Universidad Nacional Autónoma de México
Posgrado en Ciencia e Ingeniería de la Computación

Algunos resultados sobre una clase de códigos cíclicos óptimos

T E S I S

QUE PARA OPTAR POR EL GRADO DE:
Doctor en Ciencia e Ingeniería de la Computación

PRESENTA:
Félix Alejandro Hernández Fuentes

TUTOR:
Dr. Gerardo Vega Hernández
Dirección General de Cómputo y de Tecnologías de Información y Comunicación

COMITÉ TUTOR:
Dr. Francisco Javier García Ugalde
Facultad de Ingeniería
Dr. Vladislav Khartchenko
Facultad de Estudios Superiores Cuautitlán

Ciudad Universitaria, Cd. de México. Agosto 2024

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado "Algunos resultados sobre una clase de códigos cíclicos óptimos", que presenté para obtener el grado de Doctor en Ciencia e Ingeniería de la Computación, es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Programa de Posgrado, citando las fuentes, ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de graduación.

Atentamente

Félix Alejandro Hernández Fuentes
305617259

A Paulina y Frijolito

Agradecimientos

A mi tutor, el Dr. Gerardo Vega Hernández, por la oportunidad y la confianza para realizar mis estudios de posgrado bajo su supervisión, por sus enseñanzas a lo largo de este periodo, por su tiempo y energía invertida en este proyecto y por su gran compromiso y paciencia para que este trabajo de investigación se realizara de la mejor manera.

A los miembros de mi comité tutor, el Dr. Francisco Javier García Ugalde y el Dr. Vladislav Khartchenko, por estar al pendiente de mi formación académica durante estos últimos años, por su disposición a siempre escucharme y por su constante motivación y apoyo.

Al Dr. Horacio Tapia Recillas y al Dr. José Noé Gutiérrez Herrera por haber aceptado formar parte de mi jurado, por su valioso tiempo revisando esta tesis y por sus sugerencias y comentarios que hicieron de este un mejor trabajo.

A mi compañera de vida, Paulina, por haber contribuido de distintas formas a la realización de este proyecto, por su incondicional apoyo, por su infinita fe en mí, por su gran amor y por estar a mi lado en cada paso del camino. Gracias por traer a Frijolito a la familia.

A mis padres y a mi hermana por depositar su confianza en mí, por hacer mi camino más llevadero y por su amor y cuidados a lo largo de mi existencia.

A mis suegros, mis cuñados y sus hermosas mascotas por lo buenos momentos y por el cariño y apoyo constante recibido durante estos últimos años.

A la Universidad Nacional Autónoma de México (UNAM) y al Posgrado en Ciencia e Ingeniería de la Computación por haberme brindado la oportunidad de desarrollar mis estudios de posgrado y por los múltiples apoyos recibidos a lo largo de este tiempo.

Al Consejo Nacional de Humanidades, Ciencias y Tecnologías por la beca otorgada para la realización de mis estudios de posgrado y a la Dirección General de Asuntos del Personal Académico de la UNAM por el apoyo recibido mediante el proyecto PAPIIT IN107423.

Índice general

Introducción

Uno de los problemas fundamentales en la comunicación electrónica es proteger la información que se transmite o almacena entre dos puntos que se encuentran separados espacial o temporalmente. La información se envía o almacena a través de un canal de comunicación (la radio, la línea telefónica, un CD) el cual inevitablemente introduce errores en la misma debido a distintos factores (radiación cósmica, ruido en la línea, daño en el CD). Los códigos detectores correctores de error son un componente común en muchos sistemas de comunicaciones y almacenamiento de datos para garantizar que la información se reproduzca con precisión en presencia de errores en la transmisión. Su funcionamiento se basa en añadir a la información redundancia de tal forma que si la información se corrompe sea posible su recuperación. En este sentido, la teoría de códigos aborda tanto la teoría como el diseño de los códigos detectores correctores de error.

Una familia importante de códigos detectores correctores de error es la de los códigos cíclicos. Los códigos cíclicos son una subclase de los códigos lineales por bloque, la cual es utilizada ampliamente en la electrónica de consumo, la criptografía, los sistemas de almacenamiento de datos, entre otros; ya que posee una rica estructura algebraica y sus algoritmos de codificación y decodificación se pueden implementar de manera eficiente. Como ejemplos de códigos cíclicos tenemos a los códigos BCH y Reed-Solomon empleados en la exploración espacial [49], los códigos de barra de dos dimensiones [45], los CD y DVD [34], los discos de estado sólido [46], las tecnologías de transmisión de datos inalámbricas [12], etc. Otro ejemplo son los códigos lineales con dual complementario (linear complementary dual codes o LCD codes), utilizados en la electrónica de consumo, sistemas de comunicaciones, criptografía y en el almacenamiento de datos [38].

Uno de los temas centrales dentro de la investigación en teoría de códigos es la construcción de códigos lineales o cíclicos sobre campos finitos cuya distancia mínima sea máxima para valores fijos de longitud y dimensión, es decir, la construcción de códigos óptimos [3,23,27,29,58,59]. Esto es así pues un código con distancia mínima d puede corregir hasta $\lfloor (d-1)/2 \rfloor$ errores. Un método comúnmente utilizado para construir nuevos códigos óptimos es modificar códigos óptimos previamente estudiados. En los últimos años se han desarrollado distintas técnicas para modificar códigos; por ejemplo, se pueden concatenar dos códigos, también se puede perforar, extender o recortar un código dado, o incluso es posible calcular sus códigos de subcampo. De hecho, muchos de los códigos importantes que hay en la literatura surgen al modificar códigos existentes. Otras características interesantes a describir en un código lineal o cíclico, y que han llamado mucho la atención de los investigadores en los últimos años, son sus distribuciones de pesos de Hamming y completa. Conociendo la distribución de pesos de Hamming de un código es posible construir diseños combinatorios [14], grafos fuertemente regulares [8,54], esquemas de compartición de

secretos [9,36,47,48,69], entre otros; mientras que la distribución de pesos completa puede ser utilizada en la decodificación por decisión suave [5] o para el cálculo de la transformada de Walsh de funciones monomiales sobre campos finitos [22].

Recientemente, Heng y Yue [29] presentaron una clase de códigos cíclicos óptimos de tres pesos definidos sobre cualquier campo finito. El presente trabajo tiene como finalidad exponer los resultados derivados de una profundización en el estudio de dicha clase de códigos. Estos resultados representan investigaciones originales [31–33,61] en el área de teoría de códigos.

En primer lugar estudiamos los códigos de subcampo para una subclase de los códigos cíclicos óptimos reportados en [29] y determinamos sus distribuciones de pesos de Hamming. Resulta que algunos de los códigos obtenidos son óptimos y otros tienen los mejores parámetros conocidos. También investigamos los duales de los códigos de subcampo y demostramos que son casi óptimos. Además, determinamos la estructura de cobertura de los códigos de subcampo y la utilizamos para construir esquemas de compartición de secretos con buenas estructuras de acceso. Más aún, demostramos que, bajo ciertas condiciones, los códigos extendidos de los códigos cíclicos óptimos en [29] resultan en una clase de códigos lineales óptimos de dos pesos cuyos duales son casi óptimos. Como una aplicación de los códigos lineales obtenidos construimos grafos fuertemente regulares.

Por otro lado, también determinamos la distribución de pesos completa para una subclase de los códigos cíclicos óptimos presentados en [29]. Como veremos más adelante, esto se logra a través de la evaluación de un tipo de sumas exponenciales particulares. Como resultado secundario, utilizamos la distribución de valores de dichas sumas para extender la clase de códigos cíclicos óptimos de cinco pesos y dimensión 4 recientemente reportada en [27].

Por último, utilizamos las técnicas de perforado y recortado sobre los códigos cíclicos óptimos presentados en [29] y [27] para obtener tres nuevas clases de códigos lineales óptimos. Las distribuciones de pesos de Hamming para dichos códigos son determinadas utilizando el Teorema de Prange. También investigamos sus códigos duales y demostramos que son óptimos o casi óptimos. Más aún, dichos duales contienen clases de códigos de cuasidistancia máxima separable (almost maximum distance separable codes o AMDS codes) las cuales resultan ser apropiadas para la detección de errores. Además, algunos de los códigos lineales obtenidos se prestan para construir esquemas de compartición de secretos con buenas estructuras de acceso.

Con el objeto de hacer más clara la exposición de estos resultados, el presente trabajo está organizado de la siguiente manera: En el Capítulo 1 recordamos algunas definiciones básicas así como algunos resultados conocidos que serán necesarios para el desarrollo de este trabajo. Los Capítulos 2, 3 y 4 están dedicados a la exposición de los resultados de las investigaciones antes descritas. Finalmente, el Capítulo 5 está dedicado a las conclusiones.

Capítulo 1

Antecedentes

El presente capítulo tiene como finalidad recordar algunas definiciones básicas así como algunos resultados conocidos que serán necesarios para el desarrollo de este trabajo. Para más detalles, se recomienda la consulta del material en [34, 40, 45].

1.1 Campos finitos

En este trabajo estamos interesados en el estudio de códigos lineales definidos sobre campos finitos, es decir, el alfabeto subyacente de estos códigos tiene estructura de campo finito. Dada la importancia de dicha estructura algebraica, a continuación vamos a recordar su definición.

Un conjunto $\mathbb{F}$ es un *campo* si en $\mathbb{F}$ están definidas dos operaciones $(+, \cdot)$ tal que para todo $a, b, c \in \mathbb{F}$ se cumple:

(i) $\mathbb{F}$ es un grupo abeliano bajo $(+)$;

(ii) $\mathbb{F}$ es cerrado bajo $(\cdot)$, y además el conjunto de todos los elementos de $\mathbb{F}$ que son diferentes a cero, $\mathbb{F}^*$, es un grupo abeliano bajo $(\cdot)$;

(iii) las operaciones $(+, \cdot)$ cumplen con la ley distributiva, es decir,

$$a \cdot (b + c) = a \cdot b + a \cdot c \, .$$

En el contexto de un campo, al neutro bajo $(+)$ se le llama *neutro aditivo* y se le denota como 0, mientras que al neutro bajo $(\cdot)$ se le llama *neutro multiplicativo* y se le denota por 1. Al grupo abeliano $(\mathbb{F}, +)$ se le llama *estructura aditiva* del campo $\mathbb{F}$, mientras que al grupo abeliano $(\mathbb{F}^*, \cdot)$ se le llama *estructura multiplicativa* del campo $\mathbb{F}$. Por conveniencia omitiremos el símbolo de multiplicación y escribiremos ab para denotar el producto $a \cdot b$. Se dice que el campo es *finito* si $\mathbb{F}$ tiene un número finito de elementos; el número de elementos en $\mathbb{F}$ es llamado el *orden* de $\mathbb{F}$. Denotaremos un campo con q elementos por $\mathbb{F}_q$.

Se sabe que todos los campos finitos con el mismo número de elementos son isomorfos [40, Teorema 2.5, p. 49]. Sea $\mathbb{F}_q$ un campo finito con q elementos. La siguiente es una lista de propiedades básicas de $\mathbb{F}_q$ (ver [40, Capítulos 1 y 2]):

- $q = p^t$ para algún número primo p y algún entero positivo t; p es llamado la *característica* de $\mathbb{F}_q$.

- $\mathbb{F}_q$ contiene a $\mathbb{F}_p$ como subcampo.
- $\mathbb{F}_q$ es un espacio vectorial sobre $\mathbb{F}_p$ de dimensión t.
- Cada subcampo de $\mathbb{F}_q$ tiene orden p^r para algún entero r divisor de t.
- El grupo multiplicativo de elementos distintos de cero en $\mathbb{F}_q$, $\mathbb{F}_q^*$, es cíclico. Si $\gamma \in \mathbb{F}_q^*$ es un generador de $\mathbb{F}_q^*$, entonces γ es llamado *elemento primitivo* de $\mathbb{F}_q$. Bajo estas condiciones escribiremos $\mathbb{F}_q^* = \langle \gamma \rangle$.

Sea $m \geq 2$ un entero, $\mathbb{F}_{q^m}$ una extensión finita de grado m de $\mathbb{F}_q$ y $a \in \mathbb{F}_{q^m}$. Es una propiedad básica que $a^{q^m} = a$ [40, Lema 2.3, p. 48]. El polinomio mónico $f(x) \in \mathbb{F}_q[x]$ de grado menor tal que $f(a) = 0$ es llamado el *polinomio mínimo* de a sobre $\mathbb{F}_q$ y lo denotaremos por $M_a(x)$. Como $a^{q^m} - a = 0$, claramente $M_a(x)$ es un divisor de $x^{q^m} - x$. Más aún, $M_a(x)$ es único e irreducible sobre $\mathbb{F}_q$ (ver [45, Capítulo 4, p. 99]).

1.1.1 Las funciones traza y norma

A continuación se presentan dos funciones importantes que van del campo finito $\mathbb{F}_{q^m}$ al subcampo finito $\mathbb{F}_q$ (ver [45, Capítulo 2, Sección 3, p. 54]).

Sea $a \in \mathbb{F}_{q^m}$. La *traza* de a sobre $\mathbb{F}_q$, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a)$, se define como

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) := a + a^q + \cdots + a^{q^{m-1}} \in \mathbb{F}_q \ ,$$

y cumple con las siguientes propiedades [40, Teoremas 2.23 y 2.26, pp. 55-56]:

(i) $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a+b) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b)$ para todo $a, b \in \mathbb{F}_{q^m}$.

(ii) $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(ca) = c\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a)$ para todo $c \in \mathbb{F}_q, a \in \mathbb{F}_{q^m}$.

(iii) $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_p}(a) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a))$ para todo $a \in \mathbb{F}_{q^m}$.

Las propiedades (i) y (ii) implican que la traza es una transformación lineal, mientras que la propiedad (iii) implica que es transitiva. La traza juega un papel fundamental en el estudio de códigos lineales sobre campos finitos ya que estos códigos pueden ser representados a través de dicha función lo cual permite el uso de distintas herramientas matemáticas, como son las sumas exponenciales, para su análisis.

La *norma* de a sobre $\mathbb{F}_q$, $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a)$, se define como

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) := a \cdot a^q \cdot \ldots \cdot a^{q^{m-1}} = a^{\frac{q^m-1}{q-1}} \in \mathbb{F}_q \ .$$

Además, se cumple que [40, Teorema 2.28, p. 57]:

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(ab) = \mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a)\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b) \text{ para todo } a, b \in \mathbb{F}_{q^m} \ ,$$

es decir, la norma es multiplicativa.

1.2 Códigos lineales sobre campos finitos

Existen distintos tipos de códigos, de entre ellos, uno de los más importantes son los códigos lineales. Estos códigos ofrecen varias ventajas sobre otro tipo de códigos, como son: su facilidad de descripción, tienen muy buenas propiedades y son fáciles de codificar y decodificar. De hecho, la mayoría de los códigos importantes que encontramos en la literatura son lineales.

Sea $\mathbb{F}_q^n$ el espacio vectorial compuesto por los vectores de longitud n con entradas en $\mathbb{F}_q$. Un $[n,k]$ *código lineal*, $\mathcal{C}$, sobre $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k; n y k son llamadas la longitud y la dimensión del código $\mathcal{C}$, respectivamente. En este contexto, los vectores de $\mathcal{C}$ son llamados *palabras de código*. El código lineal $\mathcal{C}$ tiene q^k palabras de código. Indexamos las coordenadas de las palabras de código en $\mathcal{C}$ con los elementos del conjunto $\{0,1,\ldots,n-1\}$. Para una palabra de código $\mathbf{c} \in \mathcal{C}$ se define su *peso de Hamming* como el número de coordenadas distintas de cero en $\mathbf{c}$ y lo denotaremos por $w_H(\mathbf{c})$. La *distancia mínima* d de un código lineal $\mathcal{C}$ está dada por $d = \min\{w_H(\mathbf{c}) : \mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}\}$ [45, Teorema 1, p. 10], donde $\mathbf{0}$ es la palabra de código cuyas coordenadas son todas iguales a cero. Un código lineal $\mathcal{C}$ de longitud n, dimensión k y distancia mínima d es llamado un $[n,k,d]$ código.

Los parámetros $[n,k,d]$ de un código lineal $\mathcal{C}$ son esenciales ya que la razón k/n determina la *eficiencia de transmisión* (ver [45, p. 6]) y d es utilizada para determinar las capacidades de detección y corrección de errores de $\mathcal{C}$ [45, Teorema 2, p. 10]. Es precisamente por esta última razón que al construir un código lineal es deseable que su distancia mínima sea lo más grande posible. Un $[n,k,d]$ código lineal, $\mathcal{C}$, sobre $\mathbb{F}_q$ es llamado *óptimo* si no existe un $[n,k,d']$ código sobre $\mathbb{F}_q$ con $d' > d$, o si sus parámetros alcanzan la igualdad en alguna cota para códigos lineales. Por otro lado, $\mathcal{C}$ es llamado *casi óptimo* si existe un $[n,k,d+1]$ código óptimo sobre $\mathbb{F}_q$, o bien, si $[n,k,d+1]$ alcanza la igualdad en alguna cota para códigos lineales. Más aún, un código lineal con parámetros $[n,k,n-k+1]$ es llamado *distancia máxima separable* (maximum distance separable o MDS) (ver [45, Capítulo 11, p. 317]), mientras que un código lineal con parámetros $[n,k,n-k]$ es llamado *cuasidistancia máxima separable* (almost maximum distance separable o AMDS).

Las dos formas más comunes de describir un código lineal son a través de una matriz generadora o una matriz de chequeo de paridad. Una *matriz generadora* para un $[n,k]$ código lineal $\mathcal{C}$ sobre $\mathbb{F}_q$ es una matriz G de tamaño $k \times n$ cuyas filas forman una base para $\mathcal{C}$ sobre $\mathbb{F}_q$. Por otro lado, como un código lineal es un subespacio de un espacio vectorial, éste es el núcleo de alguna transformación lineal. En particular, existe una matriz H de tamaño $(n-k) \times n$, llamada *matriz de chequeo de paridad* de $\mathcal{C}$, definida de la siguiente manera

$$\mathcal{C} = \{x \in \mathbb{F}_q^n : Hx^T = \mathbf{0}\} ,$$

donde x^T denota el vector transpuesto de x. Note que las matrices generadora y de chequeo de paridad de un código lineal no son únicas.

Ejemplo 1. Sea $\mathcal{C}$ el código lineal de longitud 4 y dimensión 2 definido sobre el campo finito con tres elementos, $\mathbb{F}_3 = \{0,1,2\}$, dado por el conjunto

$$\begin{aligned}\mathcal{C} \;:= \big\{&(0,0,0,0),(0,1,2,1),(0,2,1,2),(1,1,1,0),(1,2,0,1),\\ &(1,0,2,2),(2,2,2,0),(2,0,1,1),(2,1,0,2)\big\} \subsetneq \mathbb{F}_3^4 .\end{aligned}$$

Entonces, note que las matrices

$$G = \begin{bmatrix} 1\,0\,2\,2 \\ 0\,1\,2\,1 \end{bmatrix} \quad \text{y} \quad H = \begin{bmatrix} 1\,1\,1\,0 \\ 1\,2\,0\,1 \end{bmatrix}$$

son matrices generadora y de chequeo de paridad, respectivamente, para el código lineal $\mathcal{C}$.

1.2.1 Las distribuciones de pesos de Hamming y completa

Un problema matemático de interés, pero a la vez difícil, es utilizar la riqueza algebraica que poseen los códigos lineales para determinar su distribución de pesos de Hamming (ver por ejemplo [15,24,25,27,29,31,32,36,44,51,53,58–60,72]). Dicho problema consiste en clasificar todas las palabras de código de acuerdo a su peso de Hamming. Formalmente hablando, sea $\mathcal{C}$ un código lineal de longitud n y sea $A_j(\mathcal{C})$, con $0 \leq j \leq n$, el número de palabras de código con peso de Hamming j en $\mathcal{C}$. El *enumerador de pesos de Hamming* (o simplemente *enumerador de pesos*) de $\mathcal{C}$ se define como el polinomio

$$1 + A_1(\mathcal{C})z + A_2(\mathcal{C})z^2 + \cdots + A_n(\mathcal{C})z^n \,,$$

mientras que la secuencia $A_0(\mathcal{C}) = 1, A_1(\mathcal{C}), \ldots, A_n(\mathcal{C})$ es llamada su *distribución de pesos de Hamming* (o simplemente *distribución de pesos*). Note que el valor más pequeño de $0 < d \leq n$ para el cual $A_d(\mathcal{C}) \neq 0$ corresponde a la distancia mínima d del código lineal $\mathcal{C}$. Diremos que el código $\mathcal{C}$ es de N *pesos* si la cardinalidad del conjunto de sus pesos distintos de cero es N, es decir, $N = \sharp\{j : A_j(\mathcal{C}) \neq 0, 0 < j \leq n\}$.

