\mathbb{F} = GF(2^8)$ , esto es, para  $N = 63$  y  $N = 255$ , obtenemos que los códigos cuyos parámetros aparecen en la tabla 2.3 tampoco tienen perfil de distancia máxima. ■

$N$	$K$	$\nu$	$\kappa$	$r$	$\delta$	MDS
63	35	9	5	1	15	No
63	42	3	2	0	14	No
63	45	7	5	4	12	Si
255	51	5	1	4	40	Si

**Tabla 2.3:** Parámetros de los códigos convolucionales del ejemplo 2.2

Ahora bien, veremos que en ciertos casos, el código convolucional  $\mathcal{C}$  obtenido de la construcción de Justesen sí puede tener perfil de distancia máxima. Es más, veremos que en ciertos casos, en caso de tener perfil de distancia máxima, entonces será fuertemente MDS.

Tal y como vimos en la sección 1.5, un código convolucional tiene perfil de distancia máxima si se verifica la condición

$$d_L^c = (\nu - \kappa)(L + 1) + 1$$

siendo  $L = \lfloor \frac{\delta}{\kappa} \rfloor + \lfloor \frac{\delta}{\nu - \kappa} \rfloor$ . Así pues, un paso previo al análisis de la propiedad de perfil de distancia máxima del código convolucional de Justesen, es el cálculo del valor del parámetro  $L$ . Comenzamos con un lema técnico.

**Lema 2.1:** Sea  $N = \lambda\nu$  y  $K = \lambda\kappa$ , con  $\lambda \geq 1$ . Sea  $r$  el parámetro definido por la expresión (2.1). Si  $\nu \geq K$ , entonces

- (a)  $\lfloor \frac{N-K}{\nu} \rfloor = \lambda - 1$ ,
- (b)  $r = \nu - K$ ,
- (c)  $0 \leq r \leq \nu - \kappa$ .

DEMOSTRACIÓN: (a) Supongamos que  $N = \lambda\nu$  y  $K = \lambda\kappa$ . Entonces,

$$\left\lfloor \frac{N-K}{\nu} \right\rfloor = \left\lfloor \frac{\lambda(\nu - \kappa)}{\nu} \right\rfloor = \left\lfloor \lambda - \frac{\lambda\kappa}{\nu} \right\rfloor = \left\lfloor \lambda - \frac{K}{\nu} \right\rfloor. \quad (2.6)$$

Ahora, si  $\nu = K$ , entonces  $\frac{N-K}{\nu} = \lambda - 1$  y, por tanto, tenemos el resultado. Si  $\nu > K$ , entonces  $0 < \frac{K}{\nu} < 1$ , y por tanto, siguiendo un razonamiento similar al empleado para obtener la expresión (2.5),

$$\lambda - 1 < \lambda - \frac{K}{\nu} < \lambda,$$

de donde  $\lfloor \lambda - \frac{K}{\nu} \rfloor = \lambda - 1$  y de la expresión (2.6),

$$\left\lfloor \frac{N - K}{\nu} \right\rfloor = \lambda - 1. \quad (2.7)$$

(b) Teniendo en cuenta las expresiones (2.1) y (2.7), el parámetro  $r$  verifica

$$r = N - K - \left\lfloor \frac{N - K}{\nu} \right\rfloor \nu = \lambda(\nu - \kappa) - (\lambda - 1)\nu = \nu - K.$$

(c) Al ser  $\nu \geq K$  y  $\kappa \leq K$ , en particular obtenemos que  $0 \leq r = \nu - K \leq \nu - \kappa$ .  $\square$

En lo que sigue, analizamos el valor del parámetro  $L$  en función de los valores de  $r$ ; en concreto, obtenemos  $L$  para  $0 < r \leq \nu - \kappa$  y  $\nu < K$  y en los casos  $r = 0$  y  $\nu - \kappa + 1 \leq r \leq \nu - 1$ , independientemente de la relación entre  $\nu$  y  $K$ , ya que por el teorema 2.2, si  $0 < r \leq \nu - \kappa$  y  $\nu > K$ , el código convolucional  $\mathcal{C}$  obtenido de la construcción de Justesen es, de hecho, el código Reed-Solomon original.

El resultado siguiente proporciona el valor del parámetro  $L$  definido por la relación (1.6), para el caso en que  $\nu$  divide a  $N - K$ .

**Lema 2.2:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$  y  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$ . Sean  $r$  y  $L$  los parámetros definidos por las expresiones (2.1) y (1.6), respectivamente. Si  $r = 0$ , entonces  $L = \lambda$ .

DEMOSTRACIÓN: Como  $r = 0$ ,  $\nu$  divide a  $N - K$  y, por tanto, aplicando el teorema 2.1, el grado de  $\mathcal{C}$  viene dado por

$$\delta = \kappa \left( \frac{N - K}{\nu} \right).$$

Observemos que en este caso  $\nu$  también divide a  $K$ , de donde

$$\begin{aligned} L &= \left\lfloor \frac{\delta}{\kappa} \right\rfloor + \left\lfloor \frac{\delta}{\nu - \kappa} \right\rfloor = \frac{N - K}{\nu} + \left\lfloor \frac{\kappa}{\nu - \kappa} \left( \frac{N - K}{\nu} \right) \right\rfloor \\ &= \frac{N - K}{\nu} + \left\lfloor \frac{\lambda \kappa}{\nu} \right\rfloor = \frac{N - K}{\nu} + \frac{K}{\nu} = \frac{N}{\nu} = \lambda. \quad \square \end{aligned}$$

**Observación 2.1:** Notemos que si  $r = 0$ , entonces del lema 2.2, obtenemos que  $\nu - \kappa$  divide a  $\delta$ .  $\blacksquare$

Observemos que si  $\nu = K$ , entonces aplicando el lema 2.1 obtenemos, en particular, que  $r = 0$ . Por tanto, como consecuencia del lema anterior, deducimos que si  $\nu = K$ , entonces  $L = \lambda$ . Tenemos así el resultado siguiente.

**Corolario 2.3:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$  y  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$ . Sean  $r$  y  $L$  los parámetros definidos en las expresiones (2.1) y (1.6), respectivamente. Si  $\nu = K$ , entonces  $r = 0$  y  $L = \lambda$ .

El resultado siguiente proporciona el valor de  $L$  para el caso  $0 < r \leq \nu - \kappa$  y  $\nu < K$ .

**Lema 2.3:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$  y  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$ . Sean  $r$  y  $L$  los parámetros definidos por las expresiones (2.1) y (1.6), respectivamente. Si  $0 < r \leq \nu - \kappa$  y  $\nu < K$ , entonces  $L + 1 = \lambda$ .

DEMOSTRACIÓN: Como  $0 < r \leq \nu - \kappa$ , aplicando el teorema 2.1,  $\mathcal{C}$  tiene grado  $\delta = \kappa \left\lfloor \frac{N-K}{\nu} \right\rfloor$ . Ahora bien, la condición  $\nu < K$ , implica que

$$\frac{\delta}{\kappa} = \left\lfloor \frac{N-K}{\nu} \right\rfloor = \left\lfloor \lambda - \frac{K}{\nu} \right\rfloor = \lambda - \left\lceil \frac{K}{\nu} \right\rceil = \lambda - \left\lfloor \frac{K}{\nu} \right\rfloor - 1. \quad (2.8)$$

Así pues, para obtener la igualdad  $L + 1 = \lambda$ , debemos probar que

$$\left\lfloor \frac{\delta}{\nu - \kappa} \right\rfloor = \left\lfloor \frac{K}{\nu} \right\rfloor. \quad (2.9)$$

Definamos  $s_1$  mediante la siguiente relación

$$\delta = \left\lfloor \frac{K}{\nu} \right\rfloor (\nu - \kappa) + s_1.$$

Entonces, para obtener (2.9), es suficiente con tener

$$0 \leq s_1 < \nu - \kappa.$$

Ahora bien, teniendo en cuenta la expresión (2.8), obtenemos

$$\begin{aligned} \delta - \left\lfloor \frac{K}{\nu} \right\rfloor (\nu - \kappa) &= \kappa \left\lfloor \frac{N-K}{\nu} \right\rfloor - \left\lfloor \frac{K}{\nu} \right\rfloor (\nu - \kappa) \\ &= \kappa \left\lfloor \frac{N-K}{\nu} \right\rfloor - \left( \lambda - \left\lfloor \frac{N-K}{\nu} \right\rfloor - 1 \right) (\nu - \kappa) \end{aligned}$$

$$\begin{aligned}
&= \nu - \kappa - \left( N - K - \nu \left\lfloor \frac{N - K}{\nu} \right\rfloor \right) \\
&= \nu - \kappa - r \geq 0
\end{aligned} \tag{2.10}$$

ya que  $r \leq \nu - \kappa$ .

Además, al ser  $\nu \neq K$ , para obtener  $s_1 < \nu - \kappa$ , basta con probar que

$$\delta < (\nu - \kappa) \left\lfloor \frac{K}{\nu} \right\rfloor,$$

pero aplicando la expresión (2.8) y teniendo en cuenta que

$$r = N - K - \nu \left\lfloor \frac{N - K}{\nu} \right\rfloor > 0,$$

tenemos

$$\begin{aligned}
(\nu - \kappa) \left\lfloor \frac{K}{\nu} \right\rfloor &= (\nu - \kappa) \left( \lambda - \left\lfloor \frac{N - K}{\nu} \right\rfloor \right) \\
&= N - K - (\nu - \kappa) \left\lfloor \frac{N - K}{\nu} \right\rfloor \\
&= r + \kappa \left\lfloor \frac{N - K}{\nu} \right\rfloor > \kappa \left\lfloor \frac{N - K}{\nu} \right\rfloor = \delta.
\end{aligned} \tag{2.11}$$

Concluimos entonces, de las expresiones (2.10) y (2.11), que

$$\left\lfloor \frac{\delta}{\nu - \kappa} \right\rfloor = \left\lfloor \frac{K}{\nu} \right\rfloor,$$

de donde tenemos la relación (2.9) y, por tanto, que  $L + 1 = \lambda$ .  $\square$

**Observación 2.2:** Notemos que si  $0 < r \leq \nu - \kappa$  y  $\nu < K$ , entonces de la relación (2.10) tenemos que  $\nu - \kappa$  divide a  $\delta$  si y sólo si  $r = \nu - \kappa$ .  $\blacksquare$

El resultado siguiente proporciona el valor del parámetro  $L$  en el caso en que  $\nu - \kappa + 1 \leq r \leq \nu - 1$ .

**Lema 2.4:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$  y  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$ . Sean  $r$  y  $L$  los parámetros definidos por las expresiones (2.1) y (1.6), respectivamente. Si  $\nu - \kappa + 1 \leq r \leq \nu - 1$ , entonces  $L + 1 = \lambda$ .

DEMOSTRACIÓN: Como  $\nu - \kappa + 1 \leq r \leq \nu - 1$ , aplicando el teorema 2.1,  $\mathcal{C}$  tiene grado

$$\delta = \kappa \left\lfloor \frac{N - K}{\nu} \right\rfloor + \kappa - \nu + r. \quad (2.12)$$

Además, de la expresión (2.4), obtenemos que

$$\left\lfloor \frac{\delta}{\kappa} \right\rfloor = \left\lfloor \frac{N - K}{\nu} \right\rfloor = \left\lfloor \lambda - \frac{K}{\nu} \right\rfloor.$$

Ahora bien, al ser  $\nu - \kappa < r$ , aplicando el lema 2.1,  $K > \nu$  y, por tanto,

$$\left\lfloor \lambda - \frac{K}{\nu} \right\rfloor = \lambda - \left\lceil \frac{K}{\nu} \right\rceil,$$

de donde

$$\left\lfloor \frac{\delta}{\kappa} \right\rfloor = \left\lfloor \frac{N - K}{\nu} \right\rfloor = \lambda - \left\lceil \frac{K}{\nu} \right\rceil. \quad (2.13)$$

Así pues, para tener  $L + 1 = \lambda$ , es suficiente con probar, ya que  $\nu$  no divide a  $K$ , que

$$\left\lfloor \frac{\delta}{\nu - \kappa} \right\rfloor = \left\lceil \frac{K}{\nu} \right\rceil - 1 = \left\lfloor \frac{K}{\nu} \right\rfloor. \quad (2.14)$$

De hecho, probaremos que  $\frac{\delta}{\nu - \kappa} = \left\lfloor \frac{K}{\nu} \right\rfloor$ . En efecto, teniendo en cuenta el valor de  $r$ , así como las expresiones (2.12) y (2.13),

$$\delta = \left( \lambda - 1 - \left\lfloor \frac{N - K}{\nu} \right\rfloor \right) (\nu - \kappa) = (\nu - \kappa) \left\lfloor \frac{K}{\nu} \right\rfloor. \quad (2.15)$$

Por tanto, obtenemos la expresión (2.14) y, en consecuencia, que  $L + 1 = \lambda$ .  $\square$

Una vez obtenido el valor del parámetro  $L$ , estamos en condiciones de estudiar si los códigos convolucionales obtenidos de la construcción de Justesen pueden tener perfil de distancia máxima y, en caso de tenerlo, si son fuertemente MDS.

En primer lugar, y como consecuencia de los lemas 2.2 y 2.3, tenemos que el código convolucional de Justesen  $\mathcal{C}$  no puede tener perfil de distancia máxima en los casos en que  $\nu = K$ ,  $r = 0$  o bien  $0 \leq r < \nu - \kappa$  y  $\nu < K$ , como ponemos de manifiesto en el resultado siguiente.

**Corolario 2.4:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$ ,  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$  y  $r$  el parámetro definido por la expresión (2.1). Si se satisface una de las condiciones siguientes

- (a)  $\nu = K$ ,
- (b)  $r = 0$ ,
- (c)  $0 < r < \nu - \kappa$  y  $\nu < K$ ,

entonces el código  $\mathcal{C}$  no tiene perfil de distancia máxima.

DEMOSTRACIÓN: Sabemos, por la definición 1.4, que  $\mathcal{C}$  tiene perfil de distancia máxima si la  $L$ -ésima distancia columna  $d_L^c(\mathcal{C})$  satisface la igualdad

$$d_L^c(\mathcal{C}) = (\nu - \kappa)(L + 1) + 1.$$

Si  $\nu = K$ , en particular, del corolario 2.3, obtenemos que  $r = 0$ , en cuyo caso, por el lema 2.2,  $L = \lambda$ , de donde

$$d_L^c(\mathcal{C}) = (\nu - \kappa)(\lambda + 1) + 1 > N - K + 1 = d_{free}(\mathcal{C}),$$

es decir, la distancia columna  $d_L^c(\mathcal{C})$  debe ser mayor que la distancia libre del código. Pero esto no es posible ya que la primera distancia columna en la que la distancia libre se puede alcanzar es  $d_M^c(\mathcal{C})$ , y en este caso, teniendo en cuenta la observación 2.1,  $\nu - \kappa$  divide a  $\delta$  y por tanto, de la observación 1.1,  $M = L$ .

Si  $0 < r < \nu - \kappa$  y  $\nu < K$ , entonces por el lema 2.3,  $L + 1 = \lambda$ , de donde

$$d_L^c(\mathcal{C}) = (\nu - \kappa)\lambda + 1 = N - K + 1 = d_{free}(\mathcal{C}).$$

Por tanto, la distancia columna  $d_L^c(\mathcal{C})$  debe ser igual a la distancia libre del código; pero esta igualdad no es posible porque al ser  $r < \nu - \kappa$  y  $\nu < K$ , de la observación 2.2, obtenemos que  $\nu - \kappa$  no divide a  $\delta$  y, por tanto,  $M = L + 1$ , de donde

$$d_M^c(\mathcal{C}) > d_L^c(\mathcal{C}) = d_{free}(\mathcal{C}). \quad \square$$

Si  $r = \nu - \kappa$  y  $\nu < K$  o bien  $\nu - \kappa + 1 \leq r \leq \nu - 1$ , como consecuencia de los lemas 2.3 y 2.4, obtenemos que si  $\mathcal{C}$  tiene perfil de distancia máxima, entonces  $\mathcal{C}$  es un código fuertemente MDS.

**Corolario 2.5:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$  y  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$ . Supongamos que el parámetro  $r$  definido en (2.1) verifica una de las condiciones siguientes:

- (a)  $r = \nu - \kappa$  y  $\nu < K$ ,

(b)  $\nu - \kappa + 1 \leq r \leq \nu - 1$ .

Si el código  $\mathcal{C}$  tiene perfil de distancia máxima, entonces  $\mathcal{C}$  es un código fuertemente MDS.

DEMOSTRACIÓN: Sea  $\lambda > 1$  tal que  $K = \lambda\kappa$  y  $N = \lambda\nu$  (si  $\lambda = 1$ , entonces  $\mathcal{C}$  es un código bloque). Como  $\mathcal{C}$  tiene perfil de distancia máxima, entonces

$$d_L^c(\mathcal{C}) = (\nu - \kappa)(L + 1) + 1,$$

y aplicando los lemas 2.3 y 2.4,  $L + 1 = \lambda$ , de donde

$$d_L^c(\mathcal{C}) = (\nu - \kappa)\lambda + 1 = N - K + 1 = d_{free}(\mathcal{C}).$$

Ahora bien, para que  $\mathcal{C}$  sea fuertemente MDS, según la observación 1.1, tenemos que probar que  $\nu - \kappa$  divide a  $\delta$ .

Si  $r = \nu - \kappa$  y  $\nu < K$ , de la observación 2.2 obtenemos que  $\nu - \kappa$  divide a  $\delta$  y  $\mathcal{C}$  es un código convolucional fuertemente MDS.

Si  $\nu - \kappa + 1 \leq r \leq \nu - 1$ , entonces de la expresión (2.15) obtenemos que  $\frac{\delta}{\nu - \kappa} = \lfloor \frac{K}{\nu} \rfloor$ . En particular,  $\nu - \kappa$  divide a  $\delta$  y, por tanto,  $\mathcal{C}$  es un código convolucional fuertemente MDS.  $\square$

## 2.4 Códigos convolucionales de Justesen perforados

En esta sección establecemos condiciones para que el código obtenido de la perforación de un código convolucional de Justesen tenga buenas propiedades relacionadas con la compacidad y con la distancia libre. Tal y como vimos en la sección 1.3.3, el  $(\tilde{N}, \kappa, \tilde{\delta})$ -código perforado verifica  $\tilde{\delta} \leq \delta$ .

### 2.4.1 Estudio de la compacidad del código obtenido por descomposición en bloques de un código convolucional arbitrario

Tal y como vimos en la subsección 1.3.3, el código  $\mathcal{C}^{[M]}$  obtenido de la descomposición en bloques de un código convolucional  $\mathcal{C}$  es la base del código perforado. Recor-

demostremos que tanto el grado como la distancia libre de los códigos  $\mathcal{C}$  y  $\mathcal{C}^{[M]}$  coinciden. Es más, como vemos en los resultados siguientes, si el código original  $\mathcal{C}$  es compacto, entonces el código obtenido de  $\mathcal{C}$  por la descomposición en bloques de profundidad  $M$  también es compacto. Es importante resaltar que éste es un resultado general, es decir,  $\mathcal{C}$  no es necesariamente un código convolucional obtenido de la construcción de Justesen.

El teorema siguiente proporciona condiciones necesarias y suficientes para que, siendo el código original compacto, el código convolucional  $\mathcal{C}^{[M]}$  sea también compacto.

**Teorema 2.3:** *Sea  $\mathcal{C}$  un  $(\nu, \kappa, \delta)$ -código arbitrario. Supongamos que  $\kappa$  no divide a  $\delta$  y sea  $\mathcal{C}^{[M]}$  el  $(\nu M, \kappa M, \delta)$ -código obtenido de la descomposición por bloques de profundidad  $M$  de  $\mathcal{C}$ . Supongamos además que  $\mathcal{C}$  es compacto. Entonces  $\mathcal{C}^{[M]}$  es compacto si y sólo si*

$$\left\lfloor \frac{\delta}{\kappa M} \right\rfloor = \left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \right\rfloor = \left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor + 1}{M} \right\rfloor. \quad (2.16)$$

DEMOSTRACIÓN: Supongamos que  $\mathcal{C}$  es un código compacto, entonces  $\mathcal{C}$  tiene  $\delta - \kappa \lfloor \frac{\delta}{\kappa} \rfloor$  índices de Forney iguales a  $\lfloor \frac{\delta}{\kappa} \rfloor + 1$  y  $\kappa - (\delta - \kappa \lfloor \frac{\delta}{\kappa} \rfloor)$  índices de Forney iguales a  $\lfloor \frac{\delta}{\kappa} \rfloor$ . Supongamos que

$$\left\lfloor \frac{\delta}{\kappa} \right\rfloor = \left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \right\rfloor M + r_1 \quad \text{con } 0 \leq r_1 < M$$

y

$$\left\lfloor \frac{\delta}{\kappa} \right\rfloor + 1 = \left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor + 1}{M} \right\rfloor M + r_2 \quad \text{con } 0 \leq r_2 < M.$$

De las relaciones entre los índices de Forney de  $\mathcal{C}$  y  $\mathcal{C}^{[M]}$  dadas en los corolarios 1.1 y 1.2, tenemos que cada índice de Forney  $\lfloor \frac{\delta}{\kappa} \rfloor$  de  $\mathcal{C}$  da lugar a  $r_1$  índices de Forney iguales a  $\left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \right\rfloor + 1$  y  $M - r_1$  índices de Forney iguales a  $\left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \right\rfloor$  en  $\mathcal{C}^{[M]}$ .

Análogamente, cada índice de Forney  $\lfloor \frac{\delta}{\kappa} \rfloor + 1$  de  $\mathcal{C}$  da lugar a  $r_2$  índices de Forney iguales a  $\left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor + 1}{M} \right\rfloor + 1$  y  $M - r_2$  índices de Forney iguales a  $\left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor + 1}{M} \right\rfloor$  en  $\mathcal{C}^{[M]}$ .

Ahora, teniendo en cuenta que

$$\left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \right\rfloor = \left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor + 1}{M} \right\rfloor$$

así como las consideraciones anteriores, obtenemos que  $\mathcal{C}^{[M]}$  tiene  $\delta - \left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \right\rfloor \kappa M$  índices de Forney iguales a  $\left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \right\rfloor + 1$  y  $\kappa M - \left( \delta - \left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \right\rfloor \kappa M \right)$  índices de Forney iguales a  $\left\lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \right\rfloor$ .

Finalmente, de la definición 1.3, sabemos que  $\mathcal{C}^{[M]}$  es compacto si y sólo si  $\mathcal{C}^{[M]}$  tiene  $\delta - \left\lfloor \frac{\delta}{\kappa M} \right\rfloor \kappa M$  índices de Forney iguales a  $\left\lfloor \frac{\delta}{\kappa M} \right\rfloor + 1$  y  $\kappa M - \left( \delta - \left\lfloor \frac{\delta}{\kappa M} \right\rfloor \kappa M \right)$  índices de Forney iguales a  $\left\lfloor \frac{\delta}{\kappa M} \right\rfloor$ . Concluimos por tanto que  $\mathcal{C}^{[M]}$  es un código compacto si y sólo si se verifica la relación (2.16).  $\square$

Para el caso en que  $\kappa$  divide a  $\delta$ , entonces todos los códigos obtenidos por la descomposición en bloques de un código compacto, son compactos.

**Teorema 2.4:** *Sea  $\mathcal{C}$  un  $(\nu, \kappa, \delta)$ -código y supongamos que  $\kappa$  divide a  $\delta$ . Sea  $\mathcal{C}^{[M]}$  el  $(\nu M, \kappa M, \delta)$ -código obtenido de la descomposición por bloques de profundidad  $M$  de  $\mathcal{C}$ . Si  $\mathcal{C}$  es compacto, entonces  $\mathcal{C}^{[M]}$  es también compacto.*

DEMOSTRACIÓN: Si  $\mathcal{C}$  es un código convolucional compacto y  $\kappa$  divide a  $\delta$ , entonces  $\mathcal{C}$  tiene  $\kappa$  índices de Forney iguales a  $\left\lfloor \frac{\delta}{\kappa} \right\rfloor = \frac{\delta}{\kappa}$ . Sea  $r_1$  el resto de la división de  $\frac{\delta}{\kappa}$  por  $M$ , es decir,

$$\frac{\delta}{\kappa} = \left\lfloor \frac{\delta}{\kappa M} \right\rfloor M + r_1 \quad \text{con} \quad 0 \leq r_1 < M.$$

De las relaciones entre los índices de Forney de  $\mathcal{C}$  y  $\mathcal{C}^{[M]}$  dadas en los corolarios 1.1 y 1.2, tenemos que cada índice de Forney  $\frac{\delta}{\kappa}$  de  $\mathcal{C}$  da lugar a  $r_1$  índices de Forney iguales a  $\left\lfloor \frac{\delta}{\kappa M} \right\rfloor + 1$  y  $M - r_1$  índices de Forney iguales a  $\left\lfloor \frac{\delta}{\kappa M} \right\rfloor$  en  $\mathcal{C}^{[M]}$ .

Ahora, teniendo en cuenta las observaciones anteriores, obtenemos que  $\mathcal{C}^{[M]}$  tiene  $\delta - \left\lfloor \frac{\delta}{\kappa M} \right\rfloor \kappa M$  índices de Forney iguales a  $\left\lfloor \frac{\delta}{\kappa M} \right\rfloor + 1$  y  $\kappa M - \left( \delta - \left\lfloor \frac{\delta}{\kappa M} \right\rfloor \kappa M \right)$  índices de Forney iguales a  $\left\lfloor \frac{\delta}{\kappa M} \right\rfloor$ . Por tanto,  $\mathcal{C}^{[M]}$  es compacto.  $\square$

## 2.4.2 Código obtenido por descomposición en bloques de un código convolucional de Justesen

En lo que sigue, nos centramos en el código convolucional obtenido de la descomposición por bloques de un código de Justesen  $\mathcal{C}$ . En la técnica que empleamos para obtener el código perforado, el primer paso consiste en obtener la matriz generadora

del código obtenido de la descomposición de  $\mathcal{C}$  por bloques de profundidad  $M$ . Según el teorema 1.6, esta matriz se obtiene a partir de la matriz generadora  $G(z)$  de  $\mathcal{C}$  reemplazando cada entrada  $g_{ij}(z)$  de  $G(z)$  por su  $M$ -ésima matriz PCPC correspondiente (véase la sección 1.3.3). Dado que la matriz generadora del código de Justesen es (véase la sección 1.3.2)

$$G(z) = \begin{pmatrix} g_0(z) & zg_{\nu-1}(z) & \cdots & zg_{\nu-\kappa+1}(z) \\ g_1(z) & g_0(z) & \cdots & zg_{\nu-\kappa+2}(z) \\ \vdots & \vdots & & \vdots \\ g_{\nu-1}(z) & g_{\nu-2}(z) & \cdots & g_{\nu-\kappa}(z) \end{pmatrix},$$

nuestro objetivo en lo que sigue es obtener la expresión algebraica de las matrices PCPC de los polinomios siguientes:

- $g_i(z)$ , con  $0 \leq i \leq r$ ,
- $g_i(z)$ , con  $r+1 \leq i \leq \nu-1$ ,
- $zg_i(z)$ , con  $r+1 \leq i \leq \nu-1$ ,
- $zg_i(z)$ , con  $\nu-\kappa+1 \leq i \leq r$ .

El lema siguiente proporciona la  $M$ -ésima matriz PCPC para el polinomio  $g_i(z)$ , con  $0 \leq i \leq r$ .

**Lema 2.5:** Sea  $g_i(z)$ , con  $0 \leq i \leq r$ , el polinomio definido por la expresión (2.2) y sea  $\alpha$  el resto de la división de  $\lfloor \frac{N-K}{\nu} \rfloor$  por  $M$ . Entonces, la  $M$ -ésima matriz PCPC asociada a  $g_i(z)$  viene dada por

$$g_i^{[M]}(z) = \begin{pmatrix} g_{i,0}(z) & zg_{i,M-1}(z) & zg_{i,M-2}(z) & \cdots & zg_{i,1}(z) \\ g_{i,1}(z) & g_{i,0}(z) & zg_{i,M-1}(z) & \cdots & zg_{i,2}(z) \\ \vdots & \vdots & \vdots & & \vdots \\ g_{i,M-1}(z) & g_{i,M-2}(z) & g_{i,M-3}(z) & \cdots & g_{i,0}(z) \end{pmatrix}$$

siendo

$$g_{i,l}(z) = \begin{cases} a_{l\nu+i} + a_{(M+l)\nu+i}z + \cdots + a_{\left(\lfloor \frac{N-K}{\nu} \rfloor\right)_{M+l}\nu+i} z^{\lfloor \frac{N-K}{M} \rfloor} \\ \text{para } l = 0, 1, \dots, \alpha \\ a_{l\nu+i} + a_{(M+l)\nu+i}z + \cdots + a_{\left(\left(\lfloor \frac{N-K}{\nu} \rfloor\right)_{M+l}\right)\nu+i} z^{\lfloor \frac{N-K}{M} \rfloor - 1} \\ \text{para } l = \alpha + 1, \dots, M - 1 \end{cases} \quad (2.17)$$

DEMOSTRACIÓN: Consideremos  $i$  fijo, con  $1 \leq i \leq r$ ; entonces, para obtener la  $M$ -ésima matriz PCPC asociada a

$$g_i(z) = a_i + a_{\nu+i}z + \cdots + a_{\lfloor \frac{N-K}{\nu} \rfloor \nu + i} z^{\lfloor \frac{N-K}{\nu} \rfloor}$$

debemos agrupar en potencias de  $M$ . Como

$$\left\lfloor \frac{N-K}{\nu} \right\rfloor = \left\lfloor \frac{\lfloor \frac{N-K}{\nu} \rfloor}{M} \right\rfloor M + \alpha, \quad \text{para cierto } \alpha \text{ con } 0 \leq \alpha < M \quad (2.18)$$

tenemos que la  $M$ -ésima descomposición polifásica de  $g_i(z)$  es

$$(g_{i,0}(z), g_{i,1}(z), \dots, g_{i,M-1}(z))$$

en donde  $g_{i,l}(z)$ , para  $l = 0, 1, \dots, M-1$ , está dado por la expresión (2.17), luego tenemos el resultado.  $\square$

En el lema siguiente, obtenemos la  $M$ -ésima matriz PCPC del polinomio  $g_i(z)$ , con  $r+1 \leq i \leq \nu-1$ .

**Lema 2.6:** Sea  $g_i(z)$  con  $r+1 \leq i \leq \nu-1$  el polinomio definido por la expresión (2.2) y sea  $\beta$  el resto de la división de  $\lfloor \frac{N-K}{\nu} \rfloor - 1$  por  $M$ . Entonces, la  $M$ -ésima matriz PCPC asociada a  $g_i(z)$  viene dada por

$$g_i^{[M]}(z) = \begin{pmatrix} g_{i,0}(z) & z g_{i,M-1}(z) & z g_{i,M-2}(z) & \cdots & z g_{i,1}(z) \\ g_{i,1}(z) & g_{i,0}(z) & z g_{i,M-1}(z) & \cdots & z g_{i,2}(z) \\ \vdots & \vdots & \vdots & & \vdots \\ g_{i,M-1}(z) & g_{i,M-2}(z) & g_{i,M-3}(z) & \cdots & g_{i,0}(z) \end{pmatrix}$$

siendo

$$g_{i,l}(z) = \begin{cases} a_{l\nu+i} + a_{(M+l)\nu+i}z + \cdots + a_{\left(\left\lfloor \frac{\lfloor \frac{N-K}{\nu} \rfloor - 1}{M} \right\rfloor M + l\right)\nu+i} z^{\left\lfloor \frac{\lfloor \frac{N-K}{\nu} \rfloor - 1}{M} \right\rfloor} \\ \text{para } l = 0, 1, \dots, \beta \\ a_{l\nu+i} + a_{(M+l)\nu+i}z + \cdots + a_{\left(\left(\left\lfloor \frac{\lfloor \frac{N-K}{\nu} \rfloor - 1}{M} \right\rfloor - 1\right)M + l\right)\nu+i} z^{\left\lfloor \frac{\lfloor \frac{N-K}{\nu} \rfloor - 1}{M} \right\rfloor - 1} \\ \text{para } l = \beta + 1, \dots, M-1 \end{cases} \quad (2.19)$$

DEMOSTRACIÓN: Consideremos  $i$  fijo, con  $r+1 \leq i \leq \nu-1$ . Debemos entonces agrupar el polinomio

$$g_i(z) = a_i + a_{\nu+i}z + \cdots + a_{(\lfloor \frac{N-K}{\nu} \rfloor - 1)\nu+i} z^{\lfloor \frac{N-K}{\nu} \rfloor - 1}$$

en potencias de  $M$  para obtener la  $M$ -ésima matriz PCPC asociada a  $g_i(z)$ . Como

$$\left\lfloor \frac{N-K}{\nu} \right\rfloor - 1 = \left\lfloor \frac{\lfloor \frac{N-K}{\nu} \rfloor - 1}{M} \right\rfloor M + \beta, \quad (2.20)$$

para cierto  $\beta$  con  $0 \leq \beta < M$ , entonces la  $M$ -ésima descomposición polifásica de  $g_i(z)$  es

$$(g_{i,0}(z), g_{i,1}(z), \dots, g_{i,M-1}(z))$$

siendo los polinomios  $g_{i,l}(z)$ , los definidos en (2.19), para  $l = 0, 1, \dots, M-1$ , luego tenemos el resultado.  $\square$

El siguiente lema proporciona la  $M$ -ésima matriz PCPC del polinomio  $zg_i(z)$ , con  $r+1 \leq i \leq \nu-1$ .

**Lema 2.7:** Sea  $g_i(z)$  con  $r+1 \leq i \leq \nu-1$  el polinomio definido por la expresión (2.2), y sea  $\alpha$  el parámetro definido en (2.18). Entonces, la  $M$ -ésima matriz PCPC asociada a  $zg_i(z)$  es

$$(zg_i)^{[M]}(z) = \begin{pmatrix} f_{i,0}(z) & zf_{i,M-1}(z) & zf_{i,M-2}(z) & \cdots & zf_{i,1}(z) \\ f_{i,1}(z) & f_{i,0}(z) & zf_{i,M-1}(z) & \cdots & zf_{i,2}(z) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{i,M-1}(z) & f_{i,M-2}(z) & f_{i,M-3}(z) & \cdots & f_{i,0}(z) \end{pmatrix}$$

donde

$$f_{i,l}(z) = \begin{cases} a_{(l-1)\nu+i} + a_{(M+l-1)\nu+i}z + \cdots + a_{\left(\left\lfloor \frac{N-K}{\nu} \right\rfloor\right)_{M+l-1}\nu+i} z^{\left\lfloor \frac{N-K}{\nu} \right\rfloor} & \text{para } l = 0, 1, \dots, \alpha \\ a_{(l-1)\nu+i} + a_{(M+l-1)\nu+i}z + \cdots + a_{\left(\left(\left\lfloor \frac{N-K}{\nu} \right\rfloor - 1\right)_{M+l-1}\right)\nu+i} z^{\left\lfloor \frac{N-K}{\nu} \right\rfloor - 1} & \text{para } l = \alpha + 1, \dots, M-1 \end{cases} \quad (2.21)$$

con  $a_{-\nu+i} = 0$ .

DEMOSTRACIÓN: Sea  $i$  fijo, con  $r + 1 \leq i \leq \nu - 1$ . De forma análoga a los lemas anteriores, debemos agrupar

$$zg_i(z) = a_i z + a_{\nu+i} z^2 + \cdots + a_{\lfloor \frac{N-K}{\nu} \rfloor - 1} z^{\lfloor \frac{N-K}{\nu} \rfloor + i}$$

en potencias de  $M$ . Si tomamos el parámetro  $\alpha$  como el definido por (2.18), obtenemos la  $M$ -ésima descomposición polifásica de  $zg_i(z)$ ,

$$(f_{i,0}(z), f_{i,1}(z), \dots, f_{i,M-1}(z))$$

siendo  $f_{i,l}(z)$  los polinomios dados en (2.21), para  $l = 0, 1, \dots, M - 1$ , luego obtenemos el resultado.  $\square$

Finalmente, obtenemos la  $M$ -ésima matriz PCPC para el polinomio  $zg_i(z)$ , con  $\nu - \kappa + 1 \leq i \leq r$ .

**Lema 2.8:** Sea  $g_i(z)$  con  $\nu - \kappa + 1 \leq i \leq r$  el polinomio definido por la expresión (2.2) y  $\gamma$  el resto de la división de  $\lfloor \frac{N-K}{\nu} \rfloor + 1$  por  $M$ . Entonces, la  $M$ -ésima matriz PCPC asociada a  $zg_i(z)$  es

$$(zg_i)^{[M]}(z) = \begin{pmatrix} h_{i,0}(z) & zh_{i,M-1}(z) & zh_{i,M-2}(z) & \cdots & zh_{i,1}(z) \\ h_{i,1}(z) & h_{i,0}(z) & zh_{i,M-1}(z) & \cdots & zh_{i,2}(z) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{i,M-1}(z) & h_{i,M-2}(z) & h_{i,M-3}(z) & \cdots & h_{i,0}(z) \end{pmatrix}$$

donde

$$h_{i,l}(z) = \begin{cases} a_{(l-1)\nu+i} + a_{(M+l-1)\nu+i} z + \cdots + a_{\left(\lfloor \frac{N-K}{\nu} \rfloor + 1\right)_{M+l-1}\nu+i} z^{\lfloor \frac{N-K}{\nu} \rfloor + 1} & \text{para } l = 0, 1, \dots, \gamma \\ a_{(l-1)\nu+i} + a_{(M+l-1)\nu+i} z + \cdots + a_{\left(\left(\lfloor \frac{N-K}{\nu} \rfloor + 1\right) - 1\right)_{M+l-1}\nu+i} z^{\lfloor \frac{N-K}{\nu} \rfloor + 1} & \text{para } l = \gamma + 1, \dots, M - 1 \end{cases} \quad (2.22)$$

con  $a_{-\nu+i} = 0$ .

DEMOSTRACIÓN: Sea  $i$  fijo, con  $\nu - \kappa + 1 \leq i \leq r$ . Nuestro objetivo es calcular la  $M$ -ésima matriz PCPC asociada a

$$zg_i(z) = a_i z + a_{\nu+i} z^2 + \cdots + a_{\lfloor \frac{N-K}{\nu} \rfloor + i} z^{\lfloor \frac{N-K}{\nu} \rfloor + 1}.$$

Por tanto, tenemos que agrupar  $zg_i(z)$  en potencias de  $M$ . Como

$$\left\lfloor \frac{N-K}{\nu} \right\rfloor + 1 = \left\lfloor \frac{\lfloor \frac{N-K}{\nu} \rfloor + 1}{M} \right\rfloor M + \gamma \quad (2.23)$$

para cierto  $\gamma$  con  $0 \leq \gamma < M$ , entonces la  $M$ -ésima descomposición polifásica asociada a  $zg_i(z)$  es

$$(h_{i,0}(z), h_{i,1}(z), \dots, h_{i,M-1}(z)),$$

siendo los polinomios  $h_{i,l}(z)$  los definidos por la relación (2.22), para  $l = 0, 1, \dots, M-1$ , luego tenemos el resultado.  $\square$

### 2.4.3 Códigos convolucionales de Justesen perforados

El resultado principal de este capítulo viene dado por los teoremas siguientes, que refuerzan las propiedades del código convolucional de Justesen perforado al requerir que la matriz generadora  $G(z)$  del código original  $\mathcal{C}$  sea minimal. El objetivo es mantener los grados fila de  $G(z)$  después de eliminar las correspondientes columnas según la matriz de perforación.

**Teorema 2.5:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$ ,  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$  y  $r$  el resto de la división de  $N - K$  entre  $\nu$ , dado por la expresión (2.1). Supongamos que  $r = \nu - \kappa$  y sean  $P$  y  $G_P(z)$  la matriz de perforación y la matriz generadora del código convolucional perforado, respectivamente. Entonces  $G_P(z)$  es también una matriz generadora minimal si la primera fila de algún  $i$ -ésimo bloque de  $M$  filas, para  $i = 1, 2, \dots, r+1$ , no está entre las filas eliminadas.

DEMOSTRACIÓN: Teniendo en cuenta que  $r = \nu - \kappa$  y la expresión (1.7), la matriz generadora  $G(z)$  de  $\mathcal{C}$  viene dada por

$$G(z) = \begin{pmatrix} g_0(z) & zg_{\nu-1}(z) & \dots & zg_{r+1}(z) \\ g_1(z) & g_0(z) & \dots & zg_{r+2}(z) \\ \vdots & \vdots & & \vdots \\ g_{\nu-1}(z) & g_{\nu-2}(z) & \dots & g_r(z) \end{pmatrix}$$

siendo  $g_i(z)$  los polinomios definidos por la expresión (2.2). Aplicando entonces la definición 1.6 y el teorema 1.6, el primer paso es considerar la  $M$ -ésima matriz PCPC

asociada a cada una de las entradas de  $G(z)$  para obtener la matriz generadora  $G^{[M]}(z)$  del  $(\nu M, \kappa M, \delta)$ -código por bloques. Ahora bien, en el caso que nos ocupa,  $r = \nu - \kappa$  y, por tanto, tenemos tres tipos de polinomios  $g_i(z)$  cuya  $M$ -ésima matriz PCPC es diferente,

- $g_i(z)$ , con  $0 \leq i \leq r$ ,
- $g_i(z)$ , con  $r + 1 \leq i \leq \nu - 1$ ,
- $zg_i(z)$ , con  $r + 1 \leq i \leq \nu - 1$ .

Los lemas 2.5, 2.6 y 2.7 nos proporcionan la expresión de la  $M$ -ésima matriz PCPC asociada a cada uno de estos polinomios.

Analicemos ahora las filas de  $G^{[M]}(z)$  que pueden ser eliminadas para mantener el grado original de cada columna, ya que aplicando entonces el teorema 1.3, obtendremos el resultado.

- Si  $M$  no divide a  $\lfloor \frac{N-K}{\nu} \rfloor$ , el grado de la columna  $M - \alpha + 1$ , viene dado únicamente por los polinomios situados en las posiciones  $((i - 1)M + 1, M - \alpha + 1)$ , para  $i = 1, 2, \dots, r + 1$ , de la matriz  $G^{[M]}(z)$ . Además, el resto de polinomios situados en las mismas filas  $(i - 1)M + 1$ , para  $i = 1, 2, \dots, r + 1$ , dan también el grado de la correspondiente columna. Por tanto, si no eliminamos la primera fila de alguno de los bloques de entre los  $r + 1$  primeros bloques de  $M$  filas, los grados columna se mantienen.
- Si  $M$  divide a  $\lfloor \frac{N-K}{\nu} \rfloor$ , entonces el grado de la primera columna viene dado únicamente por los polinomios situados en las posiciones  $((i - 1)M + 1, 1)$ , para  $i = 1, 2, \dots, r + 1$ , de la matriz  $G^{[M]}(z)$ . Además, el resto de polinomios de las filas  $(i - 1)M + 1$ , para  $i = 1, 2, \dots, r + 1$ , proporcionan también el grado de la columna correspondiente. Por tanto, si mantenemos la primera fila de alguno de los  $r + 1$  primeros bloques de  $M$  filas, los grados columna se mantienen.  $\square$

**Teorema 2.6:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$ ,  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$  y  $r$  el resto de la división de  $N - K$  entre  $\nu$ , dado por la expresión (2.1). Supongamos que  $\nu - \kappa + 1 \leq r \leq \nu - 1$  y sea  $P$  la matriz de perforación y  $G_P(z)$  la matriz generadora del código convolucional perforado. Entonces  $G_P(z)$  es también minimal si la primera fila de la matriz  $G^{[M]}(z)$  no se encuentra entre las filas eliminadas.

DEMOSTRACIÓN: La matriz generadora de  $\mathcal{C}$  viene dada por

$$G(z) = \begin{pmatrix} g_0(z) & zg_{\nu-1}(z) & \dots & zg_r(z) & \dots & zg_{\nu-\kappa+1}(z) \\ g_1(z) & g_0(z) & \dots & zg_{r+1}(z) & \dots & zg_{\nu-\kappa+2}(z) \\ \vdots & \vdots & & \vdots & & \vdots \\ g_{r+\kappa-\nu-1}(z) & g_{r+\kappa-\nu-2}(z) & \dots & & \dots & zg_r(z) \\ \vdots & \vdots & & \vdots & & \vdots \\ g_{\nu-1}(z) & g_{\nu-2}(z) & \dots & g_{r-1}(z) & \dots & g_{\nu-\kappa}(z) \end{pmatrix},$$

siendo  $g_i(z)$  los polinomios definidos en (2.2).

Para obtener la matriz generadora de  $G^{[M]}(z)$  para el  $(\nu M, \kappa M, \delta)$ -código obtenido por descomposición en bloques, de acuerdo con el teorema 1.6, debemos obtener la  $M$ -ésima matriz PCPC asociada a cada una de las entradas de  $G(z)$ . En este caso, tenemos cuatro tipos de polinomios cuya  $M$ -ésima matriz PCPC es diferente,

- $g_i(z)$ , con  $0 \leq i \leq r$ ,
- $g_i(z)$ , con  $r+1 \leq i \leq \nu-1$ ,
- $zg_i(z)$ , con  $r+1 \leq i \leq \nu-1$ ,
- $zg_i(z)$ , con  $\nu-\kappa+1 \leq i \leq r$ .

Los lemas 2.5, 2.6, 2.7 y 2.8 nos proporcionan la expresión de la  $M$ -ésima matriz PCPC asociada a cada uno de estos polinomios.

Nuestro objetivo por tanto, es analizar qué filas de  $G^{[M]}(z)$  pueden ser eliminadas para mantener el grado original de cada columna, esto es, tenemos que determinar las filas que proporcionan el grado de cada columna, ya que aplicando entonces el teorema 1.3, obtenemos el resultado.

- Si  $M$  no divide a  $\lfloor \frac{N-K}{\nu} \rfloor + 1$ , entonces únicamente el polinomio situado en la posición  $(1, (\nu-r)M + M - \alpha)$  de  $G^{[M]}(z)$  da el grado de la columna  $(\nu-r)M + M - \alpha$ , y los polinomios de la primera fila de esta matriz también dan el grado de la columna a la que pertenecen. Así pues, es suficiente con mantener esta primera fila para tener los mismos grados columna que en  $G^{[M]}(z)$  después de la perforación.
- Si  $M$  divide a  $\lfloor \frac{N-K}{\nu} \rfloor + 1$ , entonces el grado de la columna  $(\nu-r)M + 1$  viene dado únicamente por el polinomio situado en la posición  $(1, (\nu-r)M + 1)$ . Además, los restantes polinomios de la primera fila de  $G^{[M]}(z)$  también dan el grado de la columna a la que pertenecen. Por tanto, debemos mantener la primera fila de  $G^{[M]}(z)$  para que  $G_P(z)$  pueda ser una matriz generadora minimal con el mismo

grado que  $G^{[M]}(z)$ . □

Como consecuencia de los teoremas anteriores, obtenemos el resultado siguiente.

**Teorema 2.7:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$ ,  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$  y  $r$  el resto de la división de  $N - K$  entre  $\nu$ , dado por la expresión (2.1). Si  $\mathcal{C}^{[M]}$  es un código compacto, entonces el código perforado  $\mathcal{C}_P$ , en donde  $P$  es la matriz de perforación dada en los teoremas 2.5 o 2.6 es también compacto.

DEMOSTRACIÓN: Aplicando los teoremas 2.5 y 2.6, sabemos que la matriz generadora  $G_P(z)$  es también minimal; además, los índices de Forney son los mismos que los índices de Forney del código por bloques  $\mathcal{C}^{[M]}$ . Observemos que el número de cada índice de Forney, se mantiene también después de la perforación, ya que no eliminamos ninguna columna. Así pues, si  $\mathcal{C}^{[M]}$  es compacto, concluimos que el código  $\mathcal{C}_P$  también es compacto. □

Como consecuencia directa de los teoremas 2.3, 2.4 y 2.7, así como del corolario 2.2, tenemos el resultado siguiente.

**Corolario 2.6:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$ ,  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$  y  $r$  el resto de la división de  $N - K$  entre  $\nu$ , dado por la expresión (2.1). Sea  $P$  es la matriz de perforación dada en los teoremas 2.5 ó 2.6 y denotemos por  $\mathcal{C}_P$  el código perforado. Entonces

- (a) Si  $\kappa$  no divide a  $\delta$  y  $\lfloor \frac{\delta}{\kappa M} \rfloor = \lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor}{M} \rfloor = \lfloor \frac{\lfloor \frac{\delta}{\kappa} \rfloor + 1}{M} \rfloor$ , entonces el código  $\mathcal{C}_P$  es compacto.  
 (b) Si  $\kappa$  divide a  $\delta$ , entonces  $\mathcal{C}_P$  es compacto.

El teorema siguiente proporciona cotas para las columnas que debemos eliminar para que el código perforado  $\mathcal{C}_P$  pueda ser un código convolucional MDS.

**Teorema 2.8:** Sean  $\mathcal{B}$  un  $[N, K]$ -código Reed-Solomon con polinomio generador  $g(z)$ ,  $\mathcal{C}$  el  $(\nu, \kappa, \delta)$ -código de Justesen generado por el polinomio  $g(z)$  y  $r$  el resto de la división de  $N - K$  entre  $\nu$ , dado por la expresión (2.1). Sea  $P$  la matriz de perforación de tamaño  $\nu \times M$  de acuerdo con los teoremas 2.5 o 2.6, con un total de  $C$  ceros y  $\nu M - C$  unos, esto es,  $C$  es el número de filas eliminadas de  $G^{[M]}(z)$ . Entonces, el código perforado

$\mathcal{C}_P$  puede ser un código convolucional MDS si  $C$  satisface la relación

$$(\nu - \kappa)M + \frac{\delta - N + K}{\left\lfloor \frac{\delta}{\kappa M} \right\rfloor + 1} \leq C < (\nu - \kappa)M. \quad (2.24)$$

DEMOSTRACIÓN: Sabemos que la matriz generadora del código perforado se obtiene eliminando ciertas filas de la matriz generadora  $G^{[M]}(z)$  del código  $\mathcal{C}^{[M]}$  obtenido por descomposición en bloques, usando la matriz  $P$  como patrón. Entonces, el código perforado es un  $(\nu M - C, \kappa M, \delta)$ -código cuya distancia libre es menor o igual que la distancia libre del código de Justesen original, de donde tenemos que

$$d_{free}(\mathcal{C}_P) \leq d_{free}(\mathcal{C}) = N - K + 1. \quad (2.25)$$

Sabemos que  $\mathcal{C}_P$  es un código MDS si y sólo si su distancia libre es igual a la cota Singleton generalizada, esto es,

$$d_{free}(\mathcal{C}_P) = (\nu M - C - \kappa M) \left( \left\lfloor \frac{\delta}{\kappa M} \right\rfloor + 1 \right) + \delta + 1.$$

Ahora, de la expresión (2.25), obtenemos que la relación anterior puede darse si  $C$  verifica la desigualdad

$$(\nu M - C - \kappa M) \left( \left\lfloor \frac{\delta}{\kappa M} \right\rfloor + 1 \right) + \delta + 1 \leq N - K + 1,$$

esto es, si

$$(\nu - \kappa)M + \frac{\delta - N + K}{\left\lfloor \frac{\delta}{\kappa M} \right\rfloor + 1} \leq C. \quad (2.26)$$

Además, después de hacer la perforación, la longitud del vector de salidas de  $\mathcal{C}_P$  debe ser mayor que la del vector de entradas, es decir,

$$\nu M - C > \kappa M. \quad (2.27)$$

La expresión (2.24) se obtiene entonces de las desigualdades (2.26) y (2.27).  $\square$

## 2.5 Conclusiones

Los resultados de perforación de códigos convolucionales basados en la construcción de Justesen introducidos en esta memoria nos permiten elegir la matriz patrón de la

perforación de manera que la matriz generadora del código perforado obtenido sea minimal. De este modo, conocemos el grado del código y, por tanto, sabemos si su distancia libre se aproxima a la cota Singleton generalizada. También, proporcionamos los valores de los parámetros del código convolucional de Justesen y del código bloque que lo genera para los cuales el código de Justesen no puede tener perfil de distancia máxima.



# Concatenación en serie de códigos convolucionales

---

*Although to penetrate into the intimate mysteries of nature and thence to learn the true causes of phenomena is not allowed to us, nevertheless it can happen that a certain fictive hypothesis may suffice for explaining many phenomena.*

–Leonhard Euler

*Make everything as simple as possible, but not simpler.*

–Albert Einstein

## 3.1 Introducción

La teoría desarrollada por Shannon [98], permite asegurar que si la longitud de un código es suficientemente grande, entonces es bueno. Ahora bien, la complejidad de decodificación aumenta con la longitud del código. Una solución a este problema fue propuesta por Elias [38], que construyó códigos bloque potentes partiendo de códigos bloque lineales sencillos empleando una construcción conocida como el producto de Elias. Más tarde, Forney [41], en su búsqueda por encontrar una clase de códigos cuya probabilidad de error decreciera exponencialmente con la longitud del código mientras la complejidad de decodificación aumentara sólo algebraicamente, llegó a una solución consistente en una estructura de código multinivel, conocida como código concatenado. Consiste en una cascada de un código interno y un código externo, empleando en ocasiones un intercalado entre los dos codificadores para separar los errores por ráfaga producidos por el código interno. En 1974, Blokh y Zyablov [14] y Zinov'ev [119] intro-

dujeron una clase importante de códigos concatenados, que eran capaces de corregir tanto errores aleatorios como ráfagas de errores. Otra construcción importante obtenida de combinar códigos es debida a Tanner [106], que generalizó los códigos LDPC (en inglés, *Low Density Parity Check*) empleando grafos.

Motivados inicialmente por intereses teóricos únicamente, los códigos concatenados se han empleado en aplicaciones en el espacio [51], realzado de datos en GSM (EDGE, en inglés, *Enhanced Data rates for GSM Evolution*) [81], sistemas de comunicación inalámbricos [73, 74], por citar sólo algunos ejemplos.

Como ya comentamos en el capítulo 1, Höst, Johannesson y Zyablov [59] desarrollaron una novedosa construcción de códigos convolucionales, llamados códigos convolucionales *woven*. Se trata de una concatenación en serie de códigos convolucionales, en la que consideran como código externo o como código interno o bien como ambos, una concatenación paralela de códigos convolucionales.

Ahora bien, los códigos concatenados siempre han sido estudiados a partir de la matriz generadora. En este capítulo, caracterizaremos cuatro modelos de concatenación en serie de códigos convolucionales empleando la representación entrada-estado-salida introducida por Rosenthal, Schumacher y York [91]. Höst, Johannesson y Zyablov [60] analizan las propiedades de la matriz generadora de un tipo de concatenación en serie de dos códigos convolucionales, en función de las matrices generadoras de los códigos constituyentes. Ahora bien, además de trabajar sobre cuerpos binarios, no obtienen condiciones para asegurar que la matriz generadora de la concatenación sea minimal-básica, aun partiendo de matrices generadoras minimales-básicas de los códigos que forman la concatenación. Por tanto, no disponen de herramientas para obtener el grado del código. Es más, las propiedades que obtienen son propiedades de las matrices generadoras y no del código, ya que trabajan en espacios vectoriales y no en módulos. En este capítulo, empleando la teoría de sistemas, damos condiciones para obtener una representación entrada-estado-salida minimal para los diferentes modelos de concatenación que estudiamos y, en consecuencia, obtenemos el grado de los códigos concatenados.

Comenzamos describiendo dos modelos de concatenación en serie en la sección 3.2, que llamamos sistemáticos ya que la entrada del código interno es únicamente el vector de paridad del código externo. Uno de estos modelos corresponde al empleado en la teoría de control. Proporcionamos la representación entrada-estado-salida de los modelos, así como condiciones para obtener un código concatenado observable con realización minimal. Obtenemos también cotas inferiores de la distancia libre de uno de los mode-

los de concatenación en función de las distancia libres de los códigos externo e interno. En la sección 3.3 estudiamos dos modelos diferentes de concatenación en serie, uno de ellos introducido por Forney, en los que la entrada del código interno es toda la palabra código del código externo. De forma análoga a los modelos anteriores, obtenemos la representación entrada-estado-salida, proporcionando condiciones para que ésta sea minimal, y para que el código concatenado sea observable. Finalizamos obteniendo cotas inferiores de la distancia libre de uno de los modelos en función de las distancias libres de los códigos constituyentes. Es importante señalar que trabajamos sobre un cuerpo de Galois arbitrario  $\mathbb{F}$ , no necesariamente binario.

Como ya hemos comentado anteriormente, en este capítulo estudiamos y caracterizamos diferentes tipos de concatenación en serie de códigos convolucionales. En dicha concatenación, los códigos se ordenan en serie uno tras otro. En el caso de dos códigos constituyentes, se habla de código externo y código interno. Denotamos por  $\mathcal{C}_o$  el **código externo** y por  $\mathcal{C}_i$  el **código interno**. También, denotamos por  $x_t^{(1)}$ ,  $u_t^{(1)}$ ,  $y_t^{(1)}$  y  $v_t^{(1)}$  el vector de estados, el vector información, el vector de paridad y la palabra código de  $\mathcal{C}_o$ , respectivamente; del mismo modo, denotamos por  $x_t^{(2)}$ ,  $u_t^{(2)}$ ,  $y_t^{(2)}$  y  $v_t^{(2)}$  el vector de estados, el vector información, el vector de paridad y la palabra código de  $\mathcal{C}_i$ , respectivamente. En los diferentes modelos de concatenación en serie, las palabras código  $v_t^{(1)}$  y  $v_t^{(2)}$  de  $\mathcal{C}_o$  y  $\mathcal{C}_i$ , respectivamente, vienen dadas por las expresiones

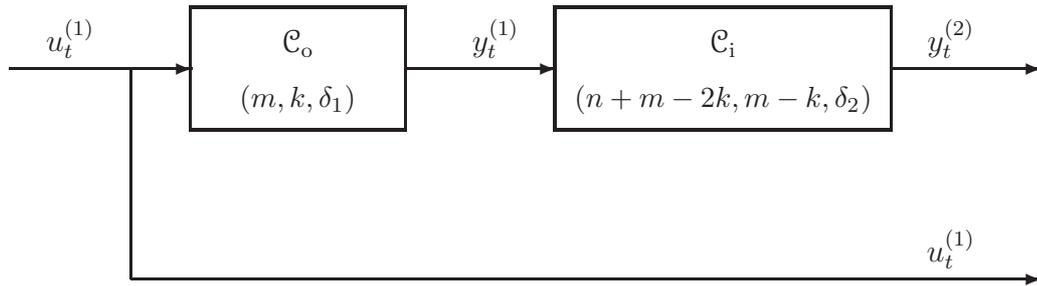
$$v_t^{(1)} = \begin{pmatrix} y_t^{(1)} \\ u_t^{(1)} \end{pmatrix} \quad \text{y} \quad v_t^{(2)} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(2)} \end{pmatrix}. \quad (3.1)$$

Análogamente,  $x_t$ ,  $u_t$ ,  $y_t$  y  $v_t$  serán el vector de estados, el vector información, el vector de paridad y la palabra código, respectivamente, del correspondiente modelo de código concatenado que estamos tratando.

Finalmente, denotamos por  $T_1(z)$ ,  $T_2(z)$  y  $T(z)$  la función de transferencia del código  $\widehat{\mathcal{C}}_o$ , del código  $\widehat{\mathcal{C}}_i$  y del código concatenado correspondiente, considerado como un  $\mathcal{F}$ -subespacio vectorial de  $\mathcal{F}^n$  (véase la sección 1.5), respectivamente.

## 3.2 Concatenación en serie sistemática

En esta sección, estudiamos y caracterizamos dos modelos de concatenación en serie de códigos convolucionales, uno de ellos utilizado en la teoría clásica de control. Analizamos la representación entrada-estado-salida de los modelos, así como condiciones para obtener la controlabilidad del par  $(A, B)$  y la observabilidad del par  $(A, C)$ .



**Figura 3.1:** Código concatenado  $\mathcal{SC}^{(1)}$

Finalizamos la sección con resultados sobre las distancias columnas y distancias libres de los modelos.

## 3.2.1 Representación entrada-estado-salida

### Modelo 1

El primer tipo de concatenación que estudiamos es uno de los modelos clásicos empleado en la teoría clásica de control en el espacio de estados. El código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$  se serializan, uno tras otro (véase la figura 3.1), de manera que el vector información  $u_t^{(1)}$  es codificado por  $\mathcal{C}_o$  y el vector de paridad  $y_t^{(1)}$  de la palabra código obtenida  $v_t^{(1)}$  es, a su vez, el vector información para el código interno  $\mathcal{C}_i$ , es decir,

$$u_t^{(2)} = y_t^{(1)}. \quad (3.2)$$

Denotamos por  $\mathcal{SC}^{(1)}$  el código convolucional obtenido. El estado del sistema es entonces la unión de los estados de los dos códigos constituyentes, es decir,

$$x_t = \begin{pmatrix} x_t^{(2)} \\ x_t^{(1)} \end{pmatrix}. \quad (3.3)$$

Observemos que el vector información o entrada  $u_t$  y el vector de paridad  $y_t$  de  $\mathcal{SC}^{(1)}$  vienen dados por

$$u_t = u_t^{(1)} \quad \text{e} \quad y_t = y_t^{(2)}, \quad (3.4)$$

respectivamente. De este modo, la palabra código de  $\mathcal{SC}^{(1)}$  resulta ser

$$v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(1)} \end{pmatrix}. \quad (3.5)$$

**Observación 3.1:** Si queremos obtener un código convolucional  $\mathcal{SC}^{(1)}$  de tasa  $k/n$ , entonces debemos considerar un  $(m, k, \delta_1)$ -código externo y un  $(n + m - 2k, m - k, \delta_2)$ -código interno (véase la figura 3.1). En cambio, si partimos de un código externo  $\mathcal{C}_o$  y un código interno  $\mathcal{C}_i$  de tasas  $k/m$  y  $(m - k)/n$ , respectivamente, entonces el código convolucional  $\mathcal{SC}^{(1)}$  obtenido de la concatenación de dichos códigos tiene tasa  $k/(n - m + 2k)$ . ■

El teorema siguiente proporciona la representación entrada-estado-salida para el código concatenado  $\mathcal{SC}^{(1)}$  en función de la representación entrada-estado-salida de los códigos externo e interno.

**Teorema 3.1:** Si  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, \delta_1)$ -código y  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n + m - 2k, m - k, \delta_2)$ -código, entonces la representación entrada-estado-salida para el código concatenado  $\mathcal{SC}^{(1)}$  de tasa  $k/n$  viene dada por el sistema lineal (1.11), donde

$$A = \begin{pmatrix} A_2 & B_2C_1 \\ O & A_1 \end{pmatrix}, \quad B = \begin{pmatrix} B_2D_1 \\ B_1 \end{pmatrix}, \quad C = \begin{pmatrix} C_2 & D_2C_1 \end{pmatrix} \quad y \quad D = D_2D_1. \quad (3.6)$$

DEMOSTRACIÓN: De la expresión (1.11) tenemos, para el código externo  $\mathcal{C}_o$ ,

$$\begin{aligned} x_{t+1}^{(1)} &= A_1x_t^{(1)} + B_1u_t^{(1)}, \\ y_t^{(1)} &= C_1x_t^{(1)} + D_1u_t^{(1)}, \end{aligned}$$

y para el código interno  $\mathcal{C}_i$ ,

$$\begin{aligned} x_{t+1}^{(2)} &= A_2x_t^{(2)} + B_2u_t^{(2)}, \\ y_t^{(2)} &= C_2x_t^{(2)} + D_2u_t^{(2)}. \end{aligned}$$

Ahora bien, teniendo en cuenta las expresiones (3.2), (3.3) y (3.4), la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(1)}$  viene dada por

$$\begin{aligned} x_{t+1} &= \begin{pmatrix} A_2 & B_2C_1 \\ O & A_1 \end{pmatrix} x_t + \begin{pmatrix} B_2D_1 \\ B_1 \end{pmatrix} u_t, \\ y_t &= \begin{pmatrix} C_2 & D_2C_1 \end{pmatrix} x_t + \begin{pmatrix} D_2D_1 \end{pmatrix} u_t. \end{aligned} \quad \square$$

Empleando el resultado anterior y el teorema 1.12, obtenemos la función de transferencia  $T(z)$  asociada al código convolucional  $\widehat{\mathcal{SC}}^{(1)}$  (véase la sección 1.5) en términos de las funciones de transferencia  $T_1(z)$  y  $T_2(z)$  asociadas a los códigos  $\widehat{\mathcal{C}}_o$  y  $\widehat{\mathcal{C}}_i$ , respectivamente.

**Teorema 3.2:** Si  $\mathcal{SC}^{(1)}(A, B, C, D)$  es el código concatenado descrito por las matrices de la expresión (3.6), entonces

$$T(z) = T_2(z)T_1(z)$$

es la función de transferencia asociada a  $\widehat{\mathcal{SC}}^{(1)}$ .

## Modelo 2

Como podemos observar en la expresión (3.5), una palabra código de  $\mathcal{SC}^{(1)}$  está formada por el vector de paridad del código interno  $\mathcal{C}_i$  y el vector de información del código externo  $\mathcal{C}_o$ . Por tanto, no tenemos ninguna relación entre las palabras código del código concatenado y las palabras código completas de los códigos constituyentes, hecho que representa un problema a la hora de relacionar la distancia libre de  $\mathcal{SC}^{(1)}$  con las distancias libres de  $\mathcal{C}_o$  y  $\mathcal{C}_i$ , como veremos posteriormente. Esto motiva la consideración de una variación de la concatenación  $\mathcal{SC}^{(1)}$  de manera que la entrada para el código interno  $u_t^{(2)}$  siga siendo el vector de paridad  $y_t^{(1)}$  del código externo  $\mathcal{C}_o$ , es decir,

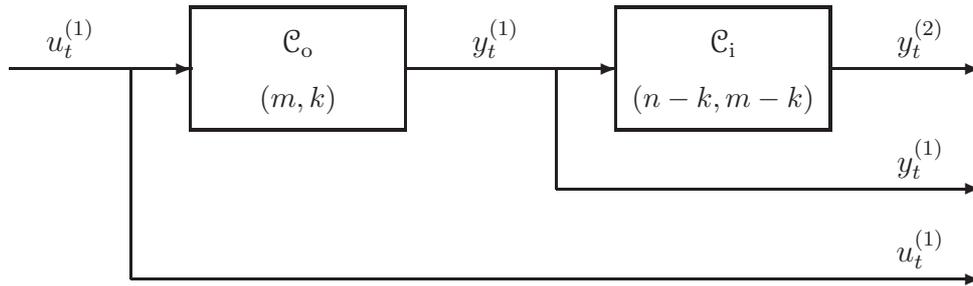
$$u_t^{(2)} = y_t^{(1)}, \quad (3.7)$$

pero que a su vez,  $u_t^{(2)}$  forme parte de la palabra código de la concatenación (véase la figura 3.2), esto es,

$$v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ y_t^{(1)} \\ u_t^{(1)} \end{pmatrix}. \quad (3.8)$$

Denotamos por  $\mathcal{SC}^{(2)}$  el código concatenado obtenido. Observamos entonces que las palabras código de  $\mathcal{C}_o$  y de  $\mathcal{C}_i$  están dadas por

$$v_t^{(1)} = \begin{pmatrix} y_t^{(1)} \\ u_t^{(1)} \end{pmatrix} \quad \text{y} \quad v_t^{(2)} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(2)} \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ y_t^{(1)} \end{pmatrix} \quad (3.9)$$



**Figura 3.2:** Código concatenado  $\mathcal{SC}^{(2)}$

y, por tanto, la relación entre las palabras código de  $\mathcal{SC}^{(2)}$  y las de  $\mathcal{C}_o$  y  $\mathcal{C}_i$ , es

$$v_t = \begin{pmatrix} y_t^{(2)} \\ y_t^{(1)} \\ u_t^{(1)} \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ v_t^{(1)} \end{pmatrix} = \begin{pmatrix} v_t^{(2)} \\ u_t^{(1)} \end{pmatrix}.$$

Es decir, una palabra código de  $\mathcal{SC}^{(2)}$  contiene a su vez una palabra código de  $\mathcal{C}_o$  y una palabra código de  $\mathcal{C}_i$ . Esto nos permite asegurar que la distancia libre del código concatenado es mayor o igual a las distancias libres de los códigos externo e interno, tal como vemos en la sección 3.2.4.

Al igual que en el código concatenado  $\mathcal{SC}^{(1)}$ , el vector de estados  $x_t$  y el vector información  $u_t$  de  $\mathcal{SC}^{(2)}$  son

$$x_t = \begin{pmatrix} x_t^{(2)} \\ x_t^{(1)} \end{pmatrix} \quad \text{y} \quad u_t = u_t^{(1)}, \quad (3.10)$$

respectivamente. Ahora bien, en este modelo, a diferencia de lo que ocurre con el modelo 1, el vector de paridad está formado por los vectores de paridad de los códigos externo e interno, es decir,

$$y_t = \begin{pmatrix} y_t^{(2)} \\ y_t^{(1)} \end{pmatrix}. \quad (3.11)$$

**Observación 3.2:** Del mismo modo a como comentábamos en la observación 3.1, si queremos obtener un código convolucional  $\mathcal{SC}^{(2)}$  de tasa  $k/n$ , entonces debemos considerar un  $(m, k, \delta_1)$ -código externo y un  $(n - k, m - k, \delta_2)$ -código interno (véase la figura 3.2). En cambio, si partimos de un código externo  $\mathcal{C}_o$  y un código interno

$\mathcal{C}_i$  de tasas  $k/m$  y  $(m-k)/n$ , respectivamente, entonces el código convolucional  $\mathcal{SC}^{(2)}$  obtenido de la concatenación de dichos códigos tiene tasa  $k/(n+k)$ . ■

La representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(2)}$  viene dada en función de la representación entrada-estado-salida de los códigos constituyentes, como vemos en el teorema siguiente.

**Teorema 3.3:** Si  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, \delta_1)$ -código y  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n-k, m-k, \delta_2)$ -código, entonces la representación entrada-estado-salida para el código concatenado  $\mathcal{SC}^{(2)}$  de tasa  $k/n$  viene dada por el sistema lineal (1.11), donde

$$\begin{aligned} A &= \begin{pmatrix} A_2 & B_2C_1 \\ O & A_1 \end{pmatrix}, & B &= \begin{pmatrix} B_2D_1 \\ B_1 \end{pmatrix}, \\ C &= \begin{pmatrix} C_2 & D_2C_1 \\ O & C_1 \end{pmatrix}, & D &= \begin{pmatrix} D_2D_1 \\ D_1 \end{pmatrix}. \end{aligned} \tag{3.12}$$

DEMOSTRACIÓN: Siguiendo los mismos pasos que en la demostración del teorema 3.1, tenemos que,

$$\begin{aligned} x_{t+1}^{(1)} &= A_1x_t^{(1)} + B_1u_t^{(1)}, & x_{t+1}^{(2)} &= A_2x_t^{(2)} + B_2u_t^{(2)}, \\ y_t^{(1)} &= C_1x_t^{(1)} + D_1u_t^{(1)}, & y_t^{(2)} &= C_2x_t^{(2)} + D_2u_t^{(2)}. \end{aligned}$$

Ahora bien, teniendo en cuenta las expresiones (3.7), (3.10) y (3.11), la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(2)}$  viene dada por

$$\begin{aligned} x_{t+1} &= \begin{pmatrix} A_2 & B_2C_1 \\ O & A_1 \end{pmatrix} x_t + \begin{pmatrix} B_2D_1 \\ B_1 \end{pmatrix} u_t, \\ y_t &= \begin{pmatrix} C_2 & D_2C_1 \\ O & C_1 \end{pmatrix} x_t + \begin{pmatrix} D_2D_1 \\ D_1 \end{pmatrix} u_t. \end{aligned} \quad \square$$

Al igual que en el modelo  $\mathcal{SC}^{(1)}$ , a partir del resultado anterior y del teorema 1.12, obtenemos la función de transferencia  $T(z)$  asociada al código convolucional  $\widehat{\mathcal{SC}}^{(2)}$  en términos de las funciones de transferencia  $T_1(z)$  y  $T_2(z)$  asociadas a los códigos  $\widehat{\mathcal{C}}_o$  y  $\widehat{\mathcal{C}}_i$ , respectivamente.

**Teorema 3.4:** Si  $\mathcal{SC}^{(2)}(A, B, C, D)$  es el código concatenado descrito por las matrices de la expresión (3.12), entonces

$$T(z) = \begin{pmatrix} T_2(z)T_1(z) \\ T_1(z) \end{pmatrix}$$

es la función de transferencia asociada a  $\widehat{\mathcal{SC}}^{(2)}$ .

### 3.2.2 Controlabilidad

Tal y como comentamos en la sección 1.5, el concepto de controlabilidad del par  $(A, B)$  está relacionado con el de minimalidad de una representación entrada-estado-salida  $(A, B, C, D)$ . Así pues, nuestro objetivo para esta sección, es analizar las condiciones que deben cumplir las matrices  $A_l, B_l, C_l$  y  $D_l$ , para  $l = 1, 2$  de los códigos constituyentes para que el código concatenado tenga una representación minimal. Dado que las matrices  $A$  y  $B$  de los códigos  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$  tienen la misma expresión, los resultados que presentamos, serán válidos para ambos tipos de concatenación. Por tanto, a lo largo de esta sección,  $\mathcal{SCC}_{\text{sys}}$  denota el código concatenado  $\mathcal{SC}^{(1)}$  descrito por la expresión (3.6) así como el código  $\mathcal{SC}^{(2)}$  descrito por la expresión (3.12). Consideramos como código externo  $\mathcal{C}_o$  un  $(m, k, \delta_1)$ -código y como código interno  $\mathcal{C}_i$ , un  $(n, m - k, \delta_2)$ -código. Entonces, teniendo en cuenta las observaciones 3.1 y 3.2,  $\mathcal{SCC}_{\text{sys}}$  es un  $(n - m + 2k, k, \delta)$ -código si consideramos la concatenación  $\mathcal{SC}^{(1)}$  y es un  $(n + k, k, \delta)$ -código si consideramos la concatenación  $\mathcal{SC}^{(2)}$ .

El ejemplo siguiente pone de manifiesto que no es suficiente con que los pares  $(A_l, B_l)$ , para  $l = 1, 2$ , de los códigos constituyentes sean controlables, para que el par  $(A, B)$  del código concatenado  $\mathcal{SCC}_{\text{sys}}$  sea controlable.

**Ejemplo 3.1:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y consideremos el  $(6, 4, 2)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , donde

$$A_1 = \begin{pmatrix} \alpha^3 & \alpha \\ \alpha & \alpha^4 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 & \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \end{pmatrix}$$

$$C_1 = \begin{pmatrix} 1 & \alpha \\ \alpha & 1 \end{pmatrix} \quad \text{y} \quad D_1 = \begin{pmatrix} \alpha^3 & \alpha^4 & \alpha^3 & \alpha^4 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Observemos que  $(A_1, B_1)$  es controlable.

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  el  $(5, 2, 1)$ -código interno descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}, \quad B_2 = \begin{pmatrix} \alpha^3 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \alpha & 0 \end{pmatrix}.$$

Claramente, el par  $(A_2, B_2)$  es controlable.

Por otro lado, aplicando los teoremas 3.1 y 3.3, las matrices  $A$  y  $B$  de la representación entrada-estado-salida de los código concatenados  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$  son

$$A = \begin{pmatrix} \alpha & \alpha^3 & \alpha^4 \\ 0 & \alpha^3 & \alpha \\ 0 & \alpha & \alpha^4 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} \alpha^6 & 1 & \alpha^6 & 1 \\ 1 & \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \end{pmatrix}.$$

Pero el par  $(A, B)$  no es controlable, ya que

$$\text{rg} \begin{pmatrix} \alpha I - A & B \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & \alpha^3 & \alpha^4 & \alpha^6 & 1 & \alpha^6 & 1 \\ 0 & 1 & \alpha & 1 & \alpha & \alpha^3 & \alpha^4 \\ 0 & \alpha & \alpha^2 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \end{pmatrix} = 2 \neq 3. \quad \blacksquare$$

Así pues, necesitamos más condiciones sobre las matrices que describen los códigos externo e interno para obtener la controlabilidad del par  $(A, B)$  del código convolucional concatenado. El resultado siguiente introduce condiciones que aseguran dicha controlabilidad.

**Teorema 3.5:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m - k, \delta_2)$ -código y  $\mathcal{SC}_{\text{sys}}(A, B, C, D)$  el código concatenado correspondiente. Si  $\text{rg}(B) = \delta_1 + \delta_2$ , entonces  $(A, B, C, D)$  es una representación minimal de  $\mathcal{SC}_{\text{sys}}(A, B, C, D)$  con complejidad  $\delta_1 + \delta_2$ .

DEMOSTRACIÓN: Como  $\text{rg}(B) = \delta_1 + \delta_2$ , entonces

$$\text{rg} \begin{pmatrix} zI - A & B \end{pmatrix} = \delta_1 + \delta_2 \quad \text{para todo } z \in \overline{\mathbb{F}}.$$

De este modo, por el test PBH (véase la sección 1.4), el par  $(A, B)$  es controlable y por tanto,  $(A, B, C, D)$  es una representación minimal de  $\mathcal{SC}_{\text{sys}}$ .  $\square$

**Observación 3.3:** Notemos que la condición  $\text{rg}(B) = \delta_1 + \delta_2$  del teorema 3.5 implica, en particular, que  $\text{rg}(B_1) = \delta_1$  y  $\text{rg}(B_2 D_1) = \delta_2$ . Por tanto,  $(A_1, B_1)$  es controlable. Además,  $\delta_2 = \text{rg}(B_2 D_1) \leq \text{rg}(B_2) \leq \delta_2$ , de donde  $\text{rg}(B_2) = \delta_2$ , es decir, el par  $(A_2, B_2)$  es controlable. ■

**Observación 3.4:** El ejemplo 3.1 muestra también que el recíproco de la observación 3.3 no es cierto en general, ya que el par  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ , pero  $\text{rg}(B) = 2 \neq 2 + 1 = \delta_1 + \delta_2$ . ■

Como hemos visto, el ejemplo 3.1 pone de manifiesto que la propiedad de controlabilidad de los códigos constituyentes no son necesariamente heredadas por el código concatenado. Así pues, necesitamos condiciones adicionales a las dadas en el teorema 3.8 para obtener una representación entrada-estado-salida minimal. El resultado siguiente presenta condiciones suficientes para que el par  $(A, B)$  sea controlable en el caso particular en que el código externo tenga tasa  $1/2$  y complejidad  $\delta_1 = 1$  y la matriz  $A_2$  sea diagonal.

**Teorema 3.6:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(2, 1, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, 1, \delta_2)$ -código y que  $\mathcal{S}\mathcal{C}\mathcal{C}_{sys}(A, B, C, D)$  es el código concatenado correspondiente. Supongamos que también se verifican las condiciones siguientes:*

- (a)  $A_2$  es una matriz diagonal.
- (b) El par  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ .
- (c) Todos los elementos de la matriz  $B_2$  son no nulos.
- (d)  $\text{rg} \begin{pmatrix} -C_1 & D_1 \\ \lambda I - A_1 & B_1 \end{pmatrix} = 2$  para todo  $\lambda$  valor propio de  $A$ .

Entonces  $(A, B, C, D)$  es una representación minimal de  $\mathcal{S}\mathcal{C}\mathcal{C}_{sys}$  con complejidad  $\delta_1 + \delta_2 = 1 + \delta_2$ .

DEMOSTRACIÓN: Teniendo en cuenta que el código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(2, 1, 1)$ -código, las matrices que lo describen son escalares. Sean entonces

$$A_1 = (a_1), \quad B_1 = (b_1), \quad C_1 = (c_1) \quad \text{y} \quad D_1 = (d_1).$$

Observemos en primer lugar que al tener el código interno tasa  $1/n$ , el tamaño de la matriz  $B_2$  es  $\delta_2 \times 1$ . Por tanto, al ser  $(A_2, B_2)$  controlable, necesariamente todos los

valores propios de  $A_2$  deben ser distintos. Sean entonces

$$A_2 = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_{\delta_2}) \quad \text{y} \quad B_2 = \begin{pmatrix} b_{12} \\ b_{22} \\ \vdots \\ b_{\delta_2 2} \end{pmatrix},$$

con  $\lambda_i \neq \lambda_j$  si  $i \neq j$ . Supongamos primero que  $\lambda$  es un valor propio de  $A$  que no es de  $A_1$ , es decir,  $\lambda \neq a_1$  es un valor propio de  $A_2$ . Podemos suponer, sin pérdida de generalidad, que  $\lambda = \lambda_1$ . Entonces,

$$\begin{pmatrix} \lambda_1 I - A & B \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -b_{12}c_1 & b_{12}d_1 \\ 0 & \lambda_1 - \lambda_2 & \cdots & 0 & -b_{22}c_1 & b_{22}d_1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_1 - \lambda_{\delta_2} & -b_{\delta_2 2}c_1 & b_{\delta_2 2}d_1 \\ 0 & 0 & \cdots & 0 & \lambda_1 - a_1 & b_1 \end{pmatrix},$$

de manera que al ser todos los valores propios de  $A_2$  distintos,

$$\text{rg}(\text{diag}(\lambda_1 - \lambda_2, \lambda_1 - \lambda_3, \dots, \lambda_1 - \lambda_{\delta_2})) = \delta_2 - 1$$

y aplicando las condiciones (c) y (d),

$$\text{rg} \begin{pmatrix} -b_{12}c_1 & b_{12}d_1 \\ \lambda_1 - a_1 & b_1 \end{pmatrix} = \text{rg} \begin{pmatrix} -C_1 & D_1 \\ \lambda_1 I - A_1 & B_1 \end{pmatrix} = 2.$$

Por tanto,

$$\text{rg}(\lambda_1 I - A \quad B) = 2 + \delta_2 - 1 = 1 + \delta_2 = \delta_1 + \delta_2.$$

Sea ahora  $\lambda$  un valor propio de  $A$  que coincide con  $a_1$ . Si  $\lambda$  no es un valor propio de  $A_2$  y denotamos por

$$\begin{aligned} \tilde{A}_2 &= \text{diag}(\lambda - \lambda_1, \lambda - \lambda_2, \dots, \lambda - \lambda_{\delta_2}) \\ &= \text{diag}(a_1 - \lambda_1, a_1 - \lambda_2, \dots, a_1 - \lambda_{\delta_2}), \end{aligned}$$

entonces  $\text{rg}(\tilde{A}_2) = \delta_2$  y, por tanto,

$$\text{rg}(\lambda I - A \quad B) = \text{rg}(a_1 I - A \quad B) = \text{rg} \begin{pmatrix} \tilde{A}_2 & -B_2 C_1 & B_2 D_1 \\ O & O & B_1 \end{pmatrix} = \delta_2 + 1,$$

ya que por la condición (b), el par  $(A_1, B_1)$  es controlable y, en particular,  $b_1 \neq 0$ , por ser  $\delta_1 = 1$ .

Finalmente, si  $\lambda = a_1$  es también un valor propio de  $A_2$ , entonces podemos suponer, sin pérdida de generalidad, que  $\lambda = \lambda_1$ . Así, teniendo en cuenta que todos los valores propios de  $A_2$  son distintos,

$$\text{rg} \begin{pmatrix} \lambda I - A & B \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & 0 & \cdots & 0 & -b_{12}c_1 & b_{12}d_1 \\ 0 & \lambda_1 - \lambda_2 & \cdots & 0 & -b_{22}c_1 & b_{22}d_1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_1 - \lambda_{\delta_2} & -b_{\delta_2 2}c_1 & b_{\delta_2 2}d_1 \\ 0 & 0 & \cdots & 0 & 0 & b_1 \end{pmatrix} = \delta_2 + 1$$

ya que por las condiciones (c) y (d),

$$\text{rg} \begin{pmatrix} -b_{12}c_1 & b_{12}d_1 \\ 0 & b_1 \end{pmatrix} = \text{rg} \begin{pmatrix} -b_{12}c_1 & b_{12}d_1 \\ \lambda - a_1 & b_1 \end{pmatrix} = \text{rg} \begin{pmatrix} -C_1 & D_1 \\ \lambda I - A_1 & B_1 \end{pmatrix} = 2.$$

Por tanto, tenemos que

$$\text{rg} \begin{pmatrix} zI - A & B \end{pmatrix} = \delta_1 + \delta_2 \quad \text{para todo } z \in \overline{\mathbb{F}},$$

es decir, el par  $(A, B)$  es controlable.  $\square$

**Observación 3.5:** Con las condiciones dadas en el teorema anterior,  $\lambda = a_1$  es un valor propio de la matriz  $A$ , y por tanto, en este caso, la condición (d) se reduce a

$$\text{rg} \begin{pmatrix} -C_1 & D_1 \\ \lambda I - A_1 & B_1 \end{pmatrix} = \text{rg} \begin{pmatrix} -C_1 & D_1 \\ O & B_1 \end{pmatrix} = 2,$$

de donde se deduce en particular que el par  $(A_1, C_1)$  es observable por ser  $\delta_1 = 1$ .  $\blacksquare$

Para el caso particular en que la complejidad de los códigos externo e interno sea 1, es decir,  $\delta_1 = \delta_2 = 1$ , obtenemos el resultado siguiente.

**Teorema 3.7:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, m-k, 1)$ -código y que  $\mathcal{SCC}_{sys}(A, B, C, D)$  es el código concatenado correspondiente. Supongamos que también se verifican las condiciones siguientes:*

(a) El par  $(A_1, B_1)$  es controlable.

(b) La matriz  $\begin{pmatrix} -B_2C_1 & B_2D_1 \\ A_2 - A_1 & B_1 \end{pmatrix}$ , de tamaño  $2 \times (k+1)$ , tiene rango 2.

Entonces  $(A, B, C, D)$  es una representación minimal del código concatenado  $\text{SCC}_{\text{sys}}$  con complejidad  $\delta_1 + \delta_2 = 2$ .

DEMOSTRACIÓN: Dado que las matrices  $A_1 = \begin{pmatrix} a_1 \end{pmatrix}$  y  $A_2 = \begin{pmatrix} a_2 \end{pmatrix}$  son de tamaño  $1 \times 1$ , los valores propios de la matriz  $A = \begin{pmatrix} A_2 & B_2C_1 \\ O & A_1 \end{pmatrix}$  del código concatenado  $\text{SCC}_{\text{sys}}$  son precisamente  $a_1$  y  $a_2$ . Supongamos en primer lugar que  $a_1 = a_2 = \lambda$ . Entonces, de la condición (b), tenemos que

$$\text{rg} \begin{pmatrix} \lambda I - A & B \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & -B_2C_1 & B_2D_1 \\ 0 & 0 & B_1 \end{pmatrix} = \text{rg} \begin{pmatrix} -B_2C_1 & B_2D_1 \\ A_2 - A_1 & B_1 \end{pmatrix} = 2.$$

Por tanto,  $\text{rg} \begin{pmatrix} zI - A & B \end{pmatrix} = 2 = \delta_1 + \delta_2$  para todo  $z \in \overline{\mathbb{F}}$ , es decir, el par  $(A, B)$  es controlable.

Supongamos ahora que  $a_1 \neq a_2$ , entonces,

$$2 \geq \text{rg} \begin{pmatrix} a_1 I - A & B \end{pmatrix} = \text{rg} \begin{pmatrix} a_1 - a_2 & -B_2C_1 & B_2D_1 \\ 0 & 0 & B_1 \end{pmatrix} \geq \text{rg} \begin{pmatrix} a_1 - a_2 & B_2D_1 \\ 0 & B_1 \end{pmatrix} = 2,$$

ya que por la condición (a), el par  $(A_1, B_1)$  es controlable, y por tanto, alguna componente de  $B_1$  debe ser no nula, por ser  $\delta_1 = 1$ .

Además, de la condición (b), obtenemos que

$$\text{rg} \begin{pmatrix} a_2 I - A & B \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & -B_2C_1 & B_2D_1 \\ 0 & a_2 - a_1 & B_1 \end{pmatrix} = 2.$$

En consecuencia,  $\text{rg} \begin{pmatrix} zI - A & B \end{pmatrix} = 2 = \delta_1 + \delta_2$  para todo  $z \in \overline{\mathbb{F}}$ , es decir, el par  $(A, B)$  es controlable.  $\square$

**Observación 3.6:** Notemos que la condición (b) del teorema anterior implica, en particular, que el par  $(A_2, B_2)$  es controlable, ya que si no lo fuera, al ser  $\delta_2 = 1$ , necesariamente  $B_2$  sería la matriz nula de tamaño  $1 \times (m-k)$  y la matriz

$$\begin{pmatrix} -B_2C_1 & B_2D_1 \\ A_2 - A_1 & B_1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ A_2 - A_1 & B_1 \end{pmatrix}$$

no podría tener rango 2. ■

Como consecuencia del teorema anterior, obtenemos el resultado siguiente para el caso particular en que  $A_1 = A_2$ .

**Corolario 3.1:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, m-k, 1)$ -código y que  $\text{SCC}_{\text{sys}}(A, B, C, D)$  es el código concatenado correspondiente. Supongamos que también se verifican las condiciones siguientes:*

- (a)  $A_1 = A_2$ .
- (b) El par  $(A_1, B_1)$  es controlable.
- (c)  $B_2C_1 \neq 0$ .

Entonces  $(A, B, C, D)$  es una representación minimal del código concatenado  $\text{SCC}_{\text{sys}}$  con complejidad  $\delta_1 + \delta_2 = 2$ .

DEMOSTRACIÓN: Observemos en primer lugar que la condición (b) implica, en particular, al ser  $\delta_1 = 1$ , que  $B_1 \neq O$ . Ahora, como  $A_1 = A_2$ , de las condiciones (b) y (c) obtenemos que

$$\text{rg} \begin{pmatrix} -B_2C_1 & B_2D_1 \\ A_2 - A_1 & B_1 \end{pmatrix} = \text{rg} \begin{pmatrix} -B_2C_1 & B_2D_1 \\ O & B_1 \end{pmatrix} = 2,$$

con lo que se verifican las condiciones del teorema 3.7 y por tanto,  $(A, B)$  es controlable. □

**Observación 3.7:** Notemos que la condición (c) del corolario 3.1 implica, en particular, que el par  $(A_2, B_2)$  es controlable y que el par  $(A_1, C_1)$  es observable. En efecto, al ser la matriz  $B_2C_1$  no nula, necesariamente  $B_2 \neq O$  y  $C_1 \neq O$ , de donde al ser  $\delta_1 = \delta_2 = 1$ , obtenemos el resultado. ■

Observemos que si  $\mathcal{C}_o$  y  $\mathcal{C}_i$  tienen complejidad  $\delta_1 = \delta_2 = 1$ , entonces en el caso particular en que el código externo tenga tasa  $k/(k+1)$ ,  $B_2$  y  $C_1$  son matrices escalares. Así pues, basta con exigir la controlabilidad del par  $(A_2, B_2)$  y la observabilidad del par  $(A_1, C_1)$  para que la condición (c) del corolario 3.1 se verifique. Tenemos entonces el resultado siguiente.

**Corolario 3.2:** Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(k+1, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, 1, 1)$ -código y que  $\mathcal{S}\mathcal{C}\mathcal{C}_{sys}(A, B, C, D)$  es el código concatenado correspondiente. Supongamos que también se verifican las condiciones siguientes:

- (a)  $A_1 = A_2$ .
- (b) El par  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ .
- (c) El par  $(A_1, C_1)$  es observable.

Entonces  $(A, B, C, D)$  es una representación minimal del código concatenado  $\mathcal{S}\mathcal{C}\mathcal{C}_{sys}(A, B, C, D)$  con complejidad  $\delta_1 + \delta_2 = 2$ .

En el caso particular en que el código externo tenga tasa  $1/2$  y todos valores propios de  $A_2$  sean valores propios de  $A_1$  (es decir,  $\sigma(A_2) \subseteq \sigma(A_1)$ , siendo  $\sigma(A_i)$  el espectro de  $A_i$ ), basta con exigir que el par  $(A_l, B_l)$  sea controlable, para  $l = 1, 2$ , que todos los elementos de la matriz  $B_2$  sean no nulos y que el par  $(A_1, C_1)$  sea observable, para tener la controlabilidad del par  $(A, B)$  de la concatenación, como vemos en el resultado siguiente.

**Teorema 3.8:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(2, 1, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, 1, \delta_2)$ -código y  $\mathcal{S}\mathcal{C}\mathcal{C}_{sys}(A, B, C, D)$  el código concatenado correspondiente. Supongamos que se verifican las condiciones siguientes:

- (a)  $\sigma(A_2) \subseteq \sigma(A_1)$ .
- (b) El par  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ .
- (c) Todos los elementos de la matriz  $B_2$  son no nulos.
- (d) El par  $(A_1, C_1)$  es observable.

Entonces la representación entrada-estado-salida  $(A, B, C, D)$  es una representación minimal del código concatenado  $\mathcal{S}\mathcal{C}\mathcal{C}_{sys}$  con complejidad  $\delta_1 + \delta_2$ .

DEMOSTRACIÓN: Por el test PBH (véase la sección 1.4), el par  $(A, B)$  es controlable si la matriz

$$\begin{pmatrix} zI - A & B \end{pmatrix} = \begin{pmatrix} zI_{\delta_2} - A_2 & -B_2C_1 & B_2D_1 \\ O & zI_{\delta_1} - A_1 & B_1 \end{pmatrix}$$

tiene rango completo por filas, esto es,  $\text{rg} \begin{pmatrix} zI - A & B \end{pmatrix} = \delta_1 + \delta_2$  para todo  $z \in \overline{\mathbb{F}}$ .

Supongamos en primer lugar que  $\delta_1 = 1$ . Entonces, por la condición (d), el par  $(A_1, C_1)$  es observable y, por tanto, la matriz  $C_1$ , de tamaño  $1 \times 1$ , debe ser no nula.

Del mismo modo, por ser  $(A_1, B_1)$  controlable, la matriz  $B_1$  de tamaño  $1 \times 1$ , debe ser no nula. Ahora, teniendo en cuenta que el par  $(A_2, B_2)$  es controlable por la condición (b), así como la condición (a), tenemos que

$$\text{rg} \begin{pmatrix} zI - A & B \end{pmatrix} = 1 + \delta_2 = \delta_1 + \delta_2$$

para todo  $z \in \overline{\mathbb{F}}$ .

Sea ahora  $\delta_1 > 1$  y supongamos que existe  $z \in \overline{\mathbb{F}}$  tal que

$$\text{rg} \begin{pmatrix} zI - A & B \end{pmatrix} < \delta_1 + \delta_2, \quad (3.13)$$

de manera que de la condición (a), necesariamente  $z \in \sigma(A) = \sigma(A_1)$ . Aplicando la condición (b), el par  $(A_1, B_1)$  es controlable, por tanto,

$$\text{rg} \begin{pmatrix} O & zI_{\delta_1} - A_1 & B_1 \end{pmatrix} = \text{rg} \begin{pmatrix} zI_{\delta_1} - A_1 & B_1 \end{pmatrix} = \delta_1 \quad (3.14)$$

para todo  $z \in \overline{\mathbb{F}}$ . Por otra parte, teniendo en cuenta que las matrices  $B_2$  y  $C_1$  son de tamaños  $\delta_2 \times 1$  y  $1 \times \delta_1$ , así como las condiciones (c) y (d), obtenemos que

$$\begin{aligned} \delta_2 &\geq \text{rg} \begin{pmatrix} zI_{\delta_2} - A_2 & -B_2C_1 & B_2D_1 \end{pmatrix} \\ &\geq \text{rg} \begin{pmatrix} zI_{\delta_2} - A_2 & -B_2C_1 \end{pmatrix} \\ &= \text{rg} \begin{pmatrix} zI_{\delta_2} - A_2 & B_2 \end{pmatrix} = \delta_2, \end{aligned} \quad (3.15)$$

donde la última igualdad se deduce de la condición (b). Por tanto,

$$\text{rg} \begin{pmatrix} zI_{\delta_2} - A_2 & -B_2C_1 & B_2D_1 \end{pmatrix} = \delta_2$$

para todo  $z \in \overline{\mathbb{F}}$ . Ahora bien, teniendo en cuenta las relaciones (3.13), (3.14) y (3.15), tenemos que una fila de la matriz  $\begin{pmatrix} zI_{\delta_2} - A_2 & -B_2C_1 & B_2D_1 \end{pmatrix}$  es combinación lineal de las filas de  $\begin{pmatrix} O & zI_{\delta_1} - A_1 & B_1 \end{pmatrix}$ , o bien, una fila de la matriz  $\begin{pmatrix} O & zI_{\delta_1} - A_1 & B_1 \end{pmatrix}$  es combinación lineal de las filas de la matriz  $\begin{pmatrix} zI_{\delta_2} - A_2 & -B_2C_1 & B_2D_1 \end{pmatrix}$ . Pero entonces, de la condición (c), tendríamos que

$$\text{rg} \begin{pmatrix} zI_{\delta_1} - A_1 \\ C_1 \end{pmatrix} < \delta_1$$

y por tanto, el par  $(A_1, C_1)$  no es observable, en contra de la condición (d).  $\square$

Notemos que si en el teorema 3.8 no exigimos la condición de controlabilidad de alguno de los pares  $(A_l, B_l)$ , para  $l = 1, 2$ , entonces la representación del código concatenado  $\mathcal{S}\mathcal{C}\mathcal{C}_{\text{sys}}$  puede no ser minimal, aunque  $\sigma(A_2) \subseteq \sigma(A_1)$  y  $(A_1, C_1)$  sea observable, como mostramos en el ejemplo siguiente.

**Ejemplo 3.2:** Sea  $\alpha$  un elemento primitivo del cuerpo de Galois  $\mathbb{F} = GF(8)$  y consideremos el  $(2, 1, 2)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , donde

$$A_1 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^5 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad C_1 = (1 \quad \alpha) \quad \text{y} \quad D_1 = (\alpha^5).$$

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(2, 1, 1)$ -código descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^4 & 1 \\ \alpha^2 & \alpha^3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}$$

siendo  $C_2$  y  $D_2$  matrices arbitrarias, de tamaños  $1 \times 2$  y  $1 \times 1$ , respectivamente.

Para todo  $z \in \overline{\mathbb{F}}$  tenemos entonces que

$$\text{rg} \begin{pmatrix} zI_{\delta_1} - A_1 & B_1 \end{pmatrix} = \text{rg} \begin{pmatrix} z + \alpha & 0 & 1 \\ 0 & z + \alpha^5 & 1 \end{pmatrix} = 2,$$

$$\text{rg} \begin{pmatrix} zI_{\delta_1} - A_1 \\ C_1 \end{pmatrix} = \text{rg} \begin{pmatrix} z + \alpha & 0 \\ 0 & z + \alpha^5 \\ 1 & \alpha \end{pmatrix} = 2$$

y, por tanto, el par  $(A_1, B_1)$  es controlable y el par  $(A_1, C_1)$  es observable. Ahora bien,

$$\text{rg} \begin{pmatrix} \alpha I_{\delta_2} - A_2 & B_2 \end{pmatrix} = \text{rg} \begin{pmatrix} \alpha + \alpha^4 & 1 & \alpha \\ \alpha^2 & \alpha + \alpha^3 & \alpha \end{pmatrix} = \text{rg} \begin{pmatrix} \alpha^2 & 1 & \alpha \\ \alpha^2 & 1 & \alpha \end{pmatrix} = 1 \neq 2$$

y, en consecuencia,  $(A_2, B_2)$  no es controlable. Además, notemos que

$$\sigma(A_2) = \{\alpha, \alpha^5\} = \sigma(A_1),$$

luego se verifica la condición (a) del teorema 3.8.

Por otro lado, aplicando los teoremas 3.1 y 3.3, las matrices  $A$  y  $B$  para la representación entrada-estado-salida del código concatenado  $\mathcal{SCC}_{\text{sys}}$  son

$$A = \begin{pmatrix} \alpha^4 & 1 & \alpha & \alpha^2 \\ \alpha^2 & \alpha^3 & \alpha & \alpha^2 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha^5 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} \alpha^6 \\ \alpha^6 \\ 1 \\ 1 \end{pmatrix}.$$

Entonces, el par  $(A, B)$  no es controlable, ya que

$$\begin{aligned} \text{rg} \begin{pmatrix} \alpha I - A & B \end{pmatrix} &= \text{rg} \begin{pmatrix} \alpha + \alpha^4 & 1 & \alpha & \alpha^2 & \alpha^6 \\ \alpha^2 & \alpha + \alpha^3 & \alpha & \alpha^2 & \alpha^2 \\ 0 & 0 & \alpha + \alpha & 0 & 1 \\ 0 & 0 & 0 & \alpha + \alpha^5 & 1 \end{pmatrix} \\ &= \text{rg} \begin{pmatrix} \alpha^2 & 1 & \alpha & \alpha^2 & \alpha^6 \\ \alpha^2 & 1 & \alpha & \alpha^2 & \alpha^2 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \alpha^6 & 1 \end{pmatrix} = 3 \neq 4. \quad \blacksquare \end{aligned}$$

Del mismo modo, si en el teorema 3.8 no exigimos la condición de observabilidad del par  $(A_1, C_1)$ , entonces el par  $(A, B)$  del código concatenado puede no ser controlable aunque  $\sigma(A_2) \subseteq \sigma(A_1)$  y  $(A_l, B_l)$  sea controlable para  $l = 1, 2$ , como mostramos en el ejemplo siguiente.

**Ejemplo 3.3:** Consideremos el  $(2, 1, 2)$ -código  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , siendo las matrices  $A_1, B_1$  y  $D_1$  las mismas que describen el código externo del ejemplo 3.2 y  $C_1 = \begin{pmatrix} 0 & 0 \end{pmatrix}$ . Entonces, el par  $(A_1, B_1)$  es controlable pero el par  $(A_1, C_1)$  no es observable, ya que

$$\text{rg} \begin{pmatrix} \alpha I - A_1 \\ C_1 \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & 0 \\ 0 & \alpha^6 \\ 0 & 0 \end{pmatrix} = 1 \neq 2.$$

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(2, 1, 2)$ -código descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^4 & 1 \\ \alpha^2 & \alpha^3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 \\ \alpha \end{pmatrix},$$

siendo  $C_2$  y  $D_2$  matrices arbitrarias de tamaños  $1 \times 2$  y  $1 \times 1$ , respectivamente. Teniendo en cuenta que los valores propios de la matriz  $A_2$  son  $\alpha$  y  $\alpha^5$ , obtenemos que

$$\begin{aligned} \operatorname{rg} \begin{pmatrix} \alpha I_{\delta_2} - A_2 & B_2 \end{pmatrix} &= \operatorname{rg} \begin{pmatrix} \alpha^2 & 1 & 1 \\ \alpha^2 & 1 & \alpha \end{pmatrix} = 2 = \delta_2, \\ \operatorname{rg} \begin{pmatrix} \alpha^5 I_{\delta_2} - A_2 & B_2 \end{pmatrix} &= \operatorname{rg} \begin{pmatrix} 1 & 1 & 1 \\ \alpha^2 & \alpha^2 & \alpha \end{pmatrix} = 2 = \delta_2 \end{aligned}$$

y, por tanto, el par  $(A_2, B_2)$  es controlable. Notemos que, además,  $\sigma(A_2) = \{\alpha, \alpha^5\} \subseteq \sigma(A_1)$ .

Ahora bien, por los teoremas 3.1 y 3.3, las matrices  $A$  y  $B$  de la representación entrada-estado-salida del código concatenado  $\mathcal{S}\mathcal{C}\mathcal{C}_{\text{sys}}$  son

$$A = \begin{pmatrix} \alpha^4 & 1 & 0 & 0 \\ \alpha^2 & \alpha^3 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha^5 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} \alpha^5 \\ \alpha^6 \\ 1 \\ 1 \end{pmatrix}$$

y como

$$\operatorname{rg} \begin{pmatrix} \alpha I - A & B \end{pmatrix} = \operatorname{rg} \begin{pmatrix} \alpha^2 & 1 & 0 & 0 & \alpha^5 \\ \alpha^2 & 1 & 0 & 0 & \alpha^6 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \alpha^6 & 1 \end{pmatrix} = 3 < 4,$$

el par  $(A, B)$  no es controlable. ■

Cabría preguntarse si el teorema 3.8 sigue siendo válido para el caso  $\sigma(A_2) \not\subseteq \sigma(A_1)$ . La respuesta es negativa, como mostramos en el ejemplo siguiente.

**Ejemplo 3.4:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$ . Consideremos el  $(2, 1, 1)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  descrito por las matrices

$$A_1 = \begin{pmatrix} \alpha^2 \end{pmatrix}, \quad B_1 = \begin{pmatrix} \alpha \end{pmatrix}, \quad C_1 = \begin{pmatrix} 1 \end{pmatrix} \quad \text{y} \quad D_1 = \begin{pmatrix} \alpha \end{pmatrix}$$

y un  $(2, 1, 2)$ -código interno  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$ , donde

$$A_2 = \begin{pmatrix} \alpha^2 & 0 \\ 1 & \alpha^6 \end{pmatrix}, \quad B_2 = \begin{pmatrix} \alpha \\ 1 \end{pmatrix},$$

siendo  $C_2$  y  $D_2$  matrices arbitrarias de tamaños  $1 \times 2$  y  $1 \times 1$ , respectivamente. Claramente, el par  $(A_l, B_l)$  es controlable, para  $l = 1, 2$  y el par  $(A_1, C_1)$  es observable, luego se cumplen las condiciones (b) y (d) del teorema 3.8.

Por otro lado, teniendo en cuenta los teoremas 3.1 y 3.3, las matrices  $A$  y  $B$  de la representación entrada-estado-salida del código concatenado  $\mathcal{SC}_{\text{sys}}$  son

$$A = \begin{pmatrix} \alpha^2 & 0 & \alpha \\ 1 & \alpha^6 & 1 \\ 0 & 0 & \alpha^2 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} \alpha^2 \\ \alpha \\ \alpha \end{pmatrix}.$$

Ahora bien,

$$\text{rg} \begin{pmatrix} \alpha^6 I - A & B \end{pmatrix} = \text{rg} \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 1 & 0 & 1 & \alpha \\ 0 & 0 & 1 & \alpha \end{pmatrix} = 2 \neq 3$$

con lo que  $(A, B)$  no es controlable. ■

### 3.2.3 Observabilidad

En esta sección, estudiamos las condiciones que deben cumplir las matrices que describen los códigos externo e interno para que el par  $(A, C)$  de los códigos concatenados  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$  sea observable. En la sección 1.5 vimos que el concepto de observabilidad del par  $(A, C)$  está relacionado con el hecho de que la matriz generadora inducida por la realización sea no catastrófica. Si bien las matrices  $A$  y  $B$  de los códigos  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$  tienen la misma expresión, no tenemos lo mismo para la matriz  $C$  (véanse las expresiones (3.6) y (3.12)). Por tanto, tendremos resultados diferentes para la observabilidad de cada modelo.

Empezamos la sección con resultados relacionados con la observabilidad del par  $(A, C)$  correspondiente al modelo  $\mathcal{SC}^{(1)}$ . El ejemplo siguiente pone de manifiesto que no es suficiente con que el par  $(A_l, C_l)$ , para  $l = 1, 2$ , de los códigos constituyentes sea observable, para que el par  $(A, C)$  del código concatenado  $\mathcal{SC}^{(1)}$  sea observable.

**Ejemplo 3.5:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$ . Consideremos el  $(6, 4, 2)$ -código  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , con

$$A_1 = \begin{pmatrix} \alpha^3 & \alpha \\ \alpha & \alpha^4 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 & \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \end{pmatrix},$$

$$C_1 = \begin{pmatrix} 1 & \alpha \\ \alpha & 1 \end{pmatrix} \quad \text{y} \quad D_1 = \begin{pmatrix} \alpha^3 & \alpha^4 & \alpha^3 & \alpha^4 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  el  $(5, 2, 1)$ -código descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha \end{pmatrix}, \quad B_2 = \begin{pmatrix} \alpha^3 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \alpha & 0 \end{pmatrix}.$$

Observemos que los códigos  $\mathcal{C}_o$  y  $\mathcal{C}_i$  corresponden a los códigos externo e interno, respectivamente, del ejemplo 3.1. Tenemos entonces que para todo  $z \in \overline{\mathbb{F}}$ ,

$$\text{rg} \begin{pmatrix} zI - A_1 \\ C_1 \end{pmatrix} = \text{rg} \begin{pmatrix} z - \alpha^3 & -\alpha \\ -\alpha & z - \alpha^4 \\ 1 & \alpha \\ \alpha & 1 \end{pmatrix} = 2,$$

y

$$\text{rg} \begin{pmatrix} zI - A_2 \\ C_2 \end{pmatrix} = \text{rg} \begin{pmatrix} z - \alpha \\ 0 \\ 1 \\ 0 \end{pmatrix} = 1.$$

Por tanto, el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .

Por otro lado, aplicando el teorema 3.1, las matrices  $A$  y  $C$  de la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(1)}$  son

$$A = \begin{pmatrix} \alpha & \alpha^3 & \alpha^4 \\ 0 & \alpha^3 & \alpha \\ 0 & \alpha & \alpha^4 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} 0 & 1 & \alpha \\ 1 & \alpha & 1 \\ 0 & \alpha & \alpha^2 \end{pmatrix}.$$

Tenemos entonces que el par  $(A, C)$  no es observable, ya que

$$\text{rg} \begin{pmatrix} \alpha I - A \\ C \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & \alpha^3 & \alpha^4 \\ 0 & 1 & \alpha \\ 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha \\ 1 & \alpha & 1 \\ 0 & \alpha & \alpha^2 \end{pmatrix} = 2 \neq 3. \quad \blacksquare$$

Con respecto a la observabilidad del par  $(A, C)$  del código  $\mathcal{SC}^{(1)}$ , tenemos un resultado análogo al teorema 3.5.

**Teorema 3.9:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m - k, \delta_2)$ -código y  $\mathcal{SC}^{(1)}(A, B, C, D)$  el código concatenado de tasa  $k/(n - m + 2k)$  descrito por las matrices dadas por la expresión (3.6). Si  $\text{rg}(C) = \delta_1 + \delta_2$ , entonces el par  $(A, C)$  es observable.

DEMOSTRACIÓN: Como la matriz  $C$  tiene rango completo por columnas, entonces

$$\text{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = \delta_1 + \delta_2 \quad \text{para todo } z \in \overline{\mathbb{F}}$$

y aplicando el test PBH (véase la sección 1.4), obtenemos que el par  $(A, C)$  es observable.  $\square$

**Observación 3.8:** Notemos que la condición sobre el rango de  $C = \begin{pmatrix} C_2 & D_2C_1 \end{pmatrix}$  del teorema 3.9 implica, en particular, que  $\text{rg}(C_2) = \delta_2$  y que  $\text{rg}(D_2C_1) = \delta_1$ . Por tanto,

$$\delta_1 = \text{rg}(D_2C_1) \leq \text{rg}(C_1) \leq \delta_1,$$

y así,  $\text{rg}(C_1) = \delta_1$ . Ahora, mediante un razonamiento similar al utilizado en la demostración del teorema 3.9, obtenemos que el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .  $\blacksquare$

**Observación 3.9:** El ejemplo 3.5 muestra también que el recíproco de la observación 3.8 no es cierto en general, ya que el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ , y sin embargo,  $\text{rg}(C) = 2 \neq 2 + 1 = \delta_1 + \delta_2$ .  $\blacksquare$

Ahora, como consecuencia del teorema 1.11, tenemos que las condiciones dadas en los teoremas 3.5 y 3.9, hacen que el código concatenado  $\mathcal{SC}^{(1)}$  sea un código observable.

**Corolario 3.3:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m - k, \delta_2)$ -código y  $\mathcal{SC}^{(1)}(A, B, C, D)$  el código concatenado de tasa  $k/(n - m + 2k)$  descrito por las matrices dadas por la expresión (3.6). Si  $\text{rg}(B) = \delta_1 + \delta_2 = \text{rg}(C)$ , entonces  $(A, B, C, D)$  es una representación minimal para el código observable  $\mathcal{SC}^{(1)}$  con complejidad  $\delta_1 + \delta_2$ .

**Observación 3.10:** De las condiciones del corolario anterior, tenemos que

$$2 \leq \delta_1 + \delta_2 \leq \min\{k, n - m + k\}.$$

Así pues, para aplicar el corolario 3.3, debemos considerar códigos para los que  $k \geq 2$  y  $n - m + k \geq 2$ . ■

Si el código interno tiene complejidad  $\delta_2 = 1$  tenemos, del mismo modo que para la controlabilidad del par  $(A, B)$  en el caso  $\delta_1 = 1$ , condiciones bastantes restrictivas para la observabilidad de  $(A, C)$  del código  $\mathcal{SC}^{(1)}(A, B, C, D)$ . En concreto, tenemos un resultado análogo al teorema 3.6.

**Teorema 3.10:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(2, 1, \delta_1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, 1, 1)$ -código y que  $\mathcal{SC}^{(1)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n - m + 2k)$  descrito por las matrices dadas por la expresión (3.6). Supongamos que también se verifican las condiciones siguientes:*

- (a)  $A_1$  es una matriz diagonal.
- (b) El par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .
- (c) Todos los elementos de la matriz  $C_1$  son no nulos.
- (d)  $\text{rg} \begin{pmatrix} \lambda - A_2 & -B_2 \\ C_2 & D_2 \end{pmatrix} = 2$  para todo  $\lambda$  valor propio de  $A$ .

Entonces, el par  $(A, C)$  es observable.

DEMOSTRACIÓN: Teniendo en cuenta que el código interno  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, 1, 1)$ -código, las matrices  $A_2 = \begin{pmatrix} a_2 \end{pmatrix}$  y  $B_2 = \begin{pmatrix} b_2 \end{pmatrix}$  son escalares. Observemos que el código externo tiene tasa  $1/2$  y, por tanto, la matriz  $C_1$  tiene tamaño  $1 \times \delta_1$ , con lo que necesariamente todos los valores propios de  $A_1$  son distintos, ya que el par  $(A_1, C_1)$  es observable por la condición (b). Sean entonces

$$A_1 = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_{\delta_1}), \quad \text{con } \lambda_i \neq \lambda_j \quad \text{si } i \neq j,$$

$$C_1 = (f_1, f_2, \dots, f_{\delta_1}), \quad C_2 = \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_{n-1} \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_{n-1} \end{pmatrix}.$$

Entonces, las matrices  $A$  y  $C$  para el código  $\mathcal{SC}^{(1)}$ , son

$$A = \begin{pmatrix} a_2 & b_2 f_1 & b_2 f_2 & \cdots & b_2 f_{\delta_1} \\ 0 & \lambda_1 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{\delta_1} \end{pmatrix},$$

$$C = \begin{pmatrix} g_1 & d_1 f_1 & d_1 f_2 & \cdots & d_1 f_{\delta_1} \\ g_2 & d_2 f_1 & d_2 f_2 & \cdots & d_2 f_{\delta_1} \\ \vdots & \vdots & \vdots & & \vdots \\ g_{n-1} & d_{n-1} f_1 & d_{n-1} f_2 & \cdots & d_{n-1} f_{\delta_1} \end{pmatrix}.$$

Supongamos primero que  $\lambda$  es un valor propio de  $A$  pero que no es de  $A_2$ , es decir  $\lambda \neq a_2$  es un valor propio de  $A_1$ . Podemos suponer, sin pérdida de generalidad, que  $\lambda = \lambda_1$ , entonces,

$$\begin{pmatrix} \lambda_1 I - A \\ C \end{pmatrix} = \begin{pmatrix} \lambda_1 - a_2 & -b_2 f_1 & -b_2 f_2 & \cdots & -b_2 f_{\delta_1} \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_1 - \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_1 - \lambda_{\delta_1} \\ g_1 & d_1 f_1 & d_1 f_2 & \cdots & d_1 f_{\delta_1} \\ g_2 & d_2 f_1 & d_2 f_2 & \cdots & d_2 f_{\delta_1} \\ \vdots & \vdots & \vdots & & \vdots \\ g_{n-1} & d_{n-1} f_1 & d_{n-1} f_2 & \cdots & d_{n-1} f_{\delta_1} \end{pmatrix},$$

de manera que al ser todos los valores propios de  $A_1$  distintos,

$$\text{rg}(\text{diag}(\lambda_1 - \lambda_2, \lambda_1 - \lambda_3, \dots, \lambda_1 - \lambda_{\delta_1})) = \delta_1 - 1$$

y aplicando las condiciones (c) y (d),

$$\operatorname{rg} \begin{pmatrix} \lambda_1 - a_2 & -b_2 f_1 \\ g_1 & d_1 f_1 \\ \vdots & \vdots \\ g_{n-1} & d_{n-1} f_1 \end{pmatrix} = \operatorname{rg} \begin{pmatrix} \lambda_1 I - A_2 & -B_2 \\ C_2 & D_2 \end{pmatrix} = 2.$$

Por tanto,

$$\operatorname{rg} \begin{pmatrix} \lambda_1 - A & B \end{pmatrix} = \delta_1 - 1 + 2 = \delta_1 + 1 = \delta_1 + \delta_2.$$

Sea ahora  $\lambda$  un valor propio de  $A$  que coincide con  $a_2$ . Si  $\lambda$  no es un valor propio de  $A_1$  y denotamos por

$$\tilde{A}_1 = \operatorname{diag}(\lambda - \lambda_1, \lambda - \lambda_2, \dots, \lambda - \lambda_{\delta_1}) = \operatorname{diag}(a_2 - \lambda_1, a_2 - \lambda_2, \dots, a_2 - \lambda_{\delta_1}),$$

entonces  $\operatorname{rg}(\tilde{A}_1) = \delta_1$  y, por tanto,

$$\operatorname{rg} \begin{pmatrix} \lambda I - A \\ C \end{pmatrix} = \operatorname{rg} \begin{pmatrix} O & -B_2 C_1 \\ O & \tilde{A}_1 \\ C_2 & D_2 C_1 \end{pmatrix} = \delta_1 + 1,$$

ya que por las condiciones (c) y (d), el par  $(A_2, C_2)$  es observable y, en particular, al ser  $\delta_2 = 1$ , alguna componente de  $C_2$  debe ser no nula.