Ejemplo 2. El enumerador de pesos del código $\mathcal{C}$ en el Ejemplo 1 es el polinomio $1 + 8z^3$, mientras que su distribución de pesos está dada por $A_0(\mathcal{C}) = 1, A_3(\mathcal{C}) = 8$. Note que $\mathcal{C}$ es un código lineal de un solo peso con distancia mínima 3.

Un problema aún más difícil, para códigos no binarios, es calcular su distribución de pesos completa (ver por ejemplo [2,11,37,39,65–68,71]). Esto consiste en clasificar todas las palabras de código de acuerdo al número de símbolos de cada tipo contenidos en cada palabra de código. Sea $\mathcal{C}$ un código de longitud n sobre $\mathbb{F}_q$. Denotemos a los elementos de $\mathbb{F}_q$ por $u_0 = 0, u_1, \ldots, u_{q-1}$ en algún orden fijo. Para cada palabra de código $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ sea $\mathcal{Z}(\mathbf{c})$ el monomio en q variables $(z_0, z_1, \ldots, z_{q-1})$ dado por

$$\mathcal{Z}(\mathbf{c}) := z_0^{w_0} z_1^{w_1} \cdots z_{q-1}^{w_{q-1}} \,,$$

donde la potencia w_ℓ $(0 \leq \ell < q)$ es el número de componentes c_j $(0 \leq j < n)$ de $\mathbf{c}$ que son iguales a u_ℓ. Denotemos por $V(n,q)$ el conjunto de todos los vectores enteros $\mathbf{t} = (t_0, t_1, \ldots, t_{q-1})$ tales que $t_i \geq 0$ y $\sum_{i=0}^{q-1} t_i = n$. Entonces, el *enumerador de pesos completo* de $\mathcal{C}$ (ver por ejemplo [44] y [45, p. 141]) es el polinomio

$$\mathrm{CWE}_{\mathcal{C}} := \sum_{\mathbf{c}\in\mathcal{C}} \mathcal{Z}(\mathbf{c}) = \sum_{\mathbf{t}\in V(n,q)} A_{\mathbf{t}}(\mathcal{C}) Z^{\mathbf{t}} \,, \tag{1.1}$$

donde $Z^{\mathbf{t}} = z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}}$ y

$$A_{\mathbf{t}}(\mathcal{C}) := \sharp\left\{\mathbf{c} \in \mathcal{C} : \mathcal{Z}(\mathbf{c}) = Z^{\mathbf{t}}\right\} \,.$$

La secuencia $(A_{\mathbf{t}}(\mathcal{C}))_{\mathbf{t}\in V(n,q)}$ es llamada la *distribución de pesos completa* de $\mathcal{C}$. Observe que la distribución de pesos completa coincide con la distribución de pesos de Hamming si $q = 2$ y contiene mucha más información si $q > 2$.

Ejemplo 3. El enumerador de pesos completo del código $\mathcal{C}$ en el Ejemplo 1 es el polinomio

$$z_0^4 + z_0 z_1^3 + 3z_0 z_1^2 z_2 + 3z_0 z_1 z_2^2 + z_0 z_2^3 \ ,$$

mientras que la secuencia $A_{(4,0,0)}(\mathcal{C}) = 1, A_{(1,3,0)}(\mathcal{C}) = 1, A_{(1,2,1)}(\mathcal{C}) = 3, A_{(1,1,2)}(\mathcal{C}) = 3, A_{(1,0,3)}(\mathcal{C}) = 1$, es su distribución de pesos completa.

1.2.2 Las identidades de Pless

Sea $\mathcal{C}$ un código lineal de longitud n sobre $\mathbb{F}_q$. El *código dual* $\mathcal{C}^\perp$ de $\mathcal{C}$ es el código lineal definido como

$$\mathcal{C}^\perp := \left\{ \mathbf{v} \in \mathbb{F}_q^n : \langle \mathbf{v}, \mathbf{c} \rangle = 0, \text{ para todo } \mathbf{c} \in \mathcal{C} \right\} \ ,$$

donde $\langle \cdot, \cdot \rangle$ denota el producto escalar usual en el espacio vectorial $\mathbb{F}_q^n$. Se sabe que si $\mathcal{C}$ es un $[n, k]$ código lineal, entonces $\mathcal{C}^\perp$ es un $[n, n-k]$ código lineal (ver [34, Sección 1.3, p. 5]). Más aún, se dice que el código lineal $\mathcal{C}$ es *proyectivo* si la distancia mínima de $\mathcal{C}^\perp$ es al menos 3. Ahora bien, sea $(A_j(\mathcal{C}^\perp))_{j=0}^n$ la distribución de pesos de $\mathcal{C}^\perp$, entonces las primeras cinco identidades de Pless (ver [34, pp. 259-260]) para $\mathcal{C}$ son:

$$\begin{aligned}
\sum_{j=0}^{n} A_j(\mathcal{C}) &= q^k \ , \\
\sum_{j=0}^{n} j A_j(\mathcal{C}) &= q^{k-1}(qn - n - A_1(\mathcal{C}^\perp)) \ , \\
\sum_{j=0}^{n} j^2 A_j(\mathcal{C}) &= q^{k-2}[(q-1)n(qn-n+1) - (2qn - q - 2n + 2)A_1(\mathcal{C}^\perp) \\
&\quad + 2A_2(\mathcal{C}^\perp)] \ , \\
\sum_{j=0}^{n} j^3 A_j(\mathcal{C}) &= q^{k-3}[(q-1)n(q^2n^2 - 2qn^2 + 3qn - q + n^2 - 3n + 2) - (3q^2n^2 \\
&\quad - 3q^2 n - 6qn^2 + 12qn + q^2 - 6q + 3n^2 - 9n + 6)A_1(\mathcal{C}^\perp) \\
&\quad + 6(qn - q - n + 2)A_2(\mathcal{C}^\perp) - 6A_3(\mathcal{C}^\perp)] \ , \\
\sum_{j=0}^{n} j^4 A_j(\mathcal{C}) &= q^{k-4}[(q-1)n(q^3n^3 - 3q^2n^3 + 6q^2n^2 - 4q^2n + q^2 + 3qn^3 \\
&\quad - 12qn^2 + 15qn - 6q - n^3 + 6n^2 - 11n + 6) - (4q^3n^3 - 6q^3n^2 \\
&\quad + 4q^3n - q^3 - 12q^2n^3 + 36q^2n^2 - 38q^2n + 14q^2 + 12qn^3 \\
&\quad - 54qn^2 + 78qn - 36q - 4n^3 + 24n^2 - 44n + 24)A_1(\mathcal{C}^\perp) \\
&\quad + (12q^2n^2 - 24q^2n + 14q^2 - 24qn^2 + 84qn - 72q + 12n^2 \\
&\quad - 60n + 72)A_2(\mathcal{C}^\perp) - (24qn - 36q - 24n + 72)A_3(\mathcal{C}^\perp) \\
&\quad + 24A_4(\mathcal{C}^\perp)] \ .
\end{aligned}$$

Las identidades de Pless relacionan la distribución de pesos de un código lineal con la de su código dual. En el presente trabajo utilizamos dichas identidades para determinar la distancia mínima del código dual de un código dado.

1.2.3 Cotas asociadas a un código lineal

Al construir un $[n, k, d]$ código lineal sobre $\mathbb{F}_q$ es deseable determinar la longitud n mínima fijando valores de k, d y q. Una cota inferior para la longitud n en términos de estos valores es la siguiente [34, Teorema 2.7.4, p. 81]:

Teorema 1 (Cota de Griesmer). *Sea $\mathcal{C}$ un $[n, k, d]$ código lineal sobre $\mathbb{F}_q$. Entonces,*

$$n \geq \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil ,$$

donde $\lceil x \rceil$ denota el menor entero mayor o igual a x.

Otra cota bien conocida para códigos lineales es [45, Teorema 6, p. 19]:

Teorema 2 (Cota de Hamming). *Un $[n, k, d]$ código lineal sobre $\mathbb{F}_q$ debe satisfacer*

$$q^k \left(\sum_{j=0}^{\lfloor \frac{d-1}{2} \rfloor} (q-1)^j \binom{n}{j} \right) \leq q^n ,$$

donde $\lfloor x \rfloor$ denota el mayor entero menor o igual a x.

La cota de Hamming resulta útil, por ejemplo, para saber si un código con ciertos parámetros existe. En el presente trabajo utilizamos dicha cota para determinar el valor máximo que la distancia mínima de un código q-ario puede tomar dadas su longitud y dimensión.

1.3 Construcción de nuevos códigos a partir de códigos conocidos

Existen distintas técnicas para construir nuevos códigos lineales a partir de códigos conocidos (ver [34, Sección 1.5, p. 13]). De hecho, muchos de los códigos interesantes e importantes que hay en la literatura surgen al modificar códigos existentes. En esta sección discutiremos algunas formas de llevar esto a cabo.

1.3.1 Códigos de subcampo

Sea $q_0 = p^t$, donde t es un entero positivo y p un número primo. Para un entero $r > 1$, sea $q = q_0^r = p^{tr}$. Note que, bajo estas condiciones, $\mathbb{F}_{q_0}$ es un subcampo propio de $\mathbb{F}_q$. Sea $\mathcal{C}$ un $[n, k]$ código lineal sobre $\mathbb{F}_q$. A continuación se describe una forma de construir un nuevo $[n, k']$ código lineal, $\mathcal{C}^{(q_0)}$, sobre $\mathbb{F}_{q_0}$ (ver [15]). Sea G una matriz generadora de $\mathcal{C}$. Tome una base de $\mathbb{F}_q = \mathbb{F}_{q_0}^r$ sobre $\mathbb{F}_{q_0}$ y represente cada entrada de G como un vector columna de tamaño $r \times 1$ de $\mathbb{F}_{q_0}^r$ con respecto a esa base. Reemplace cada entrada de G con el vector columna correspondiente de

$\mathbb{F}_{q_0}^r$. Con este método, G se modifica en una matriz de tamaño $kr \times n$ sobre $\mathbb{F}_{q_0}$ generando un nuevo código lineal, $\mathcal{C}^{(q_0)}$, sobre $\mathbb{F}_{q_0}$ de longitud n, llamado *código de subcampo*. Se sabe que el código de subcampo $\mathcal{C}^{(q_0)}$ es independiente tanto de la elección de la base de $\mathbb{F}_q$ sobre $\mathbb{F}_{q_0}$ como de la elección de la matriz generadora G de $\mathcal{C}$ (ver [15, Teoremas 2.1 y 2.6]). También, debe ser claro que la dimensión k' de $\mathcal{C}^{(q_0)}$ satisface $k' \leq kr$.

Observación 1. Es importante recordar que el *subcódigo de subcampo* de un código lineal $\mathcal{C}$ sobre $\mathbb{F}_q$ es el subconjunto de palabras de código en $\mathcal{C}$ cuyas coordenadas están todas en $\mathbb{F}_{q_0}$ (ver [34, p. 116]). En consecuencia, observe que un código de subcampo y un subcódigo de subcampo son códigos distintos en general. Además, note que los códigos de subcampo definidos aquí también son diferentes de los códigos de subcampo definidos en la [53, Sección 4.1] como códigos cíclicos irreducibles de un solo peso (ver [53, Proposición 4.1]).

El siguiente es un resultado útil que nos permitirá representar el código de subcampo q_0-ario, $\mathcal{C}^{(q_0)}$, de un código lineal q-ario, $\mathcal{C}$, en términos de la traza.

Lema 1 ([15, Teorema 2.5])**.** *Sea $\mathcal{C}$ un $[n,k]$ código lineal sobre $\mathbb{F}_q$. Sea $G = [g_{ij}]_{1\leq i\leq k, 1\leq j\leq n}$ una matriz generadora de $\mathcal{C}$. Entonces, la representación del código de subcampo $\mathcal{C}^{(q_0)}$ en términos de la traza está dada por*

$$\mathcal{C}^{(q_0)} := \left\{ \left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\sum_{i=1}^{k} a_i g_{i1} \right), \ldots, \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\sum_{i=1}^{k} a_i g_{in} \right) \right) : a_1, \ldots, a_k \in \mathbb{F}_q \right\}.$$

Observe que, de acuerdo con lema anterior, para determinar el código de subcampo $\mathcal{C}^{(q_0)}$ del código lineal $\mathcal{C}$ basta con tomar todas las palabras de código en $\mathcal{C}$ y aplicar la traza de $\mathbb{F}_q$ a $\mathbb{F}_{q_0}$, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}$, a cada coordenada.

1.3.2 Códigos extendidos

Dado un código lineal, es posible extenderlo agregando a cada palabra de código una coordenada extra de tal forma que al sumar todas sus coordenadas obtengamos como resultado cero. Sea $\mathcal{C}$ un $[n,k,d]$ código lineal sobre $\mathbb{F}_q$. El *código extendido*, $\widehat{\mathcal{C}}$, de $\mathcal{C}$ es el código lineal definido como

$$\widehat{\mathcal{C}} := \left\{ (c_0, \ldots, c_n) \in \mathbb{F}_q^{n+1} : (c_0, \ldots, c_{n-1}) \in \mathcal{C} \text{ con } c_0 + \cdots + c_{n-1} + c_n = 0 \right\}.$$

Se sabe que $\widehat{\mathcal{C}}$ es un $[n+1, k, \widehat{d}]$ código lineal, donde $\widehat{d} = d$ o $d+1$ (ver [34, Sección 1.5.2, p. 14]).

1.3.3 Códigos perforados y recortados

Sea $\mathcal{C}$ un código lineal de longitud n sobre $\mathbb{F}_q$ e i un entero tal que $0 \leq i \leq n-1$. Se dice que *perforamos* el código $\mathcal{C}$ si eliminamos la i-ésima coordenada de todas sus palabras de código. El código resultante es lineal, de longitud $n-1$ y se denota por $\mathcal{C}^i$ (ver [34, Sección 1.5.1, p. 13]). Por otro lado, *recortamos* el código $\mathcal{C}$ si seleccionamos solo aquellas palabras de código que tengan un cero en su i-ésima

coordenada y eliminamos dicha coordenada de estas palabras de código. El código resultante es lineal, de longitud $n-1$ y se denota por $\mathcal{C}_i$ (ver [34, Sección 1.5.3, p. 16]).

Observación 2. Sean $\mathcal{C}$, $\mathcal{C}^i$ y $\mathcal{C}_i$ como antes. Entonces, dado que $(\mathcal{C}^\perp)^i = (\mathcal{C}_i)^\perp$ (ver [34, Teorema 1.5.7 (i), p. 17]) y $(\mathcal{C}^\perp)^\perp = \mathcal{C}$, tenemos que $((\mathcal{C}^\perp)^i)^\perp = \mathcal{C}_i$.

Los parámetros de un código perforado se pueden obtener a través del siguiente:

Teorema 3 ([34, Teorema 1.5.1, p. 13])**.** *Sea $\mathcal{C}$ un $[n,k,d]$ código lineal sobre $\mathbb{F}_q$ e i un entero tal que $0 \leq i \leq n-1$. Sea $\mathcal{C}^i$ el código perforado de $\mathcal{C}$ cuya i-ésima coordenada es eliminada. Si $d > 1$, entonces $\mathcal{C}^i$ es un $[n-1,k,d^*]$ código lineal, donde $d^* = d-1$ si $\mathcal{C}$ tiene una palabra de código de peso mínimo con su i-ésima coordenada distinta de cero y $d^* = d$ en caso contrario.*

Observación 3. Del teorema anterior es importante resaltar que la dimensión k, para los dos códigos lineales $\mathcal{C}$ y $\mathcal{C}^i$, permanece sin cambios.

Cuando se cumplen ciertas condiciones de uniformidad, la distribución de pesos de un código perforado o recortado se puede determinar a partir de la distribución de pesos del código original. Para recordar este hecho, sea $\mathcal{C}$ un $[n,k]$ código lineal sobre $\mathbb{F}_q$ y sea $\mathcal{M}$ la matriz de tamaño $q^k \times n$ cuyas filas son todas las palabras de código en $\mathcal{C}$. Sea $\mathcal{M}_j$ la submatriz de $\mathcal{M}$ compuesta por las palabras de código con peso de Hamming j. Se dice que el código $\mathcal{C}$ es *homogéneo* si para todo $0 \leq j \leq n$, cada columna de $\mathcal{M}_j$ tiene el mismo peso (ver [34, Sección 7.6, p. 271]). Prange demostró el siguiente resultado sobre códigos homogéneos [34, Teorema 7.6.1, p. 271]:

Teorema 4 (Prange)**.** *Sea $\mathcal{C}$ un $[n,k,d]$ código lineal homogéneo sobre $\mathbb{F}_q$, con $d > 1$, e i un entero tal que $0 \leq i \leq n-1$. Sean $\mathcal{C}^i$ y $\mathcal{C}_i$ los códigos lineales obtenidos a partir del código $\mathcal{C}$ al perforar y recortar en la i-ésima coordenada, respectivamente. Entonces, para cada $0 \leq j \leq n-1$ se tiene que:*

$$A_j(\mathcal{C}^i) = \frac{n-j}{n}A_j(\mathcal{C}) + \frac{j+1}{n}A_{j+1}(\mathcal{C}), \quad y \quad A_j(\mathcal{C}_i) = \frac{n-j}{n}A_j(\mathcal{C})\,.$$

1.4 Códigos cíclicos sobre campos finitos

Un código lineal $\mathcal{C}$ de longitud n es llamado *cíclico* si $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implica $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. Una subclase importante de los códigos lineales es la de los códigos cíclicos. Los códigos cíclicos son utilizados ampliamente en la electrónica de consumo, las comunicaciones digitales, la criptografía, los sistemas de almacenamiento de datos, entre otros; ya que poseen una rica estructura algebraica y sus algoritmos de codificación y decodificación se pueden implementar de manera eficiente empleando registros de corrimiento con retroalimentación lineal (ver [45, Capítulo 7, Sección 8, p. 209]). En esta sección introducimos, de manera muy breve, algunos resultados básicos acerca de los códigos cíclicos.

1.4.1 Factorización de $x^n - 1$ sobre $\mathbb{F}_q$

Para tratar con códigos cíclicos de longitud n sobre $\mathbb{F}_q$ es necesario estudiar la factorización de $x^n - 1$ en producto de polinomios mínimos sobre $\mathbb{F}_q$ (ver [45, Cap. 7, Sec. 5, p. 196] y [34, Sec. 4.1, p. 122]). Con ese fin, a continuación vamos a introducir las clases q-ciclotómicas módulo n.

Observación 4. Note que $x^n - 1$ no tiene factores repetidos sobre $\mathbb{F}_q$ si y solo si (sii) $\gcd(n, q) = 1$ (ver [34, Ejercicio 201 (f), p. 122]). Así pues, a lo largo de este trabajo vamos a asumir que $\gcd(n, q) = 1$.

Sea $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ el anillo de enteros módulo n. Para cualquier $s \in \mathbb{Z}_n$, la *clase q-ciclotómica de s módulo n* se define como

$$C_s := \left\{s, sq, sq^2, \ldots, sq^{\ell_s - 1}\right\} \pmod{n} \subseteq \mathbb{Z}_n \ ,$$

donde ℓ_s es el menor entero positivo tal que $s \equiv sq^{\ell_s} \pmod{n}$ y también $\ell_s = \sharp C_s$. El menor entero en C_s es llamado el representante de la clase. Sea $\Omega_{(n,q)}$ el conjunto de todos los representantes de las clases q-ciclotómicas módulo n. Se tiene entonces que $C_s \cap C_t = \emptyset$ para cualesquiera dos elementos distintos $s, t \in \Omega_{(n,q)}$. Además

$$\bigcup_{s \in \Omega_{(n,q)}} C_s = \mathbb{Z}_n \ . \tag{1.2}$$

Por tanto, las distintas clases q-ciclotómicas módulo n forman una partición de $\mathbb{Z}_n$.