Finalmente, si  $\lambda = a_2$  es también valor propio de  $A_1$ , entonces podemos suponer, sin pérdida de generalidad, que  $\lambda = \lambda_1$ . Así, teniendo en cuenta que todos los valores propios de  $A_1$  son distintos, tenemos que

$$\operatorname{rg} \begin{pmatrix} \lambda I - A \\ C \end{pmatrix} = \operatorname{rg} \begin{pmatrix} 0 & -b_2 f_1 & -b_2 f_2 & \cdots & -b_2 f_{\delta_1} \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \lambda - \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda - \lambda_{\delta_1} \\ g_1 & d_1 f_1 & d_1 f_2 & \cdots & d_1 f_{\delta_1} \\ g_2 & d_2 f_1 & d_2 f_2 & \cdots & d_2 f_{\delta_1} \\ \vdots & \vdots & \vdots & & \vdots \\ g_{n-1} & d_{n-1} f_1 & d_{n-1} f_2 & \cdots & d_{n-1} f_{\delta_1} \end{pmatrix} = \delta_1 + 1$$

ya que por la condición (d),

$$\operatorname{rg} \begin{pmatrix} 0 & -b_2 f_1 \\ g_1 & d_1 f_1 \\ \vdots & \vdots \\ g_{n-1} & d_{n-1} f_1 \end{pmatrix} = \operatorname{rg} \begin{pmatrix} O & -B_2 \\ C_2 & D_2 \end{pmatrix} = \operatorname{rg} \begin{pmatrix} \lambda I - A_2 & -B_2 \\ C_2 & D_2 \end{pmatrix} = 2.$$

Por tanto,

$$\operatorname{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = \delta_1 + \delta_2 \quad \text{para todo } z \in \overline{\mathbb{F}}$$

es decir, el par  $(A, C)$  es observable.  $\square$

**Observación 3.11:** Notemos que con las condiciones dadas en el teorema anterior,  $\lambda = a_2$  es un valor propio de la matriz  $A$ , y por tanto, en este caso, la condición (d) se reduce a

$$\operatorname{rg} \begin{pmatrix} \lambda I - A_2 & -B_2 \\ C_2 & D_2 \end{pmatrix} = \operatorname{rg} \begin{pmatrix} O & -B_2 \\ C_2 & D_2 \end{pmatrix} = 2,$$

de donde se deduce, en particular, que alguna componente de  $B_2$  debe ser no nula y, por tanto, que el par  $(A_2, B_2)$  es controlable, por ser  $\delta_2 = 1$ .  $\blacksquare$

Tenemos el resultado siguiente en el caso en que los códigos externo e interno tengan tasas cualesquiera y complejidad  $\delta_1 = \delta_2 = 1$ .

**Teorema 3.11:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, m - k, 1)$ -código y que  $\mathcal{SC}^{(1)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n - m + 2k)$  descrito por las matrices dadas en (3.6). Supongamos que también se verifican las condiciones siguientes:*

(a) *El par  $(A_2, C_2)$  es observable.*

(b) *La matriz  $\begin{pmatrix} A_1 - A_2 & -B_2 C_1 \\ C_2 & D_2 C_1 \end{pmatrix}$ , de tamaño  $(n - m + k + 1) \times 2$ , tiene rango 2.*

*Entonces el par  $(A, C)$  es observable.*

DEMOSTRACIÓN: Dado que las matrices  $A_1 = \begin{pmatrix} a_1 \end{pmatrix}$  y  $A_2 = \begin{pmatrix} a_2 \end{pmatrix}$  son de tamaño  $1 \times 1$ , los valores propios de la matriz  $A = \begin{pmatrix} A_2 & B_2 C_1 \\ O & A_1 \end{pmatrix}$  del código concatenado  $\mathcal{SC}^{(1)}(A, B, C, D)$ , son precisamente  $a_1$  y  $a_2$ .

Supongamos en primer lugar que  $a_1 = a_2 = \lambda$ . Entonces de la condición (b), tenemos

$$\operatorname{rg} \begin{pmatrix} \lambda I - A \\ C \end{pmatrix} = \operatorname{rg} \begin{pmatrix} O & -B_2 C_1 \\ O & O \\ C_2 & D_2 C_1 \end{pmatrix} = \operatorname{rg} \begin{pmatrix} A_1 - A_2 & -B_2 C_1 \\ C_2 & D_2 C_1 \end{pmatrix} = 2.$$

Así pues,  $\operatorname{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = 2 = \delta_1 + \delta_2$  para todo  $z \in \overline{\mathbb{F}}$ , es decir, el par  $(A, C)$  es observable.

Si  $a_1 \neq a_2$ , entonces, la condición (b) permite asegurar que

$$\operatorname{rg} \begin{pmatrix} a_1 I - A \\ C \end{pmatrix} = \operatorname{rg} \begin{pmatrix} A_1 - A_2 & -B_2 C_1 \\ O & O \\ C_2 & D_2 C_1 \end{pmatrix} = 2.$$

Además, de la condición (a), obtenemos

$$\operatorname{rg} \begin{pmatrix} a_2 I - A \\ C \end{pmatrix} = \operatorname{rg} \begin{pmatrix} O & -B_2 C_1 \\ O & A_2 - A_1 \\ C_2 & D_2 C_1 \end{pmatrix} = 2,$$

ya que al ser  $(A_2, C_2)$  observable y  $\delta_2 = 1$ , en particular alguna componente de  $C_2$  debe ser no nula.

Así pues,  $\operatorname{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = 2 = \delta_1 + \delta_2$  para todo  $z \in \overline{\mathbb{F}}$ , es decir, el par  $(A, C)$  es observable.  $\square$

**Observación 3.12:** Notemos que por un razonamiento similar al hecho en la observación 3.6, la condición (b) del teorema anterior, implica, en particular, que el par  $(A_1, C_1)$  es observable, por ser  $\delta_1 = 1$ .  $\blacksquare$

Como consecuencia del teorema 3.11, tenemos el resultado siguiente, para el caso particular en que  $A_1 = A_2$ .

**Corolario 3.4:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, m - k, 1)$ -código y que  $\mathcal{SC}^{(1)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n - m + 2k)$  descrito por las matrices dadas en (3.6). Supongamos que también se verifican las condiciones siguientes:*

- (a)  $A_1 = A_2$ .
- (b) El par  $(A_2, C_2)$  es observable.
- (c)  $B_2C_1 \neq O$ .

Entonces el par  $(A, C)$  es observable.

DEMOSTRACIÓN: Observemos en primer lugar que la condición (b) implica, en particular, al ser  $\delta_2 = 1$ , que alguna componente de la matriz  $C_2$  es no nula. Ahora, dado que  $A_1 = A_2$ , entonces las condiciones (b) y (c), permiten asegurar que

$$\text{rg} \begin{pmatrix} A_1 - A_2 & -B_2C_1 \\ C_2 & D_2C_1 \end{pmatrix} = \text{rg} \begin{pmatrix} O & -B_2C_1 \\ C_2 & D_2C_1 \end{pmatrix} = 2,$$

y por tanto, se verifican las condiciones del teorema 3.11, luego el par  $(A, C)$  es observable.  $\square$

Observemos que si en el corolario 3.4 el código externo tiene tasa  $k/(k+1)$ , entonces  $B_2$  y  $C_1$  son matrices escalares. Así pues, basta con exigir la controlabilidad del par  $(A_2, B_2)$  y la observabilidad del par  $(A_1, C_1)$  para que la condición (c) del corolario 3.4 se verifique. Tenemos entonces el resultado siguiente, análogo al corolario 3.2.

**Corolario 3.5:** Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(k+1, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, 1, 1)$ -código y que  $\mathcal{SC}^{(1)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n+k-1)$  descrito por las matrices dadas en (3.6). Supongamos que también se verifican las condiciones siguientes:

- (a)  $A_1 = A_2$ .
- (b) El par  $(A_2, B_2)$  es controlable.
- (c) El par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .

Entonces el par  $(A, C)$  es observable.

Como consecuencia entonces de los corolarios 3.2 y 3.5 obtenemos el resultado siguiente, que proporciona la observabilidad del código  $\mathcal{SC}^{(1)}$  para el caso particular en que las matrices  $A_1$  y  $A_2$  sean iguales y los códigos externo e interno tengan complejidad  $\delta_1 = \delta_2 = 1$  y el código externo tenga tasa  $k/(k+1)$ .

**Corolario 3.6:** Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(k+1, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, 1, 1)$ -código y que  $\mathcal{SC}^{(1)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n+k-1)$  descrito por las matrices dadas en (3.6). Supongamos que también se verifican las condiciones siguientes:

- (a)  $A_1 = A_2$ .
- (b) El par  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ .
- (c) El par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .

Entonces,  $(A, B, C, D)$  es una representación minimal para el código observable  $\mathcal{SC}^{(1)}$ .

Para el caso particular en que el código externo tenga tasa  $1/2$  y todos los valores propios de la matriz  $A_1$  sean valores propios de la matriz  $A_2$  (es decir,  $\sigma(A_1) \subseteq \sigma(A_2)$ ), basta con exigir que todos los elementos de la matriz  $C_1$  sean no nulos así como la controlabilidad de  $(A_2, B_2)$  y la observabilidad de  $(A_l, C_l)$ , para  $l = 1, 2$ , para obtener la observabilidad del par  $(A, C)$  del código  $\mathcal{SC}^{(2)}$ , como muestra el resultado siguiente.

**Teorema 3.12:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(2, 1, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, 1, \delta_2)$ -código y  $\mathcal{SC}^{(1)}(A, B, C, D)$  el código concatenado de tasa  $k/n$  descrito por la expresión (3.6). Supongamos que se verifican las condiciones siguientes:

- (a)  $\sigma(A_1) \subseteq \sigma(A_2)$
- (b) El par  $(A_2, B_2)$  es controlable.
- (c) El par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .
- (d) Todos los elementos de la matriz  $C_1$  son no nulos.

Entonces el par  $(A, C)$  es observable.

DEMOSTRACIÓN: Por el test PBH (véase la sección 1.4), el par  $(A, C)$  es observable si la matriz

$$\begin{pmatrix} zI - A \\ C \end{pmatrix} = \begin{pmatrix} zI_{\delta_2} - A_2 & -B_2C_1 \\ O & zI_{\delta_1} - A_1 \\ C_2 & D_2C_1 \end{pmatrix}$$

tiene rango completo por columnas, esto es,  $\text{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = \delta_1 + \delta_2$  para todo  $z \in \overline{\mathbb{F}}$ .

Supongamos en primer lugar que  $\delta_2 = 1$ . Entonces, por la condición (c), el par  $(A_2, C_2)$  es observable y, por tanto, la matriz  $C_2$ , debe tener algún elemento no nulo.

Del mismo modo, por ser  $(A_2, B_2)$  controlable, la matriz  $B_2$  de tamaño  $1 \times 1$ , debe ser no nula. Ahora, teniendo en cuenta que el par  $(A_1, C_1)$  es observable, así como la condición (a), tenemos que

$$\operatorname{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = \delta_1 + 1 = \delta_1 + \delta_2$$

para todo  $z \in \overline{\mathbb{F}}$ .

Sea ahora  $\delta_2 > 1$  y supongamos que existe  $z \in \overline{\mathbb{F}}$  tal que

$$\operatorname{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} < \delta_1 + \delta_2, \quad (3.16)$$

de manera que de la condición (a), necesariamente  $z \in \sigma(A) = \sigma(A_2)$ . Por la condición (c), el par  $(A_2, C_2)$  es observable y, por tanto,

$$\operatorname{rg} \begin{pmatrix} zI_{\delta_2} - A_2 \\ O \\ C_2 \end{pmatrix} = \operatorname{rg} \begin{pmatrix} zI_{\delta_2} - A_2 \\ C_2 \end{pmatrix} = \delta_2 \quad \text{para todo } z \in \overline{\mathbb{F}}. \quad (3.17)$$

Además, teniendo en cuenta que las matrices  $B_2$  y  $C_1$  son de tamaños  $\delta_2 \times 1$  y  $1 \times \delta_1$ , respectivamente, así como las condiciones (b) y (c), tenemos que

$$\operatorname{rg} \begin{pmatrix} -B_2C_1 \\ zI_{\delta_1} - A_1 \end{pmatrix} = \operatorname{rg} \begin{pmatrix} C_1 \\ zI_{\delta_1} - A_1 \end{pmatrix} = \delta_1,$$

de donde

$$\delta_1 \geq \operatorname{rg} \begin{pmatrix} -B_2C_1 \\ zI_{\delta_1} - A_1 \\ D_2C_1 \end{pmatrix} \geq \operatorname{rg} \begin{pmatrix} -B_2C_1 \\ zI_{\delta_1} - A_1 \end{pmatrix} = \delta_1,$$

y por tanto,

$$\operatorname{rg} \begin{pmatrix} -B_2C_1 \\ zI_{\delta_1} - A_1 \\ D_2C_1 \end{pmatrix} = \delta_1. \quad (3.18)$$

Ahora bien, teniendo en cuenta las relaciones (3.16), (3.17) y (3.18), tenemos que una

columna de la matriz  $\begin{pmatrix} zI_{\delta_2} - A_2 \\ O \\ C_2 \end{pmatrix}$  es combinación lineal de las columnas de la matriz

$\begin{pmatrix} -B_2C_1 \\ zI_{\delta_1} - A_1 \\ D_2C_1 \end{pmatrix}$ , o bien, una columna de la matriz  $\begin{pmatrix} -B_2C_1 \\ zI_{\delta_1} - A_1 \\ D_2C_1 \end{pmatrix}$  es combinación lineal de las columnas de la matriz  $\begin{pmatrix} zI_{\delta_2} - A_2 \\ O \\ C_2 \end{pmatrix}$ . De este modo, de la condición (d), tendríamos que  $\text{rg} \begin{pmatrix} zI - A_2 & B_2 \end{pmatrix} < \delta_2$ , en contra de la condición (b).  $\square$

Si en el teorema 3.12 no exigimos la condición de observabilidad de alguno de los pares  $(A_l, C_l)$ , para  $l = 1, 2$ , entonces el par  $(A, C)$  del código concatenado puede no ser observable aunque se tenga  $\sigma(A_1) \subseteq \sigma(A_2)$  y el par  $(A_2, B_2)$  sea controlable, como ponemos de manifiesto en el ejemplo siguiente.

**Ejemplo 3.6:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y consideremos el  $(2, 1, 2)$ -código  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , siendo las matrices  $A_1, B_1$  y  $D_1$  las mismas que en el código externo del ejemplo 3.2 y  $C_1 = \begin{pmatrix} 0 & 0 \end{pmatrix}$ . Claramente, el par  $(A_1, C_1)$  no es observable, ya que

$$\text{rg} \begin{pmatrix} \alpha I - A_1 \\ C_1 \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & 0 \\ 0 & \alpha^6 \\ 0 & 0 \end{pmatrix} = 1 \neq 2.$$

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(2, 1, 2)$ -código descrito por la matriz  $A_2$  del ejemplo 3.2 y matrices  $B_2, C_2$  y  $D_2$  arbitrarias de tamaños  $2 \times 1, 1 \times 2$  y  $1 \times 1$ , respectivamente, tales que  $(A_2, B_2)$  es controlable (por ejemplo, basta tomar  $B_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ). Por comodidad, sea  $C_2 = \begin{pmatrix} a & b \end{pmatrix}$ , con  $a$  y  $b$  escalares arbitrarios.

Ahora, por el teorema 3.1 las matrices  $A$  y  $C$  de la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(1)}$  son

$$A = \begin{pmatrix} \alpha^4 & 1 & 0 & 0 \\ \alpha^2 & \alpha^3 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha^5 \end{pmatrix}, \quad C = \begin{pmatrix} a & b & 0 & 0 \end{pmatrix},$$

con lo que obtenemos que el par  $(A, C)$  no es observable, ya que

$$\operatorname{rg} \begin{pmatrix} \alpha I - A \\ C \end{pmatrix} = \operatorname{rg} \begin{pmatrix} \alpha^2 & 1 & 0 & 0 \\ \alpha^2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^6 \\ a & b & 0 & 0 \end{pmatrix} \leq 3 < 4. \quad \blacksquare$$

Del mismo modo, si en el teorema 3.12 no exigimos la controlabilidad del par  $(A_2, B_2)$ , el par  $(A, C)$  de la concatenación  $\mathcal{SC}^{(1)}$  puede no ser observable, aunque  $\sigma(A_1) \subseteq \sigma(A_2)$  y  $(A_l, C_l)$  sea observable, para  $l = 1, 2$ , como vemos en el ejemplo siguiente.

**Ejemplo 3.7:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y consideremos un  $(2, 1, 1)$ -código  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , con

$$A_1 = (\alpha^3), \quad C_1 = (\alpha),$$

y  $B_1$  y  $D_1$  matrices arbitrarias de tamaño  $1 \times 1$ , de manera que  $(A_1, B_1)$  sea controlable (basta tomar, por ejemplo,  $B_1 = (1)$ ). Claramente, el par  $(A_1, C_1)$  es observable.

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  el  $(3, 1, 2)$ -código descrito por las matrices

$$A_2 = \begin{pmatrix} 1 & 0 & 0 \\ \alpha & \alpha^3 & 0 \\ \alpha^2 & 0 & \alpha^6 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 & 0 & \alpha^3 \\ 1 & 1 & \alpha^3 \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Entonces, el par  $(A_2, B_2)$  no es controlable, ya que

$$\operatorname{rg} \begin{pmatrix} \alpha^3 I_3 - A_2 & B_2 \end{pmatrix} = \begin{pmatrix} \alpha & 0 & 0 & 1 \\ \alpha & 0 & 0 & 1 \\ \alpha^2 & 0 & \alpha^4 & 1 \end{pmatrix} = 2 \neq 3.$$

Por otra parte, tenemos que

$$\operatorname{rg} \begin{pmatrix} I_3 - A_2 \\ C_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ \alpha & \alpha & 0 \\ \alpha^2 & 0 & \alpha^2 \\ 1 & 0 & \alpha^3 \\ 1 & 1 & \alpha^3 \end{pmatrix} = 3, \quad \operatorname{rg} \begin{pmatrix} \alpha^3 I_3 - A_2 \\ C_2 \end{pmatrix} = \begin{pmatrix} \alpha & 0 & 0 \\ \alpha & 0 & 0 \\ \alpha^2 & 0 & \alpha^4 \\ 1 & 0 & \alpha^3 \\ 1 & 1 & \alpha^3 \end{pmatrix} = 3$$

y

$$\operatorname{rg} \begin{pmatrix} \alpha^6 I_3 - A_2 \\ C_2 \end{pmatrix} = \begin{pmatrix} \alpha^2 & 0 & 0 \\ \alpha & \alpha^4 & 0 \\ \alpha^2 & 0 & 0 \\ 1 & 0 & \alpha^3 \\ 1 & 1 & \alpha^3 \end{pmatrix} = 3.$$

Por tanto, el par  $(A_2, C_2)$  es observable. Además,  $\sigma(A_1) = \{\alpha^3\} \subseteq \{1, \alpha^3, \alpha^6\} \subseteq \sigma(A_2)$ .

Por otro lado, aplicando el teorema 3.1 las matrices  $A$  y  $C$  de la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(1)}$  son

$$A = \begin{pmatrix} 1 & 0 & 0 & \alpha \\ \alpha & \alpha^3 & 0 & \alpha \\ \alpha^2 & 0 & \alpha^6 & \alpha \\ 0 & 0 & 0 & \alpha^3 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} 1 & 0 & \alpha^3 & \alpha \\ 1 & 1 & \alpha^3 & \alpha \end{pmatrix},$$

de donde obtenemos que el par  $(A, C)$  no es observable, ya que

$$\operatorname{rg} \begin{pmatrix} \alpha^3 I_4 - A \\ C \end{pmatrix} = \operatorname{rg} \begin{pmatrix} \alpha & 0 & 0 & \alpha \\ \alpha & 0 & 0 & \alpha \\ \alpha^2 & 0 & \alpha^4 & \alpha \\ 0 & 0 & 0 & 0 \\ 1 & 0 & \alpha^3 & \alpha \\ 1 & 1 & \alpha^3 & \alpha \end{pmatrix} = 3 < 4. \quad \blacksquare$$

El ejemplo siguiente muestra que el teorema 3.12 no es cierto para el caso en que  $\sigma(A_1) \not\subseteq \sigma(A_2)$ .

**Ejemplo 3.8:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$ . Consideremos un  $(2, 1, 2)$ -código  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , siendo

$$A_1 = \begin{pmatrix} \alpha^4 & 1 \\ 0 & \alpha^3 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 1 & \alpha^2 \end{pmatrix},$$

y  $B_1$  y  $D_1$  matrices arbitrarias de tamaños  $2 \times 1$  y  $1 \times 1$ , respectivamente, de manera que el par  $(A_1, B_1)$  sea controlable (por ejemplo,  $B_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ). Notemos que el par  $(A_1, C_1)$  es observable.

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  el  $(2, 1, 1)$ -código interno descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^3 \\ \alpha^3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} \alpha \end{pmatrix}, \quad C_2 = \begin{pmatrix} \alpha^6 \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} \alpha \end{pmatrix}.$$

Claramente,  $(A_2, B_2)$  es controlable y  $(A_2, C_2)$  es observable. Así pues, se verifican las condiciones (b) y (c) del teorema 3.12. Ahora bien,  $\sigma(A_1) = \{\alpha^4, \alpha^3\} \not\subseteq \{\alpha^3\} = \sigma(A_2)$

Por otro lado, aplicando el teorema 3.1, las matrices  $A$  y  $C$  de la representación entrada-estado-salida de código concatenado  $\mathcal{SC}^{(1)}$  son

$$A = \begin{pmatrix} \alpha^3 & \alpha & \alpha^3 \\ 0 & \alpha^4 & 1 \\ 0 & 0 & \alpha^3 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} \alpha^6 & \alpha & \alpha^3 \end{pmatrix}.$$

Por tanto, el par  $(A, C)$  no es observable, ya que

$$\text{rg} \begin{pmatrix} \alpha^4 I - A \\ C \end{pmatrix} = \text{rg} \begin{pmatrix} \alpha^6 & \alpha & \alpha^3 \\ 0 & 0 & 1 \\ 0 & 0 & \alpha^6 \\ \alpha^6 & \alpha & \alpha^3 \end{pmatrix} = 2 \neq 3. \quad \blacksquare$$

Ahora bien, en el modelo  $\mathcal{SC}^{(2)}$ , la matriz  $C$  varía respecto a la correspondiente para  $\mathcal{SC}^{(1)}$ . Por tanto, tendremos resultados diferentes para obtener la observabilidad del par  $(A, C)$  de  $\mathcal{SC}^{(2)}$ . Así como en el ejemplo 3.5, mostrábamos que siendo  $(A_l, C_l)$  observables, para  $l = 1, 2$ , el par  $(A, C)$  de  $\mathcal{SC}^{(1)}$  no era necesariamente observable, en el modelo  $\mathcal{SC}^{(2)}$  no obtenemos el mismo resultado.

**Ejemplo 3.9:** Sean  $\mathcal{C}_o$  y  $\mathcal{C}_i$  los códigos externo e interno, respectivamente, del ejemplo 3.5. Aplicando entonces el teorema 3.3, las matrices  $A$  y  $C$  de la representación

entrada-estado-salida del código concatenado  $\mathcal{SC}^{(2)}$  son

$$A = \begin{pmatrix} \alpha & \alpha^3 & \alpha^4 \\ 0 & \alpha^3 & \alpha \\ 0 & \alpha & \alpha^4 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} 0 & 1 & \alpha \\ 1 & \alpha & 1 \\ 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha \\ 0 & \alpha & 1 \end{pmatrix}.$$

Observemos que  $\text{rg}(C) = 3$ , de donde

$$\text{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = 3 = \delta_1 + \delta_2, \quad \text{para todo } z \in \overline{\mathbb{F}},$$

es decir, el par  $(A, C)$  es observable. ■

Podemos generalizar este resultado para cualesquiera códigos externo e interno tales que los pares  $(A_l, C_l)$  sean observables, para  $l = 1, 2$ , como ponemos de manifiesto en el resultado siguiente.

**Teorema 3.13:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m - k, \delta_2)$ -código y  $\mathcal{SC}^{(2)}(A, B, C, D)$  el código concatenado de tasa  $k/(n + k)$  descrito por las matrices dadas por la expresión (3.12). Si el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ , entonces el par  $(A, C)$  es observable.

DEMOSTRACIÓN: Como  $(A_l, C_l)$  es observable para  $l = 1, 2$ , tenemos que para todo  $z \in \overline{\mathbb{F}}$

$$\begin{aligned} \delta_2 + \delta_1 &\geq \text{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = \text{rg} \begin{pmatrix} zI_{\delta_2} - A_2 & -B_2C_1 \\ C_2 & D_2C_1 \\ O & zI_{\delta_1} - A_1 \\ O & C_1 \end{pmatrix} \\ &\geq \text{rg} \begin{pmatrix} zI_{\delta_2} - A_2 \\ C_2 \end{pmatrix} + \text{rg} \begin{pmatrix} zI_{\delta_1} - A_1 \\ C_1 \end{pmatrix} = \delta_2 + \delta_1. \end{aligned}$$

De este modo,

$$\text{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = \delta_1 + \delta_2 \quad \text{para todo } z \in \overline{\mathbb{F}},$$

es decir, el par  $(A, C)$  es observable.  $\square$

Como consecuencia del teorema 1.11, tenemos que las condiciones dadas en los teoremas 3.5 y 3.13, hacen que el código concatenado  $\mathcal{SC}^{(2)}$  sea un código observable.

**Corolario 3.7:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m - k, \delta_2)$ -código y  $\mathcal{SC}^{(2)}(A, B, C, D)$  el código concatenado de tasa  $k/(n + k)$  descrito por las matrices dadas por la expresión (3.12). Supongamos que se verifican las condiciones siguientes:

- (a)  $\text{rg}(B) = \delta_1 + \delta_2$ .
- (b) El par  $(A_l, C_l)$  es observable para  $l = 1, 2$ .

Entonces  $(A, B, C, D)$  es una representación minimal para el código observable  $\mathcal{SC}^{(2)}$  con complejidad  $\delta_1 + \delta_2$ .

### 3.2.4 Distancias columnas y distancias libres

A continuación, estudiamos las distancias columnas así como la distancia libre de la concatenación  $\mathcal{SC}^{(2)}$ .

Recordemos que para el modelo de concatenación de la sección 3.2.1, no era posible obtener una relación entre las distancias columnas de  $\mathcal{SC}^{(1)}$  y las de los códigos externo e interno. En el caso de la concatenación  $\mathcal{SC}^{(2)}$ , el hecho de que las palabras de los códigos externo e interno sean componentes de la palabra final de la concatenación, nos permite obtener una cota inferior de  $d_{free}(\mathcal{SC}^{(2)})$  en función de  $d_{free}(\mathcal{C}_o)$  y  $d_{free}(\mathcal{C}_i)$ , bajo ciertas condiciones. Comenzamos con un lema técnico.

**Lema 3.1:** Sea  $\mathcal{SC}^{(2)}$  el código dado por el teorema 3.3 al concatenar el código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$ . Entonces

$$d_j^c(\mathcal{SC}^{(2)}) \geq d_j^c(\mathcal{C}_o) \quad \text{para } j = 0, 1, 2, \dots \quad (3.19)$$

DEMOSTRACIÓN: Teniendo en cuenta las relaciones entre  $y_t, y_t^{(1)}, y_t^{(2)}; u_t, u_t^{(1)}, u_t^{(2)}$ , y  $v_t, v_t^{(1)}, v_t^{(2)}$  dadas por las expresiones (3.7)–(3.11), tenemos que:

$$\sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) = \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)})$$

$$\geq \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}).$$

Así pues, de la expresión de la distancia columna  $d_j^c(\mathcal{SC}^{(2)})$  en términos de la representación entrada-estado-salida dada por la expresión (1.19), tenemos que

$$\begin{aligned} d_j^c(\mathcal{SC}^{(2)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(1)} \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) \right\} \\ &= d_j^c(\mathcal{C}_o) \end{aligned}$$

ya que  $u_0 = u_0^{(1)}$ . □

Ahora bien, hay casos en los que la  $j$ -ésima distancia columna del código interno no es una cota inferior para la  $j$ -ésima distancia columna del código concatenado  $\mathcal{SC}^{(2)}$ , como vemos en el ejemplo siguiente.

**Ejemplo 3.10:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$ . Consideremos el  $(3, 2, 1)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  y el  $(2, 1, 1)$ -código interno  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$ , siendo

$$\begin{aligned} A_1 &= \begin{pmatrix} \alpha^2 \\ \alpha \end{pmatrix}, & B_1 &= \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, & C_1 &= \begin{pmatrix} 1 \\ 1 \end{pmatrix}, & D_1 &= \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \\ A_2 &= \begin{pmatrix} \alpha \\ 1 \end{pmatrix}, & B_2 &= \begin{pmatrix} 1 \\ 1 \end{pmatrix}, & C_2 &= \begin{pmatrix} \alpha^4 \\ 1 \end{pmatrix}, & D_2 &= \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \end{aligned}$$

Entonces, el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$  y aplicando el teorema 3.13, el par  $(A, C)$  de  $\mathcal{SC}^{(2)}$  es observable. Además, el par  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ , y

$$\text{rg} \begin{pmatrix} -B_2 C_1 & B_2 D_1 \\ A_2 - A_1 & B_1 \end{pmatrix} = \text{rg} \begin{pmatrix} 1 & 1 & 1 \\ \alpha^4 & 1 & 1 \end{pmatrix} = 2.$$

De este modo, por el teorema 3.7, tenemos que las matrices

$$A = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha^2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} \alpha^4 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad D = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

constituyen una representación minimal del código observable  $\mathcal{SC}^{(2)}$ .

Además,  $d_{free}(\mathcal{C}_o) = 2$ ,  $d_{free}(\mathcal{C}_i) = 4$  y  $d_{free}(\mathcal{SC}^{(2)}) = 2$ . Por tanto,

$$d_{free}(\mathcal{SC}^{(2)}) \geq d_{free}(\mathcal{C}_o)$$

pero

$$d_{free}(\mathcal{SC}^{(2)}) < d_{free}(\mathcal{C}_i)$$

Obervemos que, en este caso,  $\text{rg}(D_1) = \text{rg}\begin{pmatrix} 1 & 1 \end{pmatrix} = 1 = n - k$  y  $k = 2$ . ■

Sin embargo, si exigimos que  $\text{rg}(D_1) = k$ , entonces podemos obtener un refinamiento de esta cota tal y como demostramos a continuación. Previamente, establecemos el siguiente lema técnico que nos será de utilidad para la demostración del resultado principal sobre la distancia libre de  $\mathcal{SC}^{(2)}$ .

**Lema 3.2:** *Sea  $\mathcal{SC}^{(2)}$  el código dado por el teorema 3.3 al concatenar el código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$ . Si  $\text{rg}(D_1) = k$ , entonces*

$$d_j^c(\mathcal{SC}^{(2)}) \geq \max\{d_j^c(\mathcal{C}_o), d_j^c(\mathcal{C}_i) + 1\}, \quad \text{para } j = 0, 1, 2, \dots \quad (3.20)$$

DEMOSTRACIÓN: Teniendo en cuenta las relaciones entre  $y_t, y_t^{(1)}, y_t^{(2)}$ ;  $u_t, u_t^{(1)}, u_t^{(2)}$ , y  $v_t, v_t^{(1)}, v_t^{(2)}$  dadas por las expresiones (3.7)–(3.11), tenemos que

$$\begin{aligned} \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \\ &\geq \text{wt}(u_0^{(1)}) + \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}). \end{aligned}$$

Ahora, como  $y_0^{(1)} = D_1 u_0^{(1)}$  y  $\text{rg}(D_1) = k$ , tenemos que  $u_0 = u_0^{(1)} \neq 0$  si y sólo si  $u_0^{(2)} = y_0^{(1)} \neq 0$ . Así pues, de la desigualdad anterior y de la expresión (1.19), obtenemos que

$$\begin{aligned} d_j^c(\mathcal{SC}^{(2)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(1)} \neq 0} \left\{ \text{wt}(u_0^{(1)}) + \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \right\} \\ &\geq 1 + \min_{u_0^{(2)} \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \right\} \\ &= 1 + d_j^c(\mathcal{C}_i). \end{aligned}$$

Finalmente, de la desigualdad anterior y del lema 3.1, obtenemos la desigualdad (3.20). □

Como consecuencia inmediata de la expresión de la distancia libre en términos de la representación entrada-estado-salida dada por la relación (1.5) y del lema anterior, obtenemos el resultado siguiente.

**Teorema 3.14:** *Sea  $\mathcal{SC}^{(2)}$  el código dado por el teorema 3.3 al concatenar el código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$ . Entonces*

- (a)  $d_{free}(\mathcal{SC}^{(2)}) \geq d_{free}(\mathcal{C}_o)$ .
- (b) Si  $\text{rg}(D_1) = k$ , entonces  $d_{free}(\mathcal{SC}^{(2)}) \geq d_{free}(\mathcal{C}_i) + 1$ .

### 3.2.5 Ejemplos

A continuación, presentamos varios ejemplos en los que analizamos las relaciones entre los modelos de concatenación  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ .

Sea  $\alpha$  un elemento primitivo de  $GF(8)$ , con  $\alpha^3 + \alpha + 1 = 0$  (véase la sección 1.1). Consideramos entonces el  $(2, 1, 1)$ -código  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$ , para  $l = 1, 2, 3$ , y el  $(2, 1, 2)$ -código  $\mathcal{C}_4(A_4, B_4, C_4, D_4)$  descritos por las matrices

$$\begin{aligned} A_1 &= \begin{pmatrix} \alpha \end{pmatrix}, & B_1 &= \begin{pmatrix} 1 \end{pmatrix}, & C_1 &= \begin{pmatrix} \alpha^4 \end{pmatrix}, & D_1 &= \begin{pmatrix} 1 \end{pmatrix} \\ A_2 &= \begin{pmatrix} \alpha \end{pmatrix}, & B_2 &= \begin{pmatrix} 1 \end{pmatrix}, & C_2 &= \begin{pmatrix} 1 \end{pmatrix}, & D_2 &= \begin{pmatrix} 1 \end{pmatrix}, \\ A_3 &= \begin{pmatrix} \alpha \end{pmatrix}, & B_3 &= \begin{pmatrix} 1 \end{pmatrix}, & C_3 &= \begin{pmatrix} \alpha^2 \end{pmatrix}, & D_3 &= \begin{pmatrix} \alpha^3 \end{pmatrix}, \\ A_4 &= \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^2 \end{pmatrix}, & B_4 &= \begin{pmatrix} 1 \\ \alpha \end{pmatrix}, & C_4 &= \begin{pmatrix} \alpha^3 & \alpha^4 \end{pmatrix}, & D_4 &= \begin{pmatrix} 1 \end{pmatrix} \end{aligned}$$

y consideremos también el  $(3, 1, 1)$ -código  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$ , para  $l = 5, 6$  descrito por las matrices

$$\begin{aligned} A_5 &= \begin{pmatrix} 1 \end{pmatrix}, & B_5 &= \begin{pmatrix} 1 \end{pmatrix}, & C_5 &= \begin{pmatrix} \alpha \\ 0 \end{pmatrix}, & D_5 &= \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \\ A_6 &= \begin{pmatrix} \alpha^3 \end{pmatrix}, & B_6 &= \begin{pmatrix} \alpha \end{pmatrix}, & C_6 &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, & D_6 &= \begin{pmatrix} \alpha^5 \\ \alpha^2 \end{pmatrix}. \end{aligned}$$

Entonces, el código  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  corresponde a la construcción introducida por Smarandache y Rosenthal [102] y, por tanto, es un código convolucional fuertemente

Concatenación de los códigos $\mathcal{C}_{10}$ y $\mathcal{C}_2$				
Modelo	Representación de $\mathcal{S}\mathcal{C}\mathcal{C}_{\text{sys}}$	$d_{free}(\mathcal{S}\mathcal{C}\mathcal{C}_{\text{sys}})$	Código externo	Código interno
$\mathcal{S}\mathcal{C}^{(1)}$	$A = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha^2 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & \alpha \end{pmatrix},$ $C = \begin{pmatrix} 1 & 1 \end{pmatrix}, D = \begin{pmatrix} 1 & 1 \end{pmatrix}$	$d_{free}(\mathcal{S}\mathcal{C}^{(1)}) = 4$ No MDS	$d_1^c(\mathcal{C}_{10}) = 3$	$d_2^c(\mathcal{C}_2) = 4$
$\mathcal{S}\mathcal{C}^{(2)}$	$A = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha^2 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & \alpha \end{pmatrix},$ $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, D = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	$d_{free}(\mathcal{S}\mathcal{C}^{(2)}) = 4$ No MDS	Fuertemente MDS	Fuertemente MDS

Tabla 3.1: Códigos del ejemplo 3.11

MDS. Para  $l = 2, 3$ ,  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$  también es un código fuertemente MDS y para  $l = 4, 5$ ,  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$  es un código convolucional MDS (no fuertemente MDS), mientras que  $\mathcal{C}_6(A_6, B_6, C_6, D_6)$  no es MDS.

Finalmente, consideramos como códigos con dimensión  $k = 2$ , el  $(3, 2, 1)$ -código  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$ , para  $l = 7, 8, 9, 10$ , y el  $(4, 2, 1)$ -código  $\mathcal{C}_{11}(A_{11}, B_{11}, C_{11}, D_{11})$  descritos por las matrices

$$\begin{aligned}
 A_8 &= \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}, & B_8 &= \begin{pmatrix} 1 & 0 \\ 1 & \alpha \end{pmatrix}, & C_8 &= \begin{pmatrix} 1 \\ 1 \end{pmatrix}, & D_8 &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \\
 A_9 &= \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}, & B_9 &= \begin{pmatrix} 1 & 0 \\ 1 & \alpha \end{pmatrix}, & C_9 &= \begin{pmatrix} 1 \\ 1 \end{pmatrix}, & D_9 &= \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \\
 A_{10} &= \begin{pmatrix} \alpha^2 \\ \alpha \end{pmatrix}, & B_{10} &= \begin{pmatrix} 1 & 0 \\ 1 & \alpha \end{pmatrix}, & C_{10} &= \begin{pmatrix} 1 \\ 1 \end{pmatrix}, & D_{10} &= \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \\
 A_{11} &= \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}, & B_{11} &= \begin{pmatrix} 1 & 0 \\ 1 & \alpha \end{pmatrix}, & C_{11} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, & D_{11} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
 \end{aligned}$$

Tenemos entonces que para  $l = 9, 10$ , el código  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$  es un código convolucional fuertemente MDS, mientras que para  $l = 8, 11$ ,  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$  es un código convolucional no MDS.

**Ejemplo 3.11:** En la tabla 3.1 hemos considerado como código externo e interno los códigos fuertemente MDS  $\mathcal{C}_{10}$  y  $\mathcal{C}_2$ , respectivamente. Aplicando entonces los teoremas 3.1, 3.3, 3.5, 3.11 y 3.13 tenemos que las realizaciones  $(A, B, C, D)$  son realizaciones

Concatenación de los códigos $\mathcal{C}_8$ y $\mathcal{C}_6$				
Modelo	Representación de $\mathcal{SC}_{\text{sys}}$	$d_{\text{free}}(\mathcal{SC}_{\text{sys}})$	Código externo	Código interno
$\mathcal{SC}^{(1)}$	$A = \begin{pmatrix} \alpha^3 & \alpha \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix},$ $C = \begin{pmatrix} 1 & \alpha^5 \\ 0 & \alpha^2 \end{pmatrix}, D = \begin{pmatrix} 0 & \alpha^5 \\ 0 & \alpha^2 \end{pmatrix}$	$d_{\text{free}}(\mathcal{SC}^{(1)}) = 3$ No MDS	$d_{\text{free}}(\mathcal{C}_8) = 2$ No MDS	$d_{\text{free}}(\mathcal{C}_6) = 5$ No MDS
$\mathcal{SC}^{(2)}$	$A = \begin{pmatrix} \alpha^3 & \alpha \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix},$ $C = \begin{pmatrix} 1 & \alpha^5 \\ 0 & \alpha^2 \\ 0 & 1 \end{pmatrix}, D = \begin{pmatrix} 0 & \alpha^5 \\ 0 & \alpha^2 \\ 0 & 1 \end{pmatrix}$	$d_{\text{free}}(\mathcal{SC}^{(2)}) = 3$ No MDS		

**Tabla 3.2:** Códigos del ejemplo 3.11

minimales de los códigos observables  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ . Obtenemos que ambos códigos tienen distancia libre  $d_{\text{free}}(\mathcal{SC}^{(1)}) = d_{\text{free}}(\mathcal{SC}^{(2)}) = 4$ , siendo 5 y 7 las cotas Singleton generalizadas para  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ , respectivamente. Por tanto, estos códigos concatenados no son MDS.

Del mismo modo, en la tabla 3.2, hemos considerado como código externo el código no MDS  $\mathcal{C}_8$  y como código interno, el código no MDS  $\mathcal{C}_6$ . Aplicando los teoremas 3.1, 3.3, 3.5, 3.11 y 3.13 tenemos que las realizaciones  $(A, B, C, D)$  son realizaciones minimales de los códigos observables  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ . Además, ambos códigos tienen distancia libre  $d_{\text{free}}(\mathcal{SC}^{(1)}) = d_{\text{free}}(\mathcal{SC}^{(2)}) = 3$ , siendo 7 y 9 las cotas Singleton generalizadas para  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ , respectivamente. Por tanto, estos códigos concatenados tampoco son MDS. ■

**Ejemplo 3.12:** En la tabla 3.3 consideramos como código externo e interno el código fuertemente MDS  $\mathcal{C}_1$ . Aplicando entonces los teoremas 3.1, 3.3 y 3.13, así como los corolarios 3.2 y 3.6 tenemos que las realizaciones  $(A, B, C, D)$  son realizaciones minimales de los códigos observables  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ . Obtenemos que  $d_{\text{free}}(\mathcal{SC}^{(1)}) = 4$  y  $d_{\text{free}}(\mathcal{SC}^{(2)}) = 7$ , siendo 6 y 9 las cotas Singleton generalizadas para  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ , respectivamente. Así pues, estos códigos no son MDS. Observemos que las distancias libres de ambos códigos distan 2 unidades de la cota Singleton generalizada correspondiente

Concatenación de los códigos $\mathcal{C}_1$ y $\mathcal{C}_1$				
Modelo	Representación de $\mathcal{SC}_{\text{sys}}$	$d_{free}(\mathcal{SC}_{\text{sys}})$	Código externo	Código interno
$\mathcal{SC}^{(1)}$	$A = \begin{pmatrix} \alpha & \alpha^4 \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} \alpha^4 & \alpha^4 \\ 0 & \alpha^4 \end{pmatrix}, D = \begin{pmatrix} 1 \end{pmatrix}$	$d_{free}(\mathcal{SC}^{(1)}) = 4$ No MDS	$d_2^c(\mathcal{C}_1) = 4$	$d_2^c(\mathcal{C}_1) = 4$
$\mathcal{SC}^{(2)}$	$A = \begin{pmatrix} \alpha & \alpha^4 \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} \alpha^4 & \alpha^4 \\ 0 & \alpha^4 \end{pmatrix}, D = \begin{pmatrix} 1 \end{pmatrix}$	$d_{free}(\mathcal{SC}^{(2)}) = 7$ No MDS	Fuertemente MDS	Fuertemente MDS

Tabla 3.3: Códigos del ejemplo 3.12

Concatenación de los códigos $\mathcal{C}_{11}$ y $\mathcal{C}_9$				
Modelo	Representación de $\mathcal{SC}_{\text{sys}}$	$d_{free}(\mathcal{SC}_{\text{sys}})$	Código externo	Código interno
$\mathcal{SC}^{(1)}$	$A = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} 1 & \alpha \\ 1 & 0 \end{pmatrix},$ $C = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, D = \begin{pmatrix} 1 & 1 \end{pmatrix}$	$d_{free}(\mathcal{SC}^{(1)}) = 3$ No MDS	$d_{free}(\mathcal{C}_{11}) = 2$	$d_1^c(\mathcal{C}_9) = 3$
$\mathcal{SC}^{(2)}$	$A = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} 1 & \alpha \\ 1 & 0 \end{pmatrix},$ $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$	$d_{free}(\mathcal{SC}^{(2)}) = 5$ No MDS	No MDS	Fuertemente MDS

Tabla 3.4: Códigos del ejemplo 3.12

a cada código.

Si concatenamos los códigos  $\mathcal{C}_{11}$  (no MDS) y  $\mathcal{C}_9$  (fuertemente MDS), obtenemos un resultado similar al de la tabla 3.3. Aplicamos los teoremas 3.1, 3.3, 3.5 y 3.13, así como el corolario 3.4 y obtenemos que las realizaciones  $(A, B, C, D)$  son realizaciones minimales de los códigos observables  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ . Además, tal y como podemos ver

Concatenación de los códigos $\mathcal{C}_4$ y $\mathcal{C}_3$				
Modelo	Representación de $\mathcal{SC}_{\text{sys}}$	$d_{\text{free}}(\mathcal{SC}_{\text{sys}})$	Código externo	Código interno
$\mathcal{SC}^{(1)}$	$A = \begin{pmatrix} \alpha & \alpha^3 & \alpha^4 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}, B = \begin{pmatrix} 1 \\ 1 \\ \alpha \end{pmatrix},$ $C = \begin{pmatrix} \alpha^2 & \alpha^6 & 1 \end{pmatrix}, D = \begin{pmatrix} \alpha^3 \end{pmatrix}$	$d_{\text{free}}(\mathcal{SC}^{(1)}) = 8$ MDS	$d_{\text{free}}(\mathcal{C}_4) = 6$ MDS	$d_2^c(\mathcal{C}_3) = 4$ Fuertemente MDS
$\mathcal{SC}^{(2)}$	$A = \begin{pmatrix} \alpha & \alpha^3 & \alpha^4 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}, B = \begin{pmatrix} 1 \\ 1 \\ \alpha \end{pmatrix},$ $C = \begin{pmatrix} \alpha^2 & \alpha^6 & 1 \\ 0 & \alpha^3 & \alpha^4 \end{pmatrix}, D = \begin{pmatrix} \alpha^3 \\ 1 \end{pmatrix}$	$d_{\text{free}}(\mathcal{SC}^{(2)}) = 11$ No MDS		

**Tabla 3.5:** Códigos del ejemplo 3.13

en la tabla 3.4,  $d_{\text{free}}(\mathcal{SC}^{(1)}) = 3$  y  $d_{\text{free}}(\mathcal{SC}^{(2)}) = 5$ , siendo 5 y 7 las cotas Singleton generalizadas para  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ , respectivamente, es decir, estos códigos no son MDS. ■

**Ejemplo 3.13:** En la tabla 3.5 consideramos como código externo el código MDS  $\mathcal{C}_4$  y como código interno, el código fuertemente MDS  $\mathcal{C}_3$ . Aplicando entonces los teoremas 3.1, 3.3, 3.8, 3.10 y 3.13, obtenemos que las representaciones entrada-estado-salida de los códigos concatenados  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$  que mostramos en la tabla 3.5, son representaciones minimales y el par  $(A, C)$  del código concatenado correspondiente, es observable. Es más,  $d_{\text{free}}(\mathcal{SC}^{(1)}) = 8$ , de donde tenemos que  $\mathcal{SC}^{(1)}$  es un código convolucional MDS, ya que su distancia libre alcanza la cota Singleton generalizada. Sin embargo,  $d_{\text{free}}(\mathcal{SC}^{(2)}) = 11$ , es decir, el código  $\mathcal{SC}^{(2)}$  no es MDS, ya que la cota Singleton generalizada es 12. ■

**Ejemplo 3.14:** Si intercambiamos los códigos constituyentes de las concatenaciones del ejemplo 3.13, es decir, si consideramos como código externo el código  $\mathcal{C}_3$  (fuertemente MDS) y como código interno el código  $\mathcal{C}_4$  (MDS), obtenemos mejores resultados que en el ejemplo anterior (véase la tabla 3.6). Teniendo en cuenta los teoremas 3.1, 3.3, 3.6, 3.12 y 3.13 las matrices  $A$ ,  $B$ ,  $C$  y  $D$  de las correspondientes concatenaciones describen los códigos observables  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$  de forma minimal. Además, obtenemos que  $d_{\text{free}}(\mathcal{SC}^{(1)}) = 8$  y  $d_{\text{free}}(\mathcal{SC}^{(2)}) = 12$ , es decir, los códigos concatenados  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$

Concatenación de los códigos $\mathcal{C}_3$ y $\mathcal{C}_4$				
Modelo	Representación de $\mathcal{S}\mathcal{C}\mathcal{C}_{\text{sys}}$	$d_{free}(\mathcal{S}\mathcal{C}\mathcal{C}_{\text{sys}})$	Código externo	Código interno
$\mathcal{S}\mathcal{C}^{(1)}$	$A = \begin{pmatrix} \alpha & 0 & \alpha^2 \\ 0 & \alpha^2 & \alpha^3 \\ 0 & 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha^3 \\ \alpha^4 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} \alpha^3 & \alpha^4 & \alpha^2 \\ \alpha^3 \end{pmatrix}, D = \begin{pmatrix} \alpha^3 \end{pmatrix}$	$d_{free}(\mathcal{S}\mathcal{C}^{(1)}) = 8$ MDS	$d_2^c(\mathcal{C}_3) = 4$ Fuertemente MDS	$d_{free}(\mathcal{C}_4) = 6$ MDS
$\mathcal{S}\mathcal{C}^{(2)}$	$A = \begin{pmatrix} \alpha & 0 & \alpha^2 \\ 0 & \alpha^2 & \alpha^3 \\ 0 & 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha^3 \\ \alpha^4 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} \alpha^3 & \alpha^4 & \alpha^2 \\ 0 & 0 & \alpha^2 \end{pmatrix}, D = \begin{pmatrix} \alpha^3 \\ \alpha^3 \end{pmatrix}$	$d_{free}(\mathcal{S}\mathcal{C}^{(2)}) = 12$ MDS		

Tabla 3.6: Códigos del ejemplo 3.14

son MDS. ■

### 3.3 Concatenación en serie no sistemática

En la sección 3.2, hemos estudiado dos tipos de concatenación,  $\mathcal{S}\mathcal{C}^{(1)}$  y  $\mathcal{S}\mathcal{C}^{(2)}$ , en las que la entrada del código interno es únicamente la parte de paridad del código externo. La concatenación  $\mathcal{S}\mathcal{C}^{(1)}$  es la empleada normalmente en la teoría de sistemas, pero no corresponde a la concatenación en serie introducida por Forney [41] para códigos convolucionales. Forney considera que la palabra código del código externo es precisamente la entrada para el código interno, no sólo su parte de paridad. En esta sección, estudiamos dos modelos de concatenación, uno de ellos propuesto por Forney, desde el punto de vista de sistemas lineales. Comenzamos analizando las representaciones entrada-estado-salida de dichos modelos y establecemos condiciones para que los pares  $(A, B)$  y  $(A, C)$  de ambos modelos sean controlable y observable, respectivamente. Finalizamos la sección con resultados relativos a las distancias columnas y distancias libres de los modelos de concatenación introducidos.

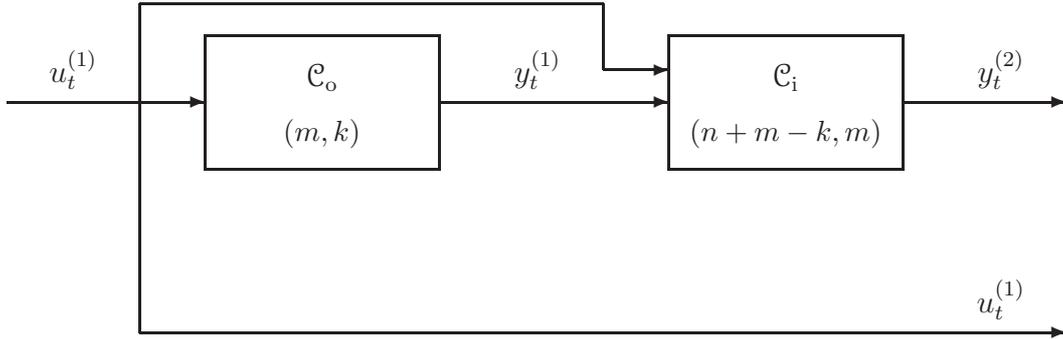


Figura 3.3: Código concatenado  $\mathcal{SC}^{(3)}$

### 3.3.1 Representación entrada-estado-salida

En esta sección, describimos el modelo de concatenación propuesto por Forney y otro modelo derivado de éste. Asimismo, proporcionamos la representación entrada-estado-salida de dichos modelos.

#### Modelo 3

En este tercer modelo, el código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$  se serializan, uno tras otro, de manera que el vector información  $u_t^{(1)}$  es codificado por  $\mathcal{C}_o$  y la palabra código obtenida  $v_t^{(1)}$  es, a su vez, el vector información para el código interno  $\mathcal{C}_i$ , es decir,

$$u_t^{(2)} = v_t^{(1)}. \quad (3.21)$$

La palabra código de la concatenación está constituida, tal y como teníamos para el código  $\mathcal{SC}^{(1)}$ , por el vector información del código externo  $u_t^{(1)}$  y el vector de paridad del código interno  $y_t^{(2)}$  (véase la figura 3.3),

$$v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(1)} \end{pmatrix}. \quad (3.22)$$

Denotamos por  $\mathcal{SC}^{(3)}$  el código convolucional obtenido. El estado del sistema es entonces la unión de los estados de los dos códigos constituyentes, es decir,

$$x_t = \begin{pmatrix} x_t^{(2)} \\ x_t^{(1)} \end{pmatrix}. \quad (3.23)$$

Los vectores información  $u_t$  y de paridad  $y_t$  de  $\mathcal{SC}^{(3)}$  vienen dados, de forma análoga a los vectores de información y de paridad de  $\mathcal{SC}^{(1)}$ , por

$$u_t = u_t^{(1)} \quad \text{e} \quad y_t = y_t^{(2)}, \quad (3.24)$$

respectivamente.

**Observación 3.13:** Recordemos que según la expresión (3.1), las palabras de los códigos externo e interno venían dadas por

$$v_t^{(1)} = \begin{pmatrix} y_t^{(1)} \\ u_t^{(1)} \end{pmatrix} \quad \text{y} \quad v_t^{(2)} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(2)} \end{pmatrix}.$$

Sin embargo, una palabra código de  $\mathcal{SC}^{(3)}$  está formada por una parte de  $v_t^{(1)}$  y una parte de  $v_t^{(2)}$ . Esto constituye un problema a la hora de relacionar las distancias columnas del código concatenado con las de los códigos constituyentes. ■

El teorema siguiente proporciona la representación entrada-estado-salida para el código concatenado  $\mathcal{SC}^{(3)}$  en función de la representación entrada-estado-salida de los códigos externo e interno.

**Teorema 3.15:** Si  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, \delta_1)$ -código y  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n + m - k, m, \delta_2)$ -código, entonces, la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(3)}$  de tasa  $k/n$  viene dada por el sistema (1.11), donde

$$A = \begin{pmatrix} A_2 & B_{21}C_1 \\ O & A_1 \end{pmatrix}, \quad B = \begin{pmatrix} B_{21}D_1 + B_{22} \\ B_1 \end{pmatrix}, \quad (3.25)$$

$$C = \begin{pmatrix} C_2 & D_{21}C_1 \end{pmatrix}, \quad D = D_{21}D_1 + D_{22}$$

en donde hemos considerado las particiones

$$B_2 = \begin{pmatrix} B_{21} & B_{22} \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} D_{21} & D_{22} \end{pmatrix},$$

con  $B_{21}, B_{22}, D_{21}$  y  $D_{22}$  matrices de tamaños  $\delta_2 \times (m - k)$ ,  $\delta_2 \times k$ ,  $(n - k) \times (m - k)$  y  $(n - k) \times k$ , respectivamente.

DEMOSTRACIÓN: Teniendo en cuenta la expresión (1.11), tenemos, para el código externo  $\mathcal{C}_o$ ,

$$\begin{aligned}x_{t+1}^{(1)} &= A_1 x_t^{(1)} + B_1 u_t^{(1)}, \\y_t^{(1)} &= C_1 x_t^{(1)} + D_1 u_t^{(1)},\end{aligned}$$

y para el código interno  $\mathcal{C}_i$ ,

$$\begin{aligned}x_{t+1}^{(2)} &= A_2 x_t^{(2)} + B_2 u_t^{(2)}, \\y_t^{(2)} &= C_2 x_t^{(2)} + D_2 u_t^{(2)}.\end{aligned}$$

Ahora, teniendo en cuenta las expresiones (3.21), (3.23) y (3.24), si consideramos la partición por bloques de la matrices  $B_2 = \begin{pmatrix} B_{21} & B_{22} \end{pmatrix}$  y  $D_2 = \begin{pmatrix} D_{21} & D_{22} \end{pmatrix}$ , de acuerdo con la partición por bloques de  $u_t^{(2)} = \begin{pmatrix} u_{t1}^{(2)} \\ u_{t2}^{(2)} \end{pmatrix}$ , siendo  $u_{t1}^{(2)} \in \mathbb{F}^{m-k}$  y  $u_{t2}^{(2)} \in \mathbb{F}^k$ , entonces la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(3)}$  viene dada por

$$\begin{aligned}x_{t+1} &= \begin{pmatrix} A_2 & B_{21}C_1 \\ O & A_1 \end{pmatrix} x_t + \begin{pmatrix} B_{21}D_1 + B_{22} \\ B_1 \end{pmatrix} u_t, \\y_t &= \begin{pmatrix} C_2 & D_{21}C_1 \end{pmatrix} x_t + \begin{pmatrix} D_{21}D_1 + D_{22} \end{pmatrix} u_t.\end{aligned}$$

□

Teniendo en cuenta el teorema 1.12, así como el teorema anterior, obtenemos la función de transferencia asociada al código convolucional  $\widehat{\mathcal{SC}}^{(3)}$ .

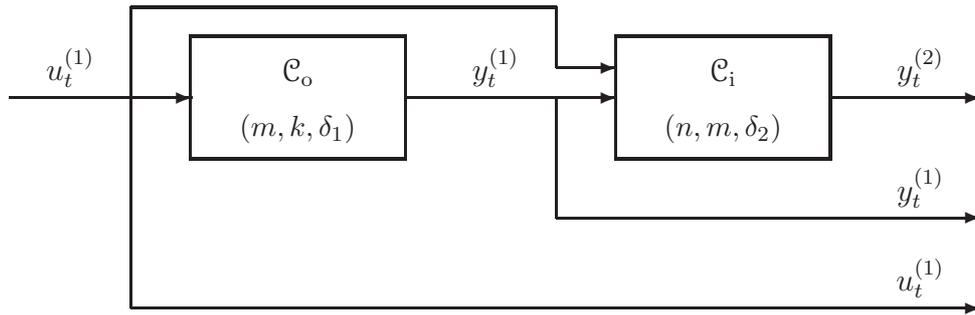
**Teorema 3.16:** Si  $T_1(z)$  y  $T_2(z)$  son las funciones de transferencia de los códigos  $\widehat{\mathcal{C}}_o(A_1, B_1, C_1, D_1)$  y  $\widehat{\mathcal{C}}_i(A_2, B_2, C_2, D_2)$ , respectivamente, entonces,

$$T(z) = T_{21}(z)T_1(z) + T_{22}(z)$$

es la función de transferencia asociada al código  $\widehat{\mathcal{SC}}^{(3)}(A, B, C, D)$ , donde

$$T_2(z) = \begin{pmatrix} T_{21}(z) & T_{22}(z) \end{pmatrix}$$

es una partición en bloque acorde con la partición en bloques de  $B_2$  y  $D_2$  del teorema 3.15.



**Figura 3.4:** Código Concatenado  $\mathcal{SC}^{(4)}$

## Modelo 4

Como hemos visto en la observación 3.13, una palabra código de  $\mathcal{SC}^{(3)}$  está formada por una parte de cada una de las palabras código de los códigos externo e interno. Esto hace que no tengamos una relación entre las distancias columnas (y por tanto, de las distancias libres) de  $\mathcal{SC}^{(3)}$  y las de  $\mathcal{C}_o$  y  $\mathcal{C}_i$ , como veremos posteriormente. Por esta razón, consideramos una variación de la concatenación del modelo 3, similar a la hecha para obtener el código  $\mathcal{SC}^{(2)}$ , de manera que la entrada para el código interno  $u_t^{(2)}$  siga siendo la palabra del código externo,

$$u_t^{(2)} = v_t^{(1)}, \quad (3.26)$$

pero en el modelo que nos ocupa, consideramos que  $u_t^{(2)}$  forma parte, a su vez, de la palabra código  $v_t$  del código convolucional obtenido de la concatenación (véase la figura 3.4),

$$v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ y_t^{(1)} \\ u_t^{(1)} \end{pmatrix}. \quad (3.27)$$

Denotamos por  $\mathcal{SC}^{(4)}$  el código convolucional obtenido. Observemos que el vector de estados  $x_t$  y el vector información  $u_t$  coinciden con los correspondientes para  $\mathcal{SC}^{(3)}$ , es decir,

$$x_t = \begin{pmatrix} x_t^{(2)} \\ x_t^{(1)} \end{pmatrix} \quad \text{y} \quad u_t = u_t^{(1)}. \quad (3.28)$$

Ahora bien, el vector de paridad  $y_t$  viene dado por

$$y_t = \begin{pmatrix} y_t^{(2)} \\ y_t^{(1)} \end{pmatrix}. \quad (3.29)$$

De este modo, teniendo en cuenta la expresión (3.27), la relación entre la palabra código de la concatenación y las palabras código de los códigos externo e interno, resulta ser

$$v_t = \begin{pmatrix} y_t^{(2)} \\ v_t^{(1)} \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(2)} \end{pmatrix} = v_t^{(2)}. \quad (3.30)$$

**Observación 3.14:** Notemos que una palabra código de  $\mathcal{SC}^{(4)}$  es una palabra código del código interno  $\mathcal{C}_i$ . Sin embargo, una palabra código de  $\mathcal{C}_i$  no tiene por qué ser necesariamente una palabra código de  $\mathcal{SC}^{(4)}$  (véase la figura 3.4). ■

La representación entrada-estado-salida para el código concatenado  $\mathcal{SC}^{(4)}$  viene dada, como en los modelos anteriores de concatenación, en función de la representación entrada-estado-salida de los códigos externo e interno, tal y como ponemos de manifiesto en el teorema siguiente.

**Teorema 3.17:** Si  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, \delta_1)$ -código y  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, m, \delta_2)$ -código, entonces, la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(4)}$  de tasa  $k/n$  viene dada por el sistema (1.11), siendo

$$\begin{aligned} A &= \begin{pmatrix} A_2 & B_{21}C_1 \\ O & A_1 \end{pmatrix}, & B &= \begin{pmatrix} B_{21}D_1 + B_{22} \\ B_1 \end{pmatrix}, \\ C &= \begin{pmatrix} C_2 & D_{21}C_1 \\ O & C_1 \end{pmatrix}, & D &= \begin{pmatrix} D_{21}D_1 + D_{22} \\ D_1 \end{pmatrix}, \end{aligned} \quad (3.31)$$

en donde hemos considerado las particiones

$$B_2 = \begin{pmatrix} B_{21} & B_{22} \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} D_{21} & D_{22} \end{pmatrix},$$

siendo  $B_{21}$ ,  $B_{22}$ ,  $D_{21}$  y  $D_{22}$  matrices de tamaños  $\delta_2 \times (m - k)$ ,  $\delta_2 \times k$ ,  $(n - m) \times (m - k)$  y  $(n - m) \times k$ , respectivamente.

DEMOSTRACIÓN: Procediendo de manera análoga a la demostración del teorema 3.15, tenemos que

$$\begin{aligned}x_{t+1}^{(1)} &= A_1 x_t^{(1)} + B_1 u_t^{(1)}, & x_{t+1}^{(2)} &= A_2 x_t^{(2)} + B_2 u_t^{(2)}, \\y_t^{(1)} &= C_1 x_t^{(1)} + D_1 u_t^{(1)}, & y_t^{(2)} &= C_2 x_t^{(2)} + D_2 u_t^{(2)}.\end{aligned}$$

Ahora, teniendo en cuenta que  $u_t^{(2)} = v_t^{(1)}$ , si consideramos la partición por bloques de la matrices  $B_2 = \begin{pmatrix} B_{21} & B_{22} \end{pmatrix}$  y  $D_2 = \begin{pmatrix} D_{21} & D_{22} \end{pmatrix}$ , como en el código  $\mathcal{SC}^{(3)}$ , entonces la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(4)}$  viene dada por

$$\begin{aligned}x_{t+1} &= \begin{pmatrix} A_2 & B_{21}C_1 \\ O & A_1 \end{pmatrix} x_t + \begin{pmatrix} B_{21}D_1 + B_{22} \\ B_1 \end{pmatrix} u_t, \\y_t &= \begin{pmatrix} C_2 & D_{21}C_1 \\ O & C_1 \end{pmatrix} x_t + \begin{pmatrix} D_{21}D_1 + D_{22} \\ D_1 \end{pmatrix} u_t.\end{aligned}$$

□

La función de transferencia asociada al código convolucional  $\widehat{\mathcal{SC}}^{(4)}$  se obtiene a partir de las funciones de transferencia  $T_1(z)$  y  $T_2(z)$  de los códigos  $\widehat{\mathcal{C}}_o$  y  $\widehat{\mathcal{C}}_i$ , respectivamente, como vemos en el teorema siguiente.

**Teorema 3.18:** Si  $T_1(z)$  y  $T_2(z)$  son las funciones de transferencia de los códigos  $\widehat{\mathcal{C}}_o(A_1, B_1, C_1, D_1)$  y  $\widehat{\mathcal{C}}_i(A_2, B_2, C_2, D_2)$ , respectivamente, entonces,

$$T(z) = \begin{pmatrix} T_{21}(z)T_1(z) + T_{22}(z) \\ T_1(z) \end{pmatrix}$$

es la función de transferencia asociada al código  $\widehat{\mathcal{SC}}^{(4)}(A, B, C, D)$ , donde

$$T_2(z) = \begin{pmatrix} T_{21}(z) & T_{22}(z) \end{pmatrix}$$

es una partición en bloque acorde con la partición en bloques de  $B_2$  y  $D_2$  del teorema 3.17.

### 3.3.2 Controlabilidad

En esta sección, estudiamos las condiciones sobre las matrices que describen los códigos externo e interno para obtener una representación entrada-estado-salida minimal

del código concatenado. Como ocurría con los dos primeros modelos de concatenación, las matrices  $A$  y  $B$  de los códigos  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$  tienen la misma expresión. Así pues, dado que los resultados que presentamos serán válidos para ambos tipos de concatenación, denotaremos por  $\mathcal{SCC}$  el código concatenado  $\mathcal{SC}^{(3)}$  descrito por la expresión (3.25) así como el código  $\mathcal{SC}^{(4)}$  descrito por la expresión (3.31). Consideramos como código externo  $\mathcal{C}_o$ , un  $(m, k, \delta_1)$ -código, y como código interno  $\mathcal{C}_i$ , un  $(n, m, \delta_2)$ -código. Entonces,  $\mathcal{SCC}$  es un  $(n - m + k, k, \delta)$ -código si consideramos la concatenación  $\mathcal{SC}^{(3)}$  y es un  $(n, k, \delta)$ -código si consideramos la concatenación  $\mathcal{SC}^{(4)}$ .

El ejemplo siguiente pone de manifiesto que no es suficiente con que el par  $(A_l, B_l)$ , para  $l = 1, 2$  de los códigos constituyentes sea controlable para que el par  $(A, B)$  del código concatenado  $\mathcal{SCC}$  sea controlable.

**Ejemplo 3.15:** Sea  $\alpha$  un elemento primitivo del cuerpo de Galois  $\mathbb{F} = GF(8)$ . Consideremos el  $(6, 4, 2)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , con

$$A_1 = \begin{pmatrix} \alpha^5 & \alpha \\ \alpha^3 & \alpha^5 \end{pmatrix}, \quad B_1 = \begin{pmatrix} \alpha^2 & \alpha & \alpha^4 & \alpha^5 \\ \alpha^4 & \alpha^3 & \alpha^5 & \alpha^6 \end{pmatrix},$$

$$C_1 = \begin{pmatrix} \alpha^2 & 1 \\ 1 & \alpha \end{pmatrix}, \quad D_1 = \begin{pmatrix} 1 & \alpha & 0 & 1 \\ \alpha & 0 & \alpha^2 & \alpha^3 \end{pmatrix}.$$

Observemos que  $(A_1, B_1)$  es controlable, ya que  $\text{rg}(B_1) = 2$ .

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(9, 6, 1)$ -código descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} \alpha^2 & 1 & \alpha^2 & \alpha & \alpha^6 & \alpha^6 \end{pmatrix},$$

$$C_2 = \begin{pmatrix} 0 \\ \alpha \\ 0 \end{pmatrix}, \quad D_{21} = \begin{pmatrix} \alpha^6 & \alpha^4 \\ \alpha^4 & \alpha^4 \\ 1 & \alpha^5 \end{pmatrix},$$

con  $D_{22}$  una matriz arbitraria de tamaño  $3 \times 4$ . Claramente, el par  $(A_2, B_2)$  es controlable.

Por otro lado, por los teoremas 3.15 y 3.17, las matrices  $A$  y  $B$  de la representación entrada-estado-salida de los códigos concatenados  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ , son

$$A = \begin{pmatrix} \alpha^3 & \alpha^5 & \alpha^4 \\ 0 & \alpha^5 & \alpha \\ 0 & \alpha^3 & \alpha^5 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} \alpha & 1 & 1 & \alpha \\ \alpha^2 & \alpha & \alpha^4 & \alpha^5 \\ \alpha^4 & \alpha^3 & \alpha^5 & \alpha^6 \end{pmatrix}.$$

Pero el par  $(A, B)$  no es controlable, ya que

$$\text{rg} \begin{pmatrix} \alpha^3 I - A & B \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & \alpha^5 & \alpha^4 & \alpha & 1 & 1 & \alpha \\ 0 & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^4 & \alpha^5 \\ 0 & \alpha^3 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^5 & \alpha^6 \end{pmatrix} = 2 \neq 3. \quad \blacksquare$$

Por tanto, tal y como teníamos para los códigos  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ , necesitamos más condiciones sobre las matrices que describen los códigos externo e interno para obtener la controlabilidad del código convolucional concatenado  $\mathcal{SCC}$ .

El teorema 3.5 sigue siendo válido para estos modelos de concatenación, como ponemos de manifiesto en el resultado siguiente cuya demostración omitimos por ser similar a la de dicho teorema.

**Teorema 3.19:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m, \delta_2)$ -código y  $\mathcal{SCC}(A, B, C, D)$  el código concatenado correspondiente.

Si  $\text{rg}(B) = \delta_1 + \delta_2$ , entonces  $(A, B, C, D)$  es una representación minimal de  $\mathcal{SCC}(A, B, C, D)$  con complejidad  $\delta_1 + \delta_2$ .

Recordemos que para los códigos  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ , la condición  $\text{rg}(B) = \delta_1 + \delta_2$  del teorema 3.5, implicaba que los pares  $(A_l, B_l)$  eran controlables, para  $l = 1, 2$ . En el caso de los códigos  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ , también se tiene esta implicación, aunque no es tan trivial como en los casos anteriores.

**Teorema 3.20:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m, \delta_2)$ -código y  $\mathcal{SCC}(A, B, C, D)$  el código concatenado correspondiente.

Si  $\text{rg}(B) = \delta_1 + \delta_2$ , entonces  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ .

DEMOSTRACIÓN: En primer lugar, de la condición sobre el rango de  $B$  y de los tamaños de las matrices  $B_1$  y  $B_2$ , tenemos que

$$\text{rg}(B_{21}D_1 + B_{22}) = \delta_2, \quad (3.32)$$

$$\text{rg}(B_1) = \delta_1. \quad (3.33)$$

Ahora, de la expresión (3.33), obtenemos que  $B_1$  tiene rango completo por filas. Así pues, empleando un argumento similar al de la demostración del teorema 3.5, el par  $(A_1, B_1)$  es controlable.

Por otra parte, si el par  $(A_2, B_2)$  no fuera controlable, entonces existiría una matriz invertible  $S$  de tamaño  $\delta_2 \times \delta_2$  tal que (véase el teorema 1.9)

$$SA_2S^{-1} = \begin{pmatrix} \tilde{A}_2 & \tilde{A}_3 \\ O & \tilde{A}_4 \end{pmatrix}, \quad SB_2 = \begin{pmatrix} \tilde{B}_2 \\ O \end{pmatrix}, \quad C_2S^{-1} = \begin{pmatrix} \tilde{C}_2 & \tilde{C}_3 \end{pmatrix},$$

con  $\tilde{A}_2, \tilde{B}_2$  y  $\tilde{C}_2$  matrices de tamaños  $\tilde{r}_2 \times \tilde{r}_2$ ,  $\tilde{r}_2 \times m$  y  $(n - m) \times \tilde{r}_2$ , respectivamente (con  $\tilde{r}_2 < \delta_2$ ) y siendo  $(\tilde{A}_2, \tilde{B}_2)$  un par controlable.

Así pues, la matriz  $B_2 = \begin{pmatrix} B_{21} & B_{22} \end{pmatrix} = S^{-1} \begin{pmatrix} \tilde{B}_2 \\ O \end{pmatrix}$  no tiene rango completo. Sea  $r_2 = \text{rg}(B_2) \leq \tilde{r}_2 < \delta_2$ . Por tanto,  $B_2$  tiene  $r_2$  filas linealmente independientes. Sin pérdida de generalidad, podemos suponer que se trata de las  $r_2$  primeras filas, de donde la matriz  $B_2$  tendrá la forma

$$\left( \begin{array}{c|cccc} f_1 & g_{11} & g_{12} & \cdots & g_{1k} \\ f_2 & g_{21} & g_{22} & \cdots & g_{2k} \\ \vdots & \vdots & \vdots & & \vdots \\ f_{r_2} & g_{r_2 1} & g_{r_2 2} & \cdots & g_{r_2 k} \\ \hline \sum_{j=1}^{r_2} \alpha_j^1 f_j & \sum_{j=1}^{r_2} \alpha_j^1 g_{j1} & \sum_{j=1}^{r_2} \alpha_j^1 g_{j2} & \cdots & \sum_{j=1}^{r_2} \alpha_j^1 g_{jk} \\ \vdots & \vdots & \vdots & & \vdots \\ \sum_{j=1}^{r_2} \alpha_j^{\delta_2 - r_2} f_j & \sum_{j=1}^{r_2} \alpha_j^{\delta_2 - r_2} g_{j1} & \sum_{j=1}^{r_2} \alpha_j^{\delta_2 - r_2} g_{j2} & \cdots & \sum_{j=1}^{r_2} \alpha_j^{\delta_2 - r_2} g_{jk} \end{array} \right)$$

con  $f_i$  y  $(g_{i1} \ g_{i2} \ \cdots \ g_{ik})$  la  $i$ -ésima fila de  $B_{21}$  y  $B_{22}$ , respectivamente, para  $i = 1, 2, \dots, r_2$ . Del mismo modo,

$$\sum_{j=1}^{r_2} \alpha_j^i f_j \quad \text{y} \quad \left( \sum_{j=1}^{r_2} \alpha_j^i g_{j1} \quad \sum_{j=1}^{r_2} \alpha_j^i g_{j2} \quad \cdots \quad \sum_{j=1}^{r_2} \alpha_j^i g_{jk} \right)$$

corresponden a la  $i$ -ésima fila de  $B_{21}$  y  $B_{22}$ , respectivamente, para  $i = r_2 + 1, \dots, \delta_2$ .

Por tanto, si denotamos por  $d_i$  la columna  $i$ -ésima de la matriz  $D_1$ , entonces

$$\begin{aligned}
 B_{21}D_1 + B_{22} &= \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_{r_2} \\ \sum_{j=1}^{r_2} \alpha_j^1 f_j \\ \vdots \\ \sum_{j=1}^{r_2} \alpha_j^{\delta_2 - r_2} f_j \end{pmatrix} \begin{pmatrix} d_1 & d_2 & \cdots & d_k \end{pmatrix} \\
 &+ \begin{pmatrix} g_{11} & \cdots & g_{1k} \\ g_{21} & \cdots & g_{2k} \\ \vdots & & \vdots \\ g_{r_2 1} & \cdots & g_{r_2 k} \\ \sum_{j=1}^{r_2} \alpha_j^1 g_{j1} & \cdots & \sum_{j=1}^{r_2} \alpha_j^1 g_{jk} \\ \vdots & & \vdots \\ \sum_{j=1}^{r_2} \alpha_j^{\delta_2 - r_2} g_{j1} & \cdots & \sum_{j=1}^{r_2} \alpha_j^{\delta_2 - r_2} g_{jk} \end{pmatrix} \\
 &= \begin{pmatrix} f_1 d_1 + g_{11} & \cdots & f_1 d_k + g_{1k} \\ f_2 d_1 + g_{21} & \cdots & f_2 d_k + g_{2k} \\ \vdots & & \vdots \\ f_{r_2} d_1 + g_{r_2 1} & \cdots & f_{r_2} d_k + g_{r_2 k} \\ \sum_{j=1}^{r_2} \alpha_j^1 (f_j d_1 + g_{j1}) & \cdots & \sum_{j=1}^{r_2} \alpha_j^1 (f_j d_k + g_{jk}) \\ \vdots & & \vdots \\ \sum_{j=1}^{r_2} \alpha_j^{\delta_2 - r_2} (f_j d_1 + g_{j1}) & \cdots & \sum_{j=1}^{r_2} \alpha_j^{\delta_2 - r_2} (f_j d_k + g_{jk}) \end{pmatrix}
 \end{aligned}$$

tiene rango menor o igual que  $r_2 < \delta_2$ , lo cual contradice la expresión (3.32).  $\square$

**Observación 3.15:** El ejemplo 3.15 pone de manifiesto también que el recíproco del teorema 3.20 no es cierto en general. En efecto, si consideramos los códigos del ejemplo 3.15, tenemos que el par  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ , y por tanto,  $\delta_1 = 2$  y  $\delta_2 = 1$ ; sin embargo,  $\text{rg}(B) = 2 \neq 2 + 1$ .  $\blacksquare$

Por tanto, necesitamos más condiciones sobre las matrices que describen los códigos externo e interno para tener la controlabilidad del par  $(A, B)$  del código convolucional

concatenado. El resultado siguiente, cuya demostración es análoga a la del teorema 3.6 cambiando  $B_2$  por  $B_{21}$ , proporciona condiciones suficientes para que el par  $(A, B)$  de SCC sea controlable en el caso particular en que el código externo tenga tasa  $1/2$  y complejidad  $\delta_1 = 1$  y la matriz  $A_2$  sea diagonal.

**Teorema 3.21:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(2, 1, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, 2, \delta_2)$ -código y que  $\text{SCC}(A, B, C, D)$  es el código concatenado correspondiente. Supongamos que también se verifican las condiciones siguientes:*

- (a)  $A_2$  es una matriz diagonal.
- (b) El par  $(A_1, B_1)$  es controlable.
- (c) El par  $(A_2, B_{21})$  es controlable.
- (d) Todos los elementos de  $B_{21}$  son no nulos y  $B_{22} = O$ .
- (e)  $\text{rg} \begin{pmatrix} -C_1 & D_1 \\ \lambda I - A_1 & B_1 \end{pmatrix} = 2$  para todo  $\lambda$  valor propio de  $A$ .

Entonces  $(A, B, C, D)$  es una representación minimal del código concatenado SCC con complejidad  $\delta_1 + \delta_2 = 1 + \delta_2$ .

**Observación 3.16:** Con las condiciones dadas en el teorema anterior, tenemos que la matriz  $A_1 = \begin{pmatrix} a_1 \end{pmatrix}$  es escalar y, además,  $a_1$  es un valor propio de la matriz  $A$ ; por tanto, en este caso, la condición (e) se reduce a

$$\text{rg} \begin{pmatrix} -C_1 & D_1 \\ O & B_1 \end{pmatrix} = 2,$$

de donde se deduce en particular que el par  $(A_1, C_1)$  es observable por ser  $\delta_1 = 1$ . ■

Ahora bien, de forma análoga a los dos primeros modelos de concatenación, tenemos el resultado siguiente para el caso particular en que los códigos externo e interno tengan complejidad  $\delta_1 = \delta_2 = 1$  y el código externo tenga tasa arbitraria  $k/n$ . La demostración es similar a la demostración del teorema 3.7, cambiando las matrices  $B_2C_1$  y  $B_2D_1$  por las matrices  $B_{21}C_1$  y  $B_{21}D_1 + B_{22}$ , respectivamente.

**Teorema 3.22:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, m, 1)$ -código y que  $\text{SCC}(A, B, C, D)$  es el código concatenado correspondiente. Supongamos que también se verifican las condiciones siguientes:*

- (a) El par  $(A_1, B_1)$  es controlable.

(b) La matriz  $\begin{pmatrix} -B_{21}C_1 & B_{21}D_1 + B_{22} \\ A_2 - A_1 & B_1 \end{pmatrix}$ , de tamaño  $2 \times (k+1)$ , tiene rango 2.

Entonces  $(A, B, C, D)$  es una representación minimal del código concatenado SCC con complejidad  $\delta_1 + \delta_2 = 2$ .

Recordemos que para el caso de las concatenaciones  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ , la condición

$$\text{rg} \begin{pmatrix} -B_2C_1 & B_2D_1 \\ A_2 - A_1 & B_1 \end{pmatrix} = 2$$

del teorema 3.7, implicaba que el par  $(A_2, B_2)$  era controlable. Sin embargo, en el caso de los modelos  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ , la condición

$$\text{rg} \begin{pmatrix} -B_{21}C_1 & B_{21}D_1 + B_{22} \\ A_2 - A_1 & B_1 \end{pmatrix} = 2$$

del teorema 3.22, no implica necesariamente que  $(A_2, B_{21})$  sea controlable. De hecho, sólo implica la controlabilidad de  $(A_2, B_{21})$  en el caso en que la matriz  $B_{22}$  sea nula. En el resto de los casos no se tiene este resultado, como mostramos en el ejemplo siguiente.

**Ejemplo 3.16:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$ . Consideremos un  $(4, 2, 1)$ -código  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , donde  $C_1$  y  $D_1$  son matrices arbitrarias de tamaños  $2 \times 1$  y  $2 \times 2$ , respectivamente, y

$$A_1 = \begin{pmatrix} \alpha \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

Sea  $C_i(A_2, B_2, C_2, D_2)$  un  $(5, 4, 1)$ -código, siendo  $C_2$  y  $D_2$  matrices arbitrarias de tamaños  $1 \times 1$  y  $1 \times 4$ , respectivamente, y

$$A_2 = \begin{pmatrix} \alpha^3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \alpha & \alpha \end{pmatrix}.$$

Observemos que el par  $(A_2, B_{21})$  no es controlable por ser  $B_{21} = \begin{pmatrix} 0 & 0 \end{pmatrix}$ ; sin embargo,

$$\text{rg} \begin{pmatrix} -B_{21}C_1 & B_{21}D_1 + B_{22} \\ A_2 - A_1 & B_1 \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & \alpha & \alpha \\ 1 & 1 & 1 \end{pmatrix} = 2,$$

por lo que se verifica la condición (b) del teorema 3.22.

Observemos que además, el par  $(A_1, B_1)$  claramente es controlable, de modo que también se verifica la condición (a) del teorema 3.22. Así, podemos concluir que el par  $(A, B)$  del código SCC es controlable, siendo

$$A = \begin{pmatrix} \alpha^3 & 0 \\ 0 & \alpha \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} \alpha & \alpha^2 \\ 1 & \alpha \end{pmatrix}. \quad \blacksquare$$

**Observación 3.17:** Si bien la condición (b) del teorema 3.22 no implica necesariamente que el par  $(A_2, B_{21})$  sea controlable, sí se deduce que el par  $(A_2, B_2)$  es controlable, ya que de lo contrario, por ser  $\delta_2 = 1$ , la matriz  $B_2$  sería nula y no se verificaría la condición (b).  $\blacksquare$

**Observación 3.18:** Si en el teorema 3.22 no exigimos la controlabilidad de  $(A_1, B_1)$ , entonces la matriz  $B_1$  ha de ser necesariamente nula, de donde

$$\text{rg} \begin{pmatrix} A_1 I - A_2 & B \end{pmatrix} = \text{rg} \begin{pmatrix} A_1 - A_2 & -B_{21}C_1 & B_{21}D_1 + B_{22} \\ O & O & O \end{pmatrix} \leq \delta_2 < 2$$

y por tanto, el par  $(A, B)$  no sería controlable.  $\blacksquare$

Si en el teorema 3.22 no exigimos la condición (b), el par  $(A, B)$  puede no ser controlable, como ponemos de manifiesto en el ejemplo siguiente.

**Ejemplo 3.17:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y sea  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  el  $(2, 1, 1)$ -código descrito por las matrices

$$A_1 = \begin{pmatrix} 1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} \alpha^2 \end{pmatrix}, \quad C_1 = \begin{pmatrix} \alpha^6 \end{pmatrix} \quad \text{y} \quad D_1 = \begin{pmatrix} 1 \end{pmatrix}.$$

Entonces, el par  $(A_1, B_1)$  es controlable.

Consideremos ahora  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, 2, 1)$ -código, con

$$A_2 = \begin{pmatrix} \alpha^3 \end{pmatrix} \quad \text{y} \quad B_2 = \begin{pmatrix} \alpha & 0 \end{pmatrix},$$

siendo  $C_2$  y  $D_2$  matrices arbitrarias de tamaños  $(n-2) \times 1$  y  $(n-2) \times 2$ , respectivamente, tales que  $(A_2, C_2)$  es observable (por ejemplo, basta tomar  $C_2 = \begin{pmatrix} 1 \end{pmatrix}$ ).

Aplicando entonces los teoremas 3.15 y 3.17, las matrices  $A$  y  $B$  para el código concatenado  $\text{SCC}(A, B, C, D)$  vienen dadas por

$$A = \begin{pmatrix} \alpha^3 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} \alpha \\ \alpha^2 \end{pmatrix}.$$

Observemos que

$$\operatorname{rg} \begin{pmatrix} -B_{21}C_1 & B_{21}D_1 + B_{22} \\ A_2 - A_1 & B_1 \end{pmatrix} = \operatorname{rg} \begin{pmatrix} 1 & \alpha \\ \alpha & \alpha^2 \end{pmatrix} = 1 < 2,$$

luego no se verifica la condición (b) del teorema 3.22. Además,

$$\operatorname{rg} \begin{pmatrix} \alpha^3 I - A & B \end{pmatrix} = \operatorname{rg} \begin{pmatrix} 0 & 1 & \alpha \\ 0 & \alpha & \alpha^2 \end{pmatrix} = 1 < 2 = \delta_1 + \delta_2$$

y por tanto, el par  $(A, B)$  no es controlable. ■

Como consecuencia del teorema 3.22, obtenemos el resultado siguiente para el caso particular en que las matrices  $A_1$  y  $A_2$  sean iguales.

**Corolario 3.8:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, m, 1)$ -código y que  $\operatorname{SCC}(A, B, C, D)$  es el código concatenado correspondiente. Supongamos que también se verifican las condiciones siguientes:*

- (a)  $A_1 = A_2$ .
- (b) *El par  $(A_1, B_1)$  es controlable.*
- (c)  $B_{21}C_1 \neq O$ .

*Entonces  $(A, B, C, D)$  es una representación minimal del código concatenado  $\operatorname{SCC}$  con complejidad  $\delta_1 + \delta_2 = 2$ .*

**Observación 3.19:** Notemos que la condición (c) del corolario 3.8 implica, en particular, que  $(A_2, B_{21})$  es controlable (y por tanto,  $(A_2, B_2)$  también lo es, por ser  $\delta_2 = 1$ ) y  $(A_1, C_1)$  es observable, ya que de lo contrario, al ser  $\delta_1 = \delta_2 = 1$ , alguna de las matrices  $B_{21}$  o  $C_1$  (o bien ambas), sería nula y no se verificaría (c). ■

Observemos que si en el corolario 3.8 el código externo tiene tasa  $k/(k+1)$ , entonces las matrices  $B_{21}$  y  $C_1$  son escalares, con lo que  $B_{21}C_1 = O$  si y sólo si alguna de ellas es nula. Basta entonces con exigir la controlabilidad de  $(A_2, B_{21})$  y la observabilidad de  $(A_1, C_1)$  para que la condición (c) del corolario 3.8 se verifique. Obtenemos entonces el resultado siguiente.

**Corolario 3.9:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(k + 1, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, k + 1, 1)$ -código y que  $\mathcal{S}\mathcal{C}\mathcal{C}$  es el código concatenado correspondiente. Supongamos que también se verifican las condiciones siguientes:*

- (a)  $A_1 = A_2$ .
- (b) *El par  $(A_1, B_1)$  es controlable.*
- (c) *El par  $(A_2, B_{21})$  es controlable.*
- (d) *El par  $(A_1, C_1)$  es observable.*

*Entonces  $(A, B, C, D)$  es una representación minimal del código concatenado  $\mathcal{S}\mathcal{C}\mathcal{C}$  con complejidad  $\delta_1 + \delta_2 = 2$ .*

Aunque tal y como hemos puesto de manifiesto en el ejemplo 3.15, la controlabilidad de los pares  $(A_1, B_1)$  y  $(A_2, B_2)$  de los códigos externo e interno, respectivamente, no implicaba la controlabilidad del par  $(A, B)$  de la concatenación  $\mathcal{S}\mathcal{C}\mathcal{C}$ , en el caso particular en que el código externo tenga tasa  $1/2$  y todos los valores propios de  $A_2$  sean valores propios de  $A_1$  (es decir,  $\sigma(A_2) \subseteq \sigma(A_1)$ ), es suficiente con que  $(A_1, B_1)$  y  $(A_2, B_{21})$  sean controlables, que todos los elementos de la matriz  $B_{21}$  sean no nulos y  $(A_1, C_1)$  sea observable para que  $(A, B, C, D)$  sea una representación entrada-estado-salida minimal de  $\mathcal{S}\mathcal{C}\mathcal{C}$ , como ponemos de manifiesto en el resultado siguiente. La demostración es análoga a la del teorema 3.8, cambiando  $B_2$  y  $D_2$  por  $B_{21}$  y  $D_{21}$ , respectivamente.

**Teorema 3.23:** *Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(2, 1, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, 2, \delta_2)$ -código y  $\mathcal{S}\mathcal{C}\mathcal{C}(A, B, C, D)$  el código concatenado correspondiente. Supongamos que se verifican las condiciones siguientes:*

- (a)  $\sigma(A_2) \subseteq \sigma(A_1)$ .
- (b) *El par  $(A_1, B_1)$  es controlable.*
- (c) *El par  $(A_2, B_{21})$  es controlable.*
- (d) *Todos los elementos de la matriz  $B_{21}$  son no nulos.*
- (e) *El par  $(A_1, C_1)$  es observable.*

*Entonces,  $(A, B, C, D)$  es una representación minimal del código concatenado  $\mathcal{S}\mathcal{C}\mathcal{C}$  con complejidad  $\delta_1 + \delta_2$ .*

Si en el teorema 3.23 no exigimos la controlabilidad del par  $(A_2, B_{21})$ , entonces la representación del código concatenado  $\mathcal{S}\mathcal{C}\mathcal{C}$  puede no ser minimal aunque  $(A_2, B_2)$  sea

controlable, tal y como vemos en el ejemplo siguiente.

**Ejemplo 3.18:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y consideremos el  $(3, 2, 2)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  descrito por las matrices

$$A_1 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^2 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad C_1 = (\alpha^4 \quad \alpha^3) \quad \text{y} \quad D_1 = (1 \quad \alpha).$$

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(4, 3, 2)$ -código, siendo

$$A_2 = \begin{pmatrix} \alpha^4 & 1 \\ \alpha^3 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 0 & \alpha^5 \\ \alpha & 1 & \alpha^6 \end{pmatrix},$$

y  $C_2$  y  $D_2$  matrices arbitrarias de tamaños  $1 \times 2$  y  $1 \times 3$ , respectivamente.

Para todo  $z \in \overline{\mathbb{F}}$  tenemos entonces que

$$\text{rg} \begin{pmatrix} zI_{\delta_1} - A_1 & B_1 \end{pmatrix} = \text{rg} \begin{pmatrix} z + \alpha & 0 & 1 & 0 \\ 0 & z + \alpha^2 & 0 & 1 \end{pmatrix} = 2,$$

$$\text{rg} \begin{pmatrix} zI_{\delta_1} - A_1 \\ C_1 \end{pmatrix} = \text{rg} \begin{pmatrix} z + \alpha & 0 \\ 0 & z + \alpha^2 \\ \alpha^4 & \alpha^3 \end{pmatrix} = 2,$$

$$\text{rg} \begin{pmatrix} zI_{\delta_2} - A_2 & B_2 \end{pmatrix} = \text{rg} \begin{pmatrix} z + \alpha^4 & 1 & 1 & 0 & \alpha^5 \\ \alpha^3 & z & \alpha & 1 & \alpha^6 \end{pmatrix} = 2$$

y, por tanto, los pares  $(A_1, B_1)$  y  $(A_2, B_2)$  son controlables y  $(A_1, C_1)$  es observable. Además,  $\sigma(A_2) = \{\alpha, \alpha^2\} = \sigma(A_1)$  y todos los elementos de la matriz  $B_{21}$  son no nulos, luego se verifican las condiciones (a), (b), (d) y (e) del teorema 3.23. Sin embargo, el par  $(A_2, B_{21}) = \left( \begin{pmatrix} \alpha^4 & 1 \\ \alpha^3 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ \alpha \end{pmatrix} \right)$  no es controlable, ya que

$$\text{rg} \begin{pmatrix} \alpha I - A_2 & B_{21} \end{pmatrix} = \text{rg} \begin{pmatrix} \alpha + \alpha^4 & 1 & 1 \\ \alpha^3 & \alpha & \alpha \end{pmatrix} = \text{rg} \begin{pmatrix} \alpha^2 & 1 & 1 \\ \alpha^3 & \alpha & \alpha \end{pmatrix} = 1 \neq 2.$$

Por otro lado, aplicando los teoremas 3.15 y 3.17, tenemos que las matrices  $A$  y  $B$

para la representación entrada-estado-salida del código concatenado  $\mathcal{S}\mathcal{C}\mathcal{C}$  son

$$A = \begin{pmatrix} \alpha^4 & 1 & \alpha^4 & \alpha^3 \\ \alpha^3 & 0 & \alpha^5 & \alpha^4 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha^2 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & \alpha^6 \\ \alpha^3 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Entonces, el par  $(A, B)$  no es controlable, ya que

$$\text{rg} \begin{pmatrix} \alpha I - A & B \end{pmatrix} = \text{rg} \begin{pmatrix} \alpha^2 & 1 & \alpha^4 & \alpha^3 & 1 & \alpha^6 \\ \alpha^3 & \alpha & \alpha^5 & \alpha^4 & \alpha^3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \alpha^4 & 0 & 1 \end{pmatrix} = 3 \neq 4. \quad \blacksquare$$

Si en el teorema 3.23 no exigimos la observabilidad del par  $(A_1, C_1)$ , entonces la representación del código concatenado  $\mathcal{S}\mathcal{C}\mathcal{C}$  puede no ser minimal aunque  $\sigma(A_2) \subseteq \sigma(A_1)$  y tanto  $(A_1, B_1)$  como  $(A_2, B_{21})$  sean controlables y, tal y como ponemos de manifiesto en el ejemplo siguiente.

**Ejemplo 3.19:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y consideremos el  $(3, 2, 2)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , siendo  $A_1$ ,  $B_1$  y  $D_1$  las matrices del código externo del ejemplo 3.18 y  $C_1 = \begin{pmatrix} 0 & 0 \end{pmatrix}$ . Claramente, el par  $(A_1, C_1)$  no es observable, pues

$$\text{rg} \begin{pmatrix} \alpha I - A_1 \\ C_1 \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & 0 \\ 0 & \alpha^4 \\ 0 & 0 \end{pmatrix} = 1 \neq 2.$$

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(4, 3, 2)$ -código, siendo  $A_2$  la matriz del código interno del ejemplo 3.18,

$$B_2 = \begin{pmatrix} B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \end{pmatrix}$$

y  $C_2$  y  $D_2$  matrices arbitrarias de tamaños  $1 \times 2$  y  $1 \times 3$ , respectivamente. Observemos que los valores propios de  $A_2$  son  $\lambda = \alpha$  y  $\lambda = \alpha^2$ , luego  $\sigma(A_2) \subseteq \sigma(A_1)$  y el par  $(A_2, B_{21})$  es controlable, ya que

$$\text{rg} \begin{pmatrix} \alpha I - A_2 & B_{21} \end{pmatrix} = \text{rg} \begin{pmatrix} \alpha^2 & 1 & 1 \\ \alpha^3 & \alpha & 0 \end{pmatrix} = 2 = \delta_2,$$

$$\operatorname{rg} \begin{pmatrix} \alpha^2 I - A_2 & B_{21} \end{pmatrix} = \operatorname{rg} \begin{pmatrix} \alpha & 1 & 1 \\ \alpha^3 & \alpha^2 & 0 \end{pmatrix} = 2 = \delta_2.$$

Por otro lado, teniendo en cuenta los teoremas 3.15 y 3.17, tenemos que las matrices  $A$  y  $B$  para la representación entrada-estado-salida del código concatenado  $\mathcal{SCC}$  son

$$A = \begin{pmatrix} \alpha^4 & 1 & 0 & 0 \\ \alpha^3 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha^2 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

pero como

$$\operatorname{rg} \begin{pmatrix} \alpha I - A & B \end{pmatrix} = \operatorname{rg} \begin{pmatrix} \alpha^2 & 1 & 0 & 0 & 1 & 0 \\ \alpha^3 & \alpha & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \alpha^4 & 0 & 1 \end{pmatrix} = 3 < 4,$$

el par  $(A, B)$  no es controlable. ■

El teorema 3.23 no es válido para el caso en que  $\sigma(A_2) \not\subseteq \sigma(A_1)$ , como mostramos en el ejemplo siguiente.

**Ejemplo 3.20:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$ . Consideremos el  $(2, 1, 1)$ -código  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  descrito por las matrices

$$A_1 = \begin{pmatrix} \alpha^2 \\ \alpha \end{pmatrix}, \quad B_1 = \begin{pmatrix} \alpha \end{pmatrix}, \quad C_1 = \begin{pmatrix} 1 \end{pmatrix} \quad \text{y} \quad D_1 = \begin{pmatrix} \alpha \end{pmatrix}.$$

Consideremos un  $(3, 2, 1)$ -código interno  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$ , descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^2 & 0 \\ 1 & \alpha^6 \end{pmatrix}, \quad B_2 = \begin{pmatrix} B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 1 & 0 \end{pmatrix},$$

siendo  $C_2$  y  $D_2$  matrices arbitrarias de tamaños  $1 \times 2$  y  $1 \times 1$ , respectivamente. Observemos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es el código externo del ejemplo 3.4 y las matrices  $A_2$  y  $B_{21}$  son las matrices  $A_2$  y  $B_2$  del código interno del ejemplo 3.4. Así pues,  $(A_l, B_l)$  es controlable, para  $l = 1, 2$  y  $(A_1, C_1)$  es observable.

Por otro lado, aplicando los teoremas 3.15 y 3.17, las matrices  $A$  y  $B$  de la representación entrada-estado-salida del código concatenado  $\mathcal{SCC}$  son

$$A = \begin{pmatrix} \alpha^2 & 0 & \alpha \\ 1 & \alpha^6 & 1 \\ 0 & 0 & \alpha^2 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} \alpha^2 \\ \alpha \\ \alpha \end{pmatrix}.$$

Dichas matrices coinciden con las matrices correspondientes del código concatenado  $\mathcal{SCC}_{\text{sys}}$  del ejemplo 3.4, y tal y como vimos en dicho ejemplo, el par  $(A, B)$  no es controlable. ■

### 3.3.3 Observabilidad

En esta sección, estudiamos las condiciones que deben cumplir las matrices que describen los códigos externo e interno para que el par  $(A, C)$  de los códigos concatenados  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$  sea observable y, por tanto, que la matriz generadora inducida por la realización  $(A, B, C, D)$  sea no catastrófica. Si bien las matrices  $A$  y  $B$  de los códigos  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$  tienen la misma expresión, no tenemos lo mismo para la matriz  $C$  (véanse las expresiones (3.25) y (3.31)), por lo que tendremos resultados diferentes para obtener la observabilidad de cada modelo.

Empezamos la sección con resultados correspondientes a la observabilidad del par  $(A, C)$  del modelo  $\mathcal{SC}^{(3)}$ . El ejemplo siguiente muestra que no es suficiente con que el par  $(A_l, C_l)$ , para  $l = 1, 2$ , de los códigos constituyentes sea observable, para que el par  $(A, C)$  del código concatenado  $\mathcal{SC}^{(3)}$  sea observable.

**Ejemplo 3.21:** Sea  $\alpha$  un elemento primitivo del cuerpo de Galois  $\mathbb{F} = GF(8)$ . Consideremos el  $(6, 4, 2)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , siendo

$$A_1 = \begin{pmatrix} \alpha^5 & \alpha \\ \alpha^3 & \alpha^5 \end{pmatrix}, \quad B_1 = \begin{pmatrix} \alpha^2 & \alpha & \alpha^4 & \alpha^5 \\ \alpha^4 & \alpha^3 & \alpha^5 & \alpha^6 \end{pmatrix},$$

$$C_1 = \begin{pmatrix} \alpha^2 & 1 \\ 1 & \alpha \end{pmatrix}, \quad D_1 = \begin{pmatrix} 1 & \alpha & 0 & 1 \\ \alpha & 0 & \alpha^2 & \alpha^3 \end{pmatrix}.$$

Observemos que  $(A_1, B_1)$  es controlable y  $(A_1, C_1)$  es observable.

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(9, 6, 1)$ -código interno descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} \alpha^2 & 1 & \alpha^2 & \alpha & \alpha^6 & \alpha^6 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 0 \\ \alpha \\ 0 \end{pmatrix}, \quad D_{21} = \begin{pmatrix} \alpha^6 & \alpha^4 \\ \alpha^4 & \alpha^4 \\ 1 & \alpha^5 \end{pmatrix},$$

siendo  $D_{22}$  una matriz arbitraria de tamaño  $3 \times 4$ .

Observemos que el código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$  son el código externo y el código interno, respectivamente, del ejemplo 3.15. Claramente, el par  $(A_2, C_2)$  es observable.

Por otro lado, aplicando el teorema 3.15, las matrices  $A$  y  $C$  de la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(3)}$  son

$$A = \begin{pmatrix} \alpha^3 & \alpha^5 & \alpha^4 \\ 0 & \alpha^5 & \alpha \\ 0 & \alpha^3 & \alpha^5 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} 0 & \alpha^2 & \alpha \\ \alpha & \alpha^3 & 1 \\ 0 & \alpha^3 & \alpha^2 \end{pmatrix}.$$

Tenemos entonces que el par  $(A, C)$  no es observable, ya que

$$\text{rg} \begin{pmatrix} \alpha^3 I - A \\ C \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & \alpha^5 & \alpha^4 \\ 0 & \alpha^2 & \alpha \\ 0 & \alpha^3 & \alpha^2 \\ 0 & \alpha^2 & \alpha \\ \alpha & \alpha^3 & 1 \\ 0 & \alpha^3 & \alpha^2 \end{pmatrix} = 2 \neq 3$$

Por tanto, necesitamos más condiciones sobre las matrices  $(A_l, B_l, C_l, D_l)$ , para  $l = 1, 2$ , que describen los códigos externo e interno para obtener la observabilidad del par  $(A, C)$  del código  $\mathcal{SC}^{(3)}$ . El teorema siguiente muestra que es suficiente con que la matriz  $C$  tenga rango completo por columnas, para que  $(A, C)$  sea observable. La demostración es análoga a la del teorema 3.9.

**Teorema 3.24:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m, \delta_2)$ -código y  $\mathcal{SC}^{(3)}(A, B, C, D)$  el código concatenado de tasa  $k/(n - m + k)$  descrito por las matrices dadas por la expresión (3.25). Si  $\text{rg}(C) = \delta_1 + \delta_2$ , entonces el par  $(A, C)$  es observable.

**Observación 3.20:** Notemos que la condición  $\text{rg}(C) = \delta_1 + \delta_2$  del teorema 3.24 implica que el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$  (véase la observación 3.8). ■

**Observación 3.21:** El ejemplo 3.21 muestra también que el recíproco de la observación 3.20 no es cierto en general, ya que el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ , y sin embargo,  $\text{rg}(C) = 2 \neq 2 + 1 = \delta_1 + \delta_2$ . ■

Como consecuencia del teorema 1.11, tenemos que las condiciones dadas en los teoremas 3.19 y 3.24, hacen que el código concatenado  $\mathcal{SC}^{(3)}$  sea un código observable.

**Corolario 3.10:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m, \delta_2)$ -código y  $\mathcal{SC}^{(3)}(A, B, C, D)$  el código concatenado de tasa  $k/(n - m + k)$  que describen las matrices dadas por la expresión (3.25). Si  $\text{rg}(B) = \delta_1 + \delta_2 = \text{rg}(C)$ , entonces  $(A, B, C, D)$  es una representación minimal para el código observable  $\mathcal{SC}^{(3)}$  con complejidad  $\delta_1 + \delta_2$ .

**Observación 3.22:** De las condiciones del corolario anterior, tenemos que

$$2 \leq \delta_1 + \delta_2 \leq \min\{k, n - m\}.$$

Así pues, para aplicar el corolario 3.10, debemos considerar códigos para los que  $k \geq 2$  y  $n - m \geq 2$ . ■

Ahora bien, si el código interno tiene complejidad  $\delta_2 = 1$ , tenemos el siguiente resultado, cuya demostración es análoga a la del teorema 3.10, cambiando  $B_2$  por  $B_{21}$  y  $D_2$  por  $D_{21}$ .

**Teorema 3.25:** Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(2, 1, \delta_1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, 2, 1)$ -código y que  $\mathcal{SC}^{(3)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n - m + k)$  descrito por las matrices dadas en (3.25). Supongamos también que se verifican las condiciones siguientes:

- (a)  $A_1$  es una matriz diagonal.
- (b) El par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .
- (c) Todos los elementos de la matriz  $C_1$  son no nulos.
- (d)  $\text{rg} \begin{pmatrix} \lambda I - A_2 & -B_{21} \\ C_2 & D_{21} \end{pmatrix} = 2$  para todo  $\lambda$  valor propio de  $A$ .

Entonces, el par  $(A, C)$  es observable.

**Observación 3.23:** Notemos que con las condiciones dadas en el teorema anterior, la matriz  $A_2 = \begin{pmatrix} a_2 \end{pmatrix}$  es una matriz escalar y  $\lambda = a_2$  es un valor propio de la matriz  $A$ ; por tanto, en este caso, la condición (d) se reduce a

$$\text{rg} \begin{pmatrix} O & -B_{21} \\ C_2 & D_{21} \end{pmatrix} = 2,$$

de donde se deduce, en particular, que alguna componente de  $B_{21}$  debe ser no nula y, por tanto, el par  $(A_2, B_{21})$  es controlable, por ser  $\delta_2 = 1$ . En particular, de nuevo por ser  $\delta_2 = 1$ , el par  $(A_2, B_2)$  es también controlable. ■

El teorema siguiente proporciona condiciones suficientes para que el par  $(A, C)$  del código concatenado  $\mathcal{SC}^{(3)}$  sea observable en el caso particular en que  $\delta_1 = \delta_2 = 1$ , siendo  $k$  cualquier número natural. La demostración es similar a la demostración del teorema 3.11, cambiando las matrices  $B_2$  y  $D_2$  por  $B_{21}$  y  $D_{21}$ , respectivamente.

**Teorema 3.26:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, m, 1)$ -código y que  $\mathcal{SC}^{(3)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n - m + k)$  descrito por las matrices dadas en (3.25). Supongamos que también se verifican las condiciones siguientes:*

- (a) *El par  $(A_2, C_2)$  es observable.*
- (b) *La matriz  $\begin{pmatrix} A_1 - A_2 & -B_{21}C_1 \\ C_2 & D_{21}C_1 \end{pmatrix}$ , de tamaño  $(n - m + 1) \times 2$ , tiene rango 2.*

*Entonces el par  $(A, C)$  es observable.*

**Observación 3.24:** Notemos que la condición (b) del teorema anterior, implica en particular que el par  $(A_1, C_1)$  es observable, por ser  $\delta_1 = 1$ . ■

Como consecuencia del teorema anterior, obtenemos un resultado similar al corolario 3.4 para el caso particular en que las matrices  $A_1$  y  $A_2$  sean iguales.

**Corolario 3.11:** *Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(m, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, m, 1)$ -código y que  $\mathcal{SC}^{(3)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n - m + k)$  descrito por las matrices dadas en (3.25). Supongamos que también se verifican las condiciones siguientes:*

- (a)  $A_1 = A_2$ .

(b) El par  $(A_2, C_2)$  es observable.

(c)  $B_{21}C_1 \neq O$ .

Entonces el par  $(A, C)$  es observable.

Observemos que si en el corolario 3.11 el código externo tiene tasa  $k/(k+1)$ , entonces las matrices  $B_{21}$  y  $C_1$  son escalares, con lo que  $B_{21}C_1 = O$  si y sólo si alguno de ellas es nula; basta entonces con exigir la controlabilidad de  $(A_2, B_{21})$  y la observabilidad de  $(A_1, C_1)$  para que la condición (c) del corolario 3.11 se verifique. Obtenemos entonces el resultado siguiente.

**Corolario 3.12:** Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(k+1, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, k+1, 1)$ -código y que  $\mathcal{SC}^{(3)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n-m+k)$  descrito por las matrices dadas en (3.25). Supongamos que también se verifican las condiciones siguientes:

(a)  $A_1 = A_2$ .

(b) El par  $(A_2, B_{21})$  es controlable.

(c) El par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .

Entonces el par  $(A, C)$  es observable.

Como consecuencia entonces de los corolarios 3.8 y 3.12, obtenemos el resultado siguiente, que proporciona la observabilidad del código  $\mathcal{SC}^{(3)}$  para el caso particular en que las matrices  $A_1$  y  $A_2$  sean iguales, los códigos externo e interno tengan complejidad  $\delta_1 = \delta_2 = 1$  y el código externo tenga tasa  $k/(k+1)$ .

**Corolario 3.13:** Supongamos que  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  es un  $(k+1, k, 1)$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n, k+1, 1)$ -código y que  $\mathcal{SC}^{(3)}(A, B, C, D)$  es el código concatenado de tasa  $k/(n-m+k)$  descrito por las matrices dadas en (3.25). Supongamos que también se verifican las condiciones siguientes:

(a)  $A_1 = A_2$ .

(b) El par  $(A_1, B_1)$  es controlable.

(c) El par  $(A_2, B_{21})$  es controlable.

(d) El par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .

Entonces  $(A, B, C, D)$  es una representación minimal para el  $(n-1, k, 2)$ -código observable  $\mathcal{SC}^{(3)}$  con complejidad  $\delta_1 + \delta_2 = 2$ .

Si bien la observabilidad de  $(A_l, C_l)$ , para  $l = 1, 2$  no implica la observabilidad del par  $(A, C)$  de  $\mathcal{SC}^{(3)}$  (véase el ejemplo 3.21), en el caso particular en que el código externo tenga tasa  $1/2$  y todos los valores propios de la matriz  $A_1$  sean valores propios de la matriz  $A_2$  (es decir,  $\sigma(A_1) \subseteq \sigma(A_2)$ ), es suficiente con exigir que todos los elementos de la matriz  $C_1$  sean no nulos así como la observabilidad de  $(A_l, C_l)$ , para  $l = 1, 2$  y la controlabilidad  $(A_2, B_{21})$  para que  $(A, C)$  sea observable, como ponemos de manifiesto en el resultado siguiente, cuya demostración es análoga a la del teorema 3.12, cambiando  $B_2$  por  $B_{21}$ .

**Teorema 3.27:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(2, 1, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, 2, \delta_2)$ -código y  $\mathcal{SC}^{(3)}(A, B, C, D)$  el código concatenado descrito por las matrices dadas en (3.25). Supongamos que se verifican las condiciones siguientes:

- (a)  $\sigma(A_1) \subseteq \sigma(A_2)$ .
- (b) El par  $(A_2, B_{21})$  es controlable.
- (c) El par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .
- (d) Todos los elementos de la matriz  $C_1$  son no nulos.

Entonces, el par  $(A, C)$  es observable.

Si en el teorema 3.27 no imponemos la condición de observabilidad de alguno de los pares  $(A_l, C_l)$ , para  $l = 1, 2$ , entonces el par  $(A, C)$  de la concatenación puede no ser observable, aunque  $\sigma(A_1) \subseteq \sigma(A_2)$  y  $(A_2, B_{21})$  sea controlable, como ponemos de manifiesto en el ejemplo siguiente.

**Ejemplo 3.22:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y consideremos el  $(2, 1, 2)$ -código  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  descrito por las matrices

$$A_1 = \begin{pmatrix} \alpha^2 & 0 \\ 0 & \alpha^4 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 0 & 0 \end{pmatrix} \quad \text{y} \quad D_1 = \begin{pmatrix} \alpha^5 \end{pmatrix}.$$

Observemos, que  $\mathcal{C}_o$  es el código externo del ejemplo 3.3. Entonces, el par  $(A_1, C_1)$  no es observable.

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(3, 2, 2)$ -código descrito por la matriz

$$A_2 = \begin{pmatrix} \alpha^6 & 1 \\ \alpha^3 & \alpha^5 \end{pmatrix}$$

y matrices  $B_2, C_2$  y  $D_2$  arbitrarias de tamaños  $2 \times 2, 1 \times 2$  y  $1 \times 2$ , respectivamente, tales

que  $(A_2, B_{21})$  es controlable (por ejemplo, basta tomar  $B_{21} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ). Por comodidad, sea  $C_2 = \begin{pmatrix} a & b \end{pmatrix}$ , con  $a$  y  $b$  escalares arbitrarios. Observemos que

$$\sigma(A_1) = \{\alpha^2, \alpha^4\} \subseteq \sigma(A_2).$$

Aplicando el teorema 3.15, las matrices  $A$  y  $C$  de la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(3)}$  son

$$A = \begin{pmatrix} \alpha^6 & 1 & 0 & 0 \\ \alpha^3 & \alpha^5 & 0 & 0 \\ 0 & 0 & \alpha^2 & 0 \\ 0 & 0 & 0 & \alpha^4 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} a & b & 0 & 0 \end{pmatrix},$$

de donde obtenemos que el par  $(A, C)$  no es observable, ya que

$$\text{rg} \begin{pmatrix} \alpha^4 I - A \\ C \end{pmatrix} = \text{rg} \begin{pmatrix} \alpha^3 & 1 & 0 & 0 \\ \alpha^3 & 1 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 \\ a & b & 0 & 0 \end{pmatrix} \leq 3 < 4. \quad \blacksquare$$

Del mismo modo, si en el teorema 3.27 no exigimos la controlabilidad del par  $(A_2, B_{21})$ , entonces la representación del código concatenado  $\mathcal{CC}^{(3)}$  puede no ser minimal aunque  $\sigma(A_1) \subseteq \sigma(A_2)$  y  $(A_l, C_l)$  sea observable, para  $l = 1, 2$ , tal y como ponemos de manifiesto en el ejemplo siguiente.

**Ejemplo 3.23:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y consideremos un  $(2, 1, 1)$ -código  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , siendo

$$A_1 = \begin{pmatrix} \alpha^3 \end{pmatrix} \quad \text{y} \quad C_1 = \begin{pmatrix} \alpha \end{pmatrix}$$

y  $B_1$  y  $D_1$  matrices arbitrarias de tamaño  $1 \times 1$ , de manera que  $(A_1, B_1)$  sea controlable (basta tomar, por ejemplo,  $B_1 = \begin{pmatrix} 1 \end{pmatrix}$ ).