Sea m el menor entero tal que n divide a $q^m - 1$, es decir, m es el *orden multiplicativo de q módulo n*. Así pues los ceros de $x^n - 1$, los cuales son llamados las n-ésimas raíces de la unidad, se encuentran en la extensión finita $\mathbb{F}_{q^m}$ y en ningún campo más pequeño. Al campo $\mathbb{F}_{q^m}$ se le conoce como el *campo de descomposición* de $x^n - 1$. Sea γ un generador de $\mathbb{F}_{q^m}^*$ y $\beta = \gamma^{(q^m-1)/n}$. Entonces, note que β es una n-ésima raíz primitiva de la unidad en $\mathbb{F}_{q^m}$, es decir, $\beta^n = \gamma^{q^m-1} = 1$ y β es un generador del subgrupo cíclico, $\langle\beta\rangle$, de $\mathbb{F}_{q^m}^*$ de orden[1] n. Sea s como antes y sea $M_{\beta^s}(x)$ el polinomio mínimo de β^s sobre $\mathbb{F}_q$ (ver Sección 1.1). Entonces

$$M_{\beta^s}(x) = \prod_{i \in C_s} (x - \beta^i) \in \mathbb{F}_q[x] \ .$$

Por lo tanto, se sigue de (1.2) que

$$x^n - 1 = \prod_{s \in \Omega_{(n,q)}} M_{\beta^s}(x) \ ,$$

que es la factorización de $x^n - 1$ en producto de polinomios mínimos sobre $\mathbb{F}_q$.

Ejemplo 4. Sea $q = 3$ y $n = 10$. Note que el orden multiplicativo de 3 módulo 10 es 4 y, por tanto, $\mathbb{F}_{3^4}$ es el campo de descomposición para $x^{10} - 1 \in \mathbb{F}_3[x]$. Ahora bien, no es difícil verificar que $\Omega_{(10,3)} = \{0, 1, 2, 5\}$ y

$$C_0 = \{0\},\ C_1 = \{1, 3, 7, 9\},\ C_2 = \{2, 4, 6, 8\},\ C_5 = \{5\} \ .$$

Sea $\mathbb{F}_{3^4} = \mathbb{F}_3(\gamma)$, con $\gamma^4 + \gamma + 1 = 0$. Entonces, $\beta = \gamma^{80/10} = \gamma^8$ y

$$x^{10} - 1 = M_{\beta^0}(x) M_{\beta^1}(x) M_{\beta^2}(x) M_{\beta^5}(x) \ ,$$

donde

$$\begin{aligned}
M_{\beta^0}(x) &= (x - \beta^0) = x + 2 \ , \\
M_{\beta^1}(x) &= (x - \beta^1)(x - \beta^3)(x - \beta^7)(x - \beta^9) = x^4 + 2x^3 + x^2 + 2x + 1 \ , \\
M_{\beta^2}(x) &= (x - \beta^2)(x - \beta^4)(x - \beta^6)(x - \beta^8) = x^4 + x^3 + x^2 + x + 1 \ , \\
M_{\beta^5}(x) &= (x - \beta^5) = x + 1 \ .
\end{aligned}$$

[1] El número de elementos en un grupo finito es llamado el orden del grupo.

1.4.2 Los polinomios generador y de chequeo de paridad

Sea $\langle x^n-1\rangle$ el ideal generado por $x^n-1\in\mathbb{F}_q[x]$. Entonces, todos los elementos de $\mathbb{F}_q[x]/\langle x^n-1\rangle$ pueden ser representados a través de polinomios de grado a lo más $n-1$. Claramente, este anillo de clases residuales es isomorfo al espacio vectorial $\mathbb{F}_q^n$. De hecho, tal isomorfismo está dado por

$$c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in\mathbb{F}_q[x]/\langle x^n-1\rangle\longleftrightarrow(c_0,c_1,\ldots,c_{n-1})\in\mathbb{F}_q^n\ .$$

De lo anterior se sigue que cualquier código lineal $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ corresponde a un subconjunto de $\mathbb{F}_q[x]/\langle x^n-1\rangle$. Más aún, el código lineal $\mathcal{C}$ es cíclico sii el subconjunto correspondiente es un ideal de $\mathbb{F}_q[x]/\langle x^n-1\rangle$ [40, Teorema 9.36, p. 484].

Ahora bien, como $\gcd(n,q)=1$, note que cada ideal de $\mathbb{F}_q[x]/\langle x^n-1\rangle$ es principal. En consecuencia, si $\mathcal{C}$ es un código cíclico de longitud n sobre $\mathbb{F}_q$, entonces existe un único polinomio mónico $g(x)\in\mathbb{F}_q[x]$ de menor grado tal que $\mathcal{C}=\langle g(x)\rangle$. Dicho polinomio $g(x)$ es un divisor de x^n-1 y es llamado el *polinomio generador* de $\mathcal{C}$ (ver [45, Capítulo 7, Sección 3, p. 190]).

Observación 5. Note que podemos encontrar todos los códigos cíclicos de longitud n sobre $\mathbb{F}_q$ factorizando a x^n-1 en producto de polinomios mínimos sobre $\mathbb{F}_q$ y tomando cualquiera de los $2^\ell-2$ factores mónicos no triviales de x^n-1 como polinomio generador, donde ℓ es el número total de clases q-ciclotómicas módulo n distintas, es decir, $\ell=\sharp\Omega_{(n,q)}$.

Sea $\mathcal{C}=\langle g(x)\rangle$ un $[n,k]$ código cíclico sobre $\mathbb{F}_q$. Entonces, se tiene que $k=n-\deg(g(x))$ y $\{g(x),xg(x),\ldots,x^{k-1}g(x)\}$ es una base para $\mathcal{C}$ (ver [34, Teorema 4.2.1, p. 125]). Sea $g(x)=\sum_{j=0}^{n-k}g_jx^j$, donde $g_{n-k}=1$. Por lo tanto, la siguiente es una matriz generadora para $\mathcal{C}$:

$$G=\begin{bmatrix}g_0&g_1&\ldots&g_{n-k}&&0&0&\ldots&0\\0&g_0&g_1&\ldots&&g_{n-k}&0&\ldots&0\\\vdots&\vdots&\vdots&&&&&&\vdots\\0&0&0&\ldots&0&g_0&g_1&\ldots&g_{n-k}\end{bmatrix}\ .$$

Por otro lado, el polinomio $h(x)=(x^n-1)/g(x)=\sum_{j=0}^{k}h_jx^j$ es llamado el *polinomio de chequeo de paridad* de $\mathcal{C}$. Además, la matriz

$$H=\begin{bmatrix}0&0&\ldots&&0&h_k&h_{k-1}&\ldots&&h_0\\0&0&\ldots&0&h_k&h_{k-1}&&\ldots&h_0&0\\\vdots&\vdots&&&&&&&&\vdots\\h_k&h_{k-1}&\ldots&&h_0&0&&\ldots&&0\end{bmatrix}$$

es una matriz de chequeo de paridad para $\mathcal{C}$. Más aún, el código con matriz generadora H es el código dual de $\mathcal{C}$, que nuevamente es cíclico (ver [45, Capítulo 7, Sección 4, p. 194]). Si $h(x)$ es irreducible (reducible) sobre $\mathbb{F}_q$, entonces el código cíclico $\mathcal{C}$ es llamado *irreducible* (*reducible*).

1.5 Sumas exponenciales

Las sumas exponenciales son una herramienta importante en teoría de números para resolver problemas que involucran números enteros, y números reales en general, que a menudo son intratables por otros métodos (ver [40, Capítulo 5, p. 186]). Sumas análogas pueden ser consideradas en el contexto de campos finitos resultando ser de gran utilidad, como es el caso del presente trabajo donde mediante la evaluación de ciertas sumas exponenciales determinamos las distribuciones de pesos de Hamming y completa de algunos códigos cíclicos.

Un rol básico en las sumas exponenciales para campos finitos es jugado por un grupo especial de homomorfismos conocidos como caracteres. Un *caracter* de un grupo G es una función que va de G al grupo multiplicativo de números complejos de valor absoluto 1 y que además preserva las operaciones definidas en dichos grupos. Se distinguen dos tipos de caracteres, aditivos y multiplicativos, dependiendo de si se hace referencia al grupo aditivo o multiplicativo del campo finito. Las sumas exponenciales se forman utilizando los valores de uno o más caracteres y posiblemente combinándolos con otras funciones. Si solo sumamos los valores de un solo caracter, hablamos de una suma de caracteres.

1.5.1 Caracteres

El *caracter aditivo canónico*, $\chi : \mathbb{F}_q \longrightarrow \mathbb{C}^*$, de $\mathbb{F}_q$ se define como

$$\chi(c) := e^{2\pi\sqrt{-1}\,\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c)/p} \qquad \text{para todo } c \in \mathbb{F}_q \ ,$$

donde $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ denota la traza de $\mathbb{F}_q$ a $\mathbb{F}_p$. Sea $a \in \mathbb{F}_q$, entonces la relación de ortogonalidad para χ está dada por (ver [40, p. 192])

$$\sum_{c\in\mathbb{F}_q} \chi(ac) = \begin{cases} q & \text{si } a = 0, \\ \\ 0 & \text{en caso contrario.} \end{cases} \tag{1.3}$$

Esta propiedad juega un papel importante en varias aplicaciones de campos finitos. Entre ellas, esta propiedad resulta útil para determinar el número de entradas iguales a cero en un vector dado. Por ejemplo, si $\mathbf{v} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ y $Z(\mathbf{v})$ representa el número de entradas iguales a cero en el vector $\mathbf{v}$, entonces

$$Z(\mathbf{v}) = \frac{1}{q}\sum_{i=0}^{n-1}\sum_{y\in\mathbb{F}_q} \chi(ya_i) \ . \tag{1.4}$$

Como consecuencia inmediata de lo anterior se tiene que el peso de Hamming del vector $\mathbf{v}$ está dado por

$$w_H(\mathbf{v}) = n - Z(\mathbf{v}) \ . \tag{1.5}$$

Ahora bien, sea $\langle\gamma\rangle = \mathbb{F}_q^*$. Para cada $j = 0, 1, \ldots, q-2$, la función $\psi_j : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*$ dada por

$$\psi_j(\gamma^k) := e^{2\pi\sqrt{-1}\,jk/(q-1)} \qquad \text{para } k = 0, 1, \ldots, q-2 \ , \tag{1.6}$$

define un *caracter multiplicativo* de $\mathbb{F}_q$ [40, Teorema 5.8, p. 191]. Comúnmente, a ψ_0 se le conoce como el *caracter multiplicativo trivial*. Para cada caracter multiplicativo

ψ de $\mathbb{F}_q$, su *conjugado* $\bar{\psi}$ se define como $\bar{\psi}(c) := \psi(c^{-1})$ para todo $c \in \mathbb{F}_q^*$. De hecho, el conjunto de caracteres multiplicativos de $\mathbb{F}_q$, $\widehat{\mathbb{F}}_q$, es un grupo cíclico de orden $q-1$ [40, Corolario 5.9, p. 191]. Para $\psi \in \widehat{\mathbb{F}}_q$, el *orden* de ψ es el menor entero positivo ℓ tal que $\psi^\ell = \psi_0$. Al igual que para el caracter aditivo canónico, para ψ se tiene la siguiente relación de ortogonalidad (ver [40, p. 192])

$$\sum_{c \in \mathbb{F}_q^*} \psi(c) = \begin{cases} q-1 & \text{si } \psi = \psi_0, \\ \\ 0 & \text{en caso contrario.} \end{cases} \tag{1.7}$$

Si q es impar, un caracter multiplicativo importante de $\mathbb{F}_q$ es el *caracter cuadrático* que se denota por η y se define como: $\eta(c) = 1$ si c es el cuadrado de un elemento de $\mathbb{F}_q^*$, y $\eta(c) = -1$ en caso contrario. Note que η puede ser obtenido a partir de (1.6) haciendo $j = (q-1)/2$ (ver [40, Ejemplo 5.10, p. 191]).

1.5.2 Sumas Gaussianas

Uno de los tipos de sumas exponenciales para campos finitos más importantes son las sumas Gaussianas (ver [40, Capítulo 5, Sección 2, p. 192]). Dichas sumas relacionan a los caracteres aditivos de un campo finito con los multiplicativos. Sean $\psi \in \widehat{\mathbb{F}}_q$ y χ el caracter aditivo canónico de $\mathbb{F}_q$. La *suma Gaussiana*, $G_{\mathbb{F}_q}(\psi, \chi)$, de ψ y χ sobre $\mathbb{F}_q$ se define como

$$G_{\mathbb{F}_q}(\psi, \chi) := \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c) \ .$$

Note que, debido a (1.3), se tiene que $G_{\mathbb{F}_q}(\psi_0, \chi) = -1$. Una propiedad importante de las sumas Gaussianas es la expansión de Fourier de la restricción de χ a $\mathbb{F}_q^*$ en términos de los caracteres multiplicativos de $\mathbb{F}_q$ con sumas Gaussianas como coeficientes de Fourier (ver [40, p. 195]):

$$\chi(c) = \frac{1}{q-1} \sum_{\psi \in \widehat{\mathbb{F}}_q} G_{\mathbb{F}_q}(\psi, \chi)\bar{\psi}(c) \qquad \text{para } c \in \mathbb{F}_q^* \ . \tag{1.8}$$

Si q es impar, entonces dos propiedades útiles de la suma Gaussiana $G_{\mathbb{F}_q}(\eta, \chi)$ son [40, Teorema 5.12, p. 193]:

$$G_{\mathbb{F}_q}(\eta, \bar{\chi}) = \eta(-1)G_{\mathbb{F}_q}(\eta, \chi) \qquad \text{y} \qquad G_{\mathbb{F}_q}(\eta, \chi)^2 = \eta(-1)q \ , \tag{1.9}$$

donde η es el caracter cuadrático de $\mathbb{F}_q$ y $\bar{\chi}$ denota el caracter conjugado de χ definido como $\bar{\chi}(c) := \chi(-c)$ para todo $c \in \mathbb{F}_q$.

Ahora bien, sea χ' el caracter aditivo canónico de $\mathbb{F}_{q^m}$. Entonces, los caracteres χ y χ' se relacionan a través de la identidad

$$\chi(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a)) = \chi'(a) \qquad \text{para todo } a \in \mathbb{F}_{q^m} \ ,$$

lo cual es una consecuencia de la transitividad de la traza (ver [40, p. 191]). Por otro lado, $\psi \in \widehat{\mathbb{F}}_q$ puede ser "levantado" a $\mathbb{F}_{q^m}$ haciendo

$$\psi'(a) = \psi(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a)) \qquad \text{para todo } a \in \mathbb{F}_{q^m}^* \ .$$

De la multiplicatividad de la norma se sigue que $\psi' \in \widehat{\mathbb{F}}_{q^m}$ (ver [40, p. 197]). El siguiente teorema establece una relación importante entre las sumas Gaussianas $G_{\mathbb{F}_q}(\psi, \chi)$ y $G_{\mathbb{F}_{q^m}}(\psi', \chi')$.

Teorema 5 (Teorema de Davenport-Hasse, [40, Teorema 5.14, p. 197]). *Sean χ y χ' los caracteres aditivos canónicos de $\mathbb{F}_q$ y $\mathbb{F}_{q^m}$, respectivamente. Sea $\psi \in \widehat{\mathbb{F}}_q$ y ψ' un levantamiento de ψ a $\mathbb{F}_{q^m}$. Entonces*

$$G_{\mathbb{F}_{q^m}}(\psi', \chi') = (-1)^{m-1} G_{\mathbb{F}_q}(\psi, \chi)^m \ .$$

1.5.3 Sumas de caracteres con argumentos polinomiales

Sea χ el caracter aditivo canónico de $\mathbb{F}_q$ y $f \in \mathbb{F}_q[x]$ un polinomio no constante. A lo largo de este documento estaremos trabajando con sumas de caracteres de la forma

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) \ ,$$

también llamadas *sumas de Weil* (ver [40, Capítulo 5, Sección 4, p. 217]). El problema de evaluar explícitamente dichas sumas es en general difícil y muy pocos resultados se tienen al respecto. Cuando f es un monomio el siguiente lema nos será de utilidad.

Lema 2 ([51, Lema, p. 3]). *Sea χ como antes, $\langle \gamma \rangle = \mathbb{F}_q^*$, $a \in \mathbb{F}_q^*$ y d un divisor de $q - 1 = \sharp \mathbb{F}_q^*$. Entonces*

$$\sum_{c \in \mathbb{F}_q^*} \chi(ac^d) = d \sum_{i=0}^{\frac{q-1}{d}-1} \chi(a\gamma^{di}) = d \sum_{c \in \langle \gamma^d \rangle} \chi(ac) \ .$$

El siguiente resultado aborda el caso en el que f es un binomio y también establece una relación interesante con las sumas Gaussianas.

Teorema 6 ([40, Teorema 5.30, p. 217]). *Sea χ como antes, $n > 0$ entero y $\psi \in \widehat{\mathbb{F}}_q$ de orden $d = \gcd(n, q-1)$. Entonces*

$$\sum_{c \in \mathbb{F}_q} \chi(ac^n + b) = \chi(b) \sum_{j=1}^{d-1} G_{\mathbb{F}_q}(\psi^j, \chi) \bar{\psi}^j(a) \ ,$$

para cualesquiera $a, b \in \mathbb{F}_q$ con $a \neq 0$.

Cuando $n = 2$ y q es impar, el teorema anterior alcanza una forma más sencilla la cual puede utilizarse para evaluar sumas de caracteres para cualquier polinomio cuadrático.

Teorema 7 ([40, Teorema 5.33, p. 218]). *Sea χ como antes, q impar y $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_q[x]$ con $a_2 \neq 0$. Entonces*

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = \chi\left(a_0 - a_1^2 (4a_2)^{-1}\right) \eta(a_2) G_{\mathbb{F}_q}(\eta, \chi) \ ,$$

donde η es el caracter cuadrático de $\mathbb{F}_q$.

Finalizamos este capítulo presentando la versión del resultado anterior para el caso q par.

Teorema 8 ([40, Corolario 5.35, p. 220])**.** *Sea χ como antes, q par y $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$. Entonces*

$$\sum_{c\in\mathbb{F}_q} \chi(f(c)) = \begin{cases} \chi(a_0)q & \text{si } a_2 = a_1^2, \\ \\ 0 & \text{en caso contrario.} \end{cases}$$

Capítulo 2

Los códigos de subcampo y extendidos de una subclase de códigos cíclicos óptimos de tres pesos

Recientemente, Heng y Yue [29] presentaron una clase de códigos cíclicos óptimos con respecto a la cota de Griesmer (c.r.a Griesmer), de tres pesos y dimensión $m+1$, con $m \geq 2$ entero, definidos sobre cualquier campo finito. En este capítulo estudiamos algunos de los códigos de subcampo para dicha clase de códigos cíclicos óptimos cuando $m = 2$ y determinamos sus distribuciones de pesos. Resulta que algunos de los códigos obtenidos son óptimos y otros tienen los mejores parámetros conocidos. También investigamos los duales de los códigos de subcampo y demostramos que son casi óptimos con respecto a la cota de Hamming (c.r.a Hamming). Además, calculamos la estructura de cobertura para los códigos de subcampo mostrando así que algunos de ellos tienen la propiedad importante de que todas sus palabras de código distintas de cero son mínimas. Esta es una propiedad deseable que resulta útil en el diseño de un esquema de compartición de secretos basado en un código lineal. Finalmente, presentamos una clase de códigos lineales óptimos c.r.a Griesmer, de dos pesos y definidos sobre cualquier campo finito, cuyos duales son casi óptimos c.r.a Hamming. A través de un enfoque distinto, esta clase de códigos lineales óptimos de dos pesos fue reportada muy recientemente por Heng [24]. Más aún, demostramos que estos códigos lineales se pueden utilizar para construir grafos fuertemente regulares. Los resultados de este capítulo fueron publicados en [32]. Una versión corta de [32] fue presentada en el congreso internacional "LATIN 2022: The 15th Latin American Theoretical Informatics Symposium" [31].

2.1 Introducción

Recientemente se presentó una clase de códigos cíclicos óptimos c.r.a Griesmer, de tres pesos y dimensión 3, definidos sobre $\mathbb{F}_q$ [58]. Poco tiempo después, este resultado fue generalizado a códigos de dimensión $m+1$, con $m \geq 2$ entero [29]. Por otro lado, en [27] se estudiaron los códigos de subcampo q_0-arios de dos familias de códigos lineales óptimos q-arios, donde q_0 es una potencia de un número primo tal que q es a su vez una potencia de q_0. Además, en [15] se obtuvieron algunos resultados

básicos sobre códigos de subcampo y se investigaron los códigos de subcampo de códigos ovales. Asimismo, en [10] se determinaron los códigos de subcampo de varias familias de códigos lineales, y los códigos de subcampo de códigos hiperovales y cónicos fueron estudiados en [25]. La idea básica en estas últimas cuatro referencias es considerar el código de subcampo de un código lineal óptimo, o casi óptimo, sobre $\mathbb{F}_q$ con la esperanza de que el código de subcampo sobre $\mathbb{F}_{q_0}$ tenga también buenos parámetros. En todos los casos se encontraron códigos de subcampo con parámetros muy atractivos.