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(3, 1, 3)$ -código descrito por las matrices

$$A_2 = \begin{pmatrix} 1 & 0 & 0 \\ \alpha & \alpha^3 & 0 \\ \alpha^2 & 0 & \alpha^6 \end{pmatrix}, \quad B_2 = \begin{pmatrix} B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$C_2 = \begin{pmatrix} 1 & 0 & \alpha^3 \\ 1 & 1 & \alpha^3 \end{pmatrix} \quad D_{21} = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

siendo  $D_{22}$  una matriz arbitraria de tamaño  $1 \times 1$ .

Observemos que las matrices  $A_1$  y  $C_1$  son las mismas que las del código externo del ejemplo 3.7. Del mismo modo, el código descrito por las matrices  $(A_2, B_{21}, C_2, D_{21})$  es precisamente el código interno del ejemplo 3.7. Por tanto, tal y como vimos en dicho ejemplo, el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$  y el par  $(A_2, B_{21})$  no es controlable (observemos que  $(A_2, B_2)$  sí es controlable). Además,  $\sigma(A_1) = \{\alpha^3\} \subseteq \{1, \alpha^3, \alpha^6\} \subseteq \sigma(A_2)$ .

Ahora, por el teorema 3.15 las matrices  $A$  y  $C$  de la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(3)}$  son

$$A = \begin{pmatrix} 1 & 0 & 0 & \alpha \\ \alpha & \alpha^3 & 0 & \alpha \\ \alpha^2 & 0 & \alpha^6 & \alpha \\ 0 & 0 & 0 & \alpha^3 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} 1 & 0 & \alpha^3 & \alpha \\ 1 & 1 & \alpha^3 & \alpha \end{pmatrix}$$

que coinciden con las correspondientes matrices  $A$  y  $C$  del código  $\mathcal{SC}^{(4)}$  del ejemplo 3.7, de manera que tal y como vimos en dicho ejemplo, el par  $(A, C)$  no es observable. ■

El ejemplo siguiente muestra que el teorema 3.27 no es cierto para el caso en que  $\sigma(A_1) \not\subseteq \sigma(A_2)$ .

**Ejemplo 3.24:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$ . Consideremos un  $(2, 1, 2)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$ , siendo

$$A_1 = \begin{pmatrix} \alpha^4 & 1 \\ 0 & \alpha^3 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 1 & \alpha^2 \end{pmatrix},$$

y  $B_1$  y  $D_1$  matrices arbitrarias de tamaños  $2 \times 1$  y  $1 \times 1$ , respectivamente tales que el par  $(A_1, B_1)$  sea controlable (basta tomar, por ejemplo,  $B_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ).

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  el  $(3, 2, 1)$ -código interno descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^3 \end{pmatrix}, \quad B_{21} = \begin{pmatrix} \alpha \end{pmatrix} \quad C_2 = \begin{pmatrix} \alpha^6 \end{pmatrix} \quad \text{y} \quad D_{21} = \begin{pmatrix} \alpha \end{pmatrix},$$

siendo  $B_{22}$  y  $D_{22}$  matrices arbitrarias de tamaños  $1 \times 1$ . Observemos que las matrices  $A_1$  y  $C_1$  coinciden con las matrices del código externo del ejemplo 3.8; del mismo

modo, el código descrito por las matrices  $(A_2, B_{21}, C_2, D_{21})$  es el código interno del ejemplo 3.8. Tenemos entonces que  $(A_1, B_1)$  es controlable y  $(A_l, C_l)$  es observable, para  $l = 1, 2$ , luego se cumplen las condiciones (b) y (c) del teorema 3.27. Ahora bien,  $\sigma(A_1) = \{\alpha^4, \alpha^3\} \not\subseteq \{\alpha^3\} = \sigma(A_2)$ .

Por otro lado, aplicando el teorema 3.1, las matrices  $A$  y  $C$  de la representación entrada-estado-salida de código concatenado  $\mathcal{SC}^{(3)}$

$$A = \begin{pmatrix} \alpha^3 & \alpha & \alpha^3 \\ 0 & \alpha^4 & 1 \\ 0 & 0 & \alpha^3 \end{pmatrix} \quad \text{y} \quad C = (\alpha^6 \quad \alpha \quad \alpha^3)$$

coinciden con las matrices  $A$  y  $C$  del código  $\mathcal{SC}^{(1)}$  del ejemplo 3.8. Por tanto, tal y como mostrábamos en dicho ejemplo, el par  $(A, C)$  no es observable. ■

Ahora bien, para la observabilidad del par  $(A, C)$  de  $\mathcal{SC}^{(4)}$ , tenemos condiciones diferentes a las dadas para  $\mathcal{SC}^{(3)}$ . De hecho, recordemos que en el ejemplo 3.21 mostrábamos que aun siendo el par  $(A_l, C_l)$  observable, para  $l = 1, 2$ , las matrices del código  $\mathcal{SC}^{(3)}$  no necesariamente heredaban esta propiedad. Ahora bien, si consideramos la concatenación  $\mathcal{SC}^{(4)}$  con los mismos códigos externo e interno, obtenemos que, en este caso, el par  $(A, C)$  es observable, como ponemos de manifiesto en el ejemplo siguiente.

**Ejemplo 3.25:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$ . Consideremos el  $(6, 4, 2)$ -código externo  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  y el  $(9, 6, 1)$ -código interno  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  del ejemplo 3.21. Entonces, el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ .

Aplicando el teorema 3.17, las matrices  $A$  y  $C$  de la representación entrada-estado-salida del código concatenado  $\mathcal{SC}^{(4)}$  son

$$A = \begin{pmatrix} \alpha^3 & \alpha^5 & \alpha^4 \\ 0 & \alpha^5 & \alpha \\ 0 & \alpha^3 & \alpha^5 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} 0 & \alpha^2 & \alpha \\ \alpha & \alpha^3 & 1 \\ 0 & \alpha^3 & \alpha^2 \\ 0 & \alpha^2 & 1 \\ 0 & 1 & \alpha \end{pmatrix}$$

y, por tanto, al ser  $\text{rg}(C) = 3$ , el par  $(A, C)$  es observable. ■

Podemos generalizar el resultado del ejemplo anterior para cualquier código externo e interno que concatenemos según el modelo  $\mathcal{SC}^{(4)}$  de conexión en serie. Basta con exigir

la observabilidad de los pares  $(A_1, C_1)$  y  $(A_2, C_2)$  del código externo e interno, respectivamente, para obtener la observabilidad del par  $(A, C)$  del código  $\mathcal{SC}^{(4)}$ , tal y como mostramos en el teorema siguiente, cuya demostración es análoga a la demostración del teorema 3.13.

**Teorema 3.28:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m, \delta_2)$ -código y  $\mathcal{SC}^{(4)}(A, B, C, D)$  el código concatenado descrito por las matrices dadas por la expresión (3.31). Si el par  $(A_l, C_l)$  es observable para  $l = 1, 2$ , entonces el par  $(A, C)$  es observable.

Como consecuencia del teorema 1.11, tenemos que las condiciones dadas en los teoremas 3.19 y 3.28, hacen que el código concatenado  $\mathcal{SC}^{(4)}$  sea un código observable.

**Corolario 3.14:** Sean  $\mathcal{C}_o(A_1, B_1, C_1, D_1)$  un  $(m, k, \delta_1)$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, m, \delta_2)$ -código y  $\mathcal{SC}^{(4)}(A, B, C, D)$  el código concatenado descrito por las matrices dadas por la expresión (3.31). Supongamos que se verifican las condiciones siguientes:

- (a)  $\text{rg}(B) = \delta_1 + \delta_2$ ,
- (b) El par  $(A_l, C_l)$  es observable para  $l = 1, 2$ .

Entonces  $(A, B, C, D)$  es una representación minimal para el código observable  $\mathcal{SC}^{(4)}$  con complejidad  $\delta_1 + \delta_2$ .

### 3.3.4 Distancias columnas y distancias libres

En esta sección, estudiamos las distancias columnas y la distancia libres de la concatenación  $\mathcal{SC}^{(4)}$ . En el caso de la concatenación  $\mathcal{SC}^{(4)}$ , el hecho de que las palabras de los códigos externo e interno sean componentes de la palabra final de la concatenación, nos permitirá obtener una cota inferior de  $d_{free}(\mathcal{SC}^{(4)})$  en función de  $d_{free}(\mathcal{C}_o)$  y  $d_{free}(\mathcal{C}_i)$ . Comenzamos con un lema técnico que nos será de utilidad para el resultado principal de esta sección.

**Lema 3.3:** Sea  $\mathcal{SC}^{(4)}$  el código dado por el teorema 3.3 al concatenar el código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$ . Entonces

$$d_j^c(\mathcal{SC}^{(4)}) \geq \max \{d_j^c(\mathcal{C}_o), d_j^c(\mathcal{C}_i)\} \quad \text{para } j = 0, 1, 2, \dots \quad (3.34)$$

DEMOSTRACIÓN: Teniendo en cuenta las relaciones entre  $y_t, y_t^{(1)}, y_t^{(2)}, u_t, u_t^{(1)}, u_t^{(2)}$ , y  $v_t, v_t^{(1)}, v_t^{(2)}$  dadas por las expresiones (3.1) y (3.26)–(3.29), tenemos que

$$\begin{aligned} \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \\ &\geq \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}). \end{aligned}$$

Así pues, de la expresión de la distancia columna  $d_j^c(\mathcal{SC}^{(4)})$  en términos de la representación entrada-estado-salida dada por la relación (1.19), obtenemos que

$$\begin{aligned} d_j^c(\mathcal{SC}^{(4)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(1)} \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) \right\} \\ &= d_j^c(\mathcal{C}_o) \end{aligned} \tag{3.35}$$

ya que  $u_0 = u_0^{(1)}$ .

Análogamente, de las expresiones (3.1), (3.26) y (3.28), tenemos que:

$$\begin{aligned} \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \\ &= \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}). \end{aligned}$$

Ahora, de  $u_0^{(2)} = \begin{pmatrix} y_0^{(1)} \\ u_0^{(1)} \end{pmatrix}$  y teniendo en cuenta la expresión (1.19) tenemos que

$$\begin{aligned} d_j^c(\mathcal{SC}^{(4)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(2)} \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \right\} \\ &= d_j^c(\mathcal{C}_i). \end{aligned} \tag{3.36}$$

Así, obtenemos la desigualdad (3.34) de las desigualdades (3.35) y (3.36).  $\square$

**Observación 3.25:** Recordemos que, tal y como vimos en el ejemplo 3.10 y en el lema 3.2, necesitamos la condición adicional de rango completo por columnas de la matriz  $D_1$  para que la  $j$ -ésima distancia columna del código interno sea una cota inferior de la correspondiente distancia columna del código concatenado  $\mathcal{SC}^{(2)}$ . En el caso del código  $\mathcal{SC}^{(4)}$  no necesitamos dicha condición, ya que  $\mathcal{C}_i$  codifica toda la palabra del código externo  $\mathcal{C}_o$  y, por tanto, al evaluar el mínimo de los pesos para  $u_0^{(1)} \neq 0$ , estamos asegurando que la entrada  $u_0^{(2)}$  del código interno  $\mathcal{C}_i$  sea no nula, ya que  $u_0^{(2)} = v_0^{(1)} = \begin{pmatrix} y_0^{(1)} \\ u_0^{(1)} \end{pmatrix}$ . ■

Ahora bien, si  $\text{rg}(D_2) = m$ , entonces tenemos un refinamiento de la cota dada en el lema 3.3, como ponemos de manifiesto en el resultado siguiente.

**Lema 3.4:** Sea  $\mathcal{SC}^{(4)}$  el código dado por el teorema 3.3 al concatenar el código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$ . Si  $\text{rg}(D_2) = m$ , entonces

$$d_j^c(\mathcal{SC}^{(4)}) \geq \max \{d_j^c(\mathcal{C}_o) + 1, d_j^c(\mathcal{C}_i)\} \quad \text{para } j = 0, 1, 2, \dots \quad (3.37)$$

DEMOSTRACIÓN: Procediendo de forma análoga a la demostración del lema 3.3, tenemos que

$$\begin{aligned} \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \\ &\geq \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \text{wt}(y_0^{(2)}). \end{aligned}$$

Ahora, como  $y_0^{(2)} = D_2 u_0^{(2)}$  (por ser  $x_0 = 0$ ) y  $\text{rg}(D_2) = m$ , entonces  $y_0^{(2)} \neq 0$  si y sólo si  $u_0^{(2)} = v_0^{(1)} = \begin{pmatrix} y_0^{(1)} \\ u_0^{(1)} \end{pmatrix} \neq 0$ . Por tanto, de la expresión de la distancia columna  $d_j^c(\mathcal{SC}^{(4)})$  en términos de la representación entrada-estado-salida dada por la relación (1.19), obtenemos

$$\begin{aligned} d_j^c(\mathcal{SC}^{(4)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(1)} \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \text{wt}(y_0^{(2)}) \right\} \end{aligned}$$

$$\geq d_j^c(\mathcal{C}_o) + 1 \quad (3.38)$$

ya que  $u_0 = u_0^{(1)}$ .

Así, del lema 3.3 y de la desigualdad (3.38), obtenemos la desigualdad (3.37).  $\square$

Como consecuencia inmediata de los lemas anteriores y de la expresión de la distancia libre en términos de la representación entrada-estado-salida dada por la relación (1.5), obtenemos el resultado siguiente.

**Teorema 3.29:** *Sea  $\mathcal{SC}^{(4)}$  el código convolucional dado por el teorema 3.17 obtenido por concatenación del código externo  $\mathcal{C}_o$  y del código interno  $\mathcal{C}_i$ . Entonces,*

- (a)  $d_{free}(\mathcal{SC}^{(4)}) \geq \max \{d_{free}(\mathcal{C}_o), d_{free}(\mathcal{C}_i)\}$ .
- (b) *Si además,  $\text{rg}(D_2) = m$ , entonces  $d_{free}(\mathcal{SC}^{(4)}) \geq \max \{d_{free}(\mathcal{C}_o) + 1, d_{free}(\mathcal{C}_i)\}$ .*

### 3.3.5 Ejemplos

Como en los modelos  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$ , finalizamos la sección con ejemplos en los que analizamos las relaciones entre los modelos de concatenación  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ .

#### Ejemplos en $\mathbb{F} = GF(4)$

Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(4)$  (véase la sección 1.1), y consideremos el  $(3, 2, 1)$ -código  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  y el  $(4, 3, 1)$ -código  $\mathcal{C}_2(A_2, B_2, C_2, D_2)$  descritos por las matrices

$$\begin{aligned} A_1 &= \begin{pmatrix} \alpha^2 \\ 1 \end{pmatrix}, & B_1 &= \begin{pmatrix} 1 & \alpha \end{pmatrix}, & C_1 &= \begin{pmatrix} 1 \end{pmatrix}, & D_1 &= \begin{pmatrix} \alpha^2 & \alpha \end{pmatrix}, \\ A_2 &= \begin{pmatrix} 1 \end{pmatrix}, & B_2 &= \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}, & C_2 &= \begin{pmatrix} 1 \end{pmatrix}, & D_2 &= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}. \end{aligned}$$

Entonces, tanto  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  como  $\mathcal{C}_2(A_2, B_2, C_2, D_2)$  son códigos fuertemente MDS.

**Ejemplo 3.26:** En la tabla 3.7 hemos considerado como códigos externo e interno los códigos fuertemente MDS  $\mathcal{C}_1$  y  $\mathcal{C}_2$ , respectivamente. Aplicando entonces los teoremas 3.15, 3.17, 3.19, 3.26 y 3.28 tenemos que las realizaciones  $(A, B, C, D)$  son realizaciones minimales de los códigos observables  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ . Obtenemos que  $d_{free}(\mathcal{SC}^{(3)}) = 4$  y  $d_{free}(\mathcal{SC}^{(4)}) = 6$ , que distan una unidad de las cotas Singleton generalizadas para  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ , respectivamente. Por tanto, estos códigos concatenados no son MDS.

Concatenación de los códigos $\mathcal{C}_1$ y $\mathcal{C}_2$				
Modelo	Representación de SCC	$d_{free}(SCC_{sys})$	Código externo	Código interno
$SC^{(3)}$	$A = \begin{pmatrix} 1 & 1 \\ 0 & \alpha^2 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & \alpha \end{pmatrix},$ $C = \begin{pmatrix} 1 & 1 \end{pmatrix}, D = \begin{pmatrix} \alpha & \alpha^2 \end{pmatrix}$	$d_{free}(SC^{(3)}) = 4$ No MDS	$d_1^c(\mathcal{C}_1) = 3$ Fuertemente MDS	$d_1^c(\mathcal{C}_2) = 3$ Fuertemente MDS
$SC^{(4)}$	$A = \begin{pmatrix} 1 & 1 \\ 0 & \alpha^2 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & \alpha \end{pmatrix},$ $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, D = \begin{pmatrix} \alpha & \alpha^2 \\ \alpha^2 & \alpha \end{pmatrix}$	$d_{free}(SC^{(4)}) = 6$ No MDS		

Tabla 3.7: Códigos del ejemplo 3.26

Ejemplos en  $\mathbb{F} = GF(8)$ 

Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$ . Consideramos entonces el  $(2, 1, 1)$ -código  $\mathcal{C}_3(A_3, B_3, C_3, D_3)$ , y el  $(2, 1, 2)$ -código  $\mathcal{C}_4(A_4, B_4, C_4, D_4)$  descritos por las matrices

$$A_3 = \begin{pmatrix} \alpha \end{pmatrix}, \quad B_3 = \begin{pmatrix} 1 \end{pmatrix}, \quad C_3 = \begin{pmatrix} \alpha^4 \end{pmatrix}, \quad D_3 = \begin{pmatrix} 1 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^2 \end{pmatrix}, \quad B_4 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad C_4 = \begin{pmatrix} \alpha^5 & \alpha^2 \end{pmatrix}, \quad D_4 = \begin{pmatrix} 1 \end{pmatrix},$$

y consideremos también los  $(3, 2, 1)$ -códigos  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$ , para  $l = 5, 6$  descritos por las matrices

$$A_5 = \begin{pmatrix} \alpha^2 \end{pmatrix}, \quad B_5 = \begin{pmatrix} 1 & 1 \end{pmatrix}, \quad C_5 = \begin{pmatrix} 1 \end{pmatrix}, \quad D_5 = \begin{pmatrix} 1 & 1 \end{pmatrix},$$

$$A_6 = \begin{pmatrix} \alpha \end{pmatrix}, \quad B_6 = \begin{pmatrix} 1 & \alpha \end{pmatrix}, \quad C_6 = \begin{pmatrix} 1 \end{pmatrix}, \quad D_6 = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

Entonces, el código  $\mathcal{C}_3(A_3, B_3, C_3, D_3)$  corresponde a la construcción introducida por Smarandache y Rosenthal [102] y, por tanto, es un código convolucional fuertemente MDS. El código  $\mathcal{C}_6(A_6, B_6, C_6, D_6)$  es también fuertemente MDS, mientras que  $\mathcal{C}_4(A_4, B_4, C_4, D_4)$  es un código convolucional MDS (no fuertemente MDS) y  $\mathcal{C}_5(A_5, B_5, C_5, D_5)$  no es MDS.

Concatenación de los códigos $\mathcal{C}_3$ y $\mathcal{C}_5$				
Modelo	Representación de $\mathcal{SCC}$	$d_{free}(\mathcal{SCC}_{sys})$	Código externo	Código interno
$\mathcal{SC}^{(3)}$	$A = \begin{pmatrix} \alpha^2 & \alpha^4 \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} 1 & \alpha^4 \\ 0 & \alpha^4 \end{pmatrix}, D = \begin{pmatrix} 0 \end{pmatrix}$	$d_{free}(\mathcal{SC}^{(3)}) = 5$ No MDS	$d_2^c(\mathcal{C}_3) = 4$ Fuertemente MDS	$d_{free}(\mathcal{C}_5) = 2$ No MDS
$\mathcal{SC}^{(4)}$	$A = \begin{pmatrix} \alpha^2 & \alpha^4 \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} 1 & \alpha^4 \\ 0 & \alpha^4 \end{pmatrix}, D = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$d_{free}(\mathcal{SC}^{(4)}) = 7$ No MDS		

**Tabla 3.8:** Códigos del ejemplo 3.27

**Ejemplo 3.27:** Si consideramos como código externo el código fuertemente MDS  $\mathcal{C}_3$  y como código interno el código no MDS  $\mathcal{C}_5$  obtenemos los resultados que mostramos en la tabla 3.8. Teniendo en cuenta los teoremas 3.15, 3.17, 3.22, 3.26 y 3.28 obtenemos las representaciones minimales  $(A, B, C, D)$  de los códigos observables  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ . Además,  $d_{free}(\mathcal{SC}^{(3)}) = 5$  y  $d_{free}(\mathcal{SC}^{(4)}) = 7$ , siendo 6 y 9 las cotas Singleton generalizadas para  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ , respectivamente. Concluimos entonces que estos códigos concatenados no son MDS.

Ahora, si consideramos como código externo el código MDS  $\mathcal{C}_4$  y como código interno el código no MDS  $\mathcal{C}_5$ , obtenemos los resultados que mostramos en la tabla 3.9. Aplicamos los teoremas 3.15, 3.17, 3.23, 3.25 y 3.28 para obtener representaciones minimales de los códigos concatenados  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ , de manera que el par  $(A, C)$  de la concatenación correspondiente es observable. Además,

$$d_{free}(\mathcal{SC}^{(3)}) = 6 \quad \text{y} \quad d_{free}(\mathcal{SC}^{(4)}) = 11. \quad \blacksquare$$

Notemos que la cota Singleton para  $\mathcal{SC}^{(3)}$  es 8 mientras que la cota Singleton para  $\mathcal{SC}^{(4)}$  es 12. Por tanto, ninguno de estos códigos es MDS, si bien la distancia libre de  $\mathcal{SC}^{(4)}$  dista únicamente una unidad de la cota Singleton generalizada.

**Ejemplo 3.28:** Finalmente, consideramos como código externo e interno los códigos fuertemente MDS  $\mathcal{C}_3$  y  $\mathcal{C}_6$ , respectivamente. Teniendo en cuenta los teoremas 3.15, 3.17,

Concatenación de los códigos $\mathcal{C}_4$ y $\mathcal{C}_5$				
Modelo	Representación de SCC	$d_{free}(\text{SCC}_{\text{sys}})$	Código externo	Código interno
$\text{SC}^{(3)}$	$A = \begin{pmatrix} \alpha^2 & \alpha^5 & \alpha^2 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}, B = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} 1 & \alpha^5 & \alpha^2 \end{pmatrix}, D = \begin{pmatrix} 0 \end{pmatrix}$	$d_{free}(\text{SC}^{(3)}) = 6$ No MDS	$d_{free}(\mathcal{C}_4) = 6$ MDS	$d_{free}(\mathcal{C}_5) = 2$ No MDS
$\text{SC}^{(4)}$	$A = \begin{pmatrix} \alpha^2 & \alpha^5 & \alpha^2 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}, B = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} 1 & \alpha^5 & \alpha^2 \\ 0 & \alpha^5 & \alpha^2 \end{pmatrix}, D = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$d_{free}(\text{SC}^{(4)}) = 11$ No MDS		

Tabla 3.9: Códigos del ejemplo 3.27

y 3.28 así como los corolarios 3.8 y 3.11, obtenemos las representaciones minimales  $(A, B, C, D)$  de los códigos observables  $\text{SC}^{(3)}$  y  $\text{SC}^{(4)}$  que mostramos en la tabla 3.10. Además, tenemos que

$$d_{free}(\text{SC}^{(3)}) = 4 \quad \text{y} \quad d_{free}(\text{SC}^{(4)}) = 7, \quad \blacksquare$$

siendo en este caso, 6 y 9 las cotas Singleton generalizadas para  $\text{SC}^{(3)}$  y  $\text{SC}^{(4)}$ , respectivamente. Concluimos entonces que estos códigos concatenados no son MDS.

## 3.4 Conclusiones

En este capítulo hemos caracterizado cuatro modelos de concatenación en serie de dos códigos convolucionales desde el punto de vista de sistemas, introduciendo condiciones para que el código concatenado correspondiente sea no catastrófico, así como para tener una representación entrada-estado-salida minimal de éste.

Como hemos visto en los ejemplos de las subsecciones 3.2.5 y 3.3.5, la concatenación en serie de dos códigos fuertemente MDS puede no ser MDS (véanse las tablas 3.3, 3.7 y 3.10). Sin embargo, si consideramos un código externo MDS y un código interno fuertemente MDS, el código concatenado  $\text{SC}^{(1)}$  puede ser MDS, tal y como ponemos

Concatenación de los códigos $\mathcal{C}_3$ y $\mathcal{C}_6$				
Modelo	Representación de $\mathcal{SCC}$	$d_{free}(\mathcal{SCC}_{\text{sys}})$	Código externo	Código interno
$\mathcal{SC}^{(3)}$	$A = \begin{pmatrix} \alpha & \alpha^4 \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha^3 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} 1 & \alpha^4 \\ 0 & 0 \end{pmatrix}, D = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$d_{free}(\mathcal{SC}^{(3)}) = 4$ No MDS	$d_2^c(\mathcal{C}_3) = 4$ Fuertemente MDS	$d_1^c(\mathcal{C}_6) = 3$ Fuertemente MDS
$\mathcal{SC}^{(4)}$	$A = \begin{pmatrix} \alpha & \alpha^4 \\ 0 & \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha^3 \\ 1 \end{pmatrix},$ $C = \begin{pmatrix} 1 & \alpha^4 \\ 0 & \alpha^4 \end{pmatrix}, D = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$d_{free}(\mathcal{SC}^{(4)}) = 7$ No MDS		

**Tabla 3.10:** Códigos del ejemplo 3.28

de manifiesto en la tabla 3.5. Si bien considerando los códigos constituyentes de dicha tabla el código  $\mathcal{SC}^{(2)}$  no es MDS, observamos que su distancia libre está muy próxima a la cota Singleton generalizada, por lo que tiene una buena capacidad de corregir errores. Es más, la tabla 3.6 muestra que al concatenar un código fuertemente MDS con un código MDS, podemos obtener que los códigos  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(2)}$  son MDS.

Además, la tabla 3.9 pone de manifiesto que la concatenación de un código MDS con un código no MDS, puede dar lugar a códigos concatenados, según los modelos  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ , con distancia libre próxima a la cota Singleton.

Finalmente, como consecuencia de los ejemplos de la subsección 3.2.5, no podemos asegurar que el código  $\mathcal{SC}^{(2)}$  sea mejor (con distancia libre próxima o igual a la cota Singleton generalizada) que el código  $\mathcal{SC}^{(1)}$ . Un resultado análogo tenemos para los códigos concatenados  $\mathcal{SC}^{(3)}$  y  $\mathcal{SC}^{(4)}$ . Ahora bien, para los códigos  $\mathcal{SC}^{(2)}$  y  $\mathcal{SC}^{(4)}$  disponemos de cotas inferiores de sus distancias libres (véanse las subsecciones 3.2.4 y 3.3.4), mientras que para los códigos  $\mathcal{SC}^{(1)}$  y  $\mathcal{SC}^{(3)}$  no las tenemos, debido a que ni la palabra código completa del código externo ni la palabra código completa del código interno forman parte de la palabra código de la concatenación.

# Concatenación de un código bloque y un código convolucional

---

*All truths are easy to understand once they are discovered;  
the point is to discover them.*

–Galileo Galilei

*Houston, Tranquillity Base here. The Eagle has landed.*

–Neil Armstrong

(transmitting from the moon, 3:18 p.m. Houston time July 20, 1969)

## 4.1 Introducción

Es frecuente combinar códigos bloque y códigos convolucionales para obtener códigos concatenados en los que el código convolucional hace la mayor parte del trabajo y el código bloque (normalmente un código Reed-Solomon) detecta cualquier error producido en el código convolucional. Es decir, la finalidad del código bloque es la detección de errores y la del código convolucional es la corrección de errores. Éste se ha convertido en un estándar de hecho en las comunicaciones espaciales desde que la sonda espacial Voyager 2 empleó por primera vez esta técnica para enviar imágenes en su encuentro con Urano [51, 61]. Esta técnica de concatenación se emplea también en los estándares de televisión digital adoptados en la actualidad: comité de normas de televisión avanzadas (en inglés, *Advanced Television Standards Committee*, ATSC) [19], difusión de vídeo digital (*Digital Video Broadcasting*, DVB) [52, 85] y el estándar japonés de la televisión digital (*Integrated Services Digital Broadcasting*, ISDB) [40]. En la codificación de canal, los tres sistemas anteriores utilizan una concatenación de

un código bloque externo Reed-Solomon y un código convolucional interno. Es más, en la codificación de canal en tecnología GSM (*Global System for Mobile Communication*), se emplea también un código obtenido de la concatenación de un código bloque Reed-Solomon externo y un código convolucional interno.

Varios autores han analizado matemáticamente la concatenación de códigos bloque. Por ejemplo, Uhlemann [108], conjuntamente con Aulin, Rasmussen y Wiberg [109] concatenan códigos bloque con un mecanismo híbrido de repetición automática (Hybrid-ARQ). Ali [2] estudia el rendimiento de concatenaciones de códigos bloque espacio-temporales con códigos convolucionales, empleando decodificación de Viterbi con decisión dura y decisión suave. Benedetto y Montorsi [11], así como Benedetto, Montorsi, Divsalar y Pollara [7] analizan el rendimiento en términos de la probabilidad de error de una alternativa a la concatenación paralela de códigos bloque desarrollada anteriormente [8]: la concatenación en serie de códigos bloque y la concatenación en serie de códigos convolucionales, empleando un intercalado en ambos casos. Ahora bien, no consideran la concatenación de código bloque con código convolucional.

En este capítulo, caracterizamos cuatro modelos de concatenación en serie de un código bloque y un código convolucional desde el punto de vista de sistemas lineales, empleando, al igual que en el capítulo anterior, la representación entrada-estado-salida introducida por Rosenthal, Schumacher y York [91]. Comenzamos describiendo dichos modelos, proporcionando la representación entrada-estado-salida en la sección 4.2. Posteriormente, en la sección 4.3, analizamos condiciones para que la representación entrada-estado-salida de los diferentes modelos sea minimal de manera que el código inducido sea no catastrófico. En las secciones 4.4 y 4.5, establecemos cotas inferiores para las distancias columnas y distancias libres de los modelos en términos de la distancia mínima del código bloque externo y de las distancias columnas y distancia libre del código convolucional interno. Además, estudiamos condiciones para que los códigos concatenados tengan perfil de distancia máxima para el caso particular en que la complejidad de éstos sea  $\delta = 1$ . Finalmente, analizamos las relaciones entre los cuatro modelos mediante una colección de ejemplos en la sección 4.6.

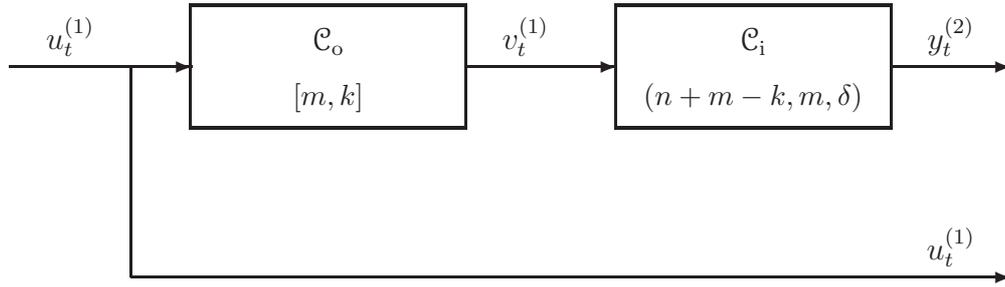


Figura 4.1: Código concatenado  $\mathcal{BC}^{(1)}$

## 4.2 Modelos de concatenación de un código bloque y un código convolucional

En esta sección, introducimos los cuatro modelos de concatenación en serie de un código bloque y un código convolucional que serán nuestro objeto de estudio en este capítulo. Estas concatenaciones consisten en una cascada de un código bloque  $\mathcal{C}_o$ , que llamamos **código externo** y un código convolucional  $\mathcal{C}_i$ , que llamamos **código interno**, que son conceptos análogos a los definidos en el capítulo 3. Denotamos por  $u_t^{(1)}$  y por  $v_t^{(1)}$  el vector información y la palabra código, respectivamente, de  $\mathcal{C}_o$ , y por  $x_t^{(2)}$ ,  $u_t^{(2)}$ ,  $y_t^{(2)}$  y  $v_t^{(2)}$  el vector de estados, el vector información, el vector de paridad y la palabra código, respectivamente, de  $\mathcal{C}_i$ . Asimismo, 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, respectivamente, del código concatenado y por  $T_2(z)$  y  $T(z)$  las matrices de transferencias asociadas al código convolucional  $\widehat{\mathcal{C}}_i$  y al código concatenado correspondiente, considerado como un  $\mathcal{F}$ -subespacio vectorial de  $\mathcal{F}^n$  (véase la sección 1.5), respectivamente.

### Modelo 1

En el primer modelo de concatenación que estudiamos, el código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$  se serializan, uno tras otro (véase la figura 4.1), de manera que el vector información  $u_t^{(1)}$  es codificado por el código bloque  $\mathcal{C}_o$  y la palabra código obtenida

$$v_t^{(1)} = Gu_t^{(1)} \quad (4.1)$$

es entonces codificada por el código convolucional  $\mathcal{C}_i$  de manera que

$$u_t^{(2)} = v_t^{(1)}. \quad (4.2)$$

De este modo, las palabras código  $v_t^{(2)}$  de  $\mathcal{C}_i$  vienen dadas por

$$v_t^{(2)} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(2)} \end{pmatrix}. \quad (4.3)$$

Denotamos por  $\mathcal{BC}^{(1)}$  el correspondiente código convolucional concatenado. Observemos que el vector de estados  $x_t$ , el vector información  $u_t$  y el vector de paridad  $y_t$  de  $\mathcal{BC}^{(1)}$  vienen dados por

$$x_t = x_t^{(2)}, \quad u_t = u_t^{(1)} \quad \text{e} \quad y_t = y_t^{(2)}. \quad (4.4)$$

Por tanto, las palabras código  $v_t$  de  $\mathcal{BC}^{(1)}$  son

$$v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(1)} \end{pmatrix}. \quad (4.5)$$

Notemos que en la figura 4.1, hemos considerado un código convolucional interno de tasa  $m/(n+m-k)$ , con el objetivo de obtener un código concatenado de tasa  $k/n$ . Ahora bien, si concatenamos un código bloque de tasa  $k/m$  y un código convolucional de tasa  $m/n$ , el código convolucional  $\mathcal{BC}^{(1)}$  obtenido de la concatenación tiene tasa  $k/(n-m+k)$ .

El teorema siguiente proporciona la representación entrada-estado-salida del código concatenado  $\mathcal{BC}^{(1)}$  a partir de la matriz generadora del código externo y la representación entrada-estado-salida del código interno.

**Teorema 4.1:** Si  $\mathcal{C}_o$  es un  $[m, k]$ -código con matriz generadora  $G$  y  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n+m-k, m, \delta)$ -código, entonces, la representación entrada-estado-salida para el código concatenado  $\mathcal{BC}^{(1)}$  de tasa  $k/n$  viene dada por el sistema lineal (1.11), donde

$$A = A_2, \quad B = B_2G, \quad C = C_2 \quad \text{y} \quad D = D_2G. \quad (4.6)$$

DEMOSTRACIÓN: De la expresión (1.11) tenemos, para el código interno  $\mathcal{C}_i$ ,

$$\begin{aligned} x_{t+1}^{(2)} &= A_2x_t^{(2)} + B_2u_t^{(2)}, \\ y_t^{(2)} &= C_2x_t^{(2)} + D_2u_t^{(2)}. \end{aligned}$$

Teniendo en cuenta ahora las expresiones (4.1), (4.2) y (4.4), la representación entrada-estado-salida del código concatenado  $\mathcal{BC}^{(1)}$  viene dada por

$$x_{t+1} = A_2x_t + B_2Gu_t,$$

$$y_t = C_2x_t + D_2Gu_t.$$

□

Empleando el resultado anterior y el teorema 1.12, obtenemos la función de transferencia  $T(z)$  asociada al código convolucional  $\widehat{\mathcal{BC}}^{(1)}$  en términos de la matriz generadora  $G(z)$  del código externo  $\mathcal{C}_o$  y de la función de transferencia  $T_2(z)$  asociada al código  $\widehat{\mathcal{C}}_i$ .

**Teorema 4.2:** Si  $\mathcal{BC}^{(1)}(A, B, C, D)$  es el código concatenado descrito por las matrices de la expresión (4.6), entonces

$$T(z) = T_2(z)G(z)$$

es la función de transferencia asociada a  $\widehat{\mathcal{BC}}^{(1)}$ .

## Modelo 2

Si en el primer modelo  $\mathcal{BC}^{(1)}$  consideramos que la matriz generadora  $G$  del código bloque  $\mathcal{C}_o$  está dada en forma sistemática, esto es,  $G = \begin{pmatrix} I_k \\ P \end{pmatrix}$  y consideramos el vector de paridad  $Pu_t^{(1)}$  de la palabra código de  $\mathcal{C}_o$

$$v_t^{(1)} = \begin{pmatrix} u_t^{(1)} \\ Pu_t^{(1)} \end{pmatrix} \quad (4.7)$$

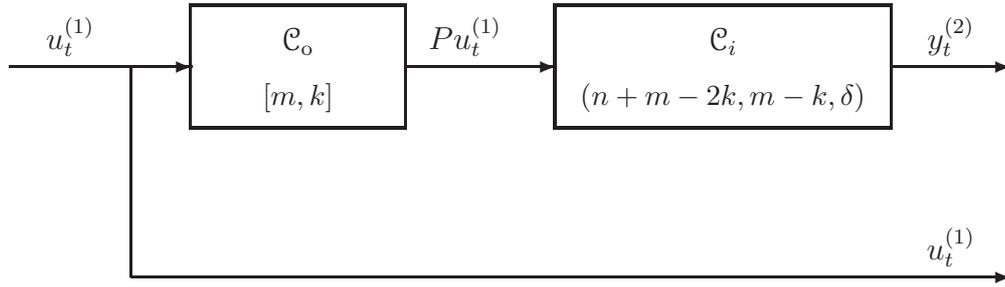
como entrada para  $\mathcal{C}_i$ , esto es,

$$u_t^{(2)} = Pu_t^{(1)}, \quad (4.8)$$

entonces obtenemos el código concatenado de la figura 4.2. En este modelo, las palabras código  $v_t^{(2)}$  de  $\mathcal{C}_i$  están dadas por

$$v_t^{(2)} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(2)} \end{pmatrix}. \quad (4.9)$$

Denotamos por  $\mathcal{BC}_{\text{sys}}^{(1)}$  el correspondiente código convolucional cocatenado. De manera análoga al modelo  $\mathcal{BC}^{(1)}$ , el vector de estados  $x_t$ , el vector información  $u_t$ , el vector de



**Figura 4.2:** Código concatenado  $\mathcal{BC}_{\text{sys}}^{(1)}$

paridad  $y_t$  y las palabras código  $v_t$  de  $\mathcal{BC}_{\text{sys}}^{(1)}$  están dadas por las expresiones (4.4) y (4.5).

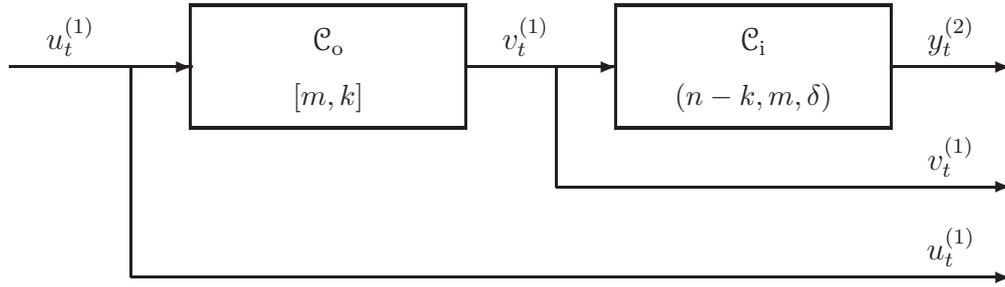
De forma análoga al modelo anterior, en la figura 4.2, hemos considerado un código interno de tasa  $(m-k)/(n+m-2k)$  para obtener un código concatenado  $\mathcal{BC}_{\text{sys}}^{(1)}$  de tasa  $k/n$ . Ahora bien, si partimos de un código bloque y un código convolucional de tasas  $k/m$  y  $(m-k)/n$ , respectivamente, entonces el código  $\mathcal{BC}_{\text{sys}}^{(1)}$  tiene tasa  $k/(n-m+2k)$ .

La representación entrada-estado-salida del código concatenado  $\mathcal{BC}_{\text{sys}}^{(1)}$  viene dada por el teorema siguiente, cuya demostración omitimos por ser similar a la del teorema 4.1.

**Teorema 4.3:** Si  $\mathcal{C}_o$  es un  $[m, k]$ -código con matriz generadora en forma sistemática  $G = \begin{pmatrix} I_k \\ P \end{pmatrix}$  y  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n + m - 2k, m - k, \delta)$ -código, entonces, la representación entrada-estado-salida para el código concatenado  $\mathcal{BC}_{\text{sys}}^{(1)}$  viene dada por el sistema lineal (1.11), donde

$$A = A_2, \quad B = B_2P, \quad C = C_2, \quad y \quad D = D_2P. \quad (4.10)$$

Empleando el resultado anterior y el teorema 1.12, obtenemos la función de transferencia  $T(z)$  asociada al código convolucional  $\widehat{\mathcal{BC}}_{\text{sys}}^{(1)}$  en términos de la submatriz  $P$  de la matriz generadora del código externo  $\mathcal{C}_o$  y de la función de transferencia  $T_2(z)$  asociada al código  $\widehat{\mathcal{C}}_i$ .



**Figura 4.3:** Código concatenado  $\mathcal{BC}^{(2)}$

**Teorema 4.4:** Si  $\mathcal{BC}_{sys}^{(1)}$  es el código concatenado descrito por las matrices de la expresión (4.10), entonces

$$T(z) = T_2(z)P(z)$$

es la función de transferencia asociada a  $\widehat{\mathcal{BC}}_{sys}^{(1)}$ .

### Modelo 3

Si variamos el código  $\mathcal{BC}^{(1)}$  de manera que la palabra código  $v_t^{(1)}$  del código externo sea una parte de la palabra código de la concatenación (véase la figura 4.3), obtenemos entonces un nuevo código convolucional que denotamos por  $\mathcal{BC}^{(2)}$ . El vector información  $u_t^{(1)}$  y la palabra código  $v_t^{(1)}$  de  $\mathcal{C}_o$  y el vector información  $u_t^{(2)}$  y las palabras código  $v_t^{(2)}$  de  $\mathcal{C}_i$  son las mismas que en el primer modelo (véase las expresiones (4.1), (4.2) y (4.3)). Entonces, el vector de estados  $x_t$ , el vector información  $u_t$  y el vector de paridad  $y_t$  de  $\mathcal{BC}^{(2)}$  vienen dados por

$$x_t = x_t^{(2)}, \quad u_t = u_t^{(1)} \quad \text{e} \quad y_t = \begin{pmatrix} y_t^{(2)} \\ v_t^{(1)} \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ Gu_t^{(1)} \end{pmatrix}. \quad (4.11)$$

Así, las palabras código  $v_t$  de  $\mathcal{BC}^{(2)}$  son

$$v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ Gu_t^{(1)} \\ u_t^{(1)} \end{pmatrix}. \quad (4.12)$$

De forma análoga a los modelos descritos anteriormente, si consideramos un código bloque y un código convolucional de tasas  $k/m$  y  $m/n$ , respectivamente, entonces el código concatenado  $\mathcal{BC}^{(2)}$  tiene tasa  $k/(n+k)$ .

El teorema siguiente, cuya demostración es similar a la del teorema 4.1, proporciona la representación entrada-estado-salida del código convolucional  $\mathcal{BC}^{(2)}$  a partir de la matriz generadora del código externo y la representación entrada-estado-salida del código interno. En este teorema, y en el resto del capítulo, denotamos por  $O$  la matriz nula del tamaño apropiado.

**Teorema 4.5:** Si  $\mathcal{C}_o$  es un  $[m, k]$ -código con matriz generadora  $G$  y  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n-k, m, \delta)$ -código, entonces, la representación entrada-estado-salida para el código concatenado  $\mathcal{BC}^{(2)}$  de tasa  $k/n$  viene dada por el sistema lineal (1.11), con

$$A = A_2, \quad B = B_2G, \quad C = \begin{pmatrix} C_2 \\ O \end{pmatrix} \quad \text{y} \quad D = \begin{pmatrix} D_2G \\ G \end{pmatrix}. \quad (4.13)$$

Del mismo modo a los modelos anteriores, la función de transferencia  $T(z)$  asociada al código convolucional  $\widehat{\mathcal{BC}}^{(2)}$  viene dada en función de la matriz generadora  $G(z)$  del código externo  $\mathcal{C}_o$  y de la función de transferencia  $T_2(z)$  asociada al código  $\widehat{\mathcal{C}}_i$ .

**Teorema 4.6:** Si  $\mathcal{BC}^{(2)}$  es el código concatenado descrito por las matrices de la expresión (4.13), entonces

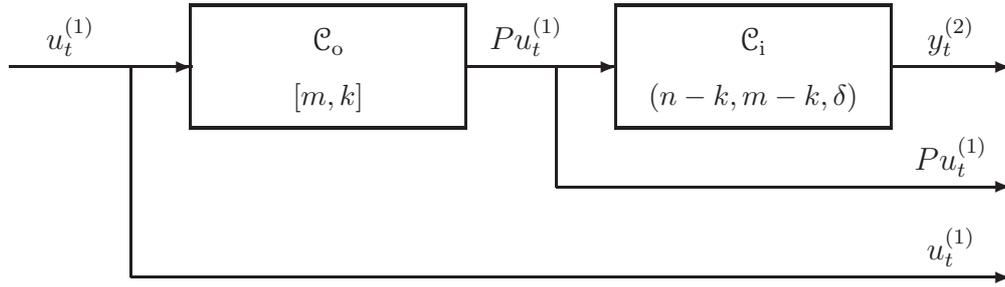
$$T(z) = \begin{pmatrix} T_2(z)G(z) \\ G(z) \end{pmatrix}.$$

es la función de transferencia asociada a  $\widehat{\mathcal{BC}}^{(2)}$ .

## Modelo 4

Por último, si aplicamos a  $\mathcal{BC}^{(2)}$  una variación similar a la hecha a  $\mathcal{BC}^{(1)}$  para obtener  $\mathcal{BC}_{\text{sys}}^{(1)}$ , obtenemos un código convolucional concatenado que denotamos por  $\mathcal{BC}_{\text{sys}}^{(2)}$  (véase la figura 4.4).

En este modelo, los vectores información  $u_t^{(1)}$  y  $u_t^{(2)}$  y las palabras código  $v_t^{(1)}$  y  $v_t^{(2)}$  de  $\mathcal{C}_o$  y  $\mathcal{C}_i$ , respectivamente, son las mismas que las del código  $\mathcal{BC}_{\text{sys}}^{(1)}$  (véanse las



**Figura 4.4:** Código concatenado  $\mathcal{BC}_{\text{sys}}^{(2)}$

expresiones (4.7), (4.8) y (4.9)). Del mismo modo, el vector de estados  $x_t$  y el vector información  $u_t$  de  $\mathcal{BC}_{\text{sys}}^{(2)}$  son los mismos que los del modelo  $\mathcal{BC}_{\text{sys}}^{(1)}$  (véase la expresión (4.4)). Ahora bien, en el código concatenado  $\mathcal{BC}_{\text{sys}}^{(2)}$ , el vector de paridad  $y_t$  y la palabra código  $v_t$  vienen dadas por

$$y_t = \begin{pmatrix} y_t^{(2)} \\ Pu_t^{(1)} \end{pmatrix} \quad \text{y} \quad v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ Pu_t^{(1)} \\ u_t^{(1)} \end{pmatrix}. \quad (4.14)$$

Notemos que el código  $\mathcal{BC}_{\text{sys}}^{(2)}$  obtenido de la concatenación de un código bloque y un código convolucional de tasas  $k/m$  y  $(m-k)/n$ , respectivamente, tiene tasa  $k/(n+k)$ .

La representación entrada-estado-salida del código concatenado  $\mathcal{BC}_{\text{sys}}^{(2)}$  viene dada por el teorema siguiente, cuya demostración es análoga a la de los teoremas anteriores, por lo que la omitimos.

**Teorema 4.7:** Si  $\mathcal{C}_o$  es un  $[m, k]$ -código con matriz generadora en forma sistemática  $G = \begin{pmatrix} I_k \\ P \end{pmatrix}$  y  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un  $(n-k, m-k, \delta)$ -código, entonces, la representación entrada-estado-salida del código concatenado  $\mathcal{BC}_{\text{sys}}^{(2)}$  de tasa  $k/n$  viene dada por el sistema lineal (1.11), donde

$$A = A_2, \quad B = B_2P, \quad C = \begin{pmatrix} C_2 \\ O \end{pmatrix} \quad \text{y} \quad D = \begin{pmatrix} D_2P \\ P \end{pmatrix}. \quad (4.15)$$

El resultado siguiente proporciona la expresión de la función de transferencia  $T(z)$  asociada al código convolucional  $\widehat{\mathcal{BC}}_{\text{sys}}^{(2)}$ .

**Teorema 4.8:** Si  $\mathcal{BC}_{\text{sys}}^{(2)}$  es el código concatenado descrito por las matrices de la expresión (4.15), entonces

$$T(z) = \begin{pmatrix} T_2(z)P(z) \\ P(z) \end{pmatrix}$$

es la función de transferencia asociada a  $\widehat{\mathcal{BC}}_{\text{sys}}^{(2)}$ .

## 4.3 Controlabilidad y observabilidad

Una vez obtenidas las representaciones entrada-estado-salida de los diferentes modelos de concatenación en serie de un código bloque con un código convolucional, establecemos en esta sección condiciones sobre la matriz generadora  $G$  del código bloque externo y de las matrices  $(A_2, B_2, C_2, D_2)$  que describen el código convolucional interno para obtener una “buena” representación de los diferentes modelos de concatenación, esto es, una representación entrada-estado-salida minimal con el par  $(A, C)$  observable.

Como algunos resultados de controlabilidad y observabilidad son válidos para los cuatro modelos  $\mathcal{BC}^{(1)}$ ,  $\mathcal{BC}_{\text{sys}}^{(1)}$ ,  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  introducidos anteriormente, adoptamos la notación siguiente a lo largo de este capítulo.

- $\mathcal{SCBC}$  denota el código concatenado  $\mathcal{BC}^{(1)}$ ,  $\mathcal{BC}_{\text{sys}}^{(1)}$ ,  $\mathcal{BC}^{(2)}$  o bien  $\mathcal{BC}_{\text{sys}}^{(2)}$ , descrito por las matrices (4.6), (4.10), (4.13) y (4.15), respectivamente. Tenemos entonces que (véase los comentarios previos a los teoremas 4.1, 4.3, 4.5 y 4.7)

$$\mathcal{SCBC} \text{ tiene tasa } \begin{cases} k/(n-m+k), & \text{si } \mathcal{SCBC} = \mathcal{BC}^{(1)} \\ k/(n-m+2k), & \text{si } \mathcal{SCBC} = \mathcal{BC}_{\text{sys}}^{(1)} \\ k/(n+k), & \text{si } \mathcal{SCBC} = \mathcal{BC}^{(2)} \\ k/(n+k), & \text{si } \mathcal{SCBC} = \mathcal{BC}_{\text{sys}}^{(2)} \end{cases}$$

- $\mathcal{C}_i$  denota el correspondiente código convolucional interno del código concatenado  $\mathcal{BC}$ .
- $\tilde{G}$  denota la matriz generadora  $G$  así como la submatriz  $P$  de la matriz generadora

sistemática  $G = \begin{pmatrix} I_k \\ P \end{pmatrix}$  del código bloque externo  $\mathcal{C}_o$ . De este modo, si denotamos por  $s$  el número de filas de  $\tilde{G}$ , entonces

$$s = \begin{cases} m, & \text{si } \tilde{G} = G, \\ m - k, & \text{si } \tilde{G} = P. \end{cases}$$

Notemos que a la vista de las relaciones entre los pares  $(A_2, C_2)$  de los códigos internos y el par  $(A, C)$  de los códigos concatenados, es obvio que  $(A, C)$  es observable si y sólo si  $(A_2, C_2)$  es observable.

Sin embargo, no tenemos el mismo resultado para la controlabilidad del par  $(A, B)$ . De hecho, la controlabilidad del código interno no implica necesariamente la controlabilidad del código concatenado, como mostramos en el ejemplo siguiente.

**Ejemplo 4.1:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  (véase la sección 1.1). Consideremos el  $[4, 2]$ -código  $\mathcal{C}_o$  con matriz generadora

$$G = \begin{pmatrix} I_2 \\ P \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \alpha^3 & \alpha^5 \\ \alpha^4 & \alpha^6 \end{pmatrix}. \quad (4.16)$$

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(n, 4, 2)$ -código, siendo  $n$  un número natural cualquiera, descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^3 & \alpha^2 \\ \alpha & 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} O & \tilde{B}_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \alpha & 0 \\ 0 & 0 & \alpha^4 & 1 \end{pmatrix},$$

siendo  $C_2$  y  $D_2$  matrices arbitrarias de tamaños  $(n-4) \times 2$  y  $(n-4) \times 4$ , respectivamente. Observemos que el par  $(A_2, \tilde{B}_2)$  es controlable, ya que

$$\text{rg} \begin{pmatrix} zI_2 - A_2 & \tilde{B}_2 \end{pmatrix} = \text{rg} \begin{pmatrix} z - \alpha^3 & \alpha^2 & \alpha & 0 \\ \alpha & z - 1 & \alpha^4 & 1 \end{pmatrix} = 2$$

para todo  $z \in \overline{\mathbb{F}}$ . Por tanto, el par  $(A_2, B_2)$  es también controlable.

Por otro lado, aplicando los teoremas 4.1, 4.3, 4.5 y 4.7, las matrices  $A$  y  $B$  de la representación entrada-estado-salida de los códigos concatenados  $\mathcal{SCBC}$  son

$$A = \begin{pmatrix} \alpha^3 & \alpha^2 \\ \alpha & 1 \end{pmatrix} \quad \text{y} \quad B = B_2G = \tilde{B}_2P = \begin{pmatrix} \alpha^4 & \alpha^6 \\ \alpha^5 & 1 \end{pmatrix}.$$

Entonces, el par  $(A, B)$  no es controlable, ya que

$$\begin{aligned} \operatorname{rg}(\alpha I - A \quad B) &= \operatorname{rg} \begin{pmatrix} \alpha - \alpha^3 & \alpha^2 & \alpha^4 & \alpha^6 \\ \alpha & \alpha - 1 & \alpha^5 & 1 \end{pmatrix} \\ &= \operatorname{rg} \begin{pmatrix} 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ \alpha & \alpha^3 & \alpha^5 & 1 \end{pmatrix} = 1 \neq 2. \quad \blacksquare \end{aligned}$$

Por tanto, necesitamos condiciones adicionales para obtener la controlabilidad del par  $(A, B)$  de los diferentes modelos. El resultado siguiente, cuya demostración es similar a la del teorema 3.5, muestra que es suficiente con que la matriz  $B$  tenga rango completo por filas para tener la controlabilidad del par  $(A, B)$ .

**Teorema 4.9:** Sean  $\mathcal{C}_o$  un  $[m, k]$ -código,  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un código convolucional con complejidad  $\delta$  y  $\mathcal{SCBC}(A, B, C, D)$  el código convolucional concatenado correspondiente. Si  $\operatorname{rg}(B) = \delta$ , entonces  $(A, B, C, D)$  es una representación minimal de  $\mathcal{SCBC}$  con complejidad  $\delta$ .

**Observación 4.1:** Notemos que en el teorema 4.9, la condición  $\operatorname{rg}(B) = \delta$  implica que  $\operatorname{rg}(B_2) = \delta$ , ya que

$$\delta = \operatorname{rg}(B) = \operatorname{rg}(B_2 \tilde{G}) \leq \operatorname{rg}(B_2) \leq \delta.$$

En particular, tenemos entonces que el par  $(A_2, B_2)$  es controlable. ■

Si la matriz  $A_2$  del código convolucional interno es diagonal y la matriz  $B$  del código concatenado verifica ciertas condiciones, entonces obtenemos que el par  $(A, B)$  de la concatenación es controlable, como ponemos de manifiesto en el resultado siguiente.

**Teorema 4.10:** Supongamos que  $\mathcal{C}_o$  es un  $[m, k]$ -código, que  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  es un código convolucional con complejidad  $\delta$  y que  $\mathcal{SCBC}(A, B, C, D)$  es el código concatenado correspondiente. Supongamos que también se satisfacen las condiciones siguientes

- (a)  $\operatorname{rg}(B) = r < \delta$ .
- (b)  $A$  es una matriz diagonal.
- (c) Si  $a_1, a_2, \dots, a_p$  son los elementos diferentes de  $A$ , entonces  $a_i$  aparece  $\beta_i$  veces en la diagonal de  $A$ , con  $\beta_i \leq r$ .
- (d) La submatriz obtenida de  $B$  al escoger las  $\beta_i$  filas correspondientes a las filas de  $A$  cuyo elemento es  $a_i$ , tiene rango completo por filas.

Entonces  $(A, B, C, D)$  es una representación minimal del código concatenado SCBC con complejidad  $\delta$ .

DEMOSTRACIÓN: Sin pérdida de generalidad, podemos suponer que

$$A = \text{diag} \left( \overbrace{a_1, a_1, \dots, a_1}^{\beta_1}, \overbrace{a_2, a_2, \dots, a_2}^{\beta_2}, \dots, \overbrace{a_p, a_p, \dots, a_p}^{\beta_p} \right)$$

Así,

$$\begin{pmatrix} a_1 I - A & B \end{pmatrix} = \begin{pmatrix} O & O & B_{11} \\ O & \tilde{A} & B_{12} \end{pmatrix},$$

siendo

$$\tilde{A} = \text{diag} \left( \overbrace{a_1 - a_2, a_1 - a_2, \dots, a_1 - a_2}^{\beta_2}, \dots, \overbrace{a_1 - a_p, a_1 - a_p, \dots, a_1 - a_p}^{\beta_p} \right)$$

Entonces, aplicando la condición (d),  $\text{rg}(B_{11}) = \beta_1$  y por tanto, al ser  $\text{rg}(\tilde{A}) = \delta - \beta_1$ , tenemos que

$$\text{rg} \begin{pmatrix} a_1 I - A & B \end{pmatrix} = \delta.$$

Empleando el mismo argumento para el resto de los elementos de la diagonal de  $A$ , obtenemos que

$$\text{rg} \begin{pmatrix} zI - A & B \end{pmatrix} = \delta$$

para todo  $z \in \overline{\mathbb{F}}$ , es decir, el par  $(A, B)$  es controlable.  $\square$

Como consecuencia inmediata del teorema anterior, tenemos el resultado siguiente para el caso particular en que todos los elementos de la matriz  $A_2$  sean distintos.