Dicho lo anterior, el primer objetivo de este capítulo es estudiar los códigos de subcampo q_0-arios para una subclase de los códigos cíclicos óptimos de tres pesos reportados en [29] y determinar sus distribuciones de pesos. Resulta que los códigos de subcampo estudiados también tienen tres pesos distintos de cero, lo cual es interesante ya que los códigos lineales con pocos pesos tienen una amplia gama de aplicaciones en muchos campos de investigación, tales como códigos de autenticación [18], diseños combinatorios [14], esquemas de compartición de secretos [9, 36, 47, 48, 69], esquemas de asociación [7], grafos fuertemente regulares [8,54] y diseño de secuencias de salto de frecuencia [19]. Como veremos más adelante, algunos de los códigos de subcampo son óptimos y otros tienen los mejores parámetros conocidos. También investigamos los duales de los códigos de subcampo y demostramos que son casi óptimos c.r.a Hamming.

El segundo objetivo es determinar la estructura de cobertura para los códigos de subcampo estudiados. Por medio del Lema de Ashikhmin-Barg (ver Lema 6 más adelante) demostramos que algunos de estos códigos tienen la propiedad importante de que todas sus palabras de código distintas de cero son mínimas. Esta es una propiedad deseable que resulta útil en el diseño de un esquema de compartición de secretos basado en un código lineal.

Finalmente, el tercer objetivo es presentar una clase de códigos lineales óptimos c.r.a Griesmer, de dos pesos sobre $\mathbb{F}_q$, cuyos duales son casi óptimos c.r.a Hamming. Esta clase de códigos se obtiene al extender algunos de los códigos cíclicos óptimos de tres pesos reportados en [29]. Es importante resaltar que, a través de un enfoque distinto, esta clase de códigos lineales óptimos de dos pesos fue reportada muy recientemente en el [24, Teorema 6.3]. Más aún, demostramos que estos códigos lineales se pueden utilizar para construir grafos fuertemente regulares.

Este capítulo está organizado de la siguiente manera: En la Sección 2.2 establecemos la notación que utilizaremos a lo largo de este capítulo y presentamos algunos resultados preliminares. En la Sección 2.3 determinamos los códigos de subcampo para la subclase de códigos cíclicos óptimos de tres pesos que nos interesa. En la Sección 2.4 calculamos la estructura de cobertura para los códigos de subcampo estudiados y la utilizamos para construir esquemas de compartición de secretos con buenas estructuras de acceso. Finalmente, en la Sección 2.5 presentamos una clase de códigos lineales óptimos de dos pesos cuyos duales son casi óptimos. Más aún, demostramos que estos códigos se pueden utilizar para construir grafos fuertemente regulares.

2.2 Notación y resultados preliminares

A lo largo de este capítulo utilizaremos la siguiente:

Notación. Sea $q_0 = p^t$, donde t es un entero positivo y p es un número primo. Para un entero $r > 1$, sea $q = q_0^r = p^{tr}$. Sea $m \geq 2$ entero y γ un elemento primitivo de $\mathbb{F}_{q^m}$.

A través del siguiente teorema recordamos la clase de códigos cíclicos óptimos de tres pesos para la cual estamos interesados en obtener sus códigos de subcampo y extendidos.

Teorema 9 ([29, Teorema 11]). *Sean e_1 y e_2 enteros positivos y sea $\mathcal{C}_{(q,m,e_1,e_2)}$ el código cíclico de longitud $q^m - 1$ sobre $\mathbb{F}_q$ dado por*

$$\mathcal{C}_{(q,m,e_1,e_2)} = \{\mathbf{c}(a,b) : a \in \mathbb{F}_q, b \in \mathbb{F}_{q^m}\} \ , \tag{2.1}$$

donde

$$\mathbf{c}(a,b) := \left(a\gamma^{\frac{q^m-1}{q-1}e_1 j} + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(b\gamma^{e_2 j}\right)\right)_{j=0}^{q^m-2} \ .$$

Si se cumple que $\gcd(\frac{q^m-1}{q-1}, e_2) = 1$ y $\gcd(q-1, me_1 - e_2) = 1$, entonces $\mathcal{C}_{(q,m,e_1,e_2)}$ es un $[q^m - 1, m+1, q^{m-1}(q-1) - 1]$ código cíclico óptimo c.r.a Griesmer, de tres pesos, cuyo enumerador de pesos es

$$1 + (q-1)(q^m-1)z^{q^{m-1}(q-1)-1} + (q^m-1)z^{q^{m-1}(q-1)} + (q-1)z^{q^m-1} \ . \tag{2.2}$$

Además, si $q > 2$, su código dual es un $[q^m - 1, q^m - m - 2, 3]$ código cíclico.

Observación 6. En el [59, Teorema 1] se demostró que los enteros e_1 y e_2 del teorema anterior pueden ser enteros cualesquiera.

A lo largo de esta y la siguiente sección estamos interesados en obtener las distribuciones de pesos para los códigos de subcampo de una subclase de los códigos cíclicos óptimos de tres pesos del Teorema 9 cuando $m = 2$. Así pues, para estas dos secciones vamos a fijar $m = 2$. Es decir, $\frac{q^2-1}{q-1} = q + 1$ y $\langle\gamma\rangle = \mathbb{F}_{q^2}^*$.

Note que si $\mathcal{C}_{(q,2,e_1,e_2)}$ es un código cíclico óptimo perteneciente al Teorema 9 entonces, de acuerdo con el Lema 1, su código de subcampo, $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$, está dado por (recordemos que $q = q_0^r$):

$$\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)} = \left\{\mathbf{c}(a,b)^{(q_0)} : a \in \mathbb{F}_q, b \in \mathbb{F}_{q^2}\right\} \ , \tag{2.3}$$

donde

$$\mathbf{c}(a,b)^{(q_0)} := \left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(a\gamma^{(q+1)e_1 j}\right) + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_{q_0}}\left(b\gamma^{e_2 j}\right)\right)_{j=0}^{q^2-2} \ . \tag{2.4}$$

Observación 7. Al igual que $\mathcal{C}_{(q,2,e_1,e_2)}$, $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ también es un código cíclico de longitud $q^2 - 1$. Más aún, si $h_\alpha(x) \in \mathbb{F}_{q_0}[x]$ es el polinomio mínimo de $\gamma^{-\alpha}$, con α entero, y si d es el menor entero positivo tal que $\alpha q_0^d \equiv \alpha \pmod{q^2-1}$, entonces observe que $\deg(h_\alpha(x)) = d$ (ver Sección 1.4.1). Por lo tanto, $h_{(q+1)e_1}(x) \neq h_{e_2}(x)$, $h_{(q+1)e_1}(x)h_{e_2}(x)$ es el polinomio de chequeo de paridad de $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ (ver Teorema de Delsarte [13]), y si k' es su dimensión, entonces $k' = d_1 + d_2$, donde d_1 y d_2 son los enteros positivos más pequeños tales que $(q+1)e_1 q_0^{d_1} \equiv (q+1)e_1 \pmod{q^2-1}$ y $e_2 q_0^{d_2} \equiv e_2 \pmod{q^2-1}$, respectivamente.

El siguiente resultado preliminar nos permitirá obtener las distribuciones de pesos para los códigos de subcampo de la forma $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$.

Lema 3. *Sean χ y χ' los caracteres aditivos canónicos de $\mathbb{F}_q$ y $\mathbb{F}_{q^2}$, respectivamente. Para $a \in \mathbb{F}_q$ y $b \in \mathbb{F}_{q^2}$, considere la siguiente suma exponencial*

$$\begin{aligned} Z(a,b) &:= \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}} \sum_{x \in \mathbb{F}^*_{q^2}} \chi(yax^{q+1}) \chi'(ybx) \ , \\ &= \frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0} \sum_{y \in \mathbb{F}^*_{q_0}} \sum_{x \in \mathbb{F}^*_{q^2}} \chi(yax^{q+1}) \chi'(ybx) \ . \end{aligned}$$

Entonces,

$$Z(a,b) = \begin{cases} q_0^{2r}-1 & si\ a=b=0, \\ (q_0^r+1)(q_0^{r-1}-1) & si\ a \neq 0\ y\ b=0, \\ q_0^{2r-1}-1 & si\ a=0\ y\ b \neq 0, \\ (q_0^r+1)(q_0^{r-1}-1) & si\ (a,b) \neq (0,0)\ y\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right) = 0, \\ q_0^{2r-1}+q_0^{r-1}-1 & si\ (a,b) \neq (0,0)\ y\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right) \neq 0. \end{cases}$$

Demostración. Claramente,

$$Z(0,0) = \frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0}(q_0-1)(q_0^{2r}-1) = q_0^{2r}-1 \ .$$

Si $a \neq 0$ y $b=0$, entonces por el Lema 2 y (1.3), concluimos que

$$\begin{aligned} Z(a,0) &= \frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0} \sum_{y \in \mathbb{F}^*_{q_0}} \sum_{x \in \mathbb{F}^*_{q^2}} \chi(yax^{q+1}) \ , \\ &= \frac{(q_0^{2r}-1)}{q_0} + \frac{(q+1)}{q_0} \sum_{y \in \mathbb{F}^*_{q_0}} \sum_{x \in \mathbb{F}^*_{q}} \chi(yax) \ , \\ &= \frac{(q_0^{2r}-1)}{q_0} + \frac{(q_0^r+1)}{q_0} \sum_{y \in \mathbb{F}^*_{q_0}} (-1) \ , \\ &= \frac{(q_0^{2r}-1)}{q_0} - \frac{(q_0^r+1)}{q_0}(q_0-1) = (q_0^r+1)(q_0^{r-1}-1) \ . \end{aligned}$$

Por otro lado, si $a=0$ y $b \neq 0$, utilizando (1.3) obtenemos que

$$\begin{aligned} Z(0,b) &= \frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0} \sum_{y \in \mathbb{F}^*_{q_0}} \sum_{x \in \mathbb{F}^*_{q^2}} \chi'(ybx) = \frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0} \sum_{y \in \mathbb{F}^*_{q_0}} (-1) \ , \\ &= \frac{(q_0^{2r}-1)}{q_0} - \frac{(q_0-1)}{q_0} = q_0^{2r-1}-1 \ . \end{aligned}$$

Ahora bien, sea φ el caracter aditivo canónico de $\mathbb{F}_{q_0}$ y supongamos que $(a,b) \neq (0,0)$. Por la transitividad y linealidad de la traza (ver Sección 1.1.1), tenemos que

$$\begin{aligned} Z(a,b) &= \frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}^*} \sum_{x \in \mathbb{F}_{q^2}^*} \varphi\left(y \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(a x^{q+1}\right)\right) \varphi\left(y \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_{q_0}}(bx)\right) , \\ &= \frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}^*} \sum_{x \in \mathbb{F}_{q^2}^*} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(a x^{q+1} + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(bx)\right)\right)\right) , \\ &= \frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}^*} \sum_{x \in \mathbb{F}_{q^2}^*} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(a x^q\left(x + \frac{b^q}{a}\right) + bx\right)\right)\right) , \end{aligned}$$

donde la última igualdad se cumple ya que $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(bx) = bx + b^q x^q$. Sea $B = \mathbb{F}_{q^2} \setminus \{\frac{b^q}{a}\}$. Entonces, después de aplicar el cambio de variable $x \mapsto w - \frac{b^q}{a}$, obtenemos que $Z(a,b)$ es igual a

$$\frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}^*} \sum_{w \in B} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(a\left(w^q - \frac{b^{q^2}}{a^q}\right)w + b\left(w - \frac{b^q}{a}\right)\right)\right)\right) .$$

Sin embargo, ya que $a \in \mathbb{F}_q^*$ y $b \in \mathbb{F}_{q^2}^*$, $a^q = a$ y $b^{q^2} = b$ (ver Sección 1.1). En consecuencia, como $B = \mathbb{F}_{q^2} \setminus \{\frac{b^q}{a}\}$,

$$\begin{aligned} Z(a,b) &= \frac{(q_0^{2r}-1)}{q_0} + \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}^*} \sum_{w \in B} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(a w^{q+1} - \frac{b^{q+1}}{a}\right)\right)\right) , \\ &= \frac{(q_0^{2r}-1)}{q_0} - \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}^*} \varphi(0) + \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}^*} \varphi\left(-y \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)\right) \\ &\quad \times \sum_{w \in \mathbb{F}_{q^2}} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(a w^{q+1}\right)\right)\right) , \\ &= (q_0^{2r-1}-1) + \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}^*} \varphi\left(-y \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)\right) \sum_{w \in \mathbb{F}_{q^2}} \chi\left(y a w^{q+1}\right) , \end{aligned}$$

donde χ es el caracter aditivo canónico de $\mathbb{F}_q$ (note que $w^{q+1} \in \mathbb{F}_q$). Pero, debido al Lema 2 y (1.3), tenemos que

$$\begin{aligned} \sum_{w \in \mathbb{F}_{q^2}} \chi\left(y a w^{q+1}\right) &= 1 + \sum_{w \in \mathbb{F}_{q^2}^*} \chi\left(y a w^{q+1}\right) , \\ &= 1 + (q+1) \sum_{w \in \mathbb{F}_q^*} \chi(yaw) = -q , \end{aligned}$$

Finalmente, utilizando de nueva cuenta (1.3), concluimos que

$$Z(a,b) = (q_0^{2r-1}-1) - q_0^{r-1} \sum_{y \in \mathbb{F}_{q_0}^*} \varphi\left(-y \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)\right) ,$$

$$= \begin{cases} (q_0^r+1)(q_0^{r-1}-1) & \text{si } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)=0, \\ q_0^{2r-1}+q_0^{r-1}-1 & \text{en caso contrario.} \end{cases}$$

□

2.3 Los códigos de subcampo de una subclase de códigos cíclicos óptimos

A través del siguiente resultado determinamos los códigos de subcampo, junto con sus distribuciones de pesos, para una subclase de los códigos cíclicos óptimos de tres pesos del Teorema 9.

Teorema 10. *Sean $r>1$, e_1 y e_2 enteros positivos y sea $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ el código de subcampo de longitud $q_0^{2r}-1$, sobre $\mathbb{F}_{q_0}$, dado por (2.3). Suponga que $\gcd(q^2-1,e_2)=1$ y $\gcd(q-1,2e_1-e_2)=1$. Entonces, las siguientes afirmaciones se cumplen:*

(A) *Si $(q-1)|(q_0-1)e_1$, entonces $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ es un código cíclico óptimo de tres pesos sobre $\mathbb{F}_{q_0}$, de longitud $q_0^{2r}-1$ y dimensión $2r+1$, perteneciente a la clase de códigos cíclicos óptimos de tres pesos del Teorema 9 (tome en el teorema $m=2r$ y $q=q_0$).*

(B) *Sea $\mathcal{I}$ un entero tal que $\mathcal{I}e_2\equiv 1 \pmod{q^2-1}$. Si $(q-1)\nmid(q_0-1)e_1$ y $\mathcal{I}e_1\equiv 1 \pmod{q-1}$, entonces $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ es un código cíclico de tres pesos sobre $\mathbb{F}_{q_0}$, de longitud $q_0^{2r}-1$ y dimensión $3r$, cuyo enumerador de pesos es*

$$\begin{aligned} &1+q_0^{r-1}(q_0^{2r}-1)(q_0-1)z^{q_0^{r-1}(q_0^{r+1}-q_0^r-1)}+(q_0^{2r}-1)z^{q_0^{2r-1}(q_0-1)} \\ &+q_0^{r-1}(q_0^r-1)(q_0^r-q_0+1)z^{q_0^{r-1}(q_0-1)(q_0^r+1)}. \end{aligned} \tag{2.5}$$

Más aún, el código dual, $\mathcal{C}^{(q_0)\perp}_{(q,2,e_1,e_2)}$, de $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ es un $[q_0^{2r}-1, q_0^{2r}-3r-1, 3]$ código cíclico casi óptimo c.r.a Hamming.

Demostración. En primer lugar, como $\gcd(\frac{q^2-1}{q-1},e_2)\le\gcd(q^2-1,e_2)=1$ y $\gcd(q-1,2e_1-e_2)=1$, observe que $\mathcal{C}_{(q,2,e_1,e_2)}$ en efecto pertenece a la clase de códigos cíclicos óptimos de tres pesos del Teorema 9 (tome en el teorema $m=2$).

Parte (A): Sea $e_1'=\frac{(q_0-1)e_1}{q-1}$. Claramente, $(q+1)e_1=\frac{q^2-1}{q_0-1}e_1'$. Sean $h_{(q+1)e_1}(x)=h_{\frac{q^2-1}{q_0-1}e_1'}(x)$, $h_{e_2}(x)\in\mathbb{F}_{q_0}[x]$ los polinomios mínimos de $\gamma^{-\frac{q^2-1}{q_0-1}e_1'}$ y γ^{-e_2}, respectivamente. Entonces, de acuerdo con la Observación 7, note que $\deg(h_{(q+1)e_1}(x))=1$, pues $\frac{q^2-1}{q_0-1}e_1'q_0\equiv\frac{q^2-1}{q_0-1}e_1' \pmod{q^2-1}$. También, como $\langle\gamma\rangle=\langle\gamma^{-e_2}\rangle=\mathbb{F}_{q^2}^*=\mathbb{F}_{q_0^{2r}}^*$, $\deg(h_{e_2}(x))=2r$. En consecuencia, $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ tiene dimensión $2r+1$. De hecho, como $\gamma^{(q+1)e_1}=\gamma^{\frac{q_0^{2r}-1}{q_0-1}e_1'}\in\mathbb{F}_{q_0}^*$, note que el código $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ está dado por el conjunto (ver (2.3))

$$\begin{aligned}&\left\{\left(\gamma^{(q+1)e_1 j}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(a)+\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_{q_0}}\left(b\gamma^{e_2 j}\right)\right)_{j=0}^{q^2-2} : a\in\mathbb{F}_q, b\in\mathbb{F}_{q^2}\right\}\\ =&\left\{\left(a_0\gamma^{\frac{q_0^{2r}-1}{q_0-1}e_1' j}+\mathrm{Tr}_{\mathbb{F}_{q_0^{2r}}/\mathbb{F}_{q_0}}\left(b\gamma^{e_2 j}\right)\right)_{j=0}^{q_0^{2r}-2} : a_0\in\mathbb{F}_{q_0}, b\in\mathbb{F}_{q_0^{2r}}\right\}.\end{aligned} \tag{2.6}$$

Ahora bien, claramente $(q_0-1)|(q_0^\ell-1)$ para todo entero no negativo ℓ (es decir, $q_0^\ell\equiv 1 \pmod{q_0-1}$). Entonces, como $\frac{q_0^r-1}{q_0-1}=q_0^{r-1}+q_0^{r-2}+\cdots+q_0+1$, $(q_0-1)|(\frac{q_0^r-1}{q_0-1}-r)$. Por lo tanto, ya que $e_1'=\frac{(q_0-1)e_1}{q_0^r-1}$ y $q-1=\frac{q_0^r-1}{q_0-1}(q_0-1)$, tenemos que

$$\begin{aligned}\gcd(q_0-1,2re_1'-e_2) &= \gcd(q_0-1,2re_1'-e_2+2(\frac{q_0^r-1}{q_0-1}-r)e_1'),\\ &= \gcd(q_0-1,2\frac{q_0^r-1}{q_0-1}e_1'-e_2),\\ &= \gcd(q_0-1,2e_1-e_2)\le\gcd(q-1,2e_1-e_2)=1.\end{aligned}$$

Es decir, $\gcd(q_0-1,2re_1'-e_2)=1$. Más aún, debido a que $\gcd(q^2-1,e_2)=1$, también tenemos que $\gcd(\frac{q_0^{2r}-1}{q_0-1},e_2)=1$. Esto significa, en consecuencia y de acuerdo con el Teorema 9, que $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ es un código cíclico óptimo de tres pesos, de longitud $q_0^{2r}-1$ y dimensión $2r+1$, que pertenece a tal teorema. De hecho, de (2.6) y (2.1), note que

$$\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}=\mathcal{C}_{(q_0,2r,e_1',e_2)},$$

donde $e_1'=\frac{(q_0-1)e_1}{q-1}$.

Parte (B): Note que, por la Observación 7, $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ es cíclico. Ahora bien, sean $h_{(q+1)e_1}(x)$, $h_{e_2}(x)\in\mathbb{F}_{q_0}[x]$ como antes. Puesto que $(q-1)\nmid(q_0-1)e_1$, observe que r es el menor entero positivo tal que $(q+1)e_1q_0^r=(q_0^r+1)e_1q_0^r\equiv(q+1)e_1 \pmod{q_0^{2r}-1}$. Entonces, $\deg(h_{(q+1)e_1}(x))=r$, y como $\deg(h_{e_2}(x))=2r$, la dimensión de $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ es $3r$.

Sean φ, χ y χ' los caracteres aditivos canónicos de $\mathbb{F}_{q_0}$, $\mathbb{F}_q$ y $\mathbb{F}_{q^2}$, respectivamente. Sean $a\in\mathbb{F}_q$, $b\in\mathbb{F}_{q^2}$ y $\mathbf{c}(a,b)^{(q_0)}\in\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$. Entonces, de (2.4) y por la relación de ortogonalidad para el caracter φ (ver (1.5)), el peso de Hamming de la palabra de código $\mathbf{c}(a,b)^{(q_0)}$, $w_H(\mathbf{c}(a,b)^{(q_0)})$, es igual a

$$\begin{aligned}&q^2-1-\frac{1}{q_0}\sum_{y\in\mathbb{F}_{q_0}}\sum_{w\in\mathbb{F}_{q^2}^*}\varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(aw^{(q+1)e_1})+\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_{q_0}}(bw^{e_2})\right)\right),\\ =&\,q^2-1-\frac{1}{q_0}\sum_{y\in\mathbb{F}_{q_0}}\sum_{w\in\mathbb{F}_{q^2}^*}\chi(yaw^{(q+1)e_1})\chi'(ybw^{e_2}).\end{aligned}$$

Pero $\mathcal{I}e_2\equiv 1 \pmod{q^2-1}$ y $\mathcal{I}e_1\equiv 1 \pmod{q-1}$. En consecuencia, después de aplicar el cambio de variable $w\mapsto x^{\mathcal{I}}$, obtenemos que

$$w_H(\mathbf{c}(a,b)^{(q_0)})=q^2-1-\frac{1}{q_0}\sum_{y\in\mathbb{F}_{q_0}}\sum_{x\in\mathbb{F}_{q^2}^*}\chi(yax^{(q+1)\mathcal{I}e_1})\chi'(ybx^{\mathcal{I}e_2}),$$

$$= q^2 - 1 - \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}} \sum_{x \in \mathbb{F}_{q^2}^*} \chi(yax^{q+1}) \chi'(ybx) \ ,$$
$$= q^2 - 1 - Z(a,b) \ ,$$

donde $Z(a,b)$ es como en el Lema 3. De hecho, debido a tal lema, tenemos que

$$w_H(\mathbf{c}(a,b)^{(q_0)}) = \begin{cases} 0 & \text{si } a = b = 0, \\ q_0^{r-1}(q_0 - 1)(q_0^r + 1) & \text{si } a \neq 0 \text{ y } b = 0, \\ q_0^{2r-1}(q_0 - 1) & \text{si } a = 0 \text{ y } b \neq 0, \\ q_0^{r-1}(q_0 - 1)(q_0^r + 1) & \text{si } (a,b) \neq (0,0) \text{ y } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right) = 0, \\ q_0^{r-1}(q_0^{r+1} - q_0^r - 1) & \text{si } (a,b) \neq (0,0) \text{ y } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right) \neq 0, \end{cases}$$

lo cual coincide con (2.5). Ahora bien, observe que

$$A_{q_0^{r-1}(q_0-1)(q_0^r+1)}(\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}) = \sharp\{a \in \mathbb{F}_q^*\} + \sharp\{(a,b) \in \mathbb{F}_q^* \times \mathbb{F}_{q^2}^* : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right) = 0\},$$
$$= (q-1) + (q-1)(q+1)(\frac{q}{q_0} - 1) \ ,$$
$$= q_0^{r-1}(q_0^r - 1)(q_0^r - q_0 + 1) \ .$$

Las frecuencias de los otros pesos de $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ se pueden calcular de manera similar y por tal motivo omitimos los detalles. De esta forma, el enumerador de pesos de $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ queda determinado.

Por otro lado, utilizando (2.5) y las primeras cuatro identidades de Pless, obtenemos que $A_1(\mathcal{C}^{(q_0)\perp}_{(q,2,e_1,e_2)}) = A_2(\mathcal{C}^{(q_0)\perp}_{(q,2,e_1,e_2)}) = 0$ y

$$A_3(\mathcal{C}^{(q_0)\perp}_{(q,2,e_1,e_2)}) = \frac{(q_0^{r+2} - 3q_0^{r+1} + q_0^2 + 3q_0^r - 6q_0 + 6)(q_0^{2r} - 1)(q_0 - 1)}{6} > 0 \ .$$

Es decir, $\mathcal{C}^{(q_0)\perp}_{(q,2,e_1,e_2)}$ es un $[q_0^{2r} - 1, q_0^{2r} - 3r - 1, 3]$ código cíclico. Finalmente, por la cota de Hamming (ver Teorema 2), no es difícil verificar que para un código de longitud $q_0^{2r} - 1$ y dimensión $q_0^{2r} - 3r - 1$, su distancia mínima puede ser a lo más 4. Por lo tanto, el código $\mathcal{C}^{(q_0)\perp}_{(q,2,e_1,e_2)}$ es casi óptimo. □

Ejemplo 5. Los siguientes son algunos ejemplos del teorema anterior.

(a) Sean $(q_0, r, e_1, e_2) = (3, 2, 4, 1)$. En consecuencia, $q = 9$ y, claramente, $(q-1) | (q_0 - 1)e_1$. Entonces, por la Parte (A) del Teorema 10, el código de subcampo $\mathcal{C}^{(3)}_{(9,2,4,1)} = \mathcal{C}_{(3,4,1,1)}$ es un código cíclico óptimo de tres pesos sobre $\mathbb{F}_3$, de longitud 80 y dimensión 5, cuyo enumerador de pesos es

$$1 + 160z^{53} + 80z^{54} + 2z^{80} \ .$$

(b) Sean $(q_0, r, e_1, e_2) = (2, 2, 1, 1)$. En consecuencia, $q = 4$, $\mathcal{I} = 1$ y, claramente, $(q-1) \nmid (q_0 - 1)e_1$. Entonces, por la Parte (B) del Teorema 10, el código

de subcampo $\mathcal{C}^{(2)}_{(4,2,1,1)}$ es un $[15, 6, 6]$ código cíclico binario de tres pesos con enumerador de pesos

$$1 + 30z^6 + 15z^8 + 18z^{10} ,$$

mientras que su dual es un $[15, 9, 3]$ código cíclico casi óptimo c.r.a Hamming.

(c) Sean $(q_0, r, e_1, e_2) = (3, 2, 1, 1)$. En consecuencia, $q = 9$, $\mathcal{I} = 1$ y, claramente, $(q-1) \nmid (q_0 - 1)e_1$. Entonces, por la Parte (B) del Teorema 10, el código de subcampo $\mathcal{C}^{(3)}_{(9,2,1,1)}$ es un $[80, 6, 51]$ código cíclico de tres pesos sobre $\mathbb{F}_3$ con enumerador de pesos

$$1 + 480z^{51} + 80z^{54} + 168z^{60} ,$$

mientras que su dual es un $[80, 74, 3]$ código cíclico casi óptimo c.r.a Hamming.

(d) Sean $(q_0, r, e_1, e_2) = (2, 4, 2, 2)$. En consecuencia, $q = 16$, $\mathcal{I} = 128$ y, claramente, $(q-1) \nmid (q_0 - 1)e_1$ y $\mathcal{I}e_1 \equiv 1 \pmod{q-1}$. Entonces, por la Parte (B) del Teorema 10, el código de subcampo $\mathcal{C}^{(2)}_{(16,2,2,2)}$ es un $[255, 12, 120]$ código cíclico binario de tres pesos con enumerador de pesos

$$1 + 2040z^{120} + 255z^{128} + 1800z^{136} ,$$

mientras que su dual es un $[255, 243, 3]$ código cíclico casi óptimo c.r.a Hamming.

Observación 8. De acuerdo con las tablas de códigos mantenidas en [21], note que el código $[15, 6, 6]$ en (b) es óptimo, mientras que el código $[80, 6, 51]$ en (c) y su dual son óptimos. Finalmente, el código $[255, 12, 120]$ en (d) tiene los mejores parámetros conocidos[1].

Al fijar $m = 2$, es importante observar que la condición sobre el entero e_2 es más restrictiva en el Teorema 10 ($\gcd(q^2 - 1, e_2) = 1$) que en el Teorema 9 ($\gcd(q + 1, e_2) = 1$). Esto, por supuesto, implica que el Teorema 10 determina los códigos de subcampo solo para una subclase de los códigos cíclicos óptimos de tres pesos del Teorema 9. Específicamente, esto significa que hay códigos cíclicos óptimos de tres pesos pertenecientes al Teorema 9, cuyos códigos de subcampo no pueden describirse a través del Teorema 10. Por ejemplo, con la ayuda de un programa de computadora, no es difícil verificar que el código de subcampo $\mathcal{C}^{(2)}_{(4,2,1,3)}$ es un $[15, 6, 6]$ código cíclico binario de cuatro pesos con enumerador de pesos $1 + 25z^6 + 30z^8 + 3z^{10} + 5z^{12}$ (para este ejemplo note que $\gcd(q + 1, e_2) = 1$, pero $\gcd(q^2 - 1, e_2) \neq 1$). Este código de subcampo, al igual que el código de subcampo en el Ejemplo 5 (b), es óptimo. Sin embargo, a diferencia del dual de $\mathcal{C}^{(2)}_{(4,2,1,1)}$, el dual de $\mathcal{C}^{(2)}_{(4,2,1,3)}$ es un $[15, 9, 4]$ código cíclico óptimo binario. Este ejemplo nos deja ver que, más allá del Teorema 10, aún existen otros códigos cíclicos óptimos de tres pesos cuyos códigos de subcampo tienen buenos parámetros.

[1]Se dice que un código lineal tiene los mejores parámetros conocidos si su distancia mínima alcanza la cota inferior en [21].

2.4 La estructura de cobertura de los códigos de subcampo

Para cualquier $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q_0}^n$, el *soporte* de $\mathbf{c}$ se define como el conjunto $\{i : 0 \leq i \leq n-1, c_i \neq 0\}$. Además, para dos vectores cualesquiera $\mathbf{c}, \mathbf{c}' \in \mathbb{F}_{q_0}^n$, se dice que $\mathbf{c}$ *cubre* a $\mathbf{c}'$ si el soporte de $\mathbf{c}$ contiene el de $\mathbf{c}'$. Una palabra de código distinta de cero es llamada *mínima* si cubre solo a sus múltiplos en un código lineal. El conjunto de todas las palabras de código mínimas en un código lineal se denomina la *estructura de cobertura* del código. Más aún, se dice que un código lineal es *mínimo* si todas sus palabras de código son mínimas.

Determinar la estructura de cobertura de un código lineal es en general un problema difícil pero al mismo tiempo interesante ya que está estrechamente relacionado con la construcción de esquemas de compartición de secretos (ver por ejemplo [9, 36, 47, 48, 69]). Un *esquema de compartición de secretos* es un protocolo criptográfico cuyo objetivo principal es el de resguardar cierta información (un *secreto*) a través de un conjunto de entidades (*participantes*). Esto se logra compartiendo con dichas entidades cierta información (*partes*) aparentemente independiente del secreto, de tal forma que solo subconjuntos autorizados (*conjuntos de acceso*) de las entidades puedan acceder al contenido del secreto y que los demás subconjuntos no puedan saber nada de él (ver [4]).

En la presente sección determinamos la estructura de cobertura para los códigos de subcampo del Teorema 10. Como veremos más adelante, algunos de estos códigos son mínimos y, por tanto, se prestan para construir esquemas de compartición de secretos con buenas estructuras de acceso. Más aún, al final presentamos un ejemplo específico de un esquema de compartición de secretos basado en uno de dichos códigos.

Existen distintas formas de construir esquemas de compartición de secretos mediante el uso de códigos lineales. Una de ellas fue propuesta por Massey [47, 48] y se presenta a continuación (ver [36, 69]).

Sea $\mathcal{C}$ un $[n, k]$ código lineal sobre $\mathbb{F}_{q_0}$. En el *esquema de compartición de secretos basado en un código lineal* $\mathcal{C}$, el secreto $\mathbf{s}$ es un elemento de $\mathbb{F}_{q_0}$. Hay un repartidor P_0 y $n-1$ participantes $P_1, P_2, \ldots, P_{n-1}$ involucrados en el esquema, siendo el repartidor una persona de confianza. Sea $G^\perp = (\boldsymbol{g}_0^\perp, \boldsymbol{g}_1^\perp, \ldots, \boldsymbol{g}_{n-1}^\perp)$ una matriz generadora del código dual, $\mathcal{C}^\perp$, de $\mathcal{C}$ tal que $\boldsymbol{g}_i^\perp$ es el i-ésimo vector columna de $G^\perp$ y $\boldsymbol{g}_i^\perp \neq 0$ para $0 \leq i \leq n-1$. Entonces, el esquema de compartición de secretos basado en $\mathcal{C}$ se describe a continuación:

Paso 1) Para calcular las partes con respecto a un secreto $\mathbf{s}$, el repartidor P_0 elige aleatoriamente un vector $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-k-1}) \in \mathbb{F}_{q_0}^{n-k}$ tal que $\mathbf{s} = \boldsymbol{u}\boldsymbol{g}_0^\perp$. En total hay q_0^{n-k-1} vectores $\boldsymbol{u} \in \mathbb{F}_{q_0}^{n-k}$.

Paso 2) El repartidor P_0 trata a $\boldsymbol{u}$ como un vector de información y calcula la palabra de código correspondiente $\boldsymbol{t} = \boldsymbol{u}G^\perp = (t_0, t_1, \ldots, t_{n-1})$ en $\mathcal{C}^\perp$. Luego envía la parte t_i al participante P_i para cada $1 \leq i \leq n-1$.

Paso 3) El secreto $\mathbf{s}$ se recupera de la siguiente manera: dado que $t_0 = \boldsymbol{u}\boldsymbol{g}_0^\perp = \mathbf{s}$, un conjunto de partes $\{t_{i_1}, t_{i_2}, \ldots, t_{i_\ell}\}$ puede determinar el secreto $\mathbf{s}$ sii $\boldsymbol{g}_0^\perp$ es una combinación lineal de $\{\boldsymbol{g}_{i_1}^\perp, \boldsymbol{g}_{i_2}^\perp, \ldots, \boldsymbol{g}_{i_\ell}^\perp\}$, donde $1 \leq i_1 < i_2 < \cdots < i_\ell \leq n-1$.

Ciertamente, si un grupo de participantes $\mathcal{D}$ puede recuperar el secreto combinando sus partes, entonces cualquier grupo de participantes que contenga a $\mathcal{D}$ también podrá hacerlo. Se dice que el conjunto $\{i_1, i_2, \ldots, i_\ell\}$ es un *conjunto de acceso mínimo* si puede recuperar el secreto $\mathbf{s}$ pero ninguno de sus subconjuntos propios puede hacerlo. El conjunto de todos los conjuntos de acceso mínimo en un esquema de compartición de secretos es llamado la *estructura de acceso*.

Para un código lineal $\mathcal{C}$, el siguiente lema presentado en [47] establece una correspondencia biunívoca entre la estructura de acceso del esquema de compartición de secretos basado en $\mathcal{C}$ y el conjunto de palabras de código mínimas en $\mathcal{C}$ cuya primera coordenada es igual a 1.

Lema 4. *Sea $\mathcal{C}$ un $[n, k]$ código lineal definido sobre $\mathbb{F}_{q_0}$. Entonces, el conjunto $\{i_1, i_2, \ldots, i_\ell\} \subseteq \{1, 2, \ldots, n-1\}$ con $i_1 < i_2 < \cdots < i_\ell$ es un conjunto de acceso mínimo en el esquema de compartición de secretos basado en $\mathcal{C}$ sii existe una palabra de código mínima $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ en $\mathcal{C}$ tal que el soporte de $\mathbf{c}$ es $\{0, i_1, i_2, \ldots, i_\ell\}$ y $c_0 = 1$.*

Si $\mathbf{c}$ es una palabra de código distinta de cero cuya primera coordenada es igual a 1 y el soporte de $\mathbf{c}$ es $\{0, i_1, i_2, \ldots, i_\ell\}$ tal que $1 \leq i_1 < i_2 < \cdots < i_\ell \leq n-1$, entonces llamaremos al conjunto $\{i_1, i_2, \ldots, i_\ell\}$ el *soporte de acceso* de la palabra de código $\mathbf{c}$.

De la discusión anterior se sigue que determinar la estructura de acceso del esquema de compartición de secretos basado en un código lineal $\mathcal{C}$ es equivalente a determinar el conjunto de soportes de acceso de las palabras de código mínimas en $\mathcal{C}$ cuya primera coordenada es igual a 1. Así pues, a continuación calcularemos la estructura de cobertura para los códigos de subcampo del Teorema 10. Con ese fin, los siguientes resultados que aparecen en [1] nos serán de utilidad.

Lema 5. *Sea $\mathcal{C}$ un código lineal sobre $\mathbb{F}_{q_0}$ con distancia mínima d. Entonces, toda palabra de código cuyo peso de Hamming sea menor o igual a $\frac{dq_0 - q_0 + 1}{q_0 - 1}$ debe ser mínima.*

El siguiente lema establece que si los pesos de un código lineal son lo suficientemente cercanos entre sí, entonces el código es mínimo.

Lema 6 (Lema de Ashikhmin–Barg)**.** *Sea $\mathcal{C}$ un $[n, k]$ código lineal sobre $\mathbb{F}_{q_0}$, y sean $\mathbf{w}_{\min}$ y $\mathbf{w}_{\max}$ los pesos distintos de cero mínimo y máximo de $\mathcal{C}$, respectivamente. Si*

$$\frac{\mathbf{w}_{\min}}{\mathbf{w}_{\max}} > \frac{q_0 - 1}{q_0},$$

entonces $\mathcal{C}$ es mínimo.

Es importante notar que la condición en el lema anterior es solo una condición suficiente. Existen códigos mínimos que no satisfacen dicha condición (ver por ejemplo [69]).

Ahora bien, estamos en condiciones para calcular la estructura de cobertura para los códigos de subcampo del Teorema 10.

Teorema 11. *Suponga la misma notación que en el Teorema 10. Entonces, la estructura de cobertura para un código de subcampo de la forma $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ está dada de la siguiente manera:*

(a) *Si* $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ *pertenece a la Parte* (A) *del Teorema 10, entonces todas sus palabras de código distintas de cero con peso de Hamming* $q_0^{2r}-1$ *no son mínimas, mientras que las otras palabras de código distintas de cero son mínimas.*

(b) *Si* $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ *pertenece a la Parte* (B) *del Teorema 10, entonces el código es mínimo.*

Demostración. Parte (a): Claramente, todas las palabras de código distintas de cero con peso de Hamming $q_0^{2r}-1$ no son mínimas pues la longitud de $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ es $q_0^{2r}-1$ (ver Teorema 10). Ahora bien, debido a que $2r>2$, no es difícil verificar que

$$q_0^{2r-1}(q_0-1) \leq \frac{q_0^{2r+1}-q_0^{2r}-2q_0+1}{q_0-1}\,.$$

Y como $q_0^{2r-1}(q_0-1)-1 < q_0^{2r-1}(q_0-1)$, la afirmación de la Parte (a) se sigue del Lema 5.