**Corolario 4.1:** Con la misma notación que la empleada en el teorema 4.10, si se satisfacen las condiciones siguientes:

- (a)  $\text{rg}(B) < \delta$ .
- (b)  $A$  es una matriz diagonal.
- (c)  $\beta_1 = \beta_2 = \dots = \beta_p = 1$ .
- (d) Cada fila de  $B$  tiene al menos un elemento no nulo.

Entonces  $(A, B, C, D)$  es una representación minimal del código concatenado SCBC con complejidad  $\delta$ .

Como consecuencia del corolario 4.1, obtenemos el siguiente resultado para el caso particular en que el código bloque externo tenga dimensión uno.

**Corolario 4.2:** *Con la misma notación que la empleada en el teorema 4.10, si se satisfacen las condiciones siguientes:*

- (a)  $k = 1$ .
- (b)  $\delta > 1$ .
- (c)  $A$  es una matriz diagonal.
- (d)  $\beta_1 = \beta_2 = \dots = \beta_p = 1$ .
- (e) Todos los elementos de  $B$  son no nulos.

Entonces  $(A, B, C, D)$  es una representación minimal para el código concatenado SCBC con complejidad  $\delta$ .

## 4.4 Distancias columnas y distancia libre

Una vez que hemos obtenido condiciones que aseguran la controlabilidad del par  $(A, B)$  del código concatenado (y por tanto, sabemos cómo obtener una representación minimal) así como la observabilidad del par  $(A, C)$  del código concatenado (y por tanto, sabemos que la matriz generadora inducida por la realización es no catastrófica), analizamos en esta sección las propiedades de las distancias columnas y las distancias libres de los códigos concatenados, ya que nuestro objetivo es la construcción de códigos óptimos o bien con distancia libre próxima a la cota Singleton generalizada. Si bien para los modelos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$  obtendremos cotas inferiores de sus distancias columnas en términos únicamente de las distancias columnas del código convolucional interno, para los modelos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$ , tendremos un refinamiento de dichas cotas en función de la distancia mínima de  $\mathcal{C}_o$  y de las distancias columnas de  $\mathcal{C}_i$ .

### 4.4.1 Distancias columnas de $\mathcal{BC}^{(1)}$ y $\mathcal{BC}_{\text{sys}}^{(1)}$

Recordemos que, según la expresión (4.5), las palabras código de los modelos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$  venían dadas por

$$v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(1)} \end{pmatrix},$$

es decir, están compuestas por la componente de paridad de la palabra  $v_t^{(2)} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(2)} \end{pmatrix}$  del código convolucional interno y por el vector información del código bloque externo  $u_t^{(1)}$ . Por tanto, las palabras de los códigos externo e interno no forman parte de la palabra código de la concatenación. Esto constituye un problema a la hora de relacionar las distancias columnas de  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$  con las correspondientes distancias columnas del código interno  $\mathcal{C}_i$  y la distancia mínima del código externo  $\mathcal{C}_o$ . De hecho, tenemos que exigir que el código convolucional interno tenga perfil de distancia máxima para poder obtener una cota inferior de la  $j$ -ésima distancia columna de  $\mathcal{BC}^{(1)}$  y de  $\mathcal{BC}_{\text{sys}}^{(1)}$  en términos de la  $j$ -ésima distancia columna de  $\mathcal{C}_i$ , como vemos en los resultados siguientes.

**Teorema 4.11:** Sean  $\mathcal{C}_o$  un  $[m, k]$ -código con distancia mínima  $d_{\min}(\mathcal{C}_o)$  y con matriz generadora  $G$  y  $\mathcal{C}_i$  un  $(n + m - k, m, \delta)$ -código con perfil de distancia máxima. Si  $n \geq k + m - 2$ , entonces

$$d_j^c(\mathcal{BC}^{(1)}) \geq d_j^c(\mathcal{C}_i) - m(j + 1) + 1 \quad \text{para } j = 0, 1, \dots, \left\lfloor \frac{\delta}{m} \right\rfloor + \left\lfloor \frac{\delta}{n - k} \right\rfloor. \quad (4.17)$$

DEMOSTRACIÓN: Supongamos que  $(y_0, y_1, \dots, y_j | u_0, u_1, \dots, u_j)^T$  es una palabra código de peso finito de  $\mathcal{BC}^{(1)}$  con  $u_0 \neq 0$ ; entonces,

$$r = \text{wt}(Gu_0, Gu_1, \dots, Gu_j) \geq \text{wt}(Gu_0) \geq d_{\min}(\mathcal{C}_o). \quad (4.18)$$

Como  $\mathcal{C}_i$  tiene perfil de distancia máxima, aplicando el teorema 1.13, todo menor de la matriz  $\mathcal{T}_L$  dada por la expresión (1.20) que no es trivialmente nulo, es no nulo. Como  $Gu_0 \neq 0$ , esto significa que a lo sumo  $r - 1$  filas de  $\mathcal{T}_L$  son ortogonales a  $(Gu_0, Gu_1, \dots, Gu_j)^T$ . Así, de la expresión (1.16), obtenemos que a lo sumo  $r - 1$  componentes de  $(y_0, y_1, \dots, y_j)^T$  son nulas y, en consecuencia,

$$\text{wt}(y_0, \dots, y_j) \geq (n - k)(j + 1) - (r - 1). \quad (4.19)$$

Entonces, teniendo en cuenta que

$$\text{wt}(u_0, u_1, \dots, u_j) \geq 1, \quad \text{wt}(Gu_0, Gu_1, \dots, Gu_j) \leq m(j + 1).$$

y las expresiones (4.19) y (4.18), obtenemos que

$$\text{wt}(y_0, y_1, \dots, y_j | u_0, u_1, \dots, u_j) = \text{wt}(y_0, y_1, \dots, y_j) + \text{wt}(u_0, u_1, \dots, u_j)$$

$$\begin{aligned}
&\geq (n-k)(j+1) - (r-1) + \text{wt}(u_0, u_1, \dots, u_j) \\
&\geq (n-k)(j+1) - (r-1) + 1 \\
&\geq (n-k)(j+1) - m(j+1) + 2.
\end{aligned}$$

Ahora bien, como  $\mathcal{C}_i$  tiene perfil de distancia máxima, entonces

$$d_j^c(\mathcal{C}_i) = (n-k)(j+1) + 1 \quad \text{para } j = 0, \dots, L = \left\lfloor \frac{\delta}{m} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor,$$

y por tanto,

$$\begin{aligned}
\text{wt}(y_0, y_1, \dots, y_j | u_0, u_1, \dots, u_j) &\geq (n-k)(j+1) - m(j+1) + 2 \\
&= d_j^c(\mathcal{C}_i) - m(j+1) + 1.
\end{aligned} \tag{4.20}$$

Obtenemos entonces la expresión (4.17) de la relación (4.20) y de la expresión de la  $j$ -ésima distancia columna en términos de la representación entrada-estado-salida dada en (1.19).  $\square$

Para el código concatenado  $\mathcal{BC}_{\text{sys}}^{(1)}$ , obtenemos una cota inferior de la  $j$ -ésima distancia columna, similar a la obtenida en el teorema anterior.

**Teorema 4.12:** *Sea  $\mathcal{C}_o$  un  $[m, k]$ -código con distancia mínima  $d_{\min}(\mathcal{C}_o)$  y matriz generadora  $G = \begin{pmatrix} I_k \\ P \end{pmatrix}$  y supongamos que  $P$  tiene rango  $k$ . Sea  $\mathcal{C}_i$  un  $(n+m-2k, m-k, \delta)$ -código con perfil de distancia máxima, entonces*

$$d_j^c(\mathcal{BC}_{\text{sys}}^{(1)}) \geq (n-m)(j+1) + 2 \quad \text{para } j = 0, 1, \dots, \left\lfloor \frac{\delta}{m-k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor. \tag{4.21}$$

DEMOSTRACIÓN: Supongamos que  $(y_0, y_1, \dots, y_j | u_0, u_1, \dots, u_j)^T$  es una palabra código con peso finito de  $\mathcal{BC}_{\text{sys}}^{(1)}$  con  $u_0 \neq 0$ . Como  $\text{rg}(P) = k$ , en particular,  $Pu_0 \neq 0$  y  $\text{wt}(Pu_0) \geq 1$ , de donde

$$r = \text{wt}(Pu_0, Pu_1, \dots, Pu_j) \geq \text{wt}(Pu_0) \geq 1. \tag{4.22}$$

Empleando un argumento similar al de la demostración del teorema 4.11, tenemos que a lo sumo  $r-1$  filas de la matriz  $\mathcal{T}_L$  son ortogonales al vector  $(Pu_0, Pu_1, \dots, Pu_j)^T$ , y por tanto, a lo sumo  $r-1$  componentes de  $(y_0, y_1, \dots, y_j)^T$  son nulas, de donde

$$\text{wt}(y_0, \dots, y_j) \geq (n-k)(j+1) - (r-1). \tag{4.23}$$

Entonces, teniendo en cuenta que

$$\text{wt}(u_0, u_1, \dots, u_j) \geq 1, \quad \text{wt}(Pu_0, Pu_1, \dots, Pu_j) \leq (m - k)(j + 1), \quad (4.24)$$

así como las expresiones (4.22) y (4.23), obtenemos que

$$\begin{aligned} \text{wt}(y_0, y_1, \dots, y_j | u_0, u_1, \dots, u_j) &= \text{wt}(y_0, y_1, \dots, y_j) + \text{wt}(u_0, u_1, \dots, u_j) \\ &\geq (n - k)(j + 1) - (r - 1) + \text{wt}(u_0, u_1, \dots, u_j) \\ &\geq (n - k)(j + 1) - r + 2 \\ &\geq (n - k)(j + 1) - (m - k)(j + 1) + 2 \\ &= (n - m)(j + 1) + 2. \end{aligned} \quad (4.25)$$

Así, de la desigualdad anterior y de la expresión de la  $j$ -ésima distancia columna en términos de la representación entrada-estado-salida dada por la expresión (1.19), obtenemos la desigualdad (4.21).  $\square$

Observemos que si en el teorema anterior,  $\mathcal{C}_o$  es un código bloque MDS y  $k \leq m - k$ , entonces por el teorema 1.2, podemos asegurar, en particular, que  $\text{rg}(P) = k$  y, por tanto, obtenemos el resultado siguiente.

**Corolario 4.3:** Sea  $\mathcal{C}_o$  un  $[m, k]$ -código MDS con matriz generadora dada en forma sistemática  $G = \begin{pmatrix} I_k \\ P \end{pmatrix}$ . Supongamos que  $k \leq m - k$  y sea  $\mathcal{C}_i$  un  $(n + m - 2k, m - k, \delta)$ -código con perfil de distancia máxima; entonces,

$$d_j^c(\mathcal{BC}_{sys}^{(1)}) \geq (n - m)(j + 1) + 2 \quad \text{para } j = 0, 1, \dots, \left\lfloor \frac{\delta}{m - k} \right\rfloor + \left\lfloor \frac{\delta}{n - k} \right\rfloor.$$

#### 4.4.2 Distancias columnas y distancia libre de $\mathcal{BC}^{(2)}$ y $\mathcal{BC}_{sys}^{(2)}$

Observemos que, según la expresión (4.12), la relación entre una palabra código  $v_t$  de  $\mathcal{BC}^{(2)}$  y las palabras código  $v_t^{(1)}$  y  $v_t^{(2)}$  del código externo y del código interno,

respectivamente, es

$$v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ Gu_t^{(1)} \\ u_t^{(1)} \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ v_t^{(1)} \\ u_t^{(1)} \end{pmatrix} = \begin{pmatrix} v_t^{(2)} \\ u_t^{(1)} \end{pmatrix}.$$

Del mismo modo, la relación entre una palabra código  $v_t$  de  $\mathcal{BC}_{\text{sys}}^{(2)}$  y la palabras código  $v_t^{(1)}$  y  $v_t^{(2)}$  del código externo y del código interno, respectivamente, es (véase la relación (4.14))

$$v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ Pu_t^{(1)} \\ u_t^{(1)} \end{pmatrix} = \begin{pmatrix} y_t^{(2)} \\ v_t^{(1)} \\ u_t^{(1)} \end{pmatrix} = \begin{pmatrix} v_t^{(2)} \\ u_t^{(1)} \end{pmatrix}.$$

Es decir, tanto la palabra código  $v_t^{(1)}$  de  $\mathcal{C}_o$  como la palabra código  $v_t^{(2)}$  de  $\mathcal{C}_i$  forman parte de la palabra código de  $v_t$  de  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$ . Este hecho, nos permitirá obtener una cota inferior de la  $j$ -ésima distancia columna de estas concatenaciones en función de la distancia mínima del código bloque externo y la  $j$ -ésima distancia columna del código convolucional interno.

Comenzamos con un lema técnico sobre las distancias columnas de  $\mathcal{BC}^{(2)}$  que nos permitirá obtener la cota inferior de la distancia libre de esta concatenación.

**Lema 4.1:** *Sea  $\mathcal{BC}^{(2)}$  el código concatenado dado por el teorema 4.5 obtenido de la concatenación del código bloque externo  $\mathcal{C}_o$  y el código convolucional interno  $\mathcal{C}_i$ . Entonces,*

$$d_j^c(\mathcal{BC}^{(2)}) \geq \max\{d_{\min}(\mathcal{C}_o) + 1, d_j^c(\mathcal{C}_i) + 1\} \quad \text{para } j = 0, 1, 2, \dots \quad (4.26)$$

DEMOSTRACIÓN: Teniendo en cuenta las relaciones entre  $y_t, y_t^{(2)}$ ;  $u_t, u_t^{(1)}, u_t^{(2)}$  y  $v_t, v_t^{(1)}, v_t^{(2)}$  dadas por las expresiones (4.2), (4.3) y (4.11), tenemos

$$\begin{aligned} \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(v_t^{(1)}) \\ &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(Gu_t^{(1)}) \\ &\geq \text{wt}(u_0^{(1)}) + \sum_{t=0}^j \text{wt}(Gu_t^{(1)}) \end{aligned}$$

$$\geq \text{wt}(u_0^{(1)}) + \text{wt}(Gu_0^{(1)}). \quad (4.27)$$

De este modo, de la definición de  $d_{\min}(\mathcal{C}_o)$ , así como de la expresión de la  $j$ -ésima distancia columna en términos de la representación entrada-estado-salida dada por la relación (1.19), y teniendo en cuenta que  $u_0 = u_0^{(1)}$ , obtenemos

$$\begin{aligned} d_j^c(\mathcal{BC}^{(2)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(1)} \neq 0} \left\{ \text{wt}(u_0^{(1)}) + \text{wt}(Gu_0^{(1)}) \right\} \\ &\geq d_{\min}(\mathcal{C}_o) + 1. \end{aligned} \quad (4.28)$$

Análogamente, de las expresiones (4.2), (4.3) y (4.11), obtenemos

$$\begin{aligned} \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(v_t^{(1)}) \\ &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(u_t^{(2)}) \\ &\geq \text{wt}(u_0^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(u_t^{(2)}). \end{aligned}$$

Como  $u_0^{(2)} = Gu_0^{(1)}$  y  $\text{rg}(G) = k$ , tenemos que  $u_0 = u_0^{(1)} \neq 0$  si sólo si  $u_0^{(2)} = Gu_0^{(1)} \neq 0$ . Por tanto, de la desigualdad anterior y de la expresión de la  $j$ -ésima distancia columna dada por la relación (1.19), obtenemos

$$\begin{aligned} d_j^c(\mathcal{BC}^{(2)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(1)} \neq 0} \left\{ \text{wt}(u_0^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(u_t^{(2)}) \right\} \\ &\geq d_j^c(\mathcal{C}_i) + 1. \end{aligned} \quad (4.29)$$

Finalmente, de las desigualdades (4.28) y (4.29), obtenemos la desigualdad (4.26).  $\square$

Como consecuencia inmediata del lema 4.1 y de la expresión de la distancia libre en términos de la representación entrada-estado-salida dada por la relación (1.5), obtenemos el resultado siguiente.

**Teorema 4.13:** Sea  $\mathcal{BC}^{(2)}$  el código dado por el teorema 4.5 obtenido de la concatenación del código bloque externo  $\mathcal{C}_o$  y el código convolucional interno  $\mathcal{C}_i$ . Entonces,

$$d_{free}(\mathcal{BC}^{(2)}) \geq \max\{d_{min}(\mathcal{C}_o) + 1, d_{free}(\mathcal{C}_i) + 1\}.$$

La distancia libre del código concatenado  $\mathcal{BC}_{\text{sys}}^{(2)}$  está siempre acotada por la distancia mínima del código bloque externo, como en el caso del código  $\mathcal{BC}^{(2)}$ . Sin embargo, no podemos asegurar que la distancia libre del código convolucional interno, sea también una cota inferior para  $d_{free}(\mathcal{BC}_{\text{sys}}^{(2)})$ , como ponemos de manifiesto en el ejemplo siguiente.

**Ejemplo 4.2:** Sea  $\mathcal{C}_o$  un  $[5, 2]$ -código con matriz generadora sistemática

$$G = \begin{pmatrix} I_2 \\ P \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & \alpha \\ \alpha & \alpha^2 \\ 0 & 0 \end{pmatrix}.$$

Observemos que la parte no sistemática  $P$  de  $G$  tiene  $\text{rg}(P) = 1 < 2$ , por tanto, según el teorema 1.2,  $\mathcal{C}_o$  no es un código MDS. De hecho,  $d_{min}(\mathcal{C}_o) = 2 < 4$ , que es la cota Singleton.

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  un  $(6, 3, 1)$ -código interno descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha \end{pmatrix}, \quad B_2 = \begin{pmatrix} \alpha & 0 & 1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 \\ \alpha^2 \\ \alpha^3 \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ \alpha^2 & 1 & \alpha^3 \\ \alpha & \alpha^4 & \alpha^6 \end{pmatrix},$$

que tiene perfil de distancia máxima y distancia libre  $d_{free}(\mathcal{C}_i) = 4$ .

Por otro lado, por los teoremas 4.7 y 4.9, tenemos que las matrices

$$A = \begin{pmatrix} \alpha \end{pmatrix}, \quad B = \begin{pmatrix} \alpha & \alpha^2 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ \alpha^2 \\ \alpha^3 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{y} \quad D = \begin{pmatrix} \alpha^6 & 1 \\ \alpha^4 & \alpha^5 \\ \alpha^6 & 1 \\ 1 & \alpha \\ \alpha & \alpha^2 \\ 0 & 0 \end{pmatrix}$$

forman una representación minimal del código observable  $\mathcal{BC}_{\text{sys}}^{(2)}$ . Además,

$$d_{\text{free}}(\mathcal{BC}_{\text{sys}}^{(2)}) = 2 < 4 = d_{\text{free}}(\mathcal{C}_i). \quad \blacksquare$$

Tal y como mostramos en un resultado posterior, el hecho de que la matriz  $P$  tenga rango completo por columnas, asegura que la distancia libre de  $\mathcal{C}_i$  sea una cota inferior de  $d_{\text{free}}(\mathcal{BC}_{\text{sys}}^{(2)})$ . Previamente, proporcionamos un lema técnico acerca de las distancias columnas de  $\mathcal{BC}_{\text{sys}}^{(2)}$ .

**Lema 4.2:** *Sea  $\mathcal{BC}_{\text{sys}}^{(2)}$  el código dado por el teorema 4.7 obtenido de la concatenación del código externo  $\mathcal{C}_o$  y el código interno  $\mathcal{C}_i$ . Entonces,*

- (a)  $d_j^c(\mathcal{BC}_{\text{sys}}^{(2)}) \geq d_{\min}(\mathcal{C}_o)$  para  $j = 0, 1, 2, \dots$
- (b) Si además  $\text{rg}(P) = k$ , entonces  $d_j^c(\mathcal{BC}_{\text{sys}}^{(2)}) \geq d_j^c(\mathcal{C}_i) + 1$  para  $j = 0, 1, 2, \dots$

DEMOSTRACIÓN: Teniendo en cuenta las relaciones entre  $y_t, y_t^{(1)}, y_t^{(2)}, u_t, u_t^{(1)}, u_t^{(2)}$  y  $v_t, v_t^{(1)}, v_t^{(2)}$  dadas por las expresiones (4.7), (4.8), (4.9) y (4.14) (véanse también los comentarios previos al teorema 4.7), y empleando un argumento similar al usado para obtener la desigualdad (4.27) de la demostración del lema 4.1, obtenemos

$$\sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \geq \text{wt}(u_0^{(1)}) + \text{wt}(Pu_0^{(1)}) = \text{wt}(Gu_0^{(1)}).$$

Por tanto, de la expresión de la  $j$ -ésima distancia columna en términos de la representación entrada-estado-salida dada por la relación (1.19) y teniendo en cuenta que  $u_0 = u_0^{(1)}$ , obtenemos la desigualdad de la parte (a).

De manera similar, de las expresiones (4.8), (4.9) y (4.14) (véanse también los

comentarios previos al teorema 4.7), obtenemos

$$\begin{aligned}
\sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(v_t^{(1)}) \\
&= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(u_t^{(2)}) \\
&\geq \text{wt}(u_0^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(u_t^{(2)}).
\end{aligned}$$

Ahora, como  $u_t^{(2)} = Pu_t^{(1)}$  y  $\text{rg}(P) = k$ , tenemos que  $u_0 = u_0^{(1)} \neq 0$  si y sólo si  $u_0^{(2)} = Pu_0^{(1)} \neq 0$ . Por tanto, de la desigualdad anterior y de la expresión (1.19), tenemos que

$$\begin{aligned}
d_j^c(\mathcal{BC}_{\text{sys}}^{(2)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\
&\geq \min_{u_0^{(1)} \neq 0} \left\{ \text{wt}(u_0^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \sum_{t=0}^j \text{wt}(u_t^{(2)}) \right\} \\
&\geq d_j^c(\mathcal{C}_i) + 1,
\end{aligned} \tag{4.30}$$

ya que  $u_0 = u_0^{(1)}$ . □

Como consecuencia inmediata del lema anterior y de la expresión de la distancia libre en términos de la representación entrada-estado-salida dada por la relación (1.5), tenemos el resultado siguiente.

**Teorema 4.14:** *Sea  $\mathcal{BC}_{\text{sys}}^{(2)}$  el código dado por el teorema 4.7 obtenido de la concatenación del código bloque externo  $\mathcal{C}_o$  y del código convolucional interno  $\mathcal{C}_i$ . Entonces,*

- (a)  $d_{\text{free}}(\mathcal{BC}_{\text{sys}}^{(2)}) \geq d_{\text{min}}(\mathcal{C}_o)$ .
- (b) *Si además  $\text{rg}(P) = k$ , entonces  $d_{\text{free}}(\mathcal{BC}_{\text{sys}}^{(2)}) \geq d_{\text{free}}(\mathcal{C}_i) + 1$ .*

## 4.5 Códigos concatenados con perfil de distancia máxima y fuertemente MDS

En la sección anterior, hemos obtenido cotas inferiores para las distancias columnas de los diferentes modelos de concatenación de un código bloque con un código convolucional. Ahora bien, ¿cómo podemos obtener un código concatenado óptimo, es decir, que sea fuertemente MDS? Es lógico pensar que si los códigos constituyentes de la concatenación son los mejores posibles, esto es, el código externo es un código bloque MDS y el código interno es un código convolucional fuertemente MDS, entonces, el código concatenado tendrá la mayor distancia libre posible. Ahora bien, en general, este resultado no es válido para los códigos concatenados  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$ , como podemos comprobar en los ejemplos siguientes. A lo largo de esta sección, suponemos que los códigos concatenados están descritos por una representación entrada-estado-salida minimal de manera que el par  $(A, C)$  es observable, por lo que, en particular, dichos códigos serán no catastróficos.

**Ejemplo 4.3:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y consideremos el  $[3, 2]$ -código MDS  $\mathcal{C}_o$  con matriz generadora

$$G = \begin{pmatrix} \alpha^3 & \alpha^6 \\ \alpha & \alpha^2 \\ 1 & 1 \end{pmatrix}.$$

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  el  $(4, 3, 1)$ -código descrito por las matrices

$$A_2 = \begin{pmatrix} 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

Notemos que el par  $(A_2, C_2)$  es observable. Es más, por el teorema 1.13, tenemos que  $\mathcal{C}_i$  es un código convolucional fuertemente MDS con distancia libre  $d_{\text{free}}(\mathcal{C}_i) = d_1^c(\mathcal{C}_i) = 3$ .

Por otro lado, aplicando los teoremas 4.1 y 4.9, una representación minimal para el  $(3, 2, 1)$ -código observable  $\mathcal{BC}^{(1)}$  viene dada por las matrices

$$A = \begin{pmatrix} 1 \end{pmatrix}, \quad B = \begin{pmatrix} \alpha^3 & \alpha \end{pmatrix}, \quad C = \begin{pmatrix} 1 \end{pmatrix} \quad \text{y} \quad D = \begin{pmatrix} 0 & 0 \end{pmatrix}.$$

Pero  $\mathcal{BC}^{(1)}$  no es un código convolucional MDS ya que  $d_{\text{free}}(\mathcal{BC}^{(1)}) = 2 < 3$ , que es la cota Singleton generalizada. ■

**Ejemplo 4.4:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y consideremos el  $[4, 1]$ -código MDS  $\mathcal{C}_o$  con matriz generadora dada en forma sistemática por

$$G = \begin{pmatrix} 1 \\ \alpha \\ 1 \\ \alpha^3 \end{pmatrix} = \begin{pmatrix} I_1 \\ P \end{pmatrix}.$$

Sea  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  el  $(4, 3, 1)$ -código fuertemente MDS del ejemplo 4.3.

Aplicando los teoremas 4.3 y 4.9, una representación minimal del  $(2, 1, 1)$ -código observable  $\mathcal{BC}_{\text{sys}}^{(1)}$  viene dada por las matrices

$$A = \begin{pmatrix} 1 \end{pmatrix}, \quad B = \begin{pmatrix} \alpha^5 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \end{pmatrix} \quad \text{y} \quad D = \begin{pmatrix} 0 \end{pmatrix}.$$

Pero  $d_{\text{free}}(\mathcal{BC}_{\text{sys}}^{(1)}) = 3 < 4$ , que es la cota Singleton generalizada. Por tanto, el código concatenado  $\mathcal{BC}_{\text{sys}}^{(1)}$  no es un código covolucional MDS. ■

Como consecuencia de los ejemplos anteriores, tenemos que el hecho de que los códigos constituyentes sean códigos óptimos, no garantiza que los códigos concatenados  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$  tengan la mayor distancia libre posible. Es más, puede ocurrir que los códigos externo e interno tengan distancia mínima no buena y distancia libre no buena, respectivamente, y sin embargo, los códigos concatenados  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$  sean fuertemente MDS, como podemos ver en los ejemplos siguientes.

**Ejemplo 4.5:** Sea  $\alpha$  un elemento primitivo de  $GF(8)$  y sea  $\mathcal{C}_o$  el  $[2, 1]$ -código con matriz generadora

$$G = \begin{pmatrix} \alpha \\ 0 \end{pmatrix}.$$

Como  $d_{\text{min}}(\mathcal{C}_o) = 1 < 2$ , tenemos que  $\mathcal{C}_o$  no es MDS.

Consideremos ahora el  $(3, 2, 1)$ -código  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} 1 & 0 \end{pmatrix}.$$

Entonces, el par  $(A_2, C_2)$  es observable. Es más, obtenemos que  $d_{\text{free}}(\mathcal{C}_i) = 1 < 3$ , que es la cota Singleton generalizada, luego  $\mathcal{C}_i$  no es un código convolucional MDS.

Por otro lado, aplicando los teoremas 4.1 y 4.9, una representación minimal para el  $(2, 1, 1)$ -código observable  $\mathcal{BC}^{(1)}$  viene dada por las matrices

$$A = \begin{pmatrix} \alpha \end{pmatrix}, \quad B = \begin{pmatrix} \alpha \end{pmatrix}, \quad C = \begin{pmatrix} 1 \end{pmatrix} \quad \text{y} \quad D = \begin{pmatrix} \alpha \end{pmatrix}.$$

Es más,  $d_2^c(\mathcal{BC}^{(1)}) = 4$ , que es la cota Singleton generalizada, luego el código concatenado  $\mathcal{BC}^{(1)}$  es un código convolucional fuertemente MDS. ■

**Ejemplo 4.6:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  y sea  $\mathcal{C}_o$  el  $[3, 1]$ -código con matriz generadora en forma sistemática dada por

$$G = \begin{pmatrix} 1 \\ \alpha \\ 0 \end{pmatrix} = \begin{pmatrix} I_1 \\ P \end{pmatrix}.$$

Obtenemos entonces que  $d_{min}(\mathcal{C}_o) = 2 < 3$ , que es la cota Singleton. Por tanto,  $\mathcal{C}_o$  es un código bloque no MDS.

Consideremos ahora el  $(3, 2, 1)$ -código  $\mathcal{C}_i(A_2, B_2, C_2, D_2)$  descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} \alpha^6 \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} 1 & 0 \end{pmatrix}.$$

Notemos que el par  $(A_2, C_2)$  es observable. Es más, obtenemos que  $d_{free}(\mathcal{C}_i) = 1 < 3$ , que es la cota Singleton generalizada, luego  $\mathcal{C}_i$  es un código convolucional no MDS.

Por otro lado, aplicando los teoremas 4.3 y 4.9, una representación minimal para el  $(2, 1, 1)$ -código observable  $\mathcal{BC}_{sys}^{(1)}$  viene dada por las matrices

$$A = \begin{pmatrix} \alpha \end{pmatrix}, \quad B = \begin{pmatrix} \alpha \end{pmatrix}, \quad C = \begin{pmatrix} \alpha^6 \end{pmatrix} \quad \text{y} \quad D = \begin{pmatrix} \alpha \end{pmatrix}.$$

Es más,  $d_2^c(\mathcal{BC}_{sys}^{(1)}) = 4$ , que es la cota Singleton generalizada. Por tanto,  $\mathcal{BC}_{sys}^{(1)}$  es un código convolucional fuertemente MDS. ■

Observando los ejemplos anteriores, podemos concluir que los códigos concatenados  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  no heredan necesariamente las propiedades de las distancias libres de los códigos constituyentes. En el teorema siguiente proporcionamos condiciones suficientes para que los códigos concatenados sean fuertemente MDS.

**Teorema 4.15:**

- (a) Sea  $\mathcal{BC}^{(1)}$  el código descrito por la expresión (4.6) obtenido de la concatenación del  $[m, k]$ -código externo  $\mathcal{C}_o$  y del  $(m + 1, m, 1)$ -código interno  $\mathcal{C}_i$ , siendo  $k > 1$ .

Si la matriz  $\begin{pmatrix} D_2G \\ C_2B_2G \end{pmatrix}$  es la parte no sistemática de la matriz generadora de

un  $[k + 2, k]$ -código MDS, entonces  $\mathcal{BC}^{(1)}$  es un  $(k + 1, k, 1)$ -código con perfil de distancia máxima.

(b) Sea  $\mathcal{BC}_{sys}^{(1)}$  el código descrito por la expresión (4.10), obtenido de la concatenación del  $[m, k]$ -código externo  $\mathcal{C}_o$  y del  $(m - k + 1, m - k, 1)$ -código interno  $\mathcal{C}_i$ , siendo  $k > 1$ . Si la matriz  $\begin{pmatrix} D_2P \\ C_2B_2P \end{pmatrix}$  es la parte no sistemática de la matriz generadora de un  $[k + 2, k]$ -código MDS, entonces  $\mathcal{BC}_{sys}^{(1)}$  es un  $(k + 1, k, 1)$ -código con perfil de distancia máxima.

DEMOSTRACIÓN: Denotemos por  $\mathcal{BC}$  el código  $\mathcal{BC}^{(1)}$  así como el código  $\mathcal{BC}_{sys}^{(1)}$  y sea  $\tilde{G}$  la matriz generadora  $G$  o bien la parte no sistemática de  $G$ . Observemos que al ser  $\mathcal{BC}$  un  $(k + 1, k, 1)$ -código y  $k > 1$ , el valor del parámetro  $L$  definido por la relación (1.6), en este caso es  $L = \lfloor \frac{1}{k} \rfloor + \lfloor \frac{1}{1} \rfloor = 1$ . Ahora, teniendo en cuenta que

$$\begin{pmatrix} I_k \\ D_2\tilde{G} \\ C_2B_2\tilde{G} \end{pmatrix}$$

es la matriz generadora sistemática de un  $[k + 2, k]$ -código MDS, obtenemos, aplicando el teorema 1.2, que cada menor de la matriz

$$\mathcal{T}_1 = \begin{pmatrix} D_2\tilde{G} & O \\ C_2B_2\tilde{G} & D_2\tilde{G} \end{pmatrix}$$

que es no trivialmente nulo, es no nulo. Por tanto, aplicando el teorema 1.13,  $\mathcal{BC}$  es un código convolucional con perfil de distancia máxima.  $\square$

Como consecuencia del teorema anterior y teniendo en cuenta la observación 1.1, obtenemos el resultado siguiente.

**Corolario 4.4:**

(a) Sea  $\mathcal{BC}^{(1)}$  el código descrito por la expresión (4.6) obtenido de la concatenación del  $[m, k]$ -código externo  $\mathcal{C}_o$  y del  $(m + 1, m, 1)$ -código interno  $\mathcal{C}_i$ , con  $k > 1$ . Si la matriz  $\begin{pmatrix} D_2G \\ C_2B_2G \end{pmatrix}$  es la parte no sistemática de la matriz generadora de un  $[k + 2, k]$ -código MDS, entonces  $\mathcal{BC}^{(1)}$  es un  $(k + 1, k, 1)$ -código fuertemente MDS.

(b) Sea  $\mathcal{BC}_{sys}^{(1)}$  el código descrito por la expresión (4.10), obtenido de la concatenación del  $[m, k]$ -código externo  $\mathcal{C}_o$  y del  $(m - k + 1, m - k, 1)$ -código interno  $\mathcal{C}_i$ , con  $k > 1$ . Si la matriz  $\begin{pmatrix} D_2P \\ C_2B_2P \end{pmatrix}$  es la parte no sistemática de la matriz generadora de un  $[k + 2, k]$ -código MDS, entonces  $\mathcal{BC}_{sys}^{(1)}$  es un  $(k + 1, k, 1)$ -código fuertemente MDS.

Si el código bloque externo tiene dimensión  $k = 1$ , obtenemos un resultado similar al teorema 4.15.

**Teorema 4.16:** Sea  $\mathcal{BC}^{(1)}$  el código descrito por la expresión (4.6) obtenido de la concatenación del  $[m, 1]$ -código externo  $\mathcal{C}_o$  y del  $(m + 1, m, 1)$ -código interno  $\mathcal{C}_i$ . Si los vectores

$$D_2^T, \quad (C_2B_2)^T, \quad (C_2A_2B_2)^T \quad \text{y} \quad (C_2B_2GC_2B_2 - C_2A_2B_2GD_2)^T$$

no pertenecen al código dual de  $\mathcal{C}_o$ , entonces el código concatenado  $\mathcal{BC}^{(1)}$  es un  $(2, 1, 1)$ -código con perfil de distancia máxima.

DEMOSTRACIÓN: Las condiciones del teorema y la definición del código dual de  $\mathcal{C}_o$  permiten asegurar que la matriz

$$\mathcal{T}_2 = \begin{pmatrix} D & O & O \\ CB & D & O \\ CAB & CB & D \end{pmatrix} = \begin{pmatrix} D_2G & O & O \\ C_2B_2G & D_2G & O \\ C_2A_2B_2G & C_2B_2G & D_2G \end{pmatrix}$$

tiene la propiedad de que todo menor que no es trivialmente nulo, es no nulo (observemos que en este caso,  $L = \lfloor \frac{1}{1} \rfloor + \lfloor \frac{1}{1} \rfloor = 2$ ). De este modo, aplicando el teorema 1.13, obtenemos que  $\mathcal{BC}^{(1)}$  es un código con perfil de distancia máxima.  $\square$

Las condiciones del teorema anterior, permiten asegurar que  $\mathcal{BC}^{(1)}$  es un  $(2, 1, 1)$ -código con perfil de distancia máxima. Es más, con las condiciones de dicho teorema,  $n - k = 2 - 1$  divide a  $\delta = 1$ , y teniendo en cuenta la observación 1.1, obtenemos el corolario siguiente.

**Corolario 4.5:** Sea  $\mathcal{C}_o$  un  $[m, 1]$ -código y sea  $\mathcal{C}_i$  un  $(m + 1, m, 1)$ -código. Sea  $\mathcal{BC}^{(1)}(A, B, C, D)$  el código concatenado descrito por la expresión (4.6). Si los vectores

$$D_2^T, \quad (C_2B_2)^T, \quad (C_2A_2B_2)^T \quad \text{y} \quad (C_2B_2GC_2B_2 - C_2A_2B_2GD_2)^T$$

no pertenecen al código dual de  $\mathcal{C}_o$ , entonces el código concatenado  $\mathcal{BC}^{(1)}$  es un  $(2, 1, 1)$ -código fuertemente MDS.

Para el código concatenado  $\mathcal{BC}_{sys}^{(1)}$ , obtenemos un resultado similar al del teorema 4.16 para el caso particular en que el código externo tenga dimensión  $k = 1$ . La demostración es análoga a la del teorema anterior.

**Teorema 4.17:** Sea  $\mathcal{BC}_{sys}^{(1)}$  el código concatenado descrito por la expresión (4.10), obtenido de la concatenación del  $[m, 1]$ -código externo  $\mathcal{C}_o$  y del  $(m, m - 1, 1)$ -código interno  $\mathcal{C}_i$ . Si los vectores

$$\begin{pmatrix} O \\ D_2^T \end{pmatrix}, \quad \begin{pmatrix} O \\ (C_2B_2)^T \end{pmatrix}, \quad \begin{pmatrix} O \\ (C_2A_2B_2)^T \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} O \\ (C_2B_2GC_2B_2 - C_2A_2B_2GD_2)^T \end{pmatrix}$$

no pertenecen al código dual de  $\mathcal{C}_o$ , entonces el código concatenado  $\mathcal{BC}_{sys}^{(1)}$  es un  $(2, 1, 1)$ -código con perfil de distancia máxima.

Como consecuencia del teorema anterior y de la observación 1.1, obtenemos el corolario siguiente.

**Corolario 4.6:** Sea  $\mathcal{BC}_{sys}^{(1)}$  el código concatenado descrito por la expresión (4.10), obtenido de la concatenación del  $[m, 1]$ -código externo  $\mathcal{C}_o$  y del  $(m, m - 1, 1)$ -código interno  $\mathcal{C}_i$ . Si los vectores

$$\begin{pmatrix} O \\ D_2^T \end{pmatrix}, \quad \begin{pmatrix} O \\ (C_2B_2)^T \end{pmatrix}, \quad \begin{pmatrix} O \\ (C_2A_2B_2)^T \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} O \\ (C_2B_2GC_2B_2 - C_2A_2B_2GD_2)^T \end{pmatrix}$$

no pertenecen al código dual de  $\mathcal{C}_o$ , entonces el código concatenado  $\mathcal{BC}_{sys}^{(1)}$  es un  $(2, 1, 1)$ -código fuertemente MDS.

Finalmente, para los códigos concatenados  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$ , no es posible obtener condiciones para que estas concatenaciones tengan perfil de distancia máxima. De hecho, tal y como mostramos en el teorema siguiente, estos códigos nunca pueden tener perfil de distancia máxima. La demostración es consecuencia del teorema 1.13 y del hecho de que la matriz  $C$  de los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  es  $C = \begin{pmatrix} C_2 \\ 0 \end{pmatrix}$ .

**Teorema 4.18:** Sean  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  los códigos concatenados descritos por las expresiones (4.13) y (4.15), respectivamente, obtenidos de la concatenación del código bloque externo  $\mathcal{C}_0$  y del código convolucional interno  $\mathcal{C}_1$ . Supongamos que el par  $(A, C)$  es observable. Entonces,  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  no pueden tener perfil de distancia máxima.

**Observación 4.2:** Como consecuencia del teorema 4.18 y de la observación 1.1, obtenemos que en el caso en que  $(n - k)$  divida a  $\delta$ , los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  no pueden ser fuertemente MDS. ■

## 4.6 Relaciones entre los diferentes modelos

Finalizamos el capítulo analizando las relaciones entre los diferentes modelos de concatenación estudiados en las secciones anteriores. Analizamos diferentes ejemplos de concatenación, así como las propiedades relacionadas con la distancia libre de los códigos concatenados.

### 4.6.1 Ejemplos en $\mathbb{F} = GF(4)$

Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(4)$  (véase la sección 1.1). Consideramos entonces el  $[3, 1]$ -código  $\mathcal{B}_k$  sobre  $\mathbb{F}$  generado por la matriz  $P_k$ , para  $k = 1, 2, 3$ , siendo

$$P_1 = \begin{pmatrix} \alpha^2 \\ \alpha \\ 1 \end{pmatrix}, \quad P_2 = \begin{pmatrix} \alpha \\ 0 \\ 1 \end{pmatrix} \quad \text{y} \quad P_3 = \begin{pmatrix} \alpha \\ 0 \\ 0 \end{pmatrix}$$

y consideramos también el  $[3, 2]$ -código  $\mathcal{B}_k$  sobre  $\mathbb{F}$  generado por la matriz  $P_k$ , para  $k = 4, 5, \dots, 9$ , siendo

$$P_4 = \begin{pmatrix} 1 & \alpha \\ \alpha^2 & 0 \\ \alpha & 1 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & \alpha^2 \\ \alpha & \alpha \\ \alpha^2 & 1 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 1 & 1 \\ \alpha^2 & \alpha \\ \alpha^2 & 1 \end{pmatrix},$$

$$P_7 = \begin{pmatrix} 1 & \alpha \\ \alpha & \alpha^2 \\ \alpha^2 & 0 \end{pmatrix}, \quad P_8 = \begin{pmatrix} 0 & \alpha^2 \\ 1 & \alpha \\ \alpha & \alpha^2 \end{pmatrix}, \quad P_9 = \begin{pmatrix} 1 & \alpha^2 \\ \alpha^2 & \alpha^2 \\ \alpha & \alpha \end{pmatrix}$$

Entonces, para  $k = 1, 4, 5, 6$ ,  $\mathcal{B}_k$  es un código bloque MDS mientras que para  $k = 2, 3, 7, 8, 9$ ,  $\mathcal{B}_k$  es un código bloque no MDS. Asimismo, consideramos los códigos bloque  $\mathcal{B}_k^s$ , para  $k = 1, 2, 3$  generados por las matrices sistemáticas  $G_k = \begin{pmatrix} I_1 \\ P_k \end{pmatrix}$  y los códigos

bloque  $\mathcal{B}_k^s$ , para  $k = 4, 5, \dots, 9$  generados por las matrices sistemáticas  $G_k = \begin{pmatrix} I_2 \\ P_k \end{pmatrix}$ .

Entonces,  $\mathcal{B}_k^s$  es un código bloque MDS para  $k = 1, 5, 6$  y es un código bloque no MDS para  $k = 2, 3, 4, 7, 8, 9$ .

Consideremos ahora el  $(4, 3, 1)$ -código  $\mathcal{C}_i(A_k, B_k, C_k, D_k)$ , para  $k = 1, 2, 3$  descrito por las matrices  $A_k, B_k, C_k$  y  $D_k$ , siendo

$$A_1 = \begin{pmatrix} 1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 1 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 1 & 1 & \alpha \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 1 \end{pmatrix}, \quad B_3 = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}, \quad C_3 = \begin{pmatrix} 1 \end{pmatrix}, \quad D_3 = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}.$$

Entonces, para  $k = 1$ ,  $\mathcal{C}_i(A_k, B_k, C_k, D_k)$  es un código convolucional fuertemente MDS, mientras que para  $k = 2, 3$ ,  $\mathcal{C}_i(A_k, B_k, C_k, D_k)$  es un código convolucional no MDS.

Con objeto de relacionar los distintos modelos de concatenación, denotaremos por  $\tilde{\mathcal{B}}_k$  tanto el código bloque  $\mathcal{B}_k$  (si consideramos los modelos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) como el código bloque  $\mathcal{B}_k^s$  (si consideramos los modelos  $\mathcal{BC}_{\text{sys}}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$ ).

**Ejemplo 4.7:** En la tabla 4.1 hemos considerado como código externo los códigos bloque no MDS  $\mathcal{B}_3$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_3^s$  (para las concatenaciones  $\mathcal{BC}_{\text{sys}}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$ ) y como código interno, el código convolucional no MDS  $\mathcal{C}_2$ .

Concatenación de los códigos $\tilde{\mathcal{B}}_3$ y $\mathcal{C}_2$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_3) = 1$ No MDS	$d_{free}(\mathcal{C}_2) = 2$  No MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} \alpha \end{pmatrix}$	No MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 5$	$d_{min}(\mathcal{B}_3^s) = 2$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha \\ \alpha \\ 0 \\ 0 \end{pmatrix}$	No MDS		

Tabla 4.1: Códigos del ejemplo 4.7

Concatenación de los códigos $\tilde{\mathcal{B}}_7$ y $\mathcal{C}_3$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} 0 & \alpha^2 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 2$	$d_{min}(\mathcal{B}_7) = 1$ No MDS	$d_{free}(\mathcal{C}_3) = 2$  No MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} \alpha^2 & 1 \end{pmatrix}$	No MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} 0 & \alpha^2 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 5$	$d_{min}(\mathcal{B}_7^s) = 3$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha^2 & 1 \\ 1 & \alpha \\ \alpha & \alpha^2 \\ \alpha^2 & 0 \end{pmatrix}$	No MDS		

Tabla 4.2: Códigos del ejemplo 4.7

Del mismo modo, en la tabla 4.2, hemos considerado como código externo, los códigos bloque no MDS  $\mathcal{B}_7$  y  $\mathcal{B}_7^s$  y como código interno, el código convolucional no MDS  $\mathcal{C}_3$ . En ambos casos, obtenemos que los diferentes modelos de códigos concatenados son no MDS.

**Ejemplo 4.8:** En la tabla 4.3 hemos considerado como código externo los códigos

Concatenación de los códigos $\tilde{\mathcal{B}}_1$ y $\mathcal{C}_2$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^2 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_1) = 3$ No MDS	$d_{free}(\mathcal{C}_2) = 2$  No MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} \alpha^2 \end{pmatrix}$	No MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^2 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 9$	$d_{min}(\mathcal{B}_1^s) = 4$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha^2 \\ \alpha^2 \\ \alpha \\ 1 \end{pmatrix}$	No MDS		

Tabla 4.3: Códigos del ejemplo 4.8

Concatenación de los códigos $\tilde{\mathcal{B}}_5$ y $\mathcal{C}_3$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} 0 & \alpha^2 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 2$	$d_{min}(\mathcal{B}_5) = 2$ MDS	$d_{free}(\mathcal{C}_3) = 2$  No MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} \alpha^2 & 1 \end{pmatrix}$	No MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} 0 & \alpha^2 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 5$	$d_{min}(\mathcal{B}_5^s) = 4$ MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha^2 & 1 \\ 1 & \alpha^2 \\ \alpha & \alpha \\ \alpha^2 & 1 \end{pmatrix}$	No MDS		

Tabla 4.4: Códigos del ejemplo 4.8

bloque MDS  $\mathcal{B}_1$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_1^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional no MDS  $\mathcal{C}_2$ .

Análogamente, en la tabla 4.4, hemos considerado como código externo, los códigos bloque MDS  $\mathcal{B}_5$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_5^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional no MDS  $\mathcal{C}_3$ . En ambos

Concatenación de los códigos $\widetilde{\mathcal{B}}_3$ y $\mathcal{C}_1$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \\ \end{pmatrix}, B = \begin{pmatrix} \alpha \\ \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_3) = 1$ No MDS	$d_c^1(\mathcal{C}_1) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \\ \end{pmatrix}, D = \begin{pmatrix} \alpha \\ \end{pmatrix}$	No MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \\ \end{pmatrix}, B = \begin{pmatrix} \alpha \\ \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 5$	$d_{min}(\mathcal{B}_3^s) = 2$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha \\ \alpha \\ 0 \\ 0 \end{pmatrix}$	No MDS		

Tabla 4.5: Códigos del ejemplo 4.9

casos, a pesar de ser el código externo un código bloque MDS, obtenemos que los diferentes modelos de códigos concatenados no son MDS.

**Ejemplo 4.9:** En la tabla 4.5 hemos considerado como código externo los códigos bloque no MDS  $\mathcal{B}_3$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_3^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional fuertemente MDS  $\mathcal{C}_1$ . Obtenemos entonces que los diferentes modelos de códigos concatenados, son códigos convolucionales no MDS, aunque el código convolucional interno sea fuertemente MDS.

**Ejemplo 4.10:** La tabla 4.6 muestra que la concatenación de un código bloque MDS con un código convolucional fuertemente MDS no es necesariamente MDS. Hemos considerado como código externo, los códigos bloque MDS  $\mathcal{B}_1$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_1^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional fuertemente MDS  $\mathcal{C}_1$ . Ninguno de los modelos de concatenación es MDS.

**Ejemplo 4.11:** Si concatenamos un código bloque no MDS y un código convolucional no MDS, podemos obtener un código convolucional MDS, como muestra la tabla 4.7, en la que hemos considerado como código externo los códigos bloque no MDS  $\mathcal{B}_9$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_9^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y

Concatenación de los códigos $\tilde{\mathcal{B}}_1$ y $\mathcal{C}_1$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^2 \\ 0 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_1) = 3$ MDS	$d_c^1(\mathcal{C}_1) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, D = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$	No MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^2 \\ 0 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 9$	$d_{min}(\mathcal{B}_1^s) = 4$ MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} 0 \\ \alpha^2 \\ \alpha \\ 1 \end{pmatrix}$	No MDS		

Tabla 4.6: Códigos del ejemplo 4.10

Concatenación de los códigos $\tilde{\mathcal{B}}_9$ y $\mathcal{C}_3$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} 1 & \alpha^2 \\ \alpha & 0 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_9) = 1$ No MDS	$d_{free}(\mathcal{C}_3) = 2$  No MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, D = \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}$	MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} 1 & \alpha^2 \\ \alpha & 0 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 5$	$d_{min}(\mathcal{B}_9^s) = 3$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha & 0 \\ 1 & \alpha^2 \\ \alpha^2 & \alpha^2 \\ \alpha & \alpha \end{pmatrix}$	No MDS		

Tabla 4.7: Códigos del ejemplo 4.11

como código interno, el código convolucional no MDS  $\mathcal{C}_3$ . Observamos entonces que los códigos concatenados  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  son códigos convolucionales MDS, pero  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$  son códigos convolucionales no MDS.

**Ejemplo 4.12:** En la tabla 4.8, hemos considerado como código externo el código bloque MDS  $\mathcal{B}_4$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y el código bloque no MDS  $\mathcal{B}_4^s$

Concatenación de los códigos $\widetilde{\mathcal{B}}_4$ y $\mathcal{C}_1$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_4) = 2$ MDS	$d_c^1(\mathcal{C}_1) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, D = \begin{pmatrix} 0 & \alpha^2 \end{pmatrix}$	MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 6$	$d_{min}(\mathcal{B}_4^s) = 3$ No MDS	Fuertemente MDS
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} 0 & \alpha^2 \\ 1 & \alpha \\ \alpha^2 & 0 \\ \alpha & 1 \end{pmatrix}$	MDS		

Tabla 4.8: Códigos del ejemplo 4.12

(para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional fuertemente MDS  $\mathcal{C}_1$ . Obtenemos entonces que los diferentes modelos de códigos concatenados, son códigos convolucionales MDS.

**Ejemplo 4.13:** En la tabla 4.9, hemos considerado como código externo los códigos bloque no MDS  $\mathcal{B}_2$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_2^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional fuertemente MDS  $\mathcal{C}_1$ . Obtenemos entonces que los códigos concatenados  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  verifican las condiciones de los corolarios 4.5 y 4.6, y por tanto son fuertemente MDS. Ahora bien, los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$ , son códigos convolucionales no MDS.

**Ejemplo 4.14:** La tabla 4.10 muestra que la concatenación según los modelos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  puede dar lugar a un código convolucional fuertemente MDS, aunque el código interno sea un código convolucional no MDS. Hemos considerado como código externo los códigos bloque MDS  $\mathcal{B}_6$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_6^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional no MDS  $\mathcal{C}_3$ . Entonces, los códigos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  verifican las condiciones del corolario 4.4 y por tanto, son códigos convolucionales fuertemente MDS. Sin embargo, los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$  no son MDS.

Concatenación de los códigos $\tilde{\mathcal{B}}_2$ y $\mathcal{C}_1$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$	$d_2^c(\mathcal{BC}) = 4$	$d_{min}(\mathcal{B}_2) = 2$ No MDS	$d_1^c(\mathcal{C}_1) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, D = \begin{pmatrix} \alpha^2 \\ \alpha^2 \end{pmatrix}$	Fuertemente MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 8$	$d_{min}(\mathcal{B}_2^s) = 3$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha^2 \\ \alpha \\ 0 \\ 1 \end{pmatrix}$	No MDS		

Tabla 4.9: Códigos del ejemplo 4.13

Concatenación de los códigos $\tilde{\mathcal{B}}_6$ y $\mathcal{C}_3$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} \alpha & 1 \\ \alpha & 1 \end{pmatrix},$	$d_1^c(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_6) = 2$ MDS	$d_{free}(\mathcal{C}_3) = 2$  No MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, D = \begin{pmatrix} \alpha & \alpha^2 \\ \alpha & \alpha^2 \end{pmatrix}$	Fuertemente MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} \alpha & 1 \\ \alpha & 1 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 5$	$d_{min}(\mathcal{B}_6^s) = 4$ MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha & \alpha^2 \\ 1 & 1 \\ \alpha^2 & \alpha \\ \alpha^2 & 1 \end{pmatrix}$	No MDS		

Tabla 4.10: Códigos del ejemplo 4.14

**Ejemplo 4.15:** La tabla 4.11 muestra que la concatenación según los modelos 1 y 2 (códigos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$ , respectivamente), puede dar lugar a códigos convolucionales fuertemente MDS aunque tanto el código externo como el código interno no sean MDS. Hemos considerado como código externo los códigos bloque no MDS  $\mathcal{B}_8$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_8^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional no MDS  $\mathcal{C}_3$ . Entonces, los códigos  $\mathcal{BC}^{(1)}$  y

Concatenación de los códigos $\widetilde{\mathcal{B}}_8$ y $\mathcal{C}_3$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^2 & \alpha \end{pmatrix},$	$d_1^c(\mathcal{BC}) = 3$ Fuertemente MDS	$d_{min}(\mathcal{B}_8) = 1$ No MDS	$d_{free}(\mathcal{C}_3) = 2$  No MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, D = \begin{pmatrix} 1 & 1 \end{pmatrix}$			
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^2 & \alpha \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 6$ MDS	$d_{min}(\mathcal{B}_8^s) = 3$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} 1 & 1 \\ 0 & \alpha^2 \\ 1 & \alpha \\ \alpha & \alpha^2 \end{pmatrix}$			

Tabla 4.11: Códigos del ejemplo 4.15

$\mathcal{BC}_{sys}^{(1)}$  verifican las condiciones del corolario 4.4 y por tanto, son fuertemente MDS. Ahora bien, no obtenemos el mismo resultado para los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$ . Éstos son códigos convolucionales MDS pero no fuertemente MDS.

#### 4.6.2 Ejemplos en $\mathbb{F} = GF(8)$

Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(8)$  (véase la sección 1.1). Consideramos entonces el  $[2, 1]$ -código bloque  $\mathcal{B}_k$  sobre  $\mathbb{F}$  generado por la matriz  $P_k$ , para  $k = 10, 11, 12, 13$ , siendo

$$P_{10} = \begin{pmatrix} \alpha^3 \\ 1 \end{pmatrix}, \quad P_{11} = \begin{pmatrix} \alpha \\ 1 \end{pmatrix}, \quad P_{12} = \begin{pmatrix} \alpha^6 \\ \alpha \end{pmatrix}, \quad P_{13} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix}$$

y consideramos también el  $[3, 2]$ -código  $\mathcal{B}_k$  sobre  $\mathbb{F}$  generado por la matriz  $P_k$ , para  $k = 14, 15, 16, 17, 18$ , siendo

$$P_{14} = \begin{pmatrix} \alpha^3 & 1 \\ 1 & \alpha^2 \\ \alpha^6 & \alpha^4 \end{pmatrix}, \quad P_{15} = \begin{pmatrix} \alpha^3 & \alpha^6 \\ \alpha & \alpha^2 \\ 1 & 1 \end{pmatrix}, \quad P_{16} = \begin{pmatrix} \alpha^2 & \alpha^3 \\ 1 & \alpha \\ \alpha^6 & 0 \end{pmatrix},$$

$$P_{17} = \begin{pmatrix} \alpha^3 & \alpha^4 \\ 1 & \alpha \\ \alpha^6 & \alpha^3 \end{pmatrix}, \quad P_{18} = \begin{pmatrix} \alpha^3 & 1 \\ 1 & \alpha^4 \\ \alpha^6 & \alpha^2 \end{pmatrix}.$$

Entonces, para  $k = 10, 11, 12, 14, 15$ ,  $\mathcal{B}_k$  es un código bloque MDS mientras que para  $k = 13, 16, 17, 18$ ,  $\mathcal{B}_k$  es un código bloque no MDS. Asimismo, consideramos los  $[3, 1]$ -códigos  $\mathcal{B}_k^s$ , para  $k = 10, 11, 12, 13$ , generados por las matrices sistemáticas  $G_k = \begin{pmatrix} I_1 \\ P_k \end{pmatrix}$  y los  $[5, 2]$ -códigos  $\mathcal{B}_k^s$ , para  $k = 14, 15, 16, 17, 18$  generados por las matrices sistemáticas  $G_k = \begin{pmatrix} I_2 \\ P_k \end{pmatrix}$ . Entonces,  $\mathcal{B}_k^s$  es un código bloque MDS para  $k = 10, 11, 12, 14, 15$  y es un código bloque no MDS para  $k = 13, 16, 17, 18$ .