Parte (b): Sean $\mathbf{w}_{\min}$ y $\mathbf{w}_{\max}$ como en el Lema 6. Entonces, de (2.5), $\mathbf{w}_{\min} = q_0^{r-1}(q_0^{r+1}-q_0^r-1)$ y $\mathbf{w}_{\max} = q_0^{r-1}(q_0-1)(q_0^r+1)$. El resultado se sigue directamente del Lema 6. □

Los códigos mínimos se prestan para construir esquemas de compartición de secretos con buenas estructuras de acceso tal como se describe en la siguiente:

Proposición 1 ([69, Proposición 2])**.** *Sea* $\mathcal{C}$ *un* $[n,k]$ *código lineal sobre* $\mathbb{F}_{q_0}$ *y sea* $G=(\boldsymbol{g}_0,\boldsymbol{g}_1,\ldots,\boldsymbol{g}_{n-1})$ *una matriz generadora de* $\mathcal{C}$ *tal que* $\boldsymbol{g}_i$ *es el* i*-ésimo vector columna de* G *y* $\boldsymbol{g}_i \neq 0$ *para* $0\leq i\leq n-1$*. Si* $\mathcal{C}$ *es mínimo, entonces la estructura de acceso del esquema de compartición de secretos basado en* $\mathcal{C}$ *está compuesta de* q_0^{k-1} *conjuntos de acceso mínimo, que es igual al conjunto de soportes de acceso de las palabras de código distintas de cero en* $\mathcal{C}$ *cuya primera coordenada es igual a* 1*. Además se tiene que:*

(a) *Si* $\boldsymbol{g}_i$ *es un múltiplo escalar de* $\boldsymbol{g}_0$*,* $1\leq i\leq n-1$*, entonces el participante* P_i *debe estar en cada conjunto de acceso mínimo. Tal participante es llamado* dictatorial*.*

(b) *Si* $\boldsymbol{g}_i$ *no es un múltiplo escalar de* $\boldsymbol{g}_0$*,* $1\leq i\leq n-1$*, entonces el participante* P_i *debe estar en* $(q_0-1)q_0^{k-2}$ *de los* q_0^{k-1} *conjuntos de acceso mínimo totales. Bajo estas condiciones, el esquema de compartición de secretos es llamado* democrático*.*

Finalizamos esta sección presentando un ejemplo específico de un esquema de compartición de secretos basado en uno de los códigos de subcampo del Teorema 10.

Ejemplo 6. Sean $(q_0,r,e_1,e_2)=(2,2,1,1)$. Entonces $q=4$ y, por el Ejemplo 5 (b), sabemos que el código de subcampo $\mathcal{C}^{(2)}_{(4,2,1,1)}$ es un $[15,6,6]$ código cíclico binario de tres pesos con enumerador de pesos $1+30z^6+15z^8+18z^{10}$. Considere el campo finito $\mathbb{F}_{16}=\mathbb{F}_2(\gamma)$ con $\gamma^4+\gamma+1=0$. Con esta elección, y utilizando la notación de la Observación 7, $h_5(x)=x^2+x+1$ y $h_1(x)=x^4+x^3+1$. Por lo tanto, $(x^{15}-1)/(h_5(x)h_1(x))=x^9+x^6+x^5+x^4+x+1$ y $h_5(x)h_1(x)=x^6+x^3+x^2+x+1$ son los polinomios generador y de chequeo de paridad de $\mathcal{C}^{(2)}_{(4,2,1,1)}$, respectivamente.

En consecuencia, las matrices generadoras, G y $G^{\perp}$, para $\mathcal{C}^{(2)}_{(4,2,1,1)}$ y su código dual son:

$$G=\begin{bmatrix} 1\,1\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,1\,1\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,0\,0\,1 \end{bmatrix}, \quad G^{\perp}=\begin{bmatrix} 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0 \end{bmatrix}.$$

De este modo, en el esquema de compartición de secretos basado en $\mathcal{C}^{(2)}_{(4,2,1,1)}$, 14 participantes y un repartidor están involucrados. Por el Lema 4, la Parte (b) del Teorema 11 y la Proposición 1, hay un total de $q_0^{k-1} = 2^5 = 32$ conjuntos de acceso mínimo, a saber:

$$\{4,5,6,7,8,9,11,12,13\}, \{1,2,3,4,6,7,8,10,14\}, \{1,4,10,11,14\}, \{2,5,7,8,13\},$$
$$\{2,3,4,6,10,11,12,13,14\}, \{1,2,3,7,10,11,13\}, \{5,7,9,12,14\}, \{6,7,10,11,12\},$$
$$\{1,2,4,5,6,8,12,13,14\}, \{1,2,4,8,9,10,11,12,13\}, \{1,2,5,11,12\}, \{1,4,5,6,9\},$$
$$\{1,3,4,5,7,11,12,13,14\}, \{1,3,4,6,7,9,10,12,13\}, \{2,4,7,9,10\}, \{1,6,8,10,13\},$$
$$\{1,3,7,8,9,10,11,12,14\}, \{1,2,3,5,6,7,9,13,14\}, \{2,3,8,10,12\}, \{3,9,10,13,14\},$$
$$\{2,3,5,6,8,9,11,12,14\}, \{2,6,7,8,9,10,11,13,14\}, \{3,4,5,8,14\}, \{3,5,6,11,13\},$$
$$\{1,2,3,4,5,7,8,9,11\}, \{1,3,5,6,7,8,12\}, \{3,4,6,8,9,10,11\}, \{2,4,5,6,7,11,14\},$$
$$\{4,7,8,10,12,13,14\}, \{1,2,6,9,10,12,14\}, \{1,5,8,9,11,13,14\}, \{2,3,4,5,9,12,13\}\,.$$

Más aún, de acuerdo con la Parte (b) de la Proposición 1, note que cualquier participante P_i $(1 \leq i \leq 14)$ aparece en $(q_0-1)q_0^{k-2} = 16$ de los $q_0^{k-1} = 32$ conjuntos de acceso mínimo totales. Es decir, el esquema de compartición de secretos construido es democrático.

Para apreciar el uso de los conjuntos de acceso mínimo, suponga que deseamos "dividir" un secreto $\mathbf{s}$ de 4 bits, en partes de 4 bits, para catorce participantes $P_1, P_2, \ldots, P_{14}$. Siguiendo [47], $\mathbf{s} \in \mathrm{GF}(2^4) = \mathbb{F}_{16} := \{0,1,2,\ldots,9,a,b,c,d,e,f\}$ y suponga que $\mathbf{s} = b = [1011]$. El repartidor elige al azar cuatro palabras de código $\mathbf{c}_1$, $\mathbf{c}_2$, $\mathbf{c}_3$ y $\mathbf{c}_4$ en el dual de $\mathcal{C}^{(2)}_{(4,2,1,1)}$, con la condición de que cada bit en el secreto $\mathbf{s}$ coincida con la primera coordenada de una de estas cuatro palabras de código. Supongamos que la elección del repartidor es:

$$\begin{aligned} \mathbf{c}_1 &= [100101110111111]\,, \\ \mathbf{c}_2 &= [000000000000000]\,, \\ \mathbf{c}_3 &= [100010111101011]\,, \\ \mathbf{c}_4 &= [110100100100010]\,. \end{aligned}$$

Por medio de estas palabras de código, el repartidor procede a generar las partes de 4 bits para los catorce participantes:

1	0	0	1	0	1	1	1	0	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	1	1	1	1	0	1	0	1	1
1	1	0	1	0	0	1	0	0	1	0	0	0	1	0
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
b	1	0	9	2	8	b	a	2	b	8	a	8	b	a
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
$\mathbf{s}$	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}

De esta forma, la parte del participante P_1 es 1, la del participante P_2 es 0 y así sucesivamente. Finalmente, note que cualquiera de los conjuntos de acceso mínimo anteriores puede recuperar el secreto $\mathbf{s} = b$. Por ejemplo, al usar las partes del conjunto de acceso mínimo $\{1, 4, 5, 6, 9\}$, obtenemos $1 + 2 + 8 + b + b = b$.

2.5 Una clase de códigos lineales óptimos de dos pesos

A través del siguiente resultado presentamos una clase de códigos lineales óptimos de dos pesos, definidos sobre cualquier campo finito, cuyos duales son casi óptimos.

Teorema 12. *Sea $\widehat{\mathcal{C}}_{(q,m,e_1,e_2)}$ el código extendido (ver Sección 1.3.2) del código cíclico $\mathcal{C}_{(q,m,e_1,e_2)}$ en el Teorema 9. Si $e_1 = 0$ (ver Observación 6), entonces el código extendido $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$ es un $[q^m, m+1, q^{m-1}(q-1)]$ código lineal óptimo c.r.a Griesmer, de dos pesos sobre $\mathbb{F}_q$, con enumerador de pesos*

$$1 + q(q^m - 1)z^{q^{m-1}(q-1)} + (q-1)z^{q^m} \ . \tag{2.7}$$

Más aún, si $q > 2$, entonces $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$ es proyectivo y su dual $\widehat{\mathcal{C}}^{\perp}_{(q,m,0,e_2)}$ es un código lineal casi óptimo c.r.a Hamming con parámetros $[q^m, q^m - m - 1, 3]$.

Demostración. Recordemos que cada palabra de código en el código cíclico $\mathcal{C}_{(q,m,0,e_2)}$ es de la forma

$$\mathbf{c}(a,b) = \left(a + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(bx^{e_2}\right)\right)_{x \in \mathbb{F}^*_{q^m}} \qquad \text{con } a \in \mathbb{F}_q \text{ y } b \in \mathbb{F}_{q^m} \ .$$

Para cada palabra de código $\mathbf{c}(a,b)$ en $\mathcal{C}_{(q,m,0,e_2)}$, sea $\widehat{\mathbf{c}}(a,b)$ la palabra de código extendida correspondiente en $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$.

A continuación determinamos los parámetros y el enumerador de pesos para $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$. Por definición, el código extendido $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$ tiene longitud $q^m - 1 + 1 = q^m$ y la misma dimensión que $\mathcal{C}_{(q,m,0,e_2)}$. Más aún, en los [29, Teoremas 7 y 11] se demostró que el peso de Hamming de una palabra de código en $\mathcal{C}_{(q,m,0,e_2)}$ está dado por

$$w_H(\mathbf{c}(a,b)) = \begin{cases} 0 & \text{si } a = b = 0, \\ q^m - 1 & \text{si } a \neq 0 \text{ y } b = 0, \\ q^{m-1}(q-1) & \text{si } a = 0 \text{ y } b \neq 0, \\ q^{m-1}(q-1) - 1 & \text{si } (a,b) \neq (0,0). \end{cases}$$

Así pues, para obtener el enumerador de pesos para $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$ calcularemos la suma de coordenadas de una palabra de código $\mathbf{c}(a,b)$ en cada uno de los casos anteriores. Primero, note que

$$\sum_{x\in\mathbb{F}_{q^m}^*} a = (q^m-1)a \equiv -a \pmod{q}\ .$$

También, como $\gcd(\frac{q^m-1}{q-1}, e_2) = 1$ y $\gcd(q-1,e_2)=1$, tenemos que $\gcd(q^m-1,e_2)=1$. Entonces,

$$\sum_{x\in\mathbb{F}_{q^m}^*} \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(bx^{e_2}) = \sum_{x\in\mathbb{F}_{q^m}^*} \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(bx) = q^{m-1}\sum_{x\in\mathbb{F}_q^*} x = 0\ .$$

Por lo tanto,

$$\sum_{x\in\mathbb{F}_{q^m}^*} \left(a + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(bx^{e_2})\right) = \begin{cases} 0 & \text{si } a=b=0,\\ -a & \text{si } a\neq 0 \text{ y } b=0,\\ 0 & \text{si } a=0 \text{ y } b\neq 0,\\ -a & \text{si } (a,b)\neq(0,0).\end{cases}$$

En consecuencia,

$$w_H(\widehat{\mathbf{c}}(a,b)) = \begin{cases} 0 & \text{si } a=b=0,\\ q^m & \text{si } a\neq 0 \text{ y } b=0,\\ q^{m-1}(q-1) & \text{si } a=0 \text{ y } b\neq 0,\\ q^{m-1}(q-1) & \text{si } (a,b)\neq(0,0).\end{cases}$$

Más aún, puesto que $A_{q^m-1}(\mathcal{C}_{(q,m,0,e_2)}) = (q-1)$ (ver (2.2)), podemos concluir que $A_{q^m}(\widehat{\mathcal{C}}_{(q,m,0,e_2)}) = (q-1)$. También, como $A_{q^{m-1}(q-1)}(\mathcal{C}_{(q,m,0,e_2)}) = (q^m-1)$ y $A_{q^{m-1}(q-1)-1}(\mathcal{C}_{(q,m,0,e_2)}) = (q^m-1)(q-1)$, obtenemos que

$$A_{q^{m-1}(q-1)}(\widehat{\mathcal{C}}_{(q,m,0,e_2)}) = (q^m-1)+(q^m-1)(q-1) = q(q^m-1)\ .$$

Esto completa la prueba de los parámetros y el enumerador de pesos del código $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$.

Ahora bien, observe que

$$\begin{aligned}&\left\lceil\frac{q^{m-1}(q-1)}{q^0}\right\rceil + \left\lceil\frac{q^{m-1}(q-1)}{q}\right\rceil + \cdots + \left\lceil\frac{q^{m-1}(q-1)}{q^m}\right\rceil\ ,\\ &= (q^m-q^{m-1})+(q^{m-1}-q^{m-2})+\cdots+(q-1)+1 = q^m\ ,\end{aligned}$$

lo cual implica que $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$ es óptimo c.r.a Griesmer (ver Teorema 1). Además, utilizando (2.7) y las primeras cuatro identidades de Pless, tenemos que $A_j(\widehat{\mathcal{C}}^{\perp}_{(q,m,0,e_2)}) = 0$, con $j\in\{1,2\}$, y

$$A_3(\widehat{\mathcal{C}}^{\perp}_{(q,m,0,e_2)}) = \frac{q^m(q^m-1)(q-1)(q-2)}{6}\ .$$

Como $q>2$, concluimos que $\widehat{\mathcal{C}}^{\perp}_{(q,m,0,e_2)}$ es un $[q^m, q^m-m-1, 3]$ código lineal y, en consecuencia, $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$ es proyectivo. Finalmente, por la cota de Hamming, no es difícil verificar que para un código de longitud q^m y dimensión q^m-m-1, su distancia mínima puede ser a lo más 4. Por tanto, el código $\widehat{\mathcal{C}}^{\perp}_{(q,m,0,e_2)}$ es casi óptimo. □

Observación 9. Muy recientemente se presentó en el [24, Teorema 6.3] una clase de códigos lineales óptimos, proyectivos y de dos pesos, con los mismos parámetros y distribución de pesos que los códigos del Teorema 12. Sin embargo, a diferencia de lo realizado aquí, esta clase de códigos se obtiene considerando un tipo particular de cuasiconjuntos de diferencia. Más aún, al final de la [24, Sección VI] el autor afirma correctamente que el código extendido de cualquier código cíclico en el Teorema 9 tiene parámetros $[q^m, m+1, q^{m-1}(q-1)-1]$ y tres pesos distintos de cero. Estos códigos de tres pesos no son óptimos. Sin embargo, al permitir $e_1 = 0$ en el Teorema 9, el Teorema 12 nos muestra que el código extendido obtenido es un código lineal de dos pesos el cual resulta óptimo.

Ejemplo 7. Los siguientes son algunos ejemplos del teorema anterior.

(a) Sean $(q, m, e_2) = (3, 2, 1)$. Entonces, por el Teorema 12, el código extendido $\widehat{\mathcal{C}}_{(3,2,0,1)}$ es un $[9, 3, 6]$ código lineal óptimo de dos pesos sobre $\mathbb{F}_3$ con enumerador de pesos

$$1 + 24z^6 + 2z^9 \ ,$$

mientras que su dual es un $[9, 6, 3]$ código lineal casi óptimo c.r.a Hamming.

(b) Sean $(q, m, e_2) = (4, 2, 8)$. Entonces, por el Teorema 12, el código extendido $\widehat{\mathcal{C}}_{(4,2,0,8)}$ es un $[16, 3, 12]$ código lineal óptimo de dos pesos sobre $\mathbb{F}_4$ con enumerador de pesos

$$1 + 60z^{12} + 3z^{16} \ ,$$

mientras que su dual es un $[16, 13, 3]$ código lineal casi óptimo c.r.a Hamming.

(c) Sean $(q, m, e_2) = (5, 3, 9)$. Entonces, por el Teorema 12, el código extendido $\widehat{\mathcal{C}}_{(5,3,0,9)}$ es un $[125, 4, 100]$ código lineal óptimo de dos pesos sobre $\mathbb{F}_5$ con enumerador de pesos

$$1 + 620z^{100} + 4z^{125} \ ,$$

mientras que su dual es un $[125, 121, 3]$ código lineal casi óptimo c.r.a Hamming.

(d) Sean $(q, m, e_2) = (3, 5, 7)$. Entonces, por el Teorema 12, el código extendido $\widehat{\mathcal{C}}_{(3,5,0,7)}$ es un $[243, 6, 162]$ código lineal óptimo de dos pesos sobre $\mathbb{F}_3$ con enumerador de pesos

$$1 + 726z^{162} + 2z^{243} \ ,$$

mientras que su dual es un $[243, 237, 3]$ código lineal casi óptimo c.r.a Hamming.

Observación 10. De acuerdo con las tablas de códigos mantenidas en [21], todos los códigos duales del ejemplo anterior son óptimos.

Se sabe que los códigos lineales proyectivos de dos pesos están estrechamente relacionados con espacios proyectivos finitos y grafos fuertemente regulares. Lo que es notable es que los resultados de un área se pueden trasladar inmediatamente a las otras dos (ver [8]). A continuación utilizamos los códigos lineales proyectivos de dos pesos del Teorema 12 para determinar los grafos fuertemente regulares asociados a ellos.

Un *grafo* es un conjunto V de vértices provistos de una relación simétrica $\sim$ en V llamada *adyacencia*, tal que ningún $v \in V$ es adyacente a sí mismo. Un par de vértices adyacentes $v_1, v_2 \in V$ forman una *arista* y, bajo estas condiciones, se dice que v_1 es un *vecino* de v_2 y viceversa.

Sean N, K, λ y μ enteros. Se dice que un grafo con N vértices es *fuertemente regular* con parámetros (N, K, λ, μ) si es regular de grado K (es decir, cada vértice tiene exactamente K vecinos), y cualesquiera dos vértices distintos tienen λ vecinos comunes si son adyacentes y μ vecinos comunes si no son adyacentes.

Calderbank y Kantor [8] propusieron una manera de construir grafos fuertemente regulares utilizando códigos lineales proyectivos de dos pesos. Sean $\mathbf{w}_1$ y $\mathbf{w}_2$ los pesos de un código lineal q-ario proyectivo de dos pesos, $\mathcal{C}$, de longitud n y dimensión k con matriz generadora G. Al código $\mathcal{C}$ le asociamos un grafo de la siguiente manera. Tome como vértices los elementos del espacio vectorial $\mathbb{F}_q^k$, donde dos vértices distintos v_1 y v_2 son adyacentes sii $v_1 - v_2$ es un múltiplo de alguna columna en G. El grafo obtenido de esta manera es fuertemente regular [8, Teoremas 3.1 y 3.2] con los siguientes parámetros [8, Corolario 3.7]:

$$\begin{aligned} N = q^k,\ K = n(q-1),\ \mu = \frac{q^2\mathbf{w}_1\mathbf{w}_2}{q^k}\ , \\ \lambda = K^2 + 3K - q(\mathbf{w}_1 + \mathbf{w}_2) - Kq(\mathbf{w}_1 + \mathbf{w}_2) + q^2\mathbf{w}_1\mathbf{w}_2\ . \end{aligned} \tag{2.8}$$

Como consecuencia directa de lo anterior, tenemos el siguiente:

Teorema 13. *Asuma la misma notación que en el Teorema 12. Si $q > 2$, entonces el código extendido $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$ genera un grafo fuertemente regular con parámetros $(q^{m+1}, q^m(q-1), q^m(q-2), q^m(q-1))$.*

Demostración. Como $q > 2$, entonces por el Teorema 12, el código extendido $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$ es proyectivo y de dos pesos, a saber, $\mathbf{w}_1 = q^{m-1}(q-1)$ y $\mathbf{w}_2 = q^m$. Además, $\widehat{\mathcal{C}}_{(q,m,0,e_2)}$ tiene longitud $n = q^m$ y dimensión $k = m+1$. Así pues, el resultado se sigue de sustituir los valores anteriores en (2.8). □

Finalizamos este capítulo presentando un ejemplo de la construcción de un grafo fuertemente regular a partir de uno de los códigos extendidos del Teorema 12.

Ejemplo 8. Sean $(q, m, e_2) = (3, 2, 1)$. Del Ejemplo 7 (a) sabemos que el código extendido $\widehat{\mathcal{C}}_{(3,2,0,1)}$ es un $[9, 3, 6]$ código lineal proyectivo de dos pesos sobre $\mathbb{F}_3$. Además, por el Teorema 13, el código $\widehat{\mathcal{C}}_{(3,2,0,1)}$ genera un grafo fuertemente regular con parámetros $(27, 18, 9, 18)$. Ahora bien, para construir dicho grafo necesitamos una matriz generadora para $\widehat{\mathcal{C}}_{(3,2,0,1)}$. Como $\mathcal{C}_{(3,2,0,1)}$ es cíclico, no es difícil verificar que una matriz generadora para este código está dada por

$$G = \begin{bmatrix} 2\,1\,2\,2\,0\,1\,0\,0 \\ 0\,2\,1\,2\,2\,0\,1\,0 \\ 0\,0\,2\,1\,2\,2\,0\,1 \end{bmatrix}\ .$$

Más aún, se sabe que una matriz generadora para $\widehat{\mathcal{C}}_{(3,2,0,1)}$ se puede obtener a partir de cualquier matriz generadora de $\mathcal{C}_{(3,2,0,1)}$ al agregar una columna adicional de modo que la suma de los elementos de cada fila sea igual a 0 (ver [34, p. 15]). Por lo tanto,

$$\widehat{G} = \begin{bmatrix} 2\,1\,2\,2\,0\,1\,0\,0\,1 \\ 0\,2\,1\,2\,2\,0\,1\,0\,1 \\ 0\,0\,2\,1\,2\,2\,0\,1\,1 \end{bmatrix} \tag{2.9}$$

es una matriz generadora para $\widehat{\mathcal{C}}_{(3,2,0,1)}$.