Consideremos el  $(3, 2, 1)$ -código  $\mathcal{C}_i(A_k, B_k, C_k, D_k)$ , para  $k = 4, 5, 6$  descrito por las matrices  $A_k, B_k, C_k$  y  $D_k$ , siendo

$$\begin{aligned} A_4 &= (\alpha), & B_4 &= (1 \ \alpha), & C_4 &= (1), & D_4 &= (1 \ 1), \\ A_5 &= (\alpha), & B_5 &= (1 \ \alpha), & C_5 &= (1), & D_5 &= (1 \ 0), \\ A_6 &= (\alpha), & B_6 &= (1 \ 0), & C_6 &= (1), & D_6 &= (1 \ 0), \end{aligned}$$

y consideremos el  $(4, 3, 1)$ -código  $\mathcal{C}_i(A_7, B_7, C_7, D_7)$  descrito por las matrices

$$A_7 = (1), \quad B_7 = (1 \ \alpha \ \alpha^2), \quad C_7 = (1) \quad \text{y} \quad D_7 = (1 \ 1 \ 1).$$

Entonces, para  $k = 4, 7$ ,  $\mathcal{C}_i(A_k, B_k, C_k, D_k)$  es un código convolucional fuertemente MDS; para  $k = 5$ ,  $\mathcal{C}_i(A_k, B_k, C_k, D_k)$  es un código convolucional MDS (no fuertemente MDS) y para  $k = 6$ ,  $\mathcal{C}_i(A_k, B_k, C_k, D_k)$  es un código convolucional no MDS.

**Ejemplo 4.16:** En la tabla 4.12, hemos considerado como código externo los códigos bloque MDS  $\mathcal{B}_{12}$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_{12}^s$  (para las concatenaciones  $\mathcal{BC}_{\text{sys}}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$ ) y como código interno, el código convolucional MDS (no fuertemente MDS)  $\mathcal{C}_5$ . Obtenemos entonces que todos los códigos concatenados son códigos convolucionales no MDS, aunque los códigos constituyentes sean MDS.

**Ejemplo 4.17:** Las tablas 4.13, 4.14 y 4.15 muestran que la concatenación de un código bloque no MDS y un código convolucional fuertemente MDS puede producir códigos convolucionales no MDS, MDS o bien fuertemente MDS. En las tres tablas,

Concatenación de los códigos $\tilde{\mathcal{B}}_{12}$ y $\mathcal{C}_5$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = (\alpha), B = (1),$	$d_{free}(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_{12}) = 2$ MDS	$d_{free}(\mathcal{C}_5) = 3$  MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = (1), D = (\alpha^6)$	No MDS		
$\mathcal{BC}^{(2)}$	$A = (\alpha), B = (1),$	$d_{free}(\mathcal{BC}) = 7$	$d_{min}(\mathcal{B}_{12}^s) = 3$ MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha^6 \\ \alpha^6 \\ \alpha \\ \alpha \end{pmatrix}$	No MDS		

Tabla 4.12: Códigos del ejemplo 4.16

Concatenación de los códigos $\tilde{\mathcal{B}}_{18}$ y $\mathcal{C}_7$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = (1), B = (\alpha^3 \ 0),$	$d_{free}(\mathcal{BC}) = 2$	$d_{min}(\mathcal{B}_{18}) = 1$ No MDS	$d_1^c(\mathcal{C}_7) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = (1), D = (\alpha^5 \ \alpha^3)$	No MDS		
$\mathcal{BC}^{(2)}$	$A = (1), B = (\alpha^3 \ 0),$	$d_{free}(\mathcal{BC}) = 5$	$d_{min}(\mathcal{B}_{18}^s) = 3$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha^5 & \alpha^3 \\ \alpha^3 & 1 \\ 1 & \alpha^4 \\ \alpha^6 & \alpha^2 \end{pmatrix}$	No MDS		

Tabla 4.13: Códigos del ejemplo 4.17

hemos considerado como código interno, el código convolucional  $\mathcal{C}_7$ , que es fuertemente MDS.

En la tabla 4.13, hemos considerado como código externo, los códigos bloque no MDS  $\mathcal{B}_{18}$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_{18}^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ), de manera que ninguno de los códigos concatenados es MDS.

Para la tabla 4.14, el código externo son los códigos bloque no MDS  $\mathcal{B}_{16}$  (para las

Concatenación de los códigos $\tilde{\mathcal{B}}_{16}$ y $\mathcal{C}_7$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^2 & \alpha^5 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_{16}) = 1$ No MDS	$d_1^c(\mathcal{C}_7) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \end{pmatrix}$	MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^2 & \alpha^5 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 6$	$d_{min}(\mathcal{B}_{16}^s) = 3$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \\ \alpha^2 & \alpha^3 \\ 1 & \alpha \\ \alpha^6 & 0 \end{pmatrix}$			

Tabla 4.14: Códigos del ejemplo 4.17

Concatenación de los códigos $\tilde{\mathcal{B}}_{17}$ y $\mathcal{C}_7$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^3 & \alpha^6 \end{pmatrix},$	$d_1^c(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_{17}) = 1$ No MDS	$d_1^c(\mathcal{C}_7) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} \alpha^5 & \alpha^5 \end{pmatrix}$	Fuertemente MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^3 & \alpha^6 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 6$	$d_{min}(\mathcal{B}_{17}^s) = 3$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha^5 & \alpha^5 \\ \alpha^3 & \alpha^4 \\ 1 & \alpha \\ \alpha^6 & \alpha^3 \end{pmatrix}$			

Tabla 4.15: Códigos del ejemplo 4.17

concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$  y  $\mathcal{B}_{16}^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ); obtenemos entonces que todos los códigos concatenados son MDS (aunque no fuertemente MDS).

Por último, en la tabla 4.15, como código externo hemos considerado los códigos bloque no MDS  $\mathcal{B}_{17}$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_{17}^s$  (para las con-

Concatenación de los códigos $\tilde{\mathcal{B}}_{15}$ y $\mathcal{C}_7$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^3 & \alpha \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 2$	$d_{min}(\mathcal{B}_{15}) = 2$ MDS	$d_1^c(\mathcal{C}_7) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} 0 & 0 \end{pmatrix}$	No MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^3 & \alpha \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 5$	$d_{min}(\mathcal{B}_{15}^s) = 4$ MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} 0 & 0 \\ \alpha^3 & \alpha^6 \\ \alpha & \alpha^2 \\ 1 & 1 \end{pmatrix}$	No MDS		

Tabla 4.16: Códigos del ejemplo 4.18

Concatenación de los códigos $\tilde{\mathcal{B}}_{14}$ y $\mathcal{C}_7$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^3 & \alpha^5 \end{pmatrix},$	$d_1^c(\mathcal{BC}) = 3$	$d_{min}(\mathcal{B}_{14}) = 2$ MDS	$d_1^c(\mathcal{C}_7) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} \alpha^3 & \alpha^5 \end{pmatrix}$	Fuertemente MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} 1 \end{pmatrix}, B = \begin{pmatrix} \alpha^3 & \alpha^5 \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 5$	$d_{min}(\mathcal{B}_{14}^s) = 4$ MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha^3 & \alpha^5 \\ \alpha^3 & 1 \\ 1 & \alpha^2 \\ \alpha^6 & \alpha^4 \end{pmatrix}$	No MDS		

Tabla 4.17: Códigos del ejemplo 4.18

catenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ . Obtenemos en este caso, que los códigos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  verifican las condiciones del corolario 4.4 y, por tanto, son fuertemente MDS, mientras que los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$  son MDS pero no fuertemente MDS.

**Ejemplo 4.18:** Las tablas 4.16, 4.17 y 4.18 muestran que la concatenación de un código bloque MDS y un código convolucional fuertemente MDS, puede dar lugar a

Concatenación de los códigos $\tilde{\mathcal{B}}_{10}$ y $\mathcal{C}_4$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = (\alpha), B = (1),$	$d_2^c(\mathcal{BC}) = 4$	$d_{min}(\mathcal{B}_{10}) = 2$ MDS	$d_1^c(\mathcal{C}_4) = 3$ Fuertemente MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = (1), D = (\alpha)$	Fuertemente MDS		
$\mathcal{BC}^{(2)}$	$A = (\alpha), B = (1),$	$d_{free}(\mathcal{BC}) = 8$ MDS	$d_{min}(\mathcal{B}_{10}^s) = 3$ MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha \\ \alpha^3 \\ 1 \end{pmatrix}$			

**Tabla 4.18:** Códigos del ejemplo 4.18

códigos no MDS, códigos MDS y códigos fuertemente MDS.

En concreto, para la tabla 4.16, hemos considerado como código externo, los códigos bloque MDS  $\mathcal{B}_{15}$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_{15}^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional fuertemente MDS  $\mathcal{C}_7$ . En este caso, ninguno de los modelos de concatenación es MDS.

En la tabla 4.17, hemos considerado como código externo, los códigos bloque MDS  $\mathcal{B}_{14}$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_{14}^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional fuertemente MDS  $\mathcal{C}_7$ . Entonces, los códigos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  verifican las condiciones del corolario 4.4 y por tanto, son fuertemente MDS, pero los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$  no son MDS.

Por último, en la tabla 4.18, hemos considerado como código externo el  $[2, 1]$ -código MDS  $\mathcal{B}_{10}$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y el  $[3, 1]$ -código MDS  $\mathcal{B}_{10}^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ), y como código interno, el código convolucional  $\mathcal{C}_4$  (fuertemente MDS). Obtenemos que en este caso, los códigos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  verifican las condiciones de los corolarios 4.5 y 4.6 y por tanto, son fuertemente MDS mientras que los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$  son MDS pero no fuertemente MDS.

**Ejemplo 4.19:** Las tablas 4.19 y 4.20 muestran que la concatenación de un código bloque MDS (no MDS) y un código convolucional no MDS (respectivamente, MDS) puede dar lugar a códigos fuertemente MDS.

En concreto, en la tabla 4.19 hemos considerado como código externo, los códigos

Concatenación de los códigos $\tilde{\mathcal{B}}_{11}$ y $\mathcal{C}_6$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha \end{pmatrix},$	$d_2^c(\mathcal{BC}) = 4$	$d_{min}(\mathcal{B}_{11}) = 2$ MDS	$d_{free}(\mathcal{C}_6) = 1$  No MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} \alpha \end{pmatrix}$	Fuertemente MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 8$ MDS	$d_{min}(\mathcal{B}_{11}^s) = 3$ MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha \\ \alpha \\ 1 \end{pmatrix}$			

Tabla 4.19: Códigos del ejemplo 4.19

Concatenación de los códigos $\tilde{\mathcal{B}}_{13}$ y $\mathcal{C}_5$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha \end{pmatrix},$	$d_2^c(\mathcal{BC}) = 4$	$d_{min}(\mathcal{B}_{13}) = 1$ No MDS	$d_{free}(\mathcal{C}_5) = 3$  MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} \alpha \end{pmatrix}$	Fuertemente MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 6$ No MDS	$d_{min}(\mathcal{B}_{13}^s) = 2$ No MDS	
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha \\ \alpha \\ 1 \end{pmatrix}$			

Tabla 4.20: Códigos del ejemplo 4.19

bloque MDS  $\mathcal{B}_{11}$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_{11}^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ), y como código interno, el código convolucional no MDS  $\mathcal{C}_6$ . Obtenemos entonces que los códigos concatenados  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  verifican las condiciones de los corolarios 4.5 y 4.6 y, por tanto, son fuertemente MDS. Ahora bien, los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$  son MDS pero no fuertemente MDS.

Para la tabla 4.20 hemos considerado como código externo, los códigos bloque no MDS  $\mathcal{B}_{13}$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_{13}^s$  (para las concatenaciones

Concatenación de los códigos $\tilde{\mathcal{B}}_{13}$ y $\mathcal{C}_6$				
Modelo	Representación de $\mathcal{BC}$	$d_{free}(\mathcal{BC})$	Código bloque	Código convolucional
$\mathcal{BC}^{(1)}$	$A = \begin{pmatrix} \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha \end{pmatrix},$	$d_2^c(\mathcal{BC}) = 4$	$d_{min}(\mathcal{B}_{13}) = 1$ No MDS	$d_{free}(\mathcal{C}_6) = 1$  No MDS
$\mathcal{BC}_{sys}^{(1)}$	$C = \begin{pmatrix} 1 \end{pmatrix}, D = \begin{pmatrix} \alpha \end{pmatrix}$	Fuertemente MDS		
$\mathcal{BC}^{(2)}$	$A = \begin{pmatrix} \alpha \end{pmatrix}, B = \begin{pmatrix} \alpha \end{pmatrix},$	$d_{free}(\mathcal{BC}) = 6$ No MDS	$d_{min}(\mathcal{B}_{13}^s) = 2$ No MDS	No MDS
$\mathcal{BC}_{sys}^{(2)}$	$C = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, D = \begin{pmatrix} \alpha \\ \alpha \\ 1 \end{pmatrix}$			

**Tabla 4.21:** Códigos del ejemplo 4.20

$\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional MDS  $\mathcal{C}_5$ . De nuevo, los códigos concatenados  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  son fuertemente MDS ya que verifican las condiciones de los corolarios 4.5 y 4.6, pero los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$  no son MDS. ■

**Ejemplo 4.20:** La tabla 4.21 muestra que la concatenación de dos códigos con no buenas distancias puede dar lugar a códigos fuertemente MDS. Hemos considerado como código externo, los códigos bloque no MDS  $\mathcal{B}_{13}$  (para las concatenaciones  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}^{(2)}$ ) y  $\mathcal{B}_{13}^s$  (para las concatenaciones  $\mathcal{BC}_{sys}^{(1)}$  y  $\mathcal{BC}_{sys}^{(2)}$ ) y como código interno, el código convolucional no MDS  $\mathcal{C}_6$ . Entonces, los códigos  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{sys}^{(1)}$  verifican las condiciones de los corolarios 4.5 y 4.6 y por tanto son fuertemente MDS, pero los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{sys}^{(2)}$  no son MDS. Observemos que en este ejemplo, obtenemos los mismos códigos concatenados que los obtenidos en la tabla 4.20.

## 4.7 Conclusiones

En este capítulo hemos caracterizado cuatro modelos de concatenación en serie de un código bloque con un código convolucional, introduciendo condiciones para obtener una representación entrada-estado-salida minimal y también para que el código concatenado sea no catastrófico. Del mismo modo, aportamos condiciones para obtener concatenaciones óptimas partiendo incluso de códigos no MDS. Además, teniendo en cuenta los ejemplos anteriores, podemos conjeturar que si los códigos convolucionales

$\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$  no son MDS, entonces los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  tampoco lo son (véanse las tablas 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.12, 4.13 y 4.16). Ahora bien, las tablas 4.8 y 4.14 muestran que si los dos primeros modelos de concatenación ( $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$ ) son códigos MDS, las concatenaciones  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  pueden ser MDS o bien, teniendo en cuenta la tabla 4.7, no MDS. Del mismo modo, si los códigos concatenados  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$  son fuertemente MDS, entonces los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  pueden ser MDS (véanse las tablas 4.11, 4.15, 4.18 y 4.19) o bien no ser MDS (véanse las tablas 4.9, 4.10, 4.17, 4.20 y 4.21).

Ahora bien, no podemos obtener una conjetura clara acerca de si el código  $\mathcal{BC}_{\text{sys}}^{(1)}$  es mejor (con distancia libre próxima o igual a la cota Singleton generalizada) que el código  $\mathcal{BC}^{(1)}$ . Del mismo modo, no podemos afirmar que el código  $\mathcal{BC}_{\text{sys}}^{(2)}$  sea mejor que el código  $\mathcal{BC}^{(2)}$ .

Si bien el hecho de que las palabras código de las concatenaciones  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  contengan a su vez a las palabras de los códigos constituyentes permite obtener cotas inferiores de las distancias libres de los códigos concatenados en función de las de los códigos externo e interno (relación que no tenemos para  $\mathcal{BC}^{(1)}$  y  $\mathcal{BC}_{\text{sys}}^{(1)}$ ), tal y como hemos visto en el teorema 4.18, los códigos  $\mathcal{BC}^{(2)}$  y  $\mathcal{BC}_{\text{sys}}^{(2)}$  no pueden tener perfil de distancia máxima, y por tanto, no pueden ser fuertemente MDS en los casos en que ambas propiedades sean equivalentes (véase la observación 4.2).



# Concatenación en paralelo de códigos convolucionales

---

*What is it indeed that gives us the feeling of elegance in a solution, in a demonstration? It is the harmony of the diverse parts, their symmetry, their happy balance; in a word it is all that introduces order, all that gives unity, that permits us to see clearly and to comprehend at once both the ensemble and the details.*

–Jules Henri Poincaré

*The mathematical sciences particularly exhibit order, symmetry, and limitation; and these are the greatest forms of the beautiful.*

–Aristóteles

## 5.1 Introducción

En 1993 Berrou, Glavieux y Thitimajshima, presentaron una nueva técnica correctora de errores con un esquema de decodificación iterativa asociado [13], que significó una revolución en el campo de la codificación de canal. Estos códigos fueron llamados **turbo códigos** y se conciben actualmente como el método más eficaz de generación de códigos con una alta capacidad de corrección de errores.

A finales de 1998 los turbo códigos comenzaron a considerarse en la estandarización del sistema UMTS (*Universal Mobile Telecommunications System*). Inicialmente se propusieron tres alternativas: turbo codificación convolucional en paralelo, turbo codificación convolucional en serie y turbo codificación bloque. Finalmente, se decidió optar por la turbo codificación convolucional en paralelo, y ésta, junto a la codificación

convolucional convencional, son las estrategias de codificación de canal consideradas actualmente en el foro 3GPP (*3rd Generation Partnership Project*), encargado de la estandarización de UTRA (*UMTS Terrestrial Radio Access*) [110, 111]. Es más, los turbo códigos se han convertido en un elemento imprescindible en las comunicaciones inalámbricas, vía satélite modernas y en comunicaciones en el espacio no sólo por la corrección de errores sino también porque necesita menos potencia de transmisión [16, 33, 34].

Los turbo códigos son códigos convolucionales obtenidos de la concatenación de dos o más códigos convolucionales recursivos sistemáticos separados por un entrelazado, cuya palabra código está formada por el vector de información y el vector de paridad de los dos códigos constituyentes. Costello, Massey, Collins y Takeshita [28] propusieron la posibilidad de emplear códigos recursivos no sistemáticos para los turbo códigos. Es más, Costello, Cabral y Takeshita [29] mostraron que empleando códigos recursivos no sistemáticos en los turbo códigos se podía alcanzar distancias libres más grandes que usando códigos recursivos sistemáticos. Ahora bien, los turbo códigos formados por códigos constituyentes recursivos no sistemáticos no convergen tan bien con decodificación iterativa como lo hacen los formados por códigos recursivos sistemáticos. Garello, Pierleoni y Benedetto [43], implementaron un algoritmo para computar la distancia libre de códigos concatenados en paralelo y en serie con intercalados, siendo éste aplicado por primera vez a casos prácticos de interés relevante, tales como el estándar Comité Consultivo para Sistemas de Datos Espaciales (CCSDS) y el estándar UMTS/3GPP para las comunicaciones personales de tercera generación [86, 103, 114]. Los turbo códigos han sido ampliamente estudiados, siendo la bibliografía asociada muy extensa (véase por ejemplo, [6, 7, 9, 10, 12, 43, 103, 110, 111, 114]).

Wu y Valenti [115] mostraron que los códigos convolucionales concatenados en paralelo pueden ser modelizados como un caso especial de códigos convolucionales concatenados en serie. En esta línea, Divsalar y Pollara [35] muestran la posibilidad de códigos concatenados híbridos, que combinan las concatenaciones en serie y en paralelo de códigos convolucionales de manera que se alcanza un rendimiento satisfactorio en todas las regiones SNR (*Signal to Noise Ratio*).

En este capítulo, analizamos cuatro modelos de concatenación en paralelo de códigos convolucionales desde el punto de vista de sistemas. Comenzamos describiendo, en la sección 5.2, dos modelos de concatenación, uno de ellos empleado en la teoría clásica de control, obteniendo la representación entrada-estado-salida de dichos modelos, así como condiciones para obtener tanto la controlabilidad del par  $(A, B)$  como la observabilidad

del par  $(A, C)$  (siendo  $A, B, C$  y  $D$  las matrices que describen las concatenaciones). En la sección 5.3 presentamos la construcción de un código convolucional obtenido al concatenar de forma paralela códigos convolucionales, de manera que el vector de entrada se subdivide en varios vectores que son entonces codificados por los códigos de la concatenación. Estudiamos entonces este modelo de concatenación, obteniendo propiedades de su matriz generadora y de su representación entrada-estado-salida en función de las propiedades de los códigos constituyentes. Finalmente, en la sección 5.4, analizamos el código *warp* descrito en la sección 1.6 desde el punto de vista de sistemas lineales.

## 5.2 Modelos de concatenación en paralelo

En esta sección, analizamos dos modelos de concatenación en paralelo de dos códigos convolucionales desde el punto de vista de la teoría clásica de sistemas. Consideramos la concatenación en paralelo empleada normalmente en teoría de sistemas lineales, si bien ésta no es utilizada en la teoría de códigos, ya que no da lugar a códigos óptimos. Esto motiva la construcción del segundo modelo de concatenación en paralelo, en el que podemos obtener códigos con distancia libre superior a la de los códigos constituyentes.

Denotamos por  $\mathcal{C}_1$  y  $\mathcal{C}_2$  los códigos constituyentes. También denotamos por  $x_t^{(l)}, u_t^{(l)}, y_t^{(l)}$  y  $v_t^{(l)}$ , para  $l = 1, 2$ , el vector de estados, el vector información, el vector de paridad, y la palabra código, respectivamente, de  $\mathcal{C}_l$ . En los dos modelos de concatenación en paralelo, las palabras código  $v_t^{(1)}$  y  $v_t^{(2)}$  de  $\mathcal{C}_1$  y  $\mathcal{C}_2$ , respectivamente, vienen dadas por las expresiones

$$v_t^{(1)} = \begin{pmatrix} y_t^{(1)} \\ u_t^{(1)} \end{pmatrix} \quad \text{y} \quad v_t^{(2)} = \begin{pmatrix} y_t^{(2)} \\ u_t^{(2)} \end{pmatrix}. \quad (5.1)$$

Entonces,  $x_t, u_t, y_t$  y  $v_t$  son el vector de estados, el vector información, el vector de paridad, y la palabra código, respectivamente, del correspondiente modelo de código concatenado que estemos tratando.

Denotamos por  $T_1(z), T_2(z)$  y  $T(z)$  la función de transferencia del código  $\widehat{\mathcal{C}}_1$ , del código  $\widehat{\mathcal{C}}_2$  y del código concatenado correspondiente, considerado como un  $\mathcal{F}$ -subespacio vectorial de  $\mathcal{F}^n$  (véase la sección 1.5), respectivamente.

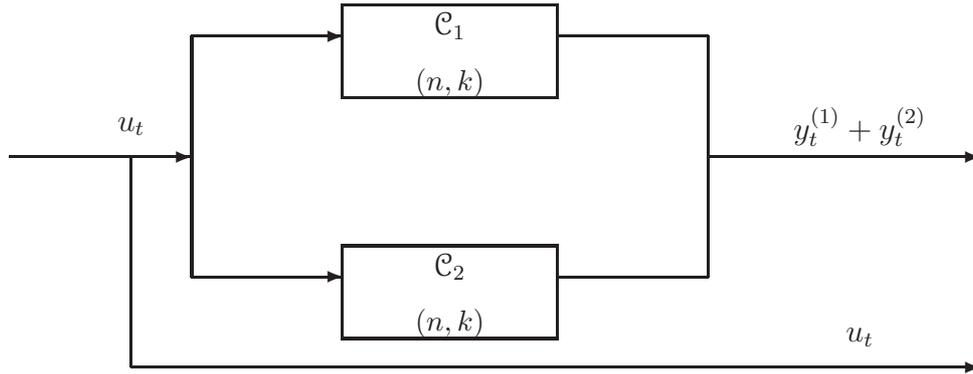


Figura 5.1: Código concatenado  $\mathcal{PC}^{(1)}$

## 5.2.1 Representación entrada-estado-salida

### Modelo 1

El primer tipo de concatenación en paralelo que estudiamos es el empleado en la teoría de control en el espacio de estados. Consideremos dos códigos  $\mathcal{C}_1$  y  $\mathcal{C}_2$  de tasa  $k/n$ . Entonces, el vector información  $u_t$  es codificado por los dos códigos convolucionales, de manera que

$$u_t = u_t^{(1)} = u_t^{(2)}, \quad (5.2)$$

y la palabra código de la concatenación está formada por la suma de los vectores de paridad de los códigos constituyentes y el vector información (véase la figura 5.1)

$$v_t = \begin{pmatrix} y_t^{(1)} + y_t^{(2)} \\ u_t \end{pmatrix}. \quad (5.3)$$

Denotamos por  $\mathcal{PC}^{(1)}$  el código concatenado obtenido. Observemos entonces que el estado del sistema es la unión de los estados de los códigos constituyentes

$$x_t = \begin{pmatrix} x_t^{(2)} \\ x_t^{(1)} \end{pmatrix}, \quad (5.4)$$

y el vector de paridad  $y_t$  de  $\mathcal{PC}^{(1)}$  es la suma de los vectores de paridad de  $\mathcal{C}_1$  y  $\mathcal{C}_2$ ,

$$y_t = \left( y_t^{(1)} + y_t^{(2)} \right). \quad (5.5)$$

El teorema siguiente proporciona la representación entrada-estado-salida para el código concatenado  $\mathcal{PC}^{(1)}$  en función de la representación entrada-estado-salida de los códigos constituyentes.

**Teorema 5.1:** Si  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$  es un  $(n, k, \delta_l)$ -código, para  $l = 1, 2$ , entonces la representación entrada-estado-salida para el código concatenado  $\mathcal{PC}^{(1)}$  de tasa  $k/n$  viene dada por el sistema lineal (1.11), donde

$$A = \begin{pmatrix} A_2 & O \\ 0 & A_1 \end{pmatrix}, \quad B = \begin{pmatrix} B_2 \\ B_1 \end{pmatrix}, \quad C = (C_2 \quad C_1) \quad y \quad D = (D_1 + D_2). \quad (5.6)$$

DEMOSTRACIÓN: De la expresión (1.11) tenemos, para el código  $\mathcal{C}_1$ ,

$$\begin{aligned} x_{t+1}^{(1)} &= A_1 x_t^{(1)} + B_1 u_t^{(1)}, \\ y_t^{(1)} &= C_1 x_t^{(1)} + D_1 u_t^{(1)}, \end{aligned}$$

y para el código  $\mathcal{C}_2$ ,

$$\begin{aligned} x_{t+1}^{(2)} &= A_2 x_t^{(2)} + B_2 u_t^{(2)}, \\ y_t^{(2)} &= C_2 x_t^{(2)} + D_2 u_t^{(2)}. \end{aligned}$$

Ahora bien, teniendo en cuenta las expresiones (5.2), (5.4) y (5.5), la representación entrada-estado-salida del código concatenado  $\mathcal{PC}^{(1)}$  viene dada por

$$x_{t+1} = \begin{pmatrix} A_2 & O \\ O & A_1 \end{pmatrix} x_t + \begin{pmatrix} B_2 \\ B_1 \end{pmatrix} u_t, \quad \square$$

$$y_t = (C_2 \quad C_1) x_t + (D_1 + D_2) u_t.$$

Empleando el resultado anterior y el teorema 1.12, obtenemos la función de transferencia  $T(z)$  asociada al código convolucional  $\widehat{\mathcal{PC}}^{(1)}$  en términos de las funciones de transferencia asociadas a los códigos constituyentes (considerados como  $\mathcal{F}$ -subespacios vectoriales de  $\mathcal{F}^n$ ).

**Teorema 5.2:** Si  $\mathcal{PC}^{(1)}(A, B, C, D)$  es el código concatenado descrito por las matrices de la expresión (5.6), entonces

$$T(z) = T_1(z) + T_2(z)$$

es la función de transferencia asociada a  $\widehat{\mathcal{PC}}^{(1)}$ .

Según la expresión (5.6), la matriz  $D$  de la representación entrada-estado-salida del código concatenado  $\mathcal{PC}^{(1)}$  es la suma de las matrices  $D_1$  y  $D_2$  de las representaciones de  $\mathcal{C}_1$  y  $\mathcal{C}_2$ , respectivamente. Esto significa que en ciertos casos, la concatenación da lugar a códigos con mala distancia libre, como ponemos de manifiesto en el ejemplo siguiente.

**Ejemplo 5.1:** Supongamos ahora que  $\mathbb{F} = GF(2)$  y consideremos el  $(4, 2, 1)$ -código  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  descrito por las matrices

$$A_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{y} \quad D_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Observemos que el par  $(A_1, B_1)$  es controlable y el par  $(A_1, C_1)$  es observable. Además,  $d_{free}(\mathcal{C}_1) = 2$ .

Sea  $\mathcal{C}_2(A_2, B_2, C_2, D_2)$  el  $(4, 2, 1)$ -código descrito por las matrices

$$A_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{y} \quad D_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Entonces, el par  $(A_2, B_2)$  es controlable y el par  $(A_2, C_2)$  es observable. Además,  $d_{free}(\mathcal{C}_2) = 3$ .

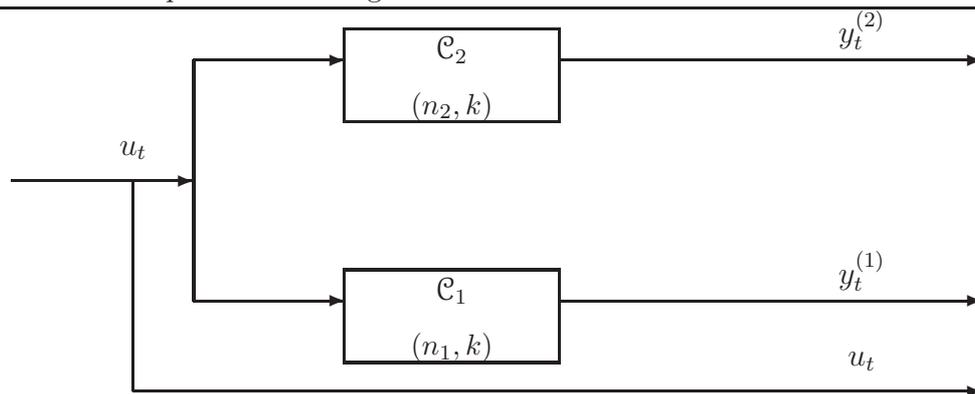
Por otro lado, aplicando el teorema 5.1, la representación entrada-estado-salida del código concatenado  $\mathcal{PC}^{(1)}(A, B, C, D)$  de tasa  $2/4$ , viene dada por las matrices

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

Observemos que el par  $(A, B)$  es controlable y el par  $(A, C)$  es observable. Además,  $d_{free}(\mathcal{PC}^{(1)}) = 3$ , de donde tenemos que la distancia libre de  $\mathcal{PC}^{(1)}$  coincide con la distancia libre de  $\mathcal{C}_2$ , es decir, no hemos mejorado la distancia libre. Es más, en este caso, la cota Singleton generalizada es 7, que dista mucho de  $d_{free}(\mathcal{PC}^{(1)})$ . ■

## Modelo 2

Como acabamos de ver, la concatenación según el modelo 1, no proporciona, en general, códigos óptimos o con distancia libre próxima a la cota Singleton generalizada. Esto nos induce a considerar un nuevo modelo de concatenación en paralelo en la



**Figura 5.2:** Código concatenado  $\mathcal{PC}^{(2)}$

que el vector de paridad no sea la suma de los vectores de paridad de los códigos constituyentes (y por tanto, la matriz  $D$  no sea la suma de las matrices correspondientes de los códigos que forman la concatenación). En este nuevo modelo, que denotamos por  $\mathcal{PC}^{(2)}$ , consideramos dos códigos  $\mathcal{C}_1$  y  $\mathcal{C}_2$  de tasas  $k/n_1$  y  $k/n_2$ , respectivamente. El vector información  $u_t$  es codificado por los dos códigos convolucionales y, por tanto,

$$u_t = u_t^{(1)} = u_t^{(2)}, \quad (5.7)$$

pero en este caso, la palabra código está formada por los vectores de paridad de  $\mathcal{C}_1$  y  $\mathcal{C}_2$  y la entrada  $u_t$  (véase la figura 5.2), es decir,

$$v_t = \begin{pmatrix} y_t^{(2)} \\ y_t^{(1)} \\ u_t \end{pmatrix}. \quad (5.8)$$

Tal y como teníamos para el código  $\mathcal{PC}^{(1)}$ , el estado  $x_t$  del código concatenado  $\mathcal{PC}^{(2)}$  es la unión de los estados de  $\mathcal{C}_1$  y  $\mathcal{C}_2$ ,

$$x_t = \begin{pmatrix} x_t^{(2)} \\ x_t^{(1)} \end{pmatrix}, \quad (5.9)$$

pero en este caso, el vector de paridad  $y_t$  de  $\mathcal{PC}^{(2)}$  viene dado por

$$y_t = \begin{pmatrix} y_t^{(2)} \\ y_t^{(1)} \end{pmatrix}. \quad (5.10)$$

La representación entrada-estado-salida del código concatenado  $\mathcal{PC}^{(2)}$  viene dada en función de la representación entrada-estado-salida de los códigos constituyentes, como vemos en el teorema siguiente.

**Teorema 5.3:** Si  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$  es un  $(n_l, k, \delta_l)$ -código, entonces la representación entrada-estado-salida para el código concatenado  $\mathcal{PC}^{(2)}$  de tasa  $k/(n_1 + n_2 - k)$  viene dada por el sistema lineal (1.11), donde

$$A = \begin{pmatrix} A_2 & O \\ 0 & A_1 \end{pmatrix}, \quad B = \begin{pmatrix} B_2 \\ B_1 \end{pmatrix}, \quad C = \begin{pmatrix} C_2 & O \\ O & C_1 \end{pmatrix} \quad y \quad D = \begin{pmatrix} D_2 \\ D_1 \end{pmatrix}. \quad (5.11)$$

DEMOSTRACIÓN: De forma análoga al teorema 5.1, tenemos que

$$\begin{aligned} x_{t+1}^{(1)} &= A_1 x_t^{(1)} + B_1 u_t^{(1)}, & x_{t+1}^{(2)} &= A_2 x_t^{(2)} + B_2 u_t^{(2)}, \\ y_t^{(1)} &= C_1 x_t^{(1)} + D_1 u_t^{(1)}, & y_t^{(2)} &= C_2 x_t^{(2)} + D_2 u_t^{(2)}. \end{aligned}$$

Entonces, teniendo en cuenta las expresiones (5.7), (5.9) y (5.10), la representación entrada-estado-salida del código concatenado  $\mathcal{PC}^{(2)}$  viene dada por

$$\begin{aligned} x_{t+1} &= \begin{pmatrix} A_2 & O \\ O & A_1 \end{pmatrix} x_t + \begin{pmatrix} B_2 \\ B_1 \end{pmatrix} u_t, \\ y_t &= \begin{pmatrix} C_2 & O \\ O & C_1 \end{pmatrix} x_t + \begin{pmatrix} D_2 \\ D_1 \end{pmatrix} u_t. \end{aligned}$$

□

Tal y como teníamos para el modelo anterior, la función de transferencia del código convolucional  $\widehat{\mathcal{PC}}^{(2)}$  viene dada en términos de las funciones de transferencia de los códigos constituyentes (considerados como  $\mathcal{F}$ -subespacios vectoriales de  $\mathcal{F}^n$ ), como muestra el resultado siguiente.

**Teorema 5.4:** Si  $\mathcal{PC}^{(2)}(A, B, C, D)$  es el código concatenado descrito por las matrices de la expresión (5.11), entonces

$$T(z) = \begin{pmatrix} T_2(z) \\ T_1(z) \end{pmatrix}$$

es la función de transferencia asociada a  $\widehat{\mathcal{PC}}^{(2)}$ .

## 5.2.2 Controlabilidad

En esta sección, estudiamos las condiciones que deben verificar las matrices  $A_l$ ,  $B_l$ ,  $C_l$  y  $D_l$ , para  $l = 1, 2$ , que describen los códigos constituyentes para obtener una representación minimal del código concatenado. Como podemos observar en las relaciones (5.6) y (5.11), las matrices  $A$  y  $B$  de los códigos  $\mathcal{PC}^{(1)}$  y  $\mathcal{PC}^{(2)}$  tienen la misma estructura (obsérvese que  $A$  y  $B$  son matrices de tamaños  $\delta \times \delta$  y  $\delta \times k$ , respectivamente, en ambos modelos de concatenación). Por tanto, dado que los resultados que presentamos en esta sección son válidos para ambos tipos de concatenación, denotamos por  $\mathcal{PCC}$  el código concatenado  $\mathcal{PC}^{(1)}$  descrito por la expresión (5.6), así como el código  $\mathcal{PC}^{(2)}$  descrito por la expresión (5.11). Consideramos entonces  $\mathcal{C}_1$  un  $(n_1, k, \delta_1)$ -código y  $\mathcal{C}_2$  un  $(n_2, k, \delta_2)$ -código, teniendo en cuenta que para la concatenación  $\mathcal{PC}^{(1)}$ , se debe verificar la condición  $n_1 = n_2$ .

El ejemplo siguiente muestra que no es suficiente con que los pares  $(A_l, B_l)$ , para  $l = 1, 2$ , de los códigos constituyentes sean controlables para que el par  $(A, B)$  del código concatenado  $\mathcal{PCC}$  sea controlable.

**Ejemplo 5.2:** Consideremos el cuerpo  $\mathbb{F} = GF(9)$ . Como dijimos en la sección 1.1, suponemos que  $\alpha$  es un elemento primitivo de  $\mathbb{F}$ , con  $\alpha^2 + \alpha + 2 = 0$ .

Consideremos un  $(8, 4, 1)$ -código  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  sobre  $\mathbb{F}$ , donde

$$A_1 = \begin{pmatrix} \alpha \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$$

y  $C_1$  y  $D_1$  son matrices arbitrarias de tamaños  $4 \times 1$  y  $4 \times 4$ , respectivamente. Observemos que  $(A_1, B_1)$  es controlable.

Sea  $\mathcal{C}_2(A_2, B_2, C_2, D_2)$  un  $(8, 4, 2)$ -código sobre  $\mathbb{F}$  descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^6 & \alpha^5 \\ \alpha^5 & \alpha^3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} \alpha & \alpha^3 & \alpha^7 & 1 \\ \alpha^3 & \alpha^4 & 1 & \alpha \end{pmatrix},$$

siendo  $C_2$  y  $D_2$  matrices arbitrarias de tamaños  $4 \times 2$  y  $4 \times 4$ , respectivamente. Claramente, el par  $(A_2, B_2)$  es controlable.

Por otro lado, aplicando los teoremas 5.1 y 5.3, las matrices  $A$  y  $B$  de la representación entrada-estado-salida de los códigos concatenados  $\mathcal{PC}^{(1)}$  y  $\mathcal{PC}^{(2)}$ , son

$$A = \begin{pmatrix} \alpha^6 & \alpha^5 & 0 \\ \alpha^5 & \alpha^3 & 0 \\ 0 & 0 & \alpha \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} \alpha & \alpha^3 & \alpha^7 & 1 \\ \alpha^3 & \alpha^4 & 1 & \alpha \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Pero el par  $(A, B)$  no es controlable, ya que

$$\text{rg} \begin{pmatrix} \alpha I - A & B \end{pmatrix} = \text{rg} \begin{pmatrix} 1 & \alpha & 0 & \alpha & \alpha^3 & \alpha^7 & 1 \\ \alpha & \alpha^2 & 0 & \alpha^3 & \alpha^4 & 1 & \alpha \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} = 2 \neq 3. \quad \blacksquare$$

Por tanto, necesitamos condiciones adicionales para las matrices que describen los códigos  $\mathcal{C}_1$  y  $\mathcal{C}_2$  para obtener la controlabilidad del par  $(A, B)$  del código concatenado. En concreto, tenemos el resultado siguiente, análogo al teorema 3.5.

**Teorema 5.5:** Sean  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  un  $(n_1, k, \delta_1)$ -código,  $\mathcal{C}_2(A_2, B_2, C_2, D_2)$  un  $(n_2, k, \delta_2)$ -código y  $\mathcal{PCC}$  el código concatenado correspondiente. Si  $\text{rg}(B) = \delta_1 + \delta_2$ , entonces  $(A, B, C, D)$  es una representación minimal de  $\mathcal{PCC}$  con complejidad  $\delta_1 + \delta_2$ .

**Observación 5.1:** Notemos que la condición  $\text{rg}(B) = \delta_1 + \delta_2$  del teorema 5.5 implica, en particular, que  $\text{rg}(B_1) = \delta_1$  y  $\text{rg}(B_2) = \delta_2$ . Por tanto,  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ . ■

**Observación 5.2:** El ejemplo 5.2 muestra también que el recíproco de la observación 5.1 no es cierto en general, ya que el par  $(A_l, B_l)$  es controlable, para  $l = 1, 2$ , pero  $\text{rg}(B) = 2 \neq 1 + 2 = \delta_1 + \delta_2$ . ■

### 5.2.3 Observabilidad

En esta sección nos centramos en las condiciones que deben verificar las matrices que describen los códigos constituyentes para que el par  $(A, C)$  de los códigos concatenados  $\mathcal{PCC}^{(1)}$  y  $\mathcal{PCC}^{(2)}$  sea observable y, por tanto, la matriz generadora inducida por la realización sea no catastrófica. Observemos que, a diferencia de como teníamos con la matriz  $B$ , la matriz  $C$  es diferente según el modelo de concatenación que estemos estudiando. Por tanto, tenemos resultados diferentes para la observabilidad de cada modelo.

El ejemplo siguiente muestra que no es suficiente con que el par  $(A_l, C_l)$ , para  $l = 1, 2$ , de los códigos constituyentes sea observable, para que el par  $(A, C)$  del código concatenado  $\mathcal{PCC}^{(1)}$  sea observable.

**Ejemplo 5.3:** Sea  $\alpha$  un elemento primitivo de  $\mathbb{F} = GF(9)$ , como en el ejemplo 5.2.

Consideremos un  $(8, 4, 1)$ -código  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  sobre  $\mathbb{F}$ , donde

$$A_1 = (\alpha), \quad C_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

y  $B_1$  y  $D_1$  son matrices arbitrarias de tamaños  $1 \times 4$  y  $4 \times 4$ , respectivamente, tales que el par  $(A_1, B_1)$  sea controlable, para lo cual, bastaría con tomar, por ejemplo,  $B_1 = \begin{pmatrix} 1 \end{pmatrix}$ . Observemos que  $(A_1, C_1)$  es observable.

Sea  $\mathcal{C}_2(A_2, B_2, C_2, D_2)$  un  $(8, 4, 2)$ -código descrito por las matrices

$$A_2 = \begin{pmatrix} \alpha^6 & \alpha^5 \\ \alpha^5 & \alpha^3 \end{pmatrix}, \quad C_2 = \begin{pmatrix} \alpha^6 & 1 \\ \alpha^2 & \alpha^3 \\ \alpha^6 & \alpha^7 \\ 1 & \alpha \end{pmatrix}$$

siendo  $B_2$  y  $D_2$  matrices arbitrarias de tamaños  $2 \times 4$  y  $4 \times 4$ , respectivamente, tales que el par  $(A_2, B_2)$  es controlable, para lo cual, bastaría con tomar, por ejemplo, la matriz  $B_2 = \begin{pmatrix} 1 & 0 & 0 & \alpha^2 \\ 0 & 1 & \alpha^4 & \alpha^3 \end{pmatrix}$ . Notemos que el par  $(A_2, C_2)$  es observable.

Por otro lado, aplicando los teoremas 5.1 y 5.3, las matrices  $A$  y  $C$  de la representación entrada-estado-salida del código concatenado  $\mathcal{PC}^{(1)}$  son

$$A = \begin{pmatrix} \alpha^6 & \alpha^5 & 0 \\ \alpha^5 & \alpha^3 & 0 \\ 0 & 0 & \alpha \end{pmatrix} \quad y \quad C = \begin{pmatrix} \alpha^6 & 1 & 1 \\ \alpha^2 & \alpha^3 & 0 \\ \alpha^6 & \alpha^7 & 0 \\ 1 & \alpha & 0 \end{pmatrix}.$$

Pero el par  $(A, C)$  no es observable, ya que

$$\operatorname{rg} \begin{pmatrix} \alpha I - A \\ C \end{pmatrix} = \operatorname{rg} \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & \alpha^2 & 0 \\ 0 & 0 & 0 \\ \alpha^6 & 1 & 1 \\ \alpha^2 & \alpha^3 & 0 \\ \alpha^6 & \alpha^7 & 0 \\ 1 & \alpha & 0 \end{pmatrix} = 2 \neq 3. \quad \blacksquare$$

Ahora bien, si la matriz  $C$  del código  $\mathcal{PC}^{(1)}$  tiene rango completo por columnas, entonces el par  $(A, C)$  es, claramente, observable. Tenemos entonces el resultado siguiente, cuya demostración es similar a la del teorema 3.9, de modo que la omitimos.

**Teorema 5.6:** Sean  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  un  $(n, k, \delta_1)$ -código,  $\mathcal{C}_2(A_2, B_2, C_2, D_2)$  un  $(n, k, \delta_2)$ -código y  $\mathcal{PC}^{(1)}$  el código concatenado de tasa  $k/n$  descrito por las matrices dadas por la expresión (5.6). Si  $\operatorname{rg}(C) = \delta_1 + \delta_2$ , entonces el par  $(A, C)$  es observable.

Si bien el ejemplo 5.3 mostraba que siendo el par  $(A_l, C_l)$  observable, para  $l = 1, 2$ , el par  $(A, C)$  del código  $\mathcal{PC}^{(1)}$  no era necesariamente observable, para el modelo  $\mathcal{PC}^{(2)}$  no tenemos el mismo resultado.

**Ejemplo 5.4:** Sea  $\alpha$ , como en el ejemplo 5.2, un elemento primitivo de  $\mathbb{F} = GF(9)$ .

Sea  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  un  $(8, 4, 1)$ -código descrito por las matrices  $A_1$  y  $C_1$  del ejemplo 5.3, siendo  $B_1$  y  $D_1$  matrices arbitrarias de tamaños  $1 \times 4$  y  $4 \times 4$ , respectivamente, tales que el par  $(A_1, B_1)$  sea controlable (basta con tomar, por ejemplo,  $B_1 = \begin{pmatrix} 1 \end{pmatrix}$ ).

Sea  $\mathcal{C}_2(A_2, B_2, C_2, D_2)$  un  $(8, 4, 2)$ -código descrito por las matrices  $A_2$  y  $C_2$  del ejemplo 5.3, siendo  $B_2$  y  $D_2$  matrices arbitrarias de tamaños  $2 \times 4$  y  $4 \times 4$ , respectivamente, tales que el par  $(A_2, B_2)$  es controlable (consideremos, por ejemplo,

$$B_2 = \begin{pmatrix} 1 & 0 & 0 & \alpha^2 \\ 0 & 1 & \alpha^4 & \alpha^3 \end{pmatrix}.$$

Teniendo en cuenta el teorema 5.3, las matrices  $A$  y  $C$  del código concatenado  $\mathcal{PC}^{(2)}$

son

$$A = \begin{pmatrix} \alpha^6 & \alpha^5 & 0 \\ \alpha^5 & \alpha^3 & 0 \\ 0 & 0 & \alpha \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} \alpha^6 & 1 & 0 \\ \alpha^2 & \alpha^3 & 0 \\ \alpha^6 & \alpha^7 & 0 \\ 1 & \alpha & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Observemos que  $\text{rg}(C) = 3$ , de donde

$$\text{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = 3 = \delta_1 + \delta_2 \quad \text{para todo } z \in \overline{\mathbb{F}},$$

es decir, el par  $(A, C)$  es observable. ■

Podemos generalizar este resultado para cualesquiera que sean los códigos  $\mathcal{C}_1$  y  $\mathcal{C}_2$  tales que el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ , como ponemos de manifiesto en el resultado siguiente.

**Teorema 5.7:** Sean  $\mathcal{C}_1(A_1, B_1, C_1, D_1)$  un  $(n_1, k, \delta_1)$ -código,  $\mathcal{C}_2(A_2, B_2, C_2, D_2)$  un  $(n_2, k, \delta_2)$ -código y  $\mathcal{PC}^{(2)}$  el código concatenado de tasa  $k/(n_1 + n_2 - k)$  descrito por las matrices dadas por la expresión (5.11). Si el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ , entonces el par  $(A, C)$  es observable.

DEMOSTRACIÓN: Como el par  $(A_l, C_l)$  es observable, para  $l = 1, 2$ , tenemos que

$$\text{rg} \begin{pmatrix} zI - A_l \\ C_l \end{pmatrix} = \delta_l \quad \text{para todo } z \in \overline{\mathbb{F}},$$

de donde

$$\text{rg} \begin{pmatrix} zI - A \\ C \end{pmatrix} = \text{rg} \begin{pmatrix} zI_{\delta_1} - A_2 & O \\ O & zI_{\delta_2} - A_1 \\ C_2 & O \\ O & C_1 \end{pmatrix} = \delta_1 + \delta_2 \quad \text{para todo } z \in \overline{\mathbb{F}}.$$

Por tanto, el par  $(A, C)$  es observable. □

### 5.2.4 Distancias columnas y distancias libres

Tal y como vimos en el ejemplo 5.1, la distancia libre del código  $\mathcal{PC}^{(1)}$  no superaba las distancias libres de los códigos constituyentes y, por tanto, no podíamos obtener buenos códigos de esta concatenación en paralelo. Ahora bien, observemos que, según la expresión (5.8), la palabra código  $v_t$  de  $\mathcal{PC}^{(2)}$  viene dada por

$$v_t = \begin{pmatrix} y_t^{(2)} \\ y_t^{(1)} \\ u_t \end{pmatrix}$$

es decir, contiene tanto a la palabra código de  $\mathcal{C}_1$  como a la palabra código de  $\mathcal{C}_2$  (véase la relación (5.1)). Esto nos permite obtener una cota inferior para la distancia libre de  $\mathcal{PC}^{(2)}$  en función de las distancias libres de los códigos de la concatenación. Comenzamos con un lema técnico, previo al resultado principal sobre  $d_{free}(\mathcal{PC}^{(2)})$ .

**Lema 5.1:** *Sea  $\mathcal{PC}^{(2)}$  el código dado por el teorema 5.3 al concatenar el código  $\mathcal{C}_1$  y el código  $\mathcal{C}_2$ . Entonces*

$$d_j^c(\mathcal{PC}^{(2)}) \geq \max \{d_j^c(\mathcal{C}_1), d_j^c(\mathcal{C}_2)\} \quad \text{para } j = 0, 1, 2, \dots \quad (5.12)$$

DEMOSTRACIÓN: Teniendo en cuenta las relaciones entre  $y_t, y_t^{(1)}, y_t^{(2)}$ ;  $u_t, u_t^{(1)}, u_t^{(2)}$  y  $v_t, v_t^{(1)}, v_t^{(2)}$  dadas por las expresiones (5.1), (5.8) y (5.10), tenemos que

$$\begin{aligned} \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \\ &\geq \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}). \end{aligned}$$

Así pues, de la expresión de la distancia columna  $d_j^c(\mathcal{PC}^{(2)})$  en términos de la representación entrada-estado-salida dada por la relación (1.19), obtenemos que

$$\begin{aligned} d_j^c(\mathcal{PC}^{(2)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(1)} \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) \right\} \end{aligned}$$

$$= d_j^c(\mathcal{C}_1) \quad (5.13)$$

ya que  $u_0 = u_0^{(1)}$ .

Análogamente, de las expresiones (5.1), (5.8) y (5.10), tenemos que

$$\begin{aligned} \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \\ &\geq \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}). \end{aligned}$$

Ahora, de la expresión (1.19) tenemos que

$$\begin{aligned} d_j^c(\mathcal{PC}^{(2)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(2)} \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \right\} \\ &= d_j^c(\mathcal{C}_2), \end{aligned} \quad (5.14)$$

ya que  $u_0 = u_0^{(2)}$ .

Finalmente, de las desigualdades (5.13) y (5.14), obtenemos la desigualdad (5.12).□

Ahora bien, si  $\text{rg}(D_1) = k$  o bien  $\text{rg}(D_2) = k$ , tenemos un refinamiento de la cota dada en el lema 5.1, como muestra el resultado siguiente.

**Lema 5.2:** *Sea  $\mathcal{PC}^{(2)}$  el código dado por el teorema 5.3 al concatenar el código  $\mathcal{C}_1$  y el código  $\mathcal{C}_2$ . Entonces*

(a) *Si  $\text{rg}(D_2) = k$ ,*

$$d_j^c(\mathcal{PC}^{(2)}) \geq \max \{d_j^c(\mathcal{C}_1) + 1, d_j^c(\mathcal{C}_2)\} \quad \text{para } j = 0, 1, 2, \dots \quad (5.15)$$

(b) *Si  $\text{rg}(D_1) = k$ ,*

$$d_j^c(\mathcal{PC}^{(2)}) \geq \max \{d_j^c(\mathcal{C}_1), d_j^c(\mathcal{C}_2) + 1\} \quad \text{para } j = 0, 1, 2, \dots \quad (5.16)$$

(c) *Si  $\text{rg}(D_1) = \text{rg}(D_2) = k$ ,*

$$d_j^c(\mathcal{PC}^{(2)}) \geq \max \{d_j^c(\mathcal{C}_1) + 1, d_j^c(\mathcal{C}_2) + 1\} \quad \text{para } j = 0, 1, 2, \dots \quad (5.17)$$

DEMOSTRACIÓN: (a) Procediendo de manera análoga a la demostración del lema 5.1, tenemos que

$$\begin{aligned} \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) &= \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) \\ &\geq \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \text{wt}(y_0^{(2)}). \end{aligned}$$

Ahora, como  $y_0^{(2)} = D_2 u_0^{(2)}$  (por ser  $x_0^{(2)} = 0$ ) y  $\text{rg}(D_2) = k$ , tenemos que  $y_0^{(2)} \neq 0$  si y sólo si  $u_0 = u_0^{(2)} \neq 0$ . Por tanto, de la expresión de la distancia columna  $d_j^c(\mathcal{PC}^{(2)})$  en términos de la representación entrada-estado-salida dada por la relación (1.19), obtenemos que

$$\begin{aligned} d_j^c(\mathcal{PC}^{(2)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(1)} \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t^{(1)}) + \sum_{t=0}^j \text{wt}(y_t^{(1)}) + \text{wt}(y_0^{(2)}) \right\} \\ &\geq d_j^c(\mathcal{C}_1) + 1 \end{aligned} \tag{5.18}$$

ya que  $u_0 = u_0^{(1)}$ . Obtenemos entonces la desigualdad (5.15) de la expresión (5.14) y de la relación (5.18).

(b) Del mismo modo que en el apartado anterior, tenemos que

$$\sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \geq \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \text{wt}(y_0^{(1)}).$$

Pero al ser  $y_0^{(1)} = D_1 u_0^{(1)}$  y  $\text{rg}(D_1) = k$ , entonces  $y_0^{(1)} \neq 0$  si y sólo si  $u_0^{(1)} = u_0 \neq 0$ . Por tanto, de la expresión de la distancia columna  $d_j^c(\mathcal{PC}^{(2)})$  en términos de la representación entrada-estado-salida dada por la relación (1.19), obtenemos que

$$\begin{aligned} d_j^c(\mathcal{PC}^{(2)}) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t) + \sum_{t=0}^j \text{wt}(y_t) \right\} \\ &\geq \min_{u_0^{(2)} \neq 0} \left\{ \sum_{t=0}^j \text{wt}(u_t^{(2)}) + \sum_{t=0}^j \text{wt}(y_t^{(2)}) + \text{wt}(y_0^{(1)}) \right\} \\ &\geq d_j^c(\mathcal{C}_2) + 1 \end{aligned} \tag{5.19}$$

ya que  $u_0 = u_0^{(2)}$ . La desigualdad (5.16) se obtiene entonces de la expresión (5.13) y de la relación (5.19).

(c) La desigualdad (5.17) se obtiene como consecuencia directa de las desigualdades (5.18) y (5.19).  $\square$

Como consecuencia inmediata de los lemas anteriores y de la expresión de la distancia libre en términos de la representación entrada-estado-salida dada por la relación (1.5), obtenemos el resultado siguiente.

**Teorema 5.8:** *Sea  $\mathcal{PC}^{(2)}$  el código dado por el teorema 5.3 al concatenar el código  $\mathcal{C}_1$  y el código  $\mathcal{C}_2$ . Entonces*

- (a)  $d_{free}(\mathcal{PC}^{(2)}) \geq \max\{d_{free}(\mathcal{C}_1), d_{free}(\mathcal{C}_2)\}$ .
- (b) Si  $\text{rg}(D_2) = k$ , entonces  $d_{free}(\mathcal{PC}^{(2)}) \geq \max\{d_{free}(\mathcal{C}_1) + 1, d_{free}(\mathcal{C}_2)\}$ .
- (c) Si  $\text{rg}(D_1) = k$ , entonces  $d_{free}(\mathcal{PC}^{(2)}) \geq \max\{d_{free}(\mathcal{C}_1), d_{free}(\mathcal{C}_2) + 1\}$ .
- (d) Si  $\text{rg}(D_1) = \text{rg}(D_2) = k$ , entonces

$$d_{free}(\mathcal{PC}^{(2)}) \geq \max\{d_{free}(\mathcal{C}_1) + 1, d_{free}(\mathcal{C}_2) + 1\}.$$

## 5.3 Concatenación en paralelo por bloques

En esta sección, describimos un nuevo código convolucional obtenido de la concatenación en paralelo de varios códigos convolucionales (véase [21]). En este caso, la palabra código se subdivide en bloques de tamaños acorde con la dimensión de las entradas de los códigos constituyentes. A diferencia de los modelos  $\mathcal{PC}^{(1)}$  y  $\mathcal{PC}^{(2)}$ , en el modelo que describimos en esta sección los códigos que forman la concatenación codifican parte del vector información.