Siguiendo el método descrito anteriormente, los vértices del grafo son los 27 vectores de $\mathbb{F}_3^3 = \{000, 001, 002, \ldots, 222\}$. Asimismo, dos vértices distintos son adyacentes sii su diferencia es un múltiplo de alguna columna en $\widehat{G}$. La Figura 2.1 muestra el grafo fuertemente regular obtenido de esta manera a partir del código extendido $\widehat{\mathcal{C}}_{(3,2,0,1)}$. El grafo se generó utilizando Maple 17.

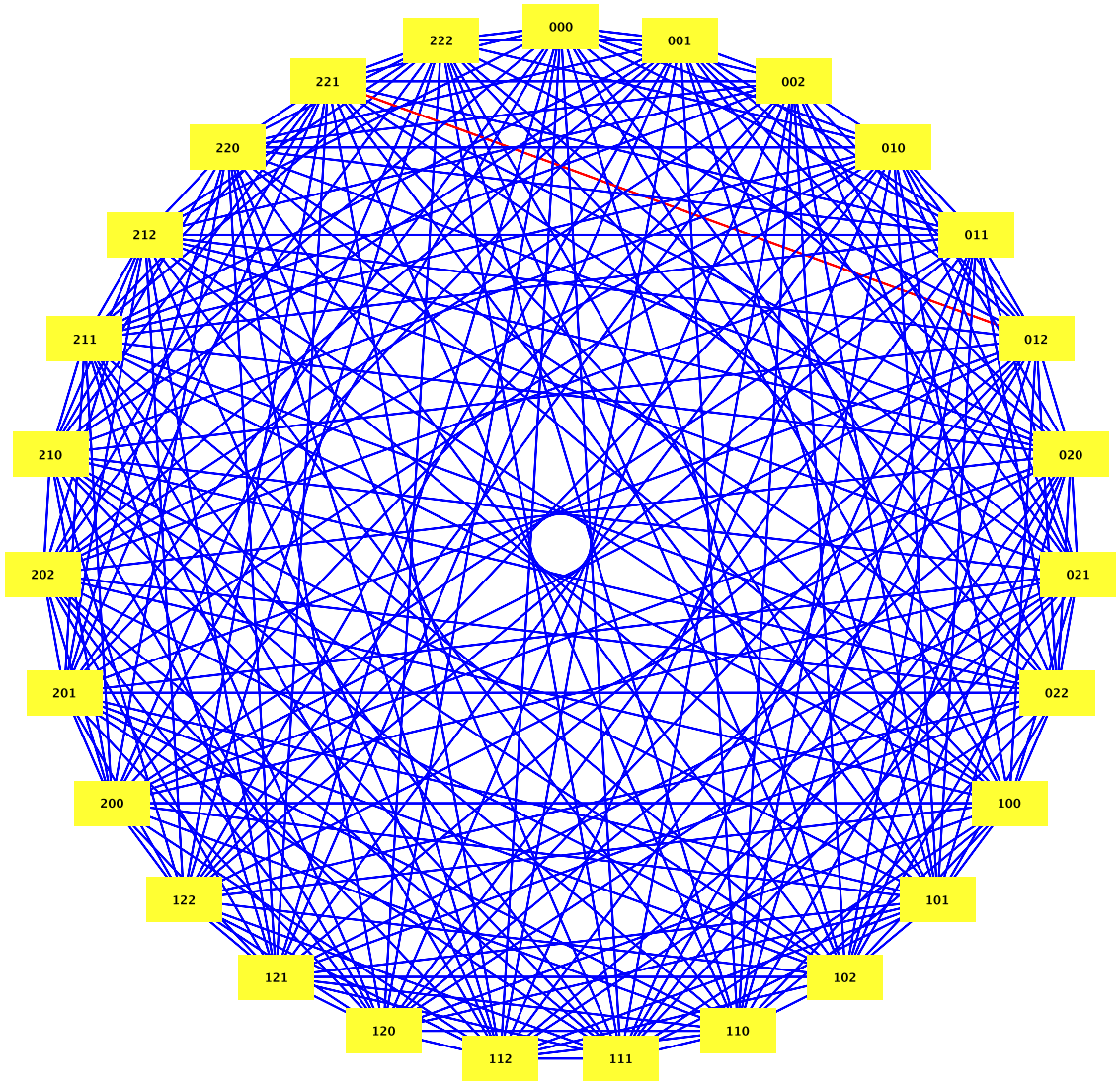

Figura 2.1: El grafo fuertemente regular con parámetros $(27, 18, 9, 18)$ obtenido a partir del código extendido $\widehat{\mathcal{C}}_{(3,2,0,1)}$. Los vértices 012 y 221 son adyacentes o vecinos ya que $2(012 - 221) = 212$ aparece en la tercera columna de la matriz $\widehat{G}$ en (2.9). Por el contrario, los vértices 012 y 000 no son adyacentes pues la diferencia $012 - 000 = 012$ no aparece como un múltiplo de alguna columna en dicha matriz.

Capítulo 3

La distribución de pesos completa de una subclase de códigos cíclicos óptimos de tres pesos

La distribución de pesos de un código es investigada generalmente con base en el peso de Hamming, bajo el cual todos los componentes distintos de cero de una palabra de código se consideran idénticos. Para describir la estructura de códigos no binarios con más detalle, cada componente distinto de cero debe distinguirse de los demás y esto se hace a través de la distribución de pesos completa. Sin embargo, obtener la distribución de pesos completa de códigos no binarios es un problema aún más difícil que obtener su distribución de pesos de Hamming. Por tal motivo, la distribución de pesos completa es desconocida para la mayoría de los códigos. Recientemente, las distribuciones de pesos completas de dos clases de códigos cíclicos p-arios fueron reportadas por Heng y Yue [30]. El propósito de este capítulo es presentar la distribución de pesos completa para una subclase de los códigos cíclicos óptimos de tres pesos del Teorema 9 cuando $m = 2$. Los resultados de este capítulo fueron publicados en [61].

3.1 Introducción

La distribución de pesos completa de un código enumera las palabras de código por el número de símbolos de cada tipo contenidos en cada palabra de código. Por tal motivo, la distribución de pesos completa de un código contiene mucha más información que su distribución de pesos de Hamming. De hecho, la distribución de pesos completa tiene una amplia gama de aplicaciones en muchos campos de investigación debido a que la información que contiene es de uso vital tanto en la práctica como en la teoría. Por ejemplo, como se señala en [5], los enumeradores de pesos completos de los códigos Reed-Solomon podrían ser de utilidad en la decodificación por decisión suave. Como otro ejemplo, el enumerador de pesos completo también resulta útil en el cálculo de la transformada de Walsh de funciones monomiales sobre campos finitos [22]. Desafortunadamente, obtener la distribución de pesos completa es un problema aún más difícil que obtener la distribución de pesos de Hamming. Como consecuencia, la distribución de pesos completa es desconocida para la mayoría de los códigos.

Por esta razón, determinar los enumeradores de pesos completos de códigos li-

neales o cíclicos sobre campos finitos ha recibido mucha atención en los últimos años (ver por ejemplo [2, 11, 37, 39, 65, 66, 68, 71, 73]). Cabe señalar que, para un campo primo $\mathbb{F}_p$, varias clases de códigos lineales p-arios de tres pesos, junto con sus distribuciones de pesos completas, fueron presentadas en [35, 67, 68, 71, 73]. Por otro lado, para códigos cíclicos, las distribuciones de pesos completas de dos clases de códigos cíclicos p-arios fueron recientemente calculadas en [30]. De hecho, las distribuciones de pesos de Hamming para estas dos clases de códigos cíclicos p-arios fueron previamente reportadas en [42, 72]. Así pues, el objetivo principal de este capítulo es calcular la distribución de pesos completa para una subclase de los códigos cíclicos óptimos de tres pesos del Teorema 9 cuando $m = 2$. Como resultado secundario, extendemos la clase de códigos cíclicos óptimos de cinco pesos presentada recientemente en el [27, Teorema 6].

Este capítulo está organizado de la siguiente manera: En la Sección 3.2 establecemos la notación que utilizaremos a lo largo de este capítulo y estudiamos una clase de sumas exponenciales que será importante para determinar, en la Sección 3.3, la distribución de pesos completa para la subclase de códigos cíclicos óptimos de tres pesos que nos interesa. Por último, como resultado secundario de las sumas exponenciales estudiadas en la Sección 3.2, en la Sección 3.4 extendemos la clase de códigos cíclicos óptimos de cinco pesos presentada recientemente en el [27, Teorema 6].

3.2 Notación y una clase de sumas exponenciales

A lo largo de este capítulo utilizaremos la siguiente:

Notación. Sea q una potencia de un número primo y γ un elemento primitivo de $\mathbb{F}_{q^2}$. Sea $\delta := \gamma^{q+1}$ y note que, en consecuencia, δ es un elemento primitivo de $\mathbb{F}_q$. Para cualquier entero α, sea $h_\alpha(x) \in \mathbb{F}_q[x]$ el polinomio mínimo de $\gamma^{-\alpha}$. Para enteros $\alpha_1, \alpha_2, \ldots, \alpha_\ell$, tal que $h_{\alpha_i}(x) \neq h_{\alpha_j}(x)$ si $1 \leq i \neq j \leq \ell$, $\mathcal{C}_{(\alpha_1,\alpha_2,\ldots,\alpha_\ell)}$ denotará el código cíclico de longitud q^2-1 sobre $\mathbb{F}_q$, cuyo polinomio de chequeo de paridad es $h_{\alpha_1}(x)h_{\alpha_2}(x)\cdots h_{\alpha_\ell}(x)$.

En esta sección estudiamos una clase de sumas exponenciales que será importante para determinar la distribución de pesos completa para la subclase de códigos cíclicos óptimos de tres pesos que nos interesa.

Lema 7. *Sean χ' y χ los caracteres aditivos canónicos de $\mathbb{F}_{q^2}$ y $\mathbb{F}_q$, respectivamente. Para enteros cualesquiera e_1, e_2 y e_3, y para todo $a, b \in \mathbb{F}_q$ y $c \in \mathbb{F}_{q^2}$, considere la suma exponencial*

$$S_{(e_1,e_2,e_3)}(a,b,c) := \sum_{x \in \mathbb{F}_{q^2}^*} \chi(ax^{(q+1)e_1} + bx^{(q+1)e_2})\chi'(cx^{e_3}) \, .$$

Si $c \neq 0$ y $\gcd(q+1, e_3) = 1$, entonces

$$S_{(e_1,e_2,e_3)}(a,b,c) = -\sum_{z \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q^*} \chi(z + ax^{e_1} + bx^{e_2} + z^{-1}c^{q+1}x^{e_3}) \, .$$

Demostración. Como $\mathbb{F}_{q^2}^* = \bigcup_{i=0}^{q-2} \gamma^i \langle \gamma^{q-1} \rangle$ y $\delta := \gamma^{q+1}$, tenemos que

$$S_{(e_1,e_2,e_3)}(a,b,c) = \sum_{i=0}^{q-2} \chi(a\delta^{ie_1} + b\delta^{ie_2}) \sum_{w\in\gamma^i\langle\gamma^{q-1}\rangle} \chi'(cw^{e_3}) \ .$$

Más aún, debido a que $\gcd(q+1, e_3) = 1$,

$$\sum_{w\in\gamma^i\langle\gamma^{q-1}\rangle} \chi'(cw^{e_3}) = \sum_{w\in\langle\gamma^{q-1}\rangle} \chi'(c\gamma^{ie_3}w) = \frac{1}{q-1} \sum_{w\in\mathbb{F}_{q^2}^*} \chi'(c\gamma^{ie_3}w^{q-1}) \ ,$$

donde la última igualdad se cumple por el Lema 2. Sea $\psi \in \widehat{\mathbb{F}}_q$, $\mathrm{N} = \mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$, $\psi' = \psi \circ \mathrm{N}$ un levantamiento de ψ a $\mathbb{F}_{q^2}$ y ψ'_0 el caracter multiplicativo trivial de $\mathbb{F}_{q^2}$. Así pues, por el Teorema 6, obtenemos

$$\begin{aligned}
\sum_{w\in\mathbb{F}_{q^2}^*} \chi'(c\gamma^{ie_3}w^{q-1}) = & -1 + \sum_{w\in\mathbb{F}_{q^2}} \chi'(c\gamma^{ie_3}w^{q-1}) \ , \\
&= G_{\mathbb{F}_{q^2}}(\psi'_0, \chi') + \sum_{j=1}^{q-2} G_{\mathbb{F}_{q^2}}(\psi'^j, \chi')\bar{\psi}'^j(c\gamma^{ie_3}) \ , \\
&= \sum_{\psi\in\widehat{\mathbb{F}}_q} G_{\mathbb{F}_{q^2}}(\psi\circ\mathrm{N}, \chi')\bar{\psi}(\mathrm{N}(c\gamma^{ie_3})) \ , \\
&= -\sum_{\psi\in\widehat{\mathbb{F}}_q} G_{\mathbb{F}_q}(\psi, \chi)^2\bar{\psi}(\mathrm{N}(c\gamma^{ie_3})) \ ,
\end{aligned}$$

donde la última igualdad se cumple debido al Teorema 5. En consecuencia, como $\gamma^{i(q+1)} = \mathrm{N}(\gamma^i) = \mathrm{N}(\gamma)^i = \delta^i$ y $\langle\delta\rangle = \mathbb{F}_q^*$, tenemos que

$$S_{(e_1,e_2,e_3)}(a,b,c) = -\frac{1}{q-1} \sum_{x\in\mathbb{F}_q^*} \chi(ax^{e_1} + bx^{e_2}) \sum_{\psi\in\widehat{\mathbb{F}}_q} G_{\mathbb{F}_q}(\psi, \chi)^2\bar{\psi}(c^{q+1}x^{e_3}) \ . \tag{3.1}$$

Por otro lado, utilizando (1.8), tenemos que para todo $x, z \in \mathbb{F}_q^*$:

$$\chi(z^{-1}c^{q+1}x^{e_3}) = \frac{1}{q-1} \sum_{\psi\in\widehat{\mathbb{F}}_q} G_{\mathbb{F}_q}(\psi, \chi)\psi(z)\bar{\psi}(c^{q+1}x^{e_3}) \ .$$

Multiplicando ambos lados de la ecuación anterior por $\chi(z)$ y sumando obtenemos

$$\sum_{z\in\mathbb{F}_q^*} \chi(z + z^{-1}c^{q+1}x^{e_3}) = \frac{1}{q-1} \sum_{\psi\in\widehat{\mathbb{F}}_q} G_{\mathbb{F}_q}(\psi, \chi)^2\bar{\psi}(c^{q+1}x^{e_3}) \ .$$

El resultado se obtiene al sustituir la ecuación anterior en (3.1). □

Lema 8. *Con la misma notación, considere la suma exponencial de la forma:*

$$T_{(e_1,e_2,e_3)}(a,b,c) := \sum_{y\in\mathbb{F}_q^*} S_{(e_1,e_2,e_3)}(ya, yb, yc) \ .$$

Si $c \neq 0$, $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2 - e_1) = 1$ *y* $e_3 \equiv e_1 + e_2 \pmod{q-1}$, *entonces*

$$T_{(e_1,e_2,e_3)}(a,b,c) = \begin{cases} 1 & \textit{si } a \textit{ o } b \textit{ es cero pero no ambos,} \\ -q^2+q+1 & \textit{si } a,b \in \mathbb{F}_q^* \textit{ y } a = \frac{c^{q+1}}{b}, \\ q+1 & \textit{si } a,b \in \mathbb{F}_q^* \textit{ y } a \neq \frac{c^{q+1}}{b}. \end{cases}$$

Demostración. Supongamos sin pérdida de generalidad que $b \neq 0$. Entonces, por el lema anterior, y ya que $y^{q+1} = y^2$,

$$T_{(e_1,e_2,e_3)}(a,b,c) = -\sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*} \chi(z+(a+bx^{e_2-e_1})x^{e_1}y+z^{-1}c^{q+1}x^{e_1+e_2}y^2)\ . \quad (3.2)$$

Supongamos que q es par. Note que $(a+bx^{e_2-e_1})^2x^{2e_1} = z^{-1}c^{q+1}x^{e_1+e_2}$ sii $z = \frac{c^{q+1}x^{e_2-e_1}}{(a+bx^{e_2-e_1})^2}$, con $x^{e_2-e_1} \in \mathbb{F}_q^* \setminus \{\frac{a}{b}\}$. Pero, como $\gcd(q-1, e_2-e_1) = 1$, la última igualdad se cumple sii $z = \frac{c^{q+1}x}{(a+bx)^2}$, con $x \in \mathbb{F}_q^* \setminus \{\frac{a}{b}\}$. Así pues, aplicando el Teorema 8, tenemos que

$$\begin{aligned} T_{(e_1,e_2,e_3)}(a,b,c) &= 1-q-\sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q} \chi(z+(a+bx^{e_2-e_1})x^{e_1}y+z^{-1}c^{q+1}x^{e_1+e_2}y^2), \\ &= 1-q-q\sum_{x\in\mathbb{F}_q^*\setminus\{\frac{a}{b}\}} \chi\left(\frac{c^{q+1}x}{(a+bx)^2}\right)\ , \\ &= 1-q-q\left(\sum_{x\in\mathbb{F}_q\setminus\{\frac{a}{b}\}} \chi\left(\frac{c^{q+1}x}{(a+bx)^2}\right) - \bar{\delta}_0(a)\right)\ , \\ &= 1-q+\bar{\delta}_0(a)q-q\sum_{x\in\mathbb{F}_q\setminus\{\frac{a}{b}\}} \chi\left(\frac{c^{q+1}x}{(a+bx)^2}\right)\ , \end{aligned}$$

donde $\bar{\delta}_0(a) = 1$ si $a \neq 0$, y 0 en caso contrario. Ahora bien, haciendo el cambio de variable $(a+bx)^{-1} \mapsto w$, con $x \in \mathbb{F}_q \setminus \{\frac{a}{b}\}$ (es decir, $x = \frac{1-aw}{bw}$ con $w \in \mathbb{F}_q^*$), obtenemos

$$\begin{aligned} T_{(e_1,e_2,e_3)}(a,b,c) &= 1-q+\bar{\delta}_0(a)q-q\sum_{w\in\mathbb{F}_q^*} \chi\left(wc^{q+1}\left(\frac{1-aw}{b}\right)\right)\ , \\ &= 1-q+\bar{\delta}_0(a)q-q\left(\sum_{w\in\mathbb{F}_q} \chi\left(\frac{c^{q+1}}{b}w-\frac{c^{q+1}a}{b}w^2\right)-1\right)\ , \\ &= 1+\bar{\delta}_0(a)q-q\sum_{w\in\mathbb{F}_q} \chi\left(\frac{c^{q+1}}{b}w-\frac{c^{q+1}a}{b}w^2\right)\ . \end{aligned}$$

En consecuencia, aplicando el Teorema 8 de nueva cuenta, el caso q par se sigue del siguiente hecho

$$\sum_{w\in\mathbb{F}_q} \chi\left(\frac{c^{q+1}}{b}w-\frac{c^{q+1}a}{b}w^2\right) = \begin{cases} q & \text{si } a = \frac{c^{q+1}}{b}, \\ 0 & \text{en caso contrario.} \end{cases}$$

Ahora bien, supongamos que q es impar y sea

$$f_{x,z} = x^{2e_1}(4z^{-1}c^{q+1}x^{e_1+e_2})^{-1} = (4z^{-1}c^{q+1}x^{e_2-e_1})^{-1} \ .$$