Consideremos un  $(n_j, k_j, \delta_j)$ -código  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$ , generado por la matriz  $G_j(z)$  y sea

$$k = \sum_{j=1}^s k_j \quad \text{y} \quad n = \sum_{j=1}^s n_j.$$

Definimos un nuevo código convolucional  $\mathcal{PC}^{(3)}$  de tasa  $k/n$  obtenido de la concatenación en paralelo de los códigos  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$ , cuya matriz generadora viene

dada por

$$G(z) = \begin{pmatrix} G_1(z) & O & \cdots & O \\ O & G_2(z) & \cdots & O \\ \vdots & \vdots & & \vdots \\ O & O & \cdots & G_s(z) \end{pmatrix} \\ = \text{diag}(G_1(z), G_2(z), \dots, G_s(z)). \quad (5.20)$$

Decimos entonces que el código  $\mathcal{PC}^{(3)}$  se obtiene de la concatenación en paralelo por bloques de los códigos  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$ .

### 5.3.1 Propiedades estructurales de $\mathcal{PC}^{(3)}$

A continuación, analizamos las propiedades de la matriz generadora  $G(z)$  de  $\mathcal{PC}^{(3)}$ . Debido a la estructura de dicha matriz, el código convolucional  $\mathcal{PC}^{(3)}$  va a heredar todas las propiedades de los códigos que lo forman. El siguiente resultado muestra que la equivalencia entre dos matrices generadoras de  $\mathcal{PC}^{(3)}$  viene dada por la equivalencia entre las matrices generadoras de los códigos constituyentes.

**Teorema 5.9:** *Sea  $\mathcal{PC}^{(3)}$  el código obtenido de la concatenación en paralelo por bloques de los códigos  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$  y sean*

$$G^{(1)}(z) = \text{diag}(G_1^{(1)}(z), G_2^{(1)}(z), \dots, G_s^{(1)}(z))$$

y

$$G^{(2)}(z) = \text{diag}(G_1^{(2)}(z), G_2^{(2)}(z), \dots, G_s^{(2)}(z))$$

*dos matrices generadoras de  $\mathcal{PC}^{(3)}$ , siendo  $G_j^{(l)}(z)$ , una matriz generadora de  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$  y  $l = 1, 2$ . Si  $G_j^{(1)}(z)$  y  $G_j^{(2)}(z)$  son equivalentes, para  $j = 1, 2, \dots, s$ , entonces  $G^{(1)}(z)$  y  $G^{(2)}(z)$  son matrices equivalentes.*

DEMOSTRACIÓN: Si las matrices  $G_j^{(1)}(z)$  y  $G_j^{(2)}(z)$  son equivalentes, para  $j = 1, 2, \dots, s$ , existe una matriz unimodular  $U_j(z)$  de tamaño  $k_j \times k_j$  tal que

$$G_j^{(1)}(z) = G_j^{(2)}(z)U_j(z),$$

para  $j = 1, 2, \dots, s$ . Así,

$$G^{(1)}(z) = \text{diag}(G_1^{(1)}(z), G_2^{(1)}(z), \dots, G_s^{(1)}(z))$$

$$\begin{aligned}
&= \text{diag} \left( G_1^{(2)}(z)U_1(z), G_2^{(2)}(z)U_2(z), \dots, G_s^{(2)}(z)U_s(z) \right) \\
&= \text{diag} \left( G_1^{(2)}(z), G_2^{(2)}(z), \dots, G_s^{(2)}(z) \right) \text{diag} (U_1(z), U_2(z), \dots, U_s(z)) \\
&= G^{(2)}(z)U(z),
\end{aligned}$$

siendo  $U(z) = \text{diag} (U_1(z), U_2(z), \dots, U_s(z))$  una matriz unimodular ya que  $U_j(z)$  es unimodular, para  $j = 1, 2, \dots, s$ . Por tanto, tenemos que  $G^{(1)}(z)$  y  $G^{(2)}(z)$  son matrices equivalentes.  $\square$

Ahora bien, el código concatenado  $\mathcal{PC}^{(3)}$  no sólo hereda las propiedades de equivalencia de matrices de los códigos constituyentes, sino que también hereda las propiedades relacionadas con matrices minimales, como mostramos en el siguiente resultado.

**Teorema 5.10:** *Si  $\mathcal{PC}^{(3)}$  es el código obtenido de la concatenación en paralelo por bloques de los códigos  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$  y  $G(z)$  es la matriz generadora de  $\mathcal{PC}^{(3)}$  dada por la relación (5.20), siendo  $G_j(z)$  una matriz generadora del código  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$ , entonces  $G(z)$  es minimal si y sólo si  $G_j(z)$  es minimal, para  $j = 1, 2, \dots, s$ .*

DEMOSTRACIÓN: Teniendo en cuenta el teorema 1.3,  $G(D)$  es una matriz minimal si y sólo si la matriz

$$\begin{aligned}
[G(z)]_h &= [\text{diag} (G_1(z), G_2(z), \dots, G_s(z))]_h \\
&= \text{diag} ([G_1(z)]_h, [G_2(z)]_h, \dots, [G_s(z)]_h)
\end{aligned}$$

tiene rango completo. Ahora bien, dada la forma de la matriz  $G(z)$ , esto es equivalente a que la matriz  $[G_j(z)]_h$  tenga rango completo, para  $j = 1, 2, \dots, s$ , es decir, a que la matriz  $G_j(z)$  sea minimal, para  $j = 1, 2, \dots, s$ .  $\square$

Dado que el grado de una matriz generadora minimal es precisamente el grado del código  $\mathcal{PC}^{(3)}$ , obtenemos, aplicando el teorema anterior, que el grado del código concatenado  $\mathcal{PC}^{(3)}$  viene dado por la suma de los grados de los códigos constituyentes, como ponemos de manifiesto en el resultado siguiente.

**Corolario 5.1:** *Sea  $\mathcal{C}_j$  un  $(n_j, k_j, \delta_j)$ -código con índices de Forney  $(e_j^{(1)}, e_j^{(2)}, \dots, e_j^{(k_j)})$ , para  $j = 1, 2, \dots, s$  y sea  $\mathcal{PC}^{(3)}$  el  $(n, k, \delta)$ -código obtenido de la concatenación en paralelo por bloques de los códigos  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$ . Entonces*

(a) Los índices de Forney de  $\mathcal{PC}^{(3)}$  son

$$(e_1^{(1)}, e_1^{(2)}, \dots, e_1^{(k_1)}, e_2^{(1)}, e_2^{(2)}, \dots, e_2^{(k_2)}, \dots, e_s^{(1)}, e_s^{(2)}, \dots, e_s^{(k_s)}).$$

(b)  $\delta = \sum_{j=1}^s \delta_j.$

DEMOSTRACIÓN: Sea  $G_j(z)$  una matriz minimal de  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$ . Aplicando el teorema 5.10, tenemos que  $G(z) = \text{diag}(G_1(z), G_2(z), \dots, G_s(z))$  es una matriz minimal de  $\mathcal{PC}^{(3)}$ . Por tanto, los índices de Forney de este código son

$$(e_1^{(1)}, e_1^{(2)}, \dots, e_1^{(k_1)}, e_2^{(1)}, e_2^{(2)}, \dots, e_2^{(k_2)}, \dots, e_s^{(1)}, e_s^{(2)}, \dots, e_s^{(k_s)})$$

y el grado viene dado por  $\delta = \sum_{j=1}^s \delta_j.$  □

Por último, notemos que la distancia libre del código  $\mathcal{PC}^{(3)}$  viene dada, de forma trivial, por el mínimo de las distancias libres de los códigos constituyentes,

$$d_{free}(\mathcal{PC}^{(3)}) = \min_{1 \leq j \leq s} d_{free}(\mathcal{C}_j).$$

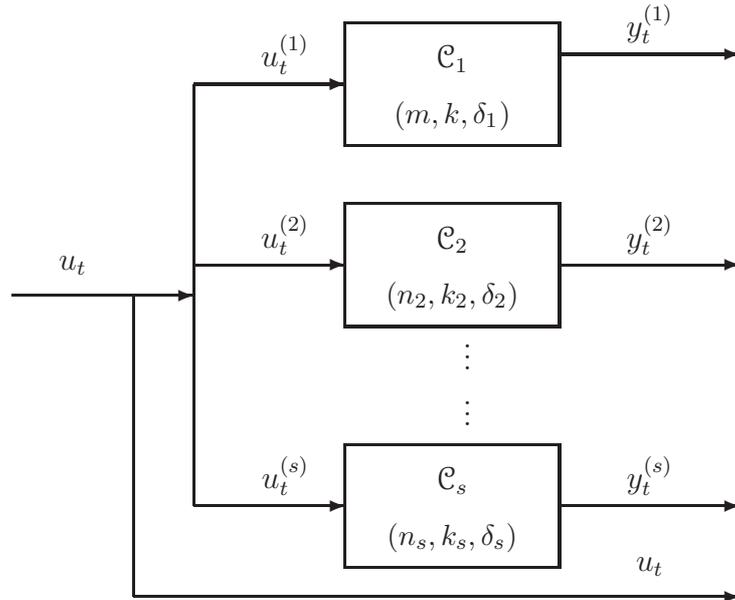
Por tanto,  $\mathcal{PC}^{(3)}$  nunca puede ser un código convolucional MDS. Si bien éste no es un código convolucional óptimo, se puede emplear para la decodificación en paralelo, tal y como se emplean los códigos *woven*.

### 5.3.2 Representación entrada-estado-salida de $\mathcal{PC}^{(3)}$

Una vez hemos analizado las propiedades relacionadas con las matrices generadoras de  $\mathcal{PC}^{(3)}$ , pasamos a describir este código desde el punto de vista de sistemas lineales.

Denotamos por  $x_t^{(l)}, u_t^{(l)}, y_t^{(l)}$  y  $v_t^{(l)}$  el vector de estados, el vector información, el vector de paridad y la palabra código, respectivamente, del código  $\mathcal{C}_l$ , para  $l = 1, 2, \dots, s$ . Del mismo modo,  $x_t, u_t, y_t$  y  $v_t$  son el vector de estados, el vector información, el vector de paridad y la palabra código, respectivamente, del código concatenado  $\mathcal{PC}^{(3)}$ .

$T_l(z)$  y  $T(z)$  denotan las matrices de transferencia de los códigos  $\widehat{\mathcal{C}}_l$  y  $\widehat{\mathcal{PC}}^{(3)}$ , respectivamente, para  $l = 1, 2, \dots, s$ .



**Figura 5.3:** Código concatenado  $\mathcal{PC}^{(3)}$

Según el modelo de concatenación  $\mathcal{PC}^{(3)}$ , el vector información  $u_t$  se divide en bloques de longitud  $k_l$ , para  $l = 1, 2, \dots, s$ ,

$$u_t = \left( u_t^{(1)}, u_t^{(2)}, \dots, u_t^{(s)} \right), \quad (5.21)$$

de manera que el vector  $u_t^{(l)} \in \mathbb{F}^{k_l}$  es codificado por el código  $\mathcal{C}_l$ , para  $l = 1, 2, \dots, s$ . El estado de la concatenación es la unión de los estados de los códigos constituyentes,

$$x_t = \begin{pmatrix} x_t^{(1)} \\ x_t^{(2)} \\ \vdots \\ x_t^{(s)} \end{pmatrix} \quad (5.22)$$

y el vector de paridad  $y_t$  viene dado por (véase la figura 5.3)

$$y_t = \begin{pmatrix} y_t^{(1)} \\ y_t^{(2)} \\ \vdots \\ y_t^{(s)} \end{pmatrix} \quad (5.23)$$

La representación entrada-estado-salida de este código viene dada en función de la representación entrada-estado-salida de los códigos constituyentes, como muestra el resultado siguiente.

**Teorema 5.11:** Si  $\mathcal{C}_j(A_j, B_j, C_j, D_j)$  un  $(n_j, k_j, \delta_j)$ -código, para  $j = 1, 2, \dots, s$  y  $\mathcal{PC}^{(3)}(A, B, C, D)$  es el código obtenido de la concatenación en paralelo por bloques de  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$ , entonces la representación entrada-estado-salida de  $\mathcal{PC}^{(3)}(A, B, C, D)$  viene dada por el sistema lineal (1.11), donde

$$\begin{aligned} A &= \text{diag}(A_1, A_2, \dots, A_s), & B &= \text{diag}(B_1, B_2, \dots, B_s), \\ C &= \text{diag}(C_1, C_2, \dots, C_s), & D &= \text{diag}(D_1, D_2, \dots, D_s). \end{aligned} \quad (5.24)$$

DEMOSTRACIÓN: De la expresión (1.11) tenemos que el código  $\mathcal{C}_j$ , para  $j = 1, 2, \dots, s$ , está descrito por el sistema lineal

$$\begin{aligned} x_{t+1}^{(j)} &= A_j x_t^{(j)} + B_j u_t^{(j)}, \\ y_t^{(j)} &= C_j x_t^{(j)} + D_j u_t^{(j)}. \end{aligned}$$

Ahora bien, teniendo en cuenta las expresiones (5.21), (5.22) y (5.23), la representación entrada-estado-salida del código concatenado  $\mathcal{PC}^{(3)}(A, B, C, D)$  viene dada por

$$\begin{aligned} x_{t+1} &= \text{diag}(A_1, A_2, \dots, A_s) x_t + \text{diag}(B_1, B_2, \dots, B_s) u_t, \\ y_t &= \text{diag}(C_1, C_2, \dots, C_s) x_t + \text{diag}(D_1, D_2, \dots, D_s) u_t. \end{aligned} \quad \square$$

La función de transferencia del código  $\widehat{\mathcal{PC}}^{(3)}$  viene dada en términos de la función de transferencia de los códigos constituyentes (considerados como  $\mathcal{F}$ -subespacios vectoriales de  $\mathcal{F}^n$ ), como mostramos en el teorema siguiente.

**Teorema 5.12:** Si  $\mathcal{PC}^{(3)}(A, B, C, D)$  es el código concatenado descrito por las matrices de la expresión (5.24), entonces

$$T(z) = \text{diag}(T_1(z), T_2(z), \dots, T_s(z))$$

es la función de transferencia asociada a  $\widehat{\mathcal{PC}}^{(3)}$ .

Teniendo en cuenta la expresión (5.24) de las matrices  $A$ ,  $B$ ,  $C$  y  $D$  que describen el código concatenado  $\mathcal{PC}^{(3)}$ , obtenemos, de manera trivial, que las propiedades de

controlabilidad y observabilidad de los códigos constituyentes, son heredadas por el código concatenado.

**Teorema 5.13:** Si  $\mathcal{PC}^{(3)}(A, B, C, D)$  es el código de tasa  $k/n$  obtenido de la concatenación en paralelo por bloques de los  $(n_j, k_j, \delta_j)$ -códigos  $\mathcal{C}_j(A_j, B_j, C_j, D_j)$ , para  $j = 1, 2, \dots, s$ , entonces:

- (a)  $(A, B)$  es controlable si y sólo si  $(A_j, B_j)$  es controlable, para  $j = 1, 2, \dots, s$ .
- (b)  $(A, C)$  es observable si y sólo si  $(A_j, C_j)$  es observable, para  $j = 1, 2, \dots, s$ .

## 5.4 Códigos convolucionales *woven* desde el punto de vista de sistemas lineales

En esta sección, estudiamos los códigos convolucionales *woven* empleando herramientas de la teoría clásica de sistemas. Obtenemos la representación entrada-estado-salida únicamente del *warp* descrito en la sección 1.6.2, ya que la sección 3.3, nos proporciona tanto la realización de un código convolucional *woven* con *warp* externo o bien con *warp* interno, como la del *twill* (observemos que estos códigos corresponden a la concatenación en serie  $\mathcal{SC}^{(4)}$  descrita en la sección 3.3.1, cuya representación entrada-estado-salida viene dada por el teorema 3.17).

A lo largo de esta sección, denotamos por  $x_t^{(l)}$ ,  $u_t^{(l)}$ ,  $y_t^{(l)}$  y  $v_t^{(l)}$ , el vector de estados, el vector información, el vector de paridad, y la palabra código, respectivamente, del código  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$ , para  $l = 1, 2, \dots, l_w$ , siendo  $l_w$  el número de códigos que componen el *warp*.

También, 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, respectivamente, del *warp*  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$ .

Finalmente,  $T_l(z)$  y  $T(z)$  son las funciones de transferencia asociadas a los códigos  $\widehat{\mathcal{C}}_l(A_l, B_l, C_l, D_l)$  y  $\widehat{\mathcal{C}}^w(A^w, B^w, C^w, D^w)$ , respectivamente, para  $l = 1, 2, \dots, l_w$ .

Recordemos, como ya se comentó en la sección 1.6, que el código *warp* nunca es MDS, ya que su distancia libre es el mínimo de las distancias libres de los códigos constituyentes.

### 5.4.1 Warp formado por códigos convolucionales idénticos

Consideremos en primer lugar que el *warp*  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  está formado por  $l_w$  códigos convolucionales  $\mathcal{C}(A, B, C, D)$  idénticos, con matriz generadora  $G(z)$ . La relación (1.25) muestra la expresión de la matriz generadora del *warp* en función de la matriz generadora de los códigos constituyentes,

$$G^w(z) = G(z) \otimes I_{l_w}. \quad (5.25)$$

Dado que ésta viene dada a través de un producto de Kronecker, emplearemos las propiedades de este caso especial de producto tensorial descritas en la sección 1.6.1. Denotamos entonces el vector de estados y el vector de paridad del  $(n, k, \delta)$ -código  $\mathcal{C}(A, B, C, D)$  que forma el *warp* por

$$x_t^{(1)} = \begin{pmatrix} x_t^{(1,1)} \\ x_t^{(2,1)} \\ \vdots \\ x_t^{(\delta,1)} \end{pmatrix} \quad \text{e} \quad y_t^{(1)} = \begin{pmatrix} y_t^{(1,1)} \\ y_t^{(2,1)} \\ \vdots \\ y_t^{(n-k,1)} \end{pmatrix},$$

Del mismo modo,  $T_1(z)$  denota la función de transferencia asociada a  $\widehat{\mathcal{C}}(A, B, C, D)$ .

Observemos que, según la construcción del *warp* dada en la sección 1.6, el vector información, el vector de estados y el vector de paridad del código  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  vienen dados por

$$u_t = u_t^{(1)} \otimes I_{l_w}, \quad x_t = x_t^{(1)} \otimes I_{l_w} \quad \text{e} \quad y_t = y_t^{(1)} \otimes I_{l_w}, \quad (5.26)$$

respectivamente. El resultado siguiente proporciona la representación entrada-estado-salida del *warp* formado por códigos convolucionales idénticos.

**Teorema 5.14:** *Si  $\mathcal{C}(A, B, C, D)$  es un  $(n, k, \delta)$ -código, entonces la representación entrada-estado-salida del warp  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  de tasa  $kl_w/nl_w$  obtenido al concatenar  $\mathcal{C}$  en paralelo  $l_w$  veces, viene dada por el sistema lineal (1.11), donde*

$$A^w = A \otimes I_{l_w}, \quad B^w = B \otimes I_{l_w}, \quad C^w = C \otimes I_{l_w} \quad \text{y} \quad D^w = D \otimes I_{l_w}.$$

DEMOSTRACIÓN: De la expresión (1.11) tenemos, para el código  $\mathcal{C}(A, B, C, D)$ ,

$$\begin{aligned}x_{t+1}^{(1)} &= A_1 x_t^{(1)} + B_1 u_t^{(1)}, \\y_t^{(1)} &= C_1 x_t^{(1)} + D_1 u_t^{(1)},\end{aligned}$$

Ahora bien, teniendo en cuenta la expresión (5.26), así como las propiedades (b) y (c) del producto de Kronecker (véase la sección 1.6.1), la representación entrada-estado-salida del código  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  viene dada por

$$\begin{aligned}x_{t+1} &= x_{t+1}^{(1)} \otimes I_{l_w} = (Ax_t^{(1)} + Bu_t^{(1)}) \otimes I_{l_w} \\&= Ax_t^{(1)} \otimes I_{l_w} + Bu_t^{(1)} \otimes I_{l_w} \\&= (A \otimes I_{l_w})(x_t^{(1)} \otimes I_{l_w}) + (B \otimes I_{l_w})(u_t^{(1)} \otimes I_{l_w}) \\&= (A \otimes I_{l_w})x_t + (B \otimes I_{l_w})u_t, \\y_t &= y_t^{(1)} \otimes I_{l_w} = (Cx_t^{(1)} + Du_t^{(1)}) \otimes I_{l_w} \\&= Cx_t^{(1)} \otimes I_{l_w} + Du_t^{(1)} \otimes I_{l_w} \\&= (C \otimes I_{l_w})(x_t^{(1)} \otimes I_{l_w}) + (D \otimes I_{l_w})(u_t^{(1)} \otimes I_{l_w}) \\&= (C \otimes I_{l_w})x_t + (D \otimes I_{l_w})u_t.\end{aligned}$$

□

La función de transferencia del código  $\widehat{\mathcal{C}}^w(A^w, B^w, C^w, D^w)$  viene dada en términos de la función de transferencia de  $\widehat{\mathcal{C}}(A, B, C, D)$ , como ponemos de manifiesto en el resultado siguiente.

**Teorema 5.15:** *Si  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  es el warp obtenido al concatenar  $\mathcal{C}(A, B, C, D)$  en paralelo  $l_w$  veces, entonces*

$$T^w(z) = T(z) \otimes I_{l_w}$$

*es la función de transferencia asociada a  $\widehat{\mathcal{C}}^w(A^w, B^w, C^w, D^w)$ .*

A continuación, estudiamos las condiciones que deben verificar las matrices  $A$ ,  $B$ ,  $C$  y  $D$  que describen el código  $\mathcal{C}$  cuya concatenación en paralelo da lugar al warp para tener una representación minimal de  $\mathcal{C}^w$ , de manera que la matriz generadora inducida por la realización sea no catastrófica. Como vemos en los resultados siguientes, las propiedades de controlabilidad y observabilidad de  $\mathcal{C}(A, B, C, D)$  son heredadas por el warp  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$ .

**Teorema 5.16:** Sean  $\mathcal{C}(A, B, C, D)$  un  $(n, k, \delta)$ -código y  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  el warp obtenido de la concatenación en paralelo  $l_w$  veces de  $\mathcal{C}(A, B, C, D)$ .

- (a) Si  $(A, B)$  es controlable, entonces  $(A^w, B^w)$  es controlable.
- (b) Si  $(A, C)$  es observable, entonces  $(A^w, C^w)$  es observable.

DEMOSTRACIÓN: (a) Como  $(A, B)$  es controlable, por el test PBH (véase la sección 1.5), sabemos que

$$\text{rg} \begin{pmatrix} zI_\delta - A & B \end{pmatrix} = \delta \quad \text{para todo } z \in \overline{\mathbb{F}}.$$

Entonces, teniendo en cuenta las propiedades (b), (g) y (h) del producto de Kronecker dadas en la sección 1.6.1, tenemos que, para todo  $z \in \overline{\mathbb{F}}$ ,

$$\begin{aligned} \text{rg} \begin{pmatrix} zI_{\delta l_w} - A^w & B^w \end{pmatrix} &= \text{rg} \begin{pmatrix} zI_\delta \otimes I_{l_w} - A \otimes I_{l_w} & B \otimes I_{l_w} \end{pmatrix} \\ &= \text{rg} \left( (zI_\delta - A) \otimes I_{l_w} \quad B \otimes I_{l_w} \right) \\ &= \text{rg} \left( \begin{pmatrix} zI_\delta - A & B \end{pmatrix} \otimes I_{l_w} \right) \\ &= \text{rg} \begin{pmatrix} zI_\delta - A & B \end{pmatrix} \text{rg}(I_{l_w}) \\ &= \delta l_w, \end{aligned}$$

y, en consecuencia, el par  $(A^w, B^w)$  es controlable.

(b) Mediante un razonamiento análogo al anterior pero ahora sobre la matriz  $\begin{pmatrix} zI_{\delta l_w} - A^w \\ C^w \end{pmatrix}$ , obtenemos que el par  $(A^w, C^w)$  es observable.  $\square$

### 5.4.2 Warp formado por códigos convolucionales distintos

Consideremos ahora que el warp está formado por la concatenación en paralelo de  $l_w$  códigos convolucionales  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$  distintos pero con la misma tasa  $k/n$  y misma complejidad  $\delta$  y con matriz generadora  $G_l(z)$ , para  $l = 1, 2, \dots, l_w$ . Entonces, de la relación (1.26), obtenemos que la expresión de la matriz generadora del warp

$\mathcal{C}^w(A^w, B^w, C^w, D^w)$  es

$$G^w(z) = \sum_{l=1}^{l_w} G_l(z) \otimes \text{diag}(e_l), \quad (5.27)$$

donde  $e_l$  denota el vector que tiene un 1 en la  $l$ -ésima componente y 0 en el resto de las componentes.

En el caso que nos ocupa, el *warp* está formado por  $l_w$  códigos distintos, de modo que el vector información, el vector de estados y el vector de paridad del código  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  vienen dados por

$$\begin{aligned} u_t &= \sum_{l=1}^{l_w} u_t^{(l)} \otimes \text{diag}(e_l), \\ x_t &= \sum_{l=1}^{l_w} x_t^{(l)} \otimes \text{diag}(e_l) \\ y_t &= \sum_{l=1}^{l_w} y_t^{(l)} \otimes \text{diag}(e_l), \end{aligned} \quad (5.28)$$

respectivamente.

La representación entrada-estado-salida del *warp* formado por  $l_w$  códigos distintos viene dada, como en el caso en que los códigos son idénticos, en función de la representación entrada-estado-salida de los códigos constituyentes, como muestra el resultado siguiente.

**Teorema 5.17:** Si  $\mathcal{C}_l(A, B, C, D)$  es un  $(n, k, \delta)$ -código, para  $l = 1, 2, \dots, l_w$ , entonces la representación entrada-estado-salida del *warp*  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  de tasa  $kl_w/nl_w$  obtenido al concatenar los códigos  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$  en paralelo, para  $l = 1, 2, \dots, l_w$ , viene dada por el sistema lineal (1.11), donde

$$\begin{aligned} A^w &= \sum_{l=1}^{l_w} A_l \otimes \text{diag}(e_l), & B^w &= \sum_{l=1}^{l_w} B_l \otimes \text{diag}(e_l), \\ C^w &= \sum_{l=1}^{l_w} C_l \otimes \text{diag}(e_l), & D^w &= \sum_{l=1}^{l_w} D_l \otimes \text{diag}(e_l), \end{aligned} \quad (5.29)$$

siendo  $e_l$  el vector que tiene un 1 en la  $l$ -ésima componente y 0 en las restantes, para  $l = 1, 2, \dots, l_w$ .

DEMOSTRACIÓN: De la expresión (1.11) tenemos, para el código  $\mathcal{C}_l(A, B, C, D)$ ,

$$\begin{aligned}x_{t+1}^{(l)} &= A_l x_t^{(l)} + B_l u_t^{(l)}, \\y_t^{(l)} &= C_l x_t^{(l)} + D_l u_t^{(l)},\end{aligned}$$

para  $l = 1, 2, \dots, l_w$ . Ahora bien, teniendo en cuenta la expresión (5.26), así como las propiedades (b) e (i) del producto de Kronecker (véase la sección 1.6.1), la representación entrada-estado-salida del código  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  viene dada por

$$\begin{aligned}x_{t+1} &= \sum_{l=1}^{l_w} x_{t+1}^{(l)} \otimes \text{diag}(e_l) \\&= \sum_{l=1}^{l_w} (A_l x_t^{(l)} + B_l u_t^{(l)}) \otimes \text{diag}(e_l) \\&= \sum_{l=1}^{l_w} (A_l x_t^{(l)} \otimes \text{diag}(e_l)) + \sum_{l=1}^{l_w} (B_l u_t^{(l)} \otimes \text{diag}(e_l)) \\&= \sum_{l=1}^{l_w} (A_l \otimes \text{diag}(e_l)) \sum_{l=1}^{l_w} (x_t^{(l)} \otimes \text{diag}(e_l)) \\&\quad + \sum_{l=1}^{l_w} (B_l \otimes \text{diag}(e_l)) \sum_{l=1}^{l_w} (x_t^{(l)} \otimes \text{diag}(e_l)) \\&= \left( \sum_{l=1}^{l_w} A_l \otimes \text{diag}(e_l) \right) x_t + \left( \sum_{l=1}^{l_w} B_l \otimes \text{diag}(e_l) \right) u_t, \\y_t &= \sum_{l=1}^{l_w} y_t^{(l)} \otimes \text{diag}(e_l) \\&= \sum_{l=1}^{l_w} (C_l x_t^{(l)} + D_l u_t^{(l)}) \otimes \text{diag}(e_l) \\&= \sum_{l=1}^{l_w} (C_l x_t^{(l)} \otimes \text{diag}(e_l)) + \sum_{l=1}^{l_w} (D_l u_t^{(l)} \otimes \text{diag}(e_l)) \\&= \sum_{l=1}^{l_w} (C_l \otimes \text{diag}(e_l)) \sum_{l=1}^{l_w} (x_t^{(l)} \otimes \text{diag}(e_l)) \\&\quad + \sum_{l=1}^{l_w} (D_l \otimes \text{diag}(e_l)) \sum_{l=1}^{l_w} (x_t^{(l)} \otimes \text{diag}(e_l))\end{aligned}$$

$$= \left( \sum_{l=1}^{l_w} C_l \otimes \text{diag}(e_l) \right) x_t + \left( \sum_{l=1}^{l_w} D_l \otimes \text{diag}(e_l) \right) u_t. \quad \square$$

De nuevo, la función de transferencia asociada a  $\widehat{\mathcal{C}}^w(A^w, B^w, C^w, D^w)$  viene dada en términos de las funciones de transferencia asociadas a los códigos constituyentes (considerados como  $\mathcal{F}$ -subespacios vectoriales de  $\mathcal{F}^n$ ), como mostramos en el siguiente resultado.

**Teorema 5.18:** *Si  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  es el warp obtenido al concatenar los códigos  $\mathcal{C}_l(A_l, B_l, C_l, D_l)$  en paralelo, para  $l = 1, 2, \dots, l_w$ , entonces*

$$T^w(z) = \sum T_l(z) \otimes \text{diag}(e_l)$$

*es la función de transferencia asociada a  $\widehat{\mathcal{C}}^w(A^w, B^w, C^w, D^w)$ .*

Tal y como teníamos para el warp formado por códigos convolucionales idénticos, para el caso que nos ocupa, las propiedades de controlabilidad y observabilidad de los códigos constituyentes también son heredadas por el warp, como pone de manifiesto el resultado siguiente.

**Teorema 5.19:** *Sea  $\mathcal{C}^w(A^w, B^w, C^w, D^w)$  el warp obtenido de la concatenación en paralelo de los  $(n, k, \delta)$ -códigos  $\mathcal{C}_l(A, B, C, D)$ , para  $l = 1, 2, \dots, l_w$ , siendo  $A^w, B^w, C^w, D^w$  las matrices dadas por la relación (5.29), entonces*

- (a) *Si  $(A_l, B_l)$  es controlable, para  $l = 1, 2, \dots, l_w$ , entonces  $(A^w, B^w)$  es controlable.*
- (b) *Si  $(A_l, C_l)$  es observable, para  $l = 1, 2, \dots, l_w$ , entonces  $(A^w, C^w)$  es observable.*

DEMOSTRACIÓN: (a) Teniendo en cuenta las propiedades (b) y (k) del producto de Kronecker dadas en la sección 1.6.1, obtenemos que

$$\begin{aligned} \left( zI_{\delta l_w} - A^w \quad B^w \right) &= \left( zI_{\delta l_w} - \sum_{l=1}^{l_w} A_l \otimes \text{diag}(e_l) \quad \sum_{l=1}^{l_w} B_l \otimes \text{diag}(e_l) \right) \\ &= \left( \sum_{l=1}^{l_w} zI_{\delta} \otimes \text{diag}(e_l) - \sum_{l=1}^{l_w} A_l \otimes \text{diag}(e_l) \quad \sum_{l=1}^{l_w} B_l \otimes \text{diag}(e_l) \right) \\ &= \left( \sum_{l=1}^{l_w} (zI_{\delta} - A_l) \otimes \text{diag}(e_l) \quad \sum_{l=1}^{l_w} B_l \otimes \text{diag}(e_l) \right) \end{aligned}$$

$$\begin{aligned}
&= \sum_{l=1}^{l_w} \left( (zI_\delta - A_l) \otimes \text{diag}(e_l) \quad B_l \otimes \text{diag}(e_l) \right) \\
&= \sum_{l=1}^{l_w} \left( zI_\delta - A_l \quad B_l \right) \otimes \text{diag}(e_l),
\end{aligned}$$

de donde aplicando la propiedad (1) del producto de Kronecker (véase la sección 1.6.1), al ser  $\text{rg} \begin{pmatrix} zI_\delta - A_l & B_l \end{pmatrix} = \delta$  para todo  $z \in \overline{\mathbb{F}}$  (ya que  $(A_l, B_l)$  es controlable, para  $l = 1, 2, \dots, l_w$ ), obtenemos que

$$\text{rg} \begin{pmatrix} zI_{\delta l_w} - A^w & B^w \end{pmatrix} = \text{rg} \left( \sum_{l=1}^{l_w} \begin{pmatrix} zI_\delta - A_l & B_l \end{pmatrix} \otimes \text{diag}(e_l) \right) = \delta l_w$$

para todo  $z \in \overline{\mathbb{F}}$ , es decir, el par  $(A^w, B^w)$  es controlable.

(b) Mediante un razonamiento similar al del apartado anterior, pero sobre la matriz  $\begin{pmatrix} zI_{\delta l_w} - A^w \\ C^w \end{pmatrix}$ , obtenemos que el par  $(A^w, C^w)$  es observable.  $\square$

## 5.5 Conclusiones

En este capítulo hemos modelizado diferentes tipos de concatenación en paralelo de códigos convolucionales, proporcionando condiciones para obtener representaciones minimales de los códigos concatenados, y también para que éstos no sean catastróficos. También hemos obtenido cotas inferiores de la distancia libre de uno de los modelos de concatenación. Además, el trabajar desde el punto de vista de sistemas, nos permite conocer el grado o complejidad del código *warp*, hecho que nos proporciona a su vez, mediante una combinación de los resultados obtenidos en este capítulo y en el capítulo 3, el grado del código *woven*.

---

## Apéndice A

# Líneas futuras

---

Los resultados de perforación de códigos convolucionales basados en la construcción de Justesen introducidos en esta memoria nos permiten elegir la matriz patrón de la perforación de manera que la matriz generadora del código perforado obtenido sea minimal. El siguiente paso que nos proponemos es evaluar las distancias columnas del código de Justesen perforado y obtener cotas de su distancia libre en función de la distancia libre del código original.

Por otra parte, hemos obtenido nuevas construcciones de códigos a partir de la concatenación de códigos convolucionales, introduciendo condiciones que nos proporcionan el grado del código y nos aseguran que la concatenación sea no catastrófica. La obtención de cotas inferiores de las distancias libres de ciertos modelos de concatenación nos permite conocer el intervalo en el que están comprendidas dichas distancias libres, empleando la cota Singleton generalizada como cota superior. El problema pendiente de abordar es la obtención de algoritmos efectivos de decodificación que exploten la estructura algebraica de estos códigos. También hemos modelizado desde el punto de vista de sistemas la concatenación de un código bloque y un código convolucional, introduciendo condiciones que aseguran que el código concatenado es un código óptimo aunque los códigos constituyentes no lo sean. Empleando dichas condiciones, pretendemos aplicar estos códigos concatenados para el caso particular de la codificación de canal en tecnología GSM y diseñar algoritmos eficientes de codificación y decodificación empleando las propiedades algebraicas tanto del código bloque como del código convolucional.

Con respecto a la concatenación en paralelo de códigos convolucionales, hemos modelizado varios tipos de concatenaciones, si bien algunas de ellas no pueden dar lugar a códigos MDS, nuestro objetivo es estudiar, desde el punto de vista de sistemas, qué tipos de entrelazados podemos emplear para la concatenación  $\mathcal{PC}^{(3)}$  y para los códigos

*woven* con la finalidad de dispersar las ráfagas de error y reducir la concentración de errores que se deben corregir por el código del canal.

Finalmente, otro problema pendiente de abordar es aplicar la técnica de perforación a códigos concatenados empleando teoría de sistemas.



# Bibliografía

---

- [1] K. A. S. ABDEL-GHAFFAR. Some convolutional codes whose free distances are maximal. *IEEE Transactions on Information Theory*, **35(1)**: 188–191 (1989).
- [2] S. ALI. *Concatenation of Space-Time Block Codes with Convolutional Codes*. Tesis Doctoral, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, 2004.
- [3] B. M. ALLEN. *Linear Systems Analysis and Decoding of Convolutional Codes*. Tesis Doctoral, University of Notre Dame, 1999.
- [4] P. J. ANTSAKLIS y A.Ñ. MICHEL. *Linear Systems*. McGraw-Hill, New York, 1997.
- [5] F. BABICH, G. MONTORSI y F. VATTA. Rate-compatible punctured serial concatenated convolutional codes. En *Proceedings of the IEEE 2003 Global Telecommunications Conference GLOBECOM '03*. IEEE, San Francisco, USA, 2003.
- [6] S. BENEDETTO, D. DIVSALAR, G. MONTORSI y F. POLLARA. Algorithm for continuous decoding of turbo codes. *Electronic Letters*, **32(4)**: 314–315 (1996).
- [7] S. BENEDETTO, D. DIVSALAR, G. MONTORSI y F. POLLARA. Serial concatenation of interleaved codes: Performance analysis, design and iterative decoding. *IEEE Transactions on Information Theory*, **44(3)**: 909–926 (1998).
- [8] S. BENEDETTO y G. MONTORSI. Average performance of parallel concatenated block codes. *Electronic Letters*, **31**: 156–158 (1994).
- [9] S. BENEDETTO y G. MONTORSI. Performance evaluation of turbo codes. *Electronic Letters*, **31(3)**: 163–165 (1995).
- [10] S. BENEDETTO y G. MONTORSI. The role of recursive convolutional codes in turbo codes. *Electronic Letters*, **31(11)**: 858–859 (1995).
- [11] S. BENEDETTO y G. MONTORSI. Serial concatenation of block and convolutional codes. *Electronic Letters*, **32(13)**: 887–888 (1996).
- [12] S. BENEDETTO y G. MONTORSI. Unveiling turbo-codes: some results on parallel concatenated coding schemes. *IEEE Transactions on Information Theory*,

- 42(2)**: 409–429 (1996).
- [13] C. BERROU, A. GLAVIEUX y P. THITIMAJSHIMA. Near Shannon limit error-correcting coding and decoding: turbo codes (1). En *International Conference on Communication*, páginas 1064–1070. IEEE, Geneva, Switzerland, 1993.
- [14] E. R. BLOKH y V. V. ZYABLOV. *Linear concatenated codes*. Nauka, Moscow, 1982.
- [15] J. B. CAIN, G. C. CLARK, JR y J. M. GEIST. Punctured convolutional codes of rate  $(n - 1)/n$  and simplified maximum likelihood decoding. *IEEE Transactions on Information Theory*, **25(1)**: 97–100 (1979).
- [16] G. P. CALZOLARI, F. CHIARALUCE, R. GARELLO y E. VASSALLO. Turbo code applications on telemetry and deep space communications. En *Turbo Code Applications a journey from a paper to realization*, páginas 321–344. Springer-Verlag, 2005.
- [17] N. CHANDRAN y M. C. VALENTI. Hybrid ARQ using serial concatenated convolutional codes over fading channels. En *Proceedings of the 2001 IEEE 53rd Vehicular Technology Conference-VTC'01*, páginas 1410–1414. IEEE, Rhodes, Greece, 2001.
- [18] C.-T. CHEN. *Linear Systems Theory and Design*. Oxford University Press, 1999.
- [19] R. S. CHERNOCK, R. J. CRINON, M. A. DOLAN y J. R. MICK. *Data Broadcasting: Understanding the Atsc Data Broadcast Standard*. McGraw-Hill, New York, 2001.
- [20] J. J. CLIMENT, V. HERRANZ y C. PEREA. Construcción de códigos convolucionales a partir de sistemas lineales de control discretos en el tiempo. En *Proceedings del XVIII Congreso de Ecuaciones Diferenciales y Aplicaciones. VIII Congreso de Matemática Aplicada*, páginas 159–160. CEDYA, 2003.
- [21] J. J. CLIMENT, V. HERRANZ y C. PEREA. A classification of convolutional codes based on Justesen's construction. En *Electronic Proceedings of the Sixteenth International Symposium on Mathematical Theory of Networks and Systems (MTNS)*. MTNS, 2004.
- [22] J. J. CLIMENT, V. HERRANZ y C. PEREA. New convolutional codes from old convolutional codes. En *Electronic Proceedings of the Sixteenth International Symposium on Mathematical Theory of Networks and Systems (MTNS)*, páginas 1–4. MTNS, 2004.
- [23] J. J. CLIMENT, V. HERRANZ y C. PEREA. Composite linear time invariant systems and its applications to convolutional codes. En *Proceedings of The Fifth International Conference on Engineering Computational Technology, Civil-Comp*

- Press*, páginas 203–204. 2006.
- [24] J. J. CLIMENT, V. HERRANZ y C. PEREA. A first approximation of concatenated convolutional codes from linear systems theory viewpoint. En proceso de evaluación.
- [25] J. J. CLIMENT, V. HERRANZ y C. PEREA. Linear system modelization of GSM digital mobile system. En proceso de evaluación.
- [26] J. J. CLIMENT, V. HERRANZ y C. PEREA. On puncturing convolutional codes based on Justesen's construction. En proceso de evaluación.
- [27] J. J. CLIMENT, V. HERRANZ y C. PEREA. Some applications of the inclusion principle to convolutional codes. En *Electronic Proceedings of the Sixteenth International Symposium on Mathematical Theory of Networks and Systems (MTNS)*, páginas 197–202. MTNS, 2006.
- [28] D. J. COSTELLO, JR., P. C. MASSEY, O. M. COLLINS y O. Y. TAKESHITA. Some reflections on the mythology of turbo codes. En *Proceedings of the 3rd ITG Conference on Source and Channel Coding*, páginas 157–160. Munich, Germany, 2000.
- [29] D. J. COSTELLO JR., H. A. CABRAL y O. Y. TAKESHITA. Some thoughts on the equivalence of systematic and non-systematic convolutional encoders. En R. E. BLAHUT y R. KOETTER (editores), *Codes, Graphs and Systems*. Kluwer Academic, 2002.
- [30] D. F. DELCHAMPS. *State Space and Input-Output Linear Systems*. Springer-Verlag, New York, 1988.
- [31] C. DELTOSO, M. CAND y L. SPONGA. A punctured viterbi decoder compatible with DVB standards. Preprint.
- [32] A. DHOLAKIA. *Introduction to Convolutional Codes With Applications*. Kluwer Academic Publishers, 1994.
- [33] D. DIVSALAR y F. POLLARA. Turbo codes for deep-space communications. *JPL TDA Progress Report*, páginas 42–120 (1995).
- [34] D. DIVSALAR y F. POLLARA. Turbo codes for PCS applications. En *Proceedings of IEEE ICC'95*, páginas 54–59. IEEE, Seattle, Washington, 1995.
- [35] D. DIVSALAR y F. POLLARA. Hybrid concatenated codes and iterative decoding. *JPL TDA Progress Report*, **42(130)**: 1–23 (1997).
- [36] J. A. DOMÍNGUEZ, J. M. MUÑOZ, J. I. IGLESIAS y G. SERRANO. Convolutional goppa codes. *IEEE Transactions on Information Theory*, **52**: 340–344 (2006).
- [37] J. A. DOMÍNGUEZ, J. M. MUÑOZ y G. SERRANO. Convolutional codes of goppa type. *Applicable Algebra in Engineering, Communication and Computing*,

- 15: 51–61 (2004).
- [38] P. ELIAS. Error-free coding. *IRE Transactions on Information Theory*, **4**: 29–37 (1954).
- [39] P. ELIAS. Coding for noisy channels. *IRE Convention Record*, **4**: 37–46 (1955).
- [40] W. FISCHER. *Digital Television: A Practical Guide for Engineers*. Springer-Verlag, Berlin Heidelberg, 2004.
- [41] G. D. FORNEY, JR. *Concatenated Codes*. MA: MIT Press, Cambridge, 1966.
- [42] G. D. FORNEY, JR. Convolutional codes i: algebraic structure. *IEEE Transactions on Information Theory*, **16(6)**: 720–738 (1970).
- [43] R. GARELLO, P. PIERLEONI y S. BENEDETTO. Computing the free distance of turbo codes and serially concatenated codes with interleavers: algorithms and applications. *IEEE Journal on Selected Areas in Communications*, **19(5)**: 800–812 (2001).
- [44] H. GLUESING-LUERSSEN, J. ROSENTHAL y R. SMARANDACHE. Strongly MDS convolutional codes. *IEEE Transactions on Information Theory*, **52(2)**: 584–598 (2006).
- [45] H. GLUESING-LUERSSEN y W. SCHMALE. On cyclic convolutional codes. Preprint.
- [46] V. D. GOPPA. *Geometry and codes*. Kluwer Academic Publisher, 1988.
- [47] A. GRAHAM. *Kronecker Products and Matrix Calculus with Applications*. John Wiley and Sons, New York, 1981.
- [48] J. HAGENAUER. Hybrid ARQ/FEC protocols on fading channels using rate compatible punctured convolutional codes. En *Proceedings of IEEE International Conference on Communications*, páginas 744–748. IEEE, 1987.
- [49] J. HAGENAUER. The performance of rate-compatible punctured convolutional codes for digital mobile radio. *IEEE Transactions on Communications*, **38(7)**: 966–980 (1990).
- [50] J. HAGENAUER. Rate-compatible punctured convolutional codes (RCPC codes) and their applications. *IEEE Transactions on Communications*, **36(4)**: 389–400 (1998).
- [51] M. HANKAMER. *Concatenated convolutional codes: Applications to deep-space telecommunication*. Tesis Doctoral, New Mexico State University, Las Cruces, 1977.
- [52] M. HATORI y T. SHIOMI. *Digital Broadcasting*. Ohmsha, Ltd, Tokyo, 2000.
- [53] M. HAUTUS. Controllability and observability condition for linear autonomous systems. En *Proceedings of Nederlandse Akademie voor Wetenschappen. Series*

- A*, 72, páginas 443–448. 1969.
- [54] K. J. HOLE. An algorithm for determining if a rate  $(n - 1)/n$  punctured convolutional encoder is catastrophic. *IEEE Transactions on Communications*, **39(3)**: 386–389 (1991).
- [55] K. J. HOLE. Punctured convolutional codes for the 1-d partial-response channel. *IEEE Transactions on Information Theory*, **37(3)**: 808–817 (1991).
- [56] K. J. HOLE. Rate  $k/(k + 1)$  minimal punctured convolutional encoders. *IEEE Transactions on Information Theory*, **37(3)**: 653–655 (1991).
- [57] K. J. HOLE. New short constraint length rate  $(n - 1)/n$  punctured convolutional codes for soft-decision Viterbi decoding. *IEEE Transactions on Information Theory*, **34(5)**: 1079–1081 (1998).
- [58] S. HÖST, R. JOHANNESSON, V. SIDORENKO, K. S. ZIGANGIROV y V. ZYABLOV. Cascaded convolutional codes. En M. DARNELL y B. HONARY (editores), *Communication and Coding*, páginas 10–29. U.K.:Research Studies/Wiley, 1998.
- [59] S. HÖST, R. JOHANNESSON y V. ZYABLOV. A first encounter with binary woven convolutional codes. En *Proceedings of the 4th International Symposium on Communication Theory and Applications*, páginas 13–18. Lake Districts, UK, 1997.
- [60] S. HÖST, R. JOHANNESSON y V. ZYABLOV. Woven convolutional codes I: Encoder properties. *IEEE Transactions on Information Theory*, **48(4)**: 149–161 (2002).
- [61] W. C. HUFFMAN y V. PLESS. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.
- [62] R. HUTCHINSON, J. ROSENTHAL y R. SMARANDACHE. Convolutional codes with maximum distance profile. *Systems and Control Letters*, **4(1)**: 53–63 (2005).
- [63] R. JOHANNESSON y Z. K. SH. *Fundamentals Convolutional Coding*. IEEE Press, 1999.
- [64] R. JOHANNESSON y Z.-X. WAN. A linear algebra approach to minimal convolutional encoders. *IEEE Transactions on Information Theory*, **39(4)**: 1219–1233 (1993).
- [65] R. JOHANNESSON y K. S. ZIGANGIROV. Distances and distance bounds for convolutional codes—an overview. En *Topics in Coding Theory—in honour of Lars H. Zetterberg*, páginas 109–136. Springer Verlag, 1989.
- [66] P. JUNG y J. PLECHINGER. Performance of rate compatible punctured turbo-codes for mobile radio applications. *IEE Electronic Letters*, **33(25)**: 2102–2103 (1997).

- [67] J. JUSTESEN, K. J. LARSEN, H. E. JENSEN, A. HAVEMOSE y T. HOHOLDT. Construction and decoding of a class of algebraic geometry codes. *IEEE Transactions on Information Theory*, **35**: 811–821 (1989).
- [68] J. JUSTESEN. New convolutional code constructions and a class of asymptotically good time-varying codes. *IEEE Transactions on Information Theory*, **19(2)**: 220–225 (1973).
- [69] J. JUSTESEN. An algebraic construction of rate  $1/\nu$  convolutional codes. *IEEE Transactions on Information Theory*, **21(1)**: 577–580 (1975).
- [70] T. KAILATH. *Linear Systems*. Prentice-Hall, 1980.
- [71] R. E. KALMAN. Mathematical description of linear dynamical systems. *SIAM Journal on Control*, **1**: 152–192 (1963).
- [72] H. KIM y G. STÜBER. Rate compatible punctured SCCC. En *Proceedings of the 2001 IEEE 54th Vehicular Technology Conference-VTC'01*, páginas 2399–2403. IEEE, Atlantic City, NJ, USA, 2001.
- [73] W. G. KIM, B. J. KU, L. H. BAEK, H. Y. YANG y C. KANG. Serially concatenated space-time code (SCSTC) for high rate wireless communication systems. *Electronics Letters*, **36(7)**: 646–648 (2000).
- [74] W. G. KIM, B. J. KU, H. Y. YANG, C. KANG y D. HONG. Serially concatenated space-time code for high data rate wireless communication systems. En *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing. ICASSP'00*, volumen 6. 2000.
- [75] Y. LEVY y D. J. COSTELLO, JR. An algebraic approach to constructing convolutional codes from quasicyclic codes. *DIMACS Ser. in Discr. Math and Theor. Comp. Sci.*, **14**: 189–198 (1993).
- [76] S. LIN y D. COSTELLO. *Error Control Coding: fundamentals and applications*. Prentice Hall, 1983.
- [77] J. L. MASSEY, D. J. COSTELLO y J. JUSTESEN. Polynomial weights and code constructions. *IEEE Transactions on Information Theory*, **19(1)**: 101–110 (1973).
- [78] J. L. MASSEY y M. SAIN. Codes, automata, and continuous systems: explicit interconnections. *IEEE Transactions on Automatic Control*, **12(6)**: 644–650 (1967).
- [79] R. J. MCELIECE. The algebraic theory of convolutional codes. En V. PLESS y W. HUFFMAN (editores), *Handbook of Coding Theory*, páginas 1065–1138. Elsevier, 1998.
- [80] F. MCWILLIAMS y N. SLOANE. *The Theory of Error-Correcting Codes*. North

- Holand, Amsterdam, 1977.
- [81] N. NEFEDOV. Application of low complexity serially concatenated codes for edge circuit switched data. En *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Communications (PIMRC'99)*, páginas 573–577. IEEE, Osaka, Japan, 1999.
- [82] P. PIRET. *Convolutional Codes, an Algebraic Approach*. MIT Press, 1988.
- [83] S. PORTER. *Decoding codes arising from Goppa's construction on algebraic curves*. Tesis Doctoral, Yale University, 1988.
- [84] I. REED y G. SOLOMON. Polynomials codes over certain finite fields. *Journal of Society for Industrial and Applied Mathematics*, **8**: 300–304 (1960).
- [85] U. REIMERS. *DVB: The Family of International Standards for Digital Video Broadcasting*. Springer-Verlag, Berlin Heidelberg, 2005.
- [86] M. REZA SOLEYMANI, Y. GAO y U. VILAIPOORSAWAI. *Turbo Coding for Satellite and Wireless Communications*. Springer, MA, USA, 2002.
- [87] S. ROMAN. *Coding and Information Theory*. Springer-Verlag, New York, 1992.
- [88] J. ROSENTHAL. An algebraic decoding algorithm for convolutional codes. Informe Técnico CIM-4, Centro Internacional de Matemática, Coimbra, Portugal, junio 1998.
- [89] J. ROSENTHAL. Connections between linear systems and convolutional codes. En B. MARCUS y J. ROSENTHAL (editores), *Codes, Systems and Graphical Models*, volumen 123 de *IMA*, páginas 39–66. Springer-Verlag, Berlin, 2001.
- [90] J. ROSENTHAL. Minimal bases of rational vector spaces and their importance in algebraic system theory. En R. E. BLAHUT y R. KOETTER (editores), *Codes, Graphs, and Systems*, páginas 345–357. Kluwer Academic Publishers, 2002.
- [91] J. ROSENTHAL, J. SCHUMACHER y E. V. YORK. On behaviors and convolutional codes. *IEEE Transactions on Information Theory*, **42(6)**: 1881–1891 (1996).
- [92] J. ROSENTHAL y R. SMARANDACHE. Construction of convolutional codes using methods from linear systems theory. En *Proceedings of the 35th Allerton Conference on Communications, Control and Computing*, páginas 953–960. Allerton House, Monticello, IL, septiembre 1997.
- [93] J. ROSENTHAL y R. SMARANDACHE. Maximum distance separable convolutional codes. *Applicable Algebra in Engineering, Communication and Computing*, **10**: 15–32 (1999).
- [94] J. ROSENTHAL y E. V. YORK. Linear systems defined over a finite field, dynamic programming and convolutional codes. En *Proceedings of the IFAC System, Structure and Control*, páginas 413–418. 1995.

- [95] J. ROSENTHAL y E. V. YORK. BCH convolutional codes. *IEEE Transactions on Information Theory*, **45(6)**: 1833–1844 (1999).
- [96] D. ROWITCH y L. MILSTEIN. Rate compatible punctured turbo (RCPT) codes in a hybrid FEC/ARQ system. En *Proceedings of the IEEE Communication Theory Mini Conference*, páginas 55–59. IEEE, Phoenix, Arizona, 1997.
- [97] D. ROWITCH y L. MILSTEIN. On the performance of hybrid FEC/ARQ systems using rate compatible punctured turbo (RCPT) codes. *IEEE Transactions on Communications*, **48(6)**: 948–959 (2000).
- [98] C. E. SHANNON. A mathematical theory of communication. *The Bell System Technical Journal*, **27**: 379–423, 623–656 (1948).
- [99] A. SKOROBOGATOV y S. VLADUT. On decoding of algebraic geometric codes. *IEEE Transactions on Information Theory*, **36**: 1051–1060 (1990).
- [100] R. SMARANDACHE, H. GLUESING-LUERSEN y J. ROSENTHAL. Generalized first order descriptions and canonical forms for convolutional codes. Preprint.
- [101] R. SMARANDACHE, H. GLUESING-LUERSEN y J. ROSENTHAL. Constructions of MDS-convolutional codes. *IEEE Transactions on Information Theory*, **47(5)**: 2045–2049 (2001).
- [102] R. SMARANDACHE y J. ROSENTHAL. A state space approach for constructing MDS rate  $1/n$  convolutional codes. En *Proceedings of the 1998 IEEE Information Theory Workshop on Information Theory*, páginas 116–117. Killarney, Kerry, Ireland, junio 1998.
- [103] K. SRIPIMANWAT. *Turbo Code Applications: a journey from a paper to realization*. Springer, The Netherlands, 2005.
- [104] W.-H. STEEB. *Matrix Calculus and the Kronecker Product with Applications and C++ Programs*. World Scientific, Singapore, 1997.
- [105] P. SWEENEY. *Error Control Coding: From Theory to Practice*. John Wiley and Sons, 2002.
- [106] R. M. TANNER. A recursive approach to low complexity codes. *IEEE Transactions on Information Theory*, **27(5)**: 533–547 (1981).
- [107] R. M. TANNER. Convolutional codes from quasicyclic codes: A link between the theories of block and convolutional codes. Informe Técnico USC-CRL-87-21, noviembre 1987.
- [108] E. UHLEMANN. *Hybrid ARQ Using Serially Concatenated Block Codes for Real-Time Communication. An Iterative Decoding Approach*. Tesis Doctoral, Chalmers University of Technology, Göteborg, Sweden, 2001.
- [109] E. UHLEMANN, T. M. AULIN, L. K. RASMUSSEN y P.-A. WIBERG. Hybrid

- ARQ based on serially concatenated block codes using iterative detection for real-time communication. En *Proceedings of Radio Vetenskap och Kommunikation*, páginas 517–521. Stockholm, Sweden, 2002.
- [110] M. C. VALENTI y J. SUN. The UMTS turbo code and an efficient decoder implementation suitable for software-defined radios. *International Journal of Wireless Information Networks*, **8(4)**: 203–215 (2001).
- [111] M. C. VALENTI y J. SUN. Turbo codes. En F. DOWLA (editor), *Handbook of RF and Wireless Technologies*, páginas 375–400. Elsevier, 2004.
- [112] C. F. VAN LOAN. The ubiquitous kronecker product. *Journal of Computational and Applied Mathematics*, **123**: 85–100 (2000).
- [113] A. VITERBI. Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. *IEEE Transactions on Information Theory*, **13**: 260–269 (1967).
- [114] B. VUCETIC y J. YUAN. *Turbo Codes: Principles and Applications*. Springer, Massachusetts, USA, 200.
- [115] Y. WU y M. VALENTI. An arq technique using related parallel and serial concatenated convolutional codes. En *Proceedings of the IEEE International Conference on Communications*, páginas 1390–1394. IEEE, New Orleans, LA, 2000.
- [116] Y. YASUDA, Y. HIRATA, K. NAKAMURA y S. OTANI. Development of variable-rate Viterbi decoder and its performance characteristics. En *Proceedings of the 6th International Conference on Digital Satellite Communications*, páginas XII–24–XII–31. Phoenix, AZ, 1983.
- [117] Y. YASUDA, K. KASHIKI y Y. HIRATA. High-rate punctured convolutional codes for soft decision viterbi decoding. *IEEE Transactions on Communications*, **32(3)**: 315–319 (1984).
- [118] E. V. YORK. *Algebraic Description and Construction of Error Correcting Codes, a Systems Theory Point of View*. Tesis Doctoral, University of Notre Dame, 1997.
- [119] V. ZINOV'EV. Generalized cascade codes. *Problemy Peredachi Informatsii*, **12(1)**: 5–15 (1976).