Entonces, de (3.2) y por el Teorema 7, tenemos que $T_{(e_1,e_2,e_3)}(a,b,c)$ es igual a

$$\begin{aligned} &- \sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*} \chi(z-(a+bx^{e_2-e_1})^2 f_{x,z})\eta(z^{-1}c^{q+1}x^{e_1+e_2})G_{\mathbb{F}_q}(\eta,\chi) - \chi(z) \ , \\ &= 1-q-G_{\mathbb{F}_q}(\eta,\chi)\sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*} \chi(z-(a+bx^{e_2-e_1})^2 f_{x,z})\eta(z^{-1}c^{q+1}x^{e_1+e_2}) \ , \\ &= 1-q-G_{\mathbb{F}_q}(\eta,\chi)\sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*} \chi(z-(a+bx^{e_2-e_1})^2 f_{x,z})\eta(z^{-1}c^{q+1}x^{e_2-e_1}) \ , \end{aligned}$$

donde η es el caracter cuadrático de $\mathbb{F}_q$ y la última igualdad se cumple ya que $\eta(x^{-2e_1}) = 1$. Pero $\gcd(q-1, e_2-e_1) = 1$. Entonces, después de aplicar el cambio de variable $z^{-1}c^{q+1}x^{e_2-e_1} \mapsto w$ (es decir, $x^{e_2-e_1} = \frac{wz}{c^{q+1}}$), tenemos que $T_{(e_1,e_2,e_3)}(a,b,c)$ es igual a

$$\begin{aligned} &1-q-G_{\mathbb{F}_q}(\eta,\chi)\sum_{w\in\mathbb{F}_q^*}\eta(w)\sum_{z\in\mathbb{F}_q^*}\chi\left(z-\frac{1}{4w}\left(a+\frac{bwz}{c^{q+1}}\right)^2\right) \ , \\ &= 1-q-G_{\mathbb{F}_q}(\eta,\chi)\sum_{w\in\mathbb{F}_q^*}\eta(w)\sum_{z\in\mathbb{F}_q^*}\chi\left(-\frac{a^2}{4w}+\left(1-\frac{ab}{2c^{q+1}}\right)z-\frac{b^2wz^2}{4c^{2(q+1)}}\right) \ . \end{aligned}$$

Después de aplicar el Teorema 7 de nueva cuenta, obtenemos que $T_{(e_1,e_2,e_3)}(a,b,c)$ es igual a

$$\begin{aligned} &1-q-G_{\mathbb{F}_q}(\eta,\chi)\sum_{w\in\mathbb{F}_q^*}\eta(w)\left[\chi\left(-\frac{a^2}{4w}-\left(1-\frac{ab}{2c^{q+1}}\right)^2\left(-\frac{b^2w}{c^{2(q+1)}}\right)^{-1}\right)\right. \\ &\left.\times\,\eta\left(-\frac{b^2w}{4c^{2(q+1)}}\right)G_{\mathbb{F}_q}(\eta,\chi)-\chi\left(-\frac{a^2}{4w}\right)\right] \ . \end{aligned}$$

Pero, debido a (1.9),

$$G_{\mathbb{F}_q}(\eta,\chi)\eta(w)\eta\left(-\frac{b^2w}{4c^{2(q+1)}}\right)G_{\mathbb{F}_q}(\eta,\chi) = \eta(-1)G_{\mathbb{F}_q}(\eta,\chi)^2 = q \ .$$

Por otro lado, note que $\sum_{w\in\mathbb{F}_q^*}\eta(w)\chi(0) = 0$ (ver (1.7)) y si $a \neq 0$, entonces $\eta(w) = \eta(\frac{a^2}{4w})$. En consecuencia,

$$\begin{aligned} -G_{\mathbb{F}_q}(\eta,\chi)\sum_{w\in\mathbb{F}_q^*}\eta(w)\left(-\chi\left(-\frac{a^2}{4w}\right)\right) &= \bar{\delta}_0(a)G_{\mathbb{F}_q}(\eta,\chi)\sum_{w\in\mathbb{F}_q^*}\eta\left(\frac{a^2}{4w}\right)\chi\left(-\frac{a^2}{4w}\right) \ , \\ &= \bar{\delta}_0(a)G_{\mathbb{F}_q}(\eta,\chi)G_{\mathbb{F}_q}(\eta,\bar{\chi}) = \bar{\delta}_0(a)q \ . \end{aligned}$$

Por lo tanto,

$$T_{(e_1,e_2,e_3)}(a,b,c) = 1 - q + \bar{\delta}_0(a)q - q \sum_{w \in \mathbb{F}_q^*} \chi\left(-\frac{a^2}{4w} + \left(1 - \frac{ab}{2c^{q+1}}\right)^2 \left(\frac{c^{2(q+1)}}{b^2 w}\right)\right) .$$

Aplicando el cambio de variable $\frac{c^{q+1}}{bw} \mapsto v$ (es decir, $w = \frac{c^{q+1}}{bv}$), tenemos que

$$\begin{aligned} T_{(e_1,e_2,e_3)}(a,b,c) &= 1 - q + \bar{\delta}_0(a)q - q \sum_{v \in \mathbb{F}_q^*} \chi\left(-\frac{a^2 bv}{4c^{q+1}} + \left(1 - \frac{ab}{2c^{q+1}}\right)^2 \left(\frac{vc^{q+1}}{b}\right)\right) , \\ &= 1 - q + \bar{\delta}_0(a)q - q \sum_{v \in \mathbb{F}_q^*} \chi\left(\left(\frac{c^{q+1}}{b} - a\right) v\right) . \end{aligned}$$

Finalmente, el resultado se sigue del siguiente hecho (ver (1.3))

$$\sum_{v \in \mathbb{F}_q^*} \chi\left(\left(\frac{c^{q+1}}{b} - a\right) v\right) = \begin{cases} q-1 & \text{si } a = \dfrac{c^{q+1}}{b}, \\ -1 & \text{en caso contrario.} \end{cases}$$

□

Corolario 1. *Asuma la misma notación que en el lema anterior. Si* $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2 - e_1) = 1$ *y* $e_3 \equiv e_1 + e_2 \pmod{q-1}$, *entonces la suma exponencial* $T_{(e_1,e_2,e_3)}(a,b,c)$ *toma seis valores distintos de acuerdo a los siguientes siete casos:*

$$\begin{cases} (q-1)(q^2-1) & \textit{si } c = a = b = 0, & \text{Caso 1,} \\ 1 - q^2 & \textit{si } c = 0 \textit{ y } a \textit{ o } b \textit{ es cero pero no ambos,} & \text{Caso 2,} \\ q+1 & \textit{si } c = 0 \textit{ y } a, b \in \mathbb{F}_q^*, & \text{Caso 3,} \\ 1 - q & \textit{si } c \neq 0 \textit{ y } a = b = 0, & \text{Caso 4,} \\ 1 & \textit{si } c \neq 0 \textit{ y } a \textit{ o } b \textit{ es cero pero no ambos,} & \text{Caso 5,} \\ -q^2 + q + 1 & \textit{si } c \neq 0 \textit{ y } a, b \in \mathbb{F}_q^* \textit{ con } a = \frac{c^{q+1}}{b}, & \text{Caso 6,} \\ q+1 & \textit{si } c \neq 0 \textit{ y } a, b \in \mathbb{F}_q^* \textit{ con } a \neq \frac{c^{q+1}}{b}, & \text{Caso 7.} \end{cases}$$

Demostración. Claramente $T_{(e_1,e_2,e_3)}(0,0,0) = (q-1)(q^2-1)$.

Caso 2: Supongamos sin pérdida de generalidad que $a = 0$ y $b \neq 0$. Note que si $x \in \mathbb{F}_{q^2}^*$, entonces $x^{(q+1)e_2} \in \mathbb{F}_q^*$. Así pues, utilizando (1.3),

$$T_{(e_1,e_2,e_3)}(0,b,0) = \sum_{x \in \mathbb{F}_{q^2}^*} \sum_{y \in \mathbb{F}_q^*} \chi(bx^{(q+1)e_2} y) = \sum_{x \in \mathbb{F}_{q^2}^*} (-1) = -(q^2-1) .$$

Caso 3: Por el Lema 2,

$$\begin{aligned} T_{(e_1,e_2,e_3)}(a,b,0) &= \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^2}^*} \chi(ax^{(q+1)e_1} y + bx^{(q+1)e_2} y) , \\ &= (q+1) \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q^*} \chi(ax^{e_1} y + bx^{e_2} y) . \end{aligned}$$

Aplicando el cambio de variable $x^{e_1}y \mapsto v$ (es decir, $y = \frac{v}{x^{e_1}}$), obtenemos

$$T_{(e_1,e_2,e_3)}(a,b,0) = (q+1)\sum_{v\in\mathbb{F}_q^*}\chi(av)\sum_{x\in\mathbb{F}_q^*}\chi(bvx^{e_2-e_1})\ .$$

Pero $\gcd(q-1, e_2-e_1) = 1$. Entonces, utilizando (1.3), concluimos que

$$T_{(e_1,e_2,e_3)}(a,b,0) = (q+1)\sum_{v\in\mathbb{F}_q^*}\chi(av)\sum_{x\in\mathbb{F}_q^*}\chi(bvx) = (q+1)\ .$$

Caso 4: Como $\mathbb{F}_{q^2}^* = \bigcup_{i=0}^{q}\gamma^i\mathbb{F}_q^*$ y $\gcd(q+1, e_3) = 1$, tenemos que

$$\begin{aligned} T_{(e_1,e_2,e_3)}(0,0,c) &= \sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{q^2}^*}\chi'(cx^{e_3}y) = \sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_q^*}\sum_{i=0}^{q}\chi'(c\gamma^{ie_3}x^{e_3}y)\ , \\ &= \sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\sum_{i=0}^{q}\chi'(cx^{e_3}(\gamma^i y)) = \sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_{q^2}^*}\chi'(cx^{e_3}z) = -(q-1)\ , \end{aligned}$$

donde la última igualdad se cumple por (1.3). La prueba de los casos restantes proviene del lema anterior. □

Resumimos nuestros resultados anteriores a través de la siguiente:

Observación 11. Al considerar la frecuencia de ocurrencia de todos los casos en el corolario anterior, obtenemos la distribución de valores de la suma exponencial

$$Z_{(e_1,e_2,e_3)}(a,b,c) := \frac{q^2-1}{q} + \frac{1}{q}T_{(e_1,e_2,e_3)}(a,b,c)\ .$$

La Tabla 3.1 muestra dicha distribución de valores.

Valor	**Frecuencia**	**Viene del/de los**
q^2-1	1	Caso 1
0	$2(q-1)$	Caso 2
$q+1$	$(q-1)^2(q^2-q-1)$	Casos 3 y 7
$q-1$	q^2-1	Caso 4
q	$2(q^2-1)(q-1)$	Caso 5
1	$(q^2-1)(q-1)$	Caso 6

Tabla 3.1: Distribución de valores de $Z_{(e_1,e_2,e_3)}(a,b,c)$. Aquí $\gcd(q+1,e_3) = 1$, $\gcd(q-1, e_2-e_1) = 1$ y $e_3 \equiv e_1 + e_2 \pmod{q-1}$.

3.3 El enumerador de pesos completo de una subclase de códigos cíclicos óptimos de tres pesos

A través del siguiente resultado obtenemos el enumerador de pesos completo para una subclase de los códigos cíclicos óptimos de tres pesos del Teorema 9 cuando $m = 2$.

Teorema 14. *Para cualesquiera dos enteros e_2 y e_3, sea $\mathcal{C}_{((q+1)e_2,e_3)}$ el código cíclico de longitud q^2-1, sobre $\mathbb{F}_q$, definido por el conjunto:*

$$\mathcal{C}_{((q+1)e_2,e_3)} := \{\mathbf{c}(b,c) : b \in \mathbb{F}_q, c \in \mathbb{F}_{q^2}\} \ ,$$

donde

$$\mathbf{c}(b,c) := \left(b\gamma^{(q+1)ie_2} + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\left(c\gamma^{ie_3}\right)\right)_{i=0}^{q^2-2} \ .$$

Si $\gcd(e_3, q^2-1) = 1$ *y* $e_3 \equiv e_2 \pmod{q-1}$, *entonces* $\mathcal{C}_{((q+1)e_2,e_3)}$ *es un código cíclico óptimo perteneciente al Teorema 9 (tome en el teorema* $m=2$ *y considere la Observación 6) cuyo enumerador de pesos completo es*

$$z_0^{q^2-1} + (q-1)\prod_{i=1}^{q-1} z_i^{q+1} + (q^2-1)z_0^{q-1}\prod_{i=1}^{q-1} z_i^q + (q^2-1)\sum_{j=1}^{q-1} z_0^q z_j \prod_{i=1, i\neq j}^{q-1} z_i^{q+1} \ .$$

Demostración. No es difícil verificar que $\gcd(q-1, 2e_2-e_3) = 1$ y $\gcd(q+1, e_3) = 1$, por tanto, $\mathcal{C}_{((q+1)e_2,e_3)}$ pertenece a la clase de códigos cíclicos óptimos de tres pesos del Teorema 9 (tome en el teorema $m=2$).

Ahora bien, sean $u_0 = 0$ y $u_\ell = \gamma^{(q+1)(\ell-1)}$, con $\ell = 1, 2, \ldots, q-1$. Note que $\{u_0, u_1, \ldots, u_{q-1}\} = \mathbb{F}_q$. Sea $\mathbf{c}(b,c) = (c_0, c_1, \ldots, c_{q^2-2}) \in \mathcal{C}_{((q+1)e_2,e_3)}$ y, para $0 \leq \ell < q$, definamos $w_\ell := w_\ell(\mathbf{c}(b,c)) = \sharp\{0 \leq j < q^2-1 : c_j = u_\ell\}$. Entonces, por definición de enumerador de pesos completo (ver (1.1)), tenemos que

$$\mathrm{CWE}_{\mathcal{C}_{((q+1)e_2,e_3)}} = \sum_{\mathbf{c}(b,c)\in\mathcal{C}_{((q+1)e_2,e_3)}} \mathcal{Z}(\mathbf{c}(b,c)) \ .$$

Sea $\bar{1} = (1, 1, \ldots, 1)$ el vector de longitud q^2-1 cuyas coordenadas son todas iguales a uno. Observe que

$$\begin{aligned} w_\ell &= q^2 - 1 - w_H\left(\mathbf{c}(b,c) - u_\ell\bar{1}\right) \ , \\ &= q^2 - 1 - w_H\left(-u_\ell\bar{1} + \left(b\gamma^{(q+1)ie_2} + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(c\gamma^{ie_3})\right)_{i=0}^{q^2-2}\right) \ , \\ &= \sharp\left\{0 \leq i < q^2-1 : -u_\ell\gamma^{(q+1)i0} + b\gamma^{(q+1)ie_2} + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(c\gamma^{ie_3}) = 0\right\} \ . \end{aligned}$$

Sean χ' y χ los caracteres aditivos canónicos de $\mathbb{F}_{q^2}$ y $\mathbb{F}_q$, respectivamente. Entonces, por la relación de ortogonalidad para el caracter χ (ver (1.4)), obtenemos

$$\begin{aligned} w_\ell &= \frac{1}{q}\sum_{i=0}^{q^2-2}\sum_{y\in\mathbb{F}_q} \chi(-yu_\ell\gamma^{(q+1)i0} + yb\gamma^{(q+1)ie_2})\chi'(yc\gamma^{ie_3}) \ , \\ &= \frac{q^2-1}{q} + \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{q^2}^*} \chi(-yu_\ell x^{(q+1)0} + ybx^{(q+1)e_2})\chi'(ycx^{e_3}) \ . \end{aligned}$$

Utilizando la notación del Lema 8 y la Observación 11, tenemos que

$$w_\ell = \frac{q^2-1}{q} + \frac{1}{q} T_{(e_1,e_2,e_3)}(-u_\ell, b, c) = Z_{(e_1,e_2,e_3)}(-u_\ell, b, c) \ ,$$

donde $e_1 = 0$, $\gcd(q^2-1, e_3) = 1$ y $e_3 \equiv e_2 \pmod{q-1}$. Pero, si las condiciones anteriores se cumplen, entonces $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2-e_1) = 1$ y $e_3 \equiv e_1+e_2 \pmod{q-1}$. Así pues, por la Observación 11,

$$w_0 = \begin{cases} q^2-1 & \text{si } c = b = 0, \quad \text{Caso 1,} \\ 0 & \text{si } c = 0 \text{ y } b \neq 0, \quad \text{Caso 2,} \\ q-1 & \text{si } c \neq 0 \text{ y } b = 0, \quad \text{Caso 4,} \\ q & \text{si } c \neq 0 \text{ y } b \neq 0, \quad \text{Caso 5.} \end{cases}$$

Mientras que si $1 \leq \ell \leq q-1$, obtenemos

$$w_\ell = \begin{cases} 0 & \text{si } c = b = 0, \quad \text{Caso 2,} \\ q+1 & \text{si } c = 0 \text{ y } b \neq 0, \quad \text{Caso 3,} \\ q & \text{si } c \neq 0 \text{ y } b = 0, \quad \text{Caso 5,} \\ 1 & \text{si } c \neq 0 \text{ y } -u_\ell = \frac{c^{q+1}}{b}, \quad \text{Caso 6,} \\ q+1 & \text{si } c \neq 0 \text{ y } -u_\ell \neq \frac{c^{q+1}}{b}, \quad \text{Caso 7.} \end{cases}$$

Pero $\mathcal{Z}(\mathbf{c}(b,c)) = z_0^{w_0} z_1^{w_1} \dots z_{q-1}^{w_{q-1}}$, por lo tanto

$$\mathcal{Z}(\mathbf{c}(b,c)) = \begin{cases} z_0^{q^2-1} & \text{si } c = b = 0, \\ \prod_{i=1}^{q-1} z_i^{q+1} & \text{si } c = 0 \text{ y } b \neq 0, \\ z_0^{q-1} \prod_{i=1}^{q-1} z_i^{q} & \text{si } c \neq 0 \text{ y } b = 0, \\ z_0^{q} z_1 \prod_{i=1, i\neq 1}^{q-1} z_i^{q+1} & \text{si } c, b \neq 0 \text{ y } -u_1 = \frac{c^{q+1}}{b}, \\ \vdots & \vdots \\ z_0^{q} z_{q-1} \prod_{i=1, i\neq q-1}^{q-1} z_i^{q+1} & \text{si } c, b \neq 0 \text{ y } -u_{q-1} = \frac{c^{q+1}}{b}. \end{cases}$$

En consecuencia, el resultado se sigue del siguiente hecho

$$\begin{aligned} &\sharp \left\{ \mathbf{c}(b,c) \in \mathcal{C}_{((q+1)e_2,e_3)} : b = c = 0 \right\} = 1 \ , \\ &\sharp \left\{ \mathbf{c}(b,c) \in \mathcal{C}_{((q+1)e_2,e_3)} : c = 0 \text{ y } b \neq 0 \right\} = q-1 \ , \\ &\sharp \left\{ \mathbf{c}(b,c) \in \mathcal{C}_{((q+1)e_2,e_3)} : c \neq 0 \text{ y } b = 0 \right\} = q^2-1 \ , \text{ y} \\ &\sharp \left\{ \mathbf{c}(b,c) \in \mathcal{C}_{((q+1)e_2,e_3)} : c, b \neq 0 \text{ y } -u_\ell = \frac{c^{q+1}}{b} \right\} = q^2-1 \ , \end{aligned}$$

para $\ell = 1, 2, \dots, q-1$. □

Observación 12. Al fijar q no es difícil verificar que el número, $\mathcal{N}_{(e_2,e_3)}(q)$, de códigos cíclicos distintos de la forma $\mathcal{C}_{((q+1)e_2,e_3)}$ que satisfacen las condiciones del teorema anterior es $\mathcal{N}_{(e_2,e_3)}(q) = \frac{\phi(q^2-1)}{2}$, donde ϕ denota la función de Euler[1].

[1]La función $\phi(n)$ de Euler indica el número de enteros m tales que $1 \leq m \leq n$ y $\gcd(m,n) = 1$.

El siguiente es un ejemplo del Teorema 14.

Ejemplo 9. Sea $q = 4$. Entonces, por el Teorema 14 y la Observación 12, tenemos que los 4 códigos: $\mathcal{C}_{(5,1)}$, $\mathcal{C}_{(5,7)}$, $\mathcal{C}_{(10,2)}$ y $\mathcal{C}_{(10,11)}$ son $[15, 3, 11]$ códigos cíclicos óptimos de tres pesos sobre $\mathbb{F}_4$, cuyo enumerador de pesos completo es

$$z_0^{15} + 3z_1^5 z_2^5 z_3^5 + 15z_0^3 z_1^4 z_2^4 z_3^4 + 15z_0^4 z_1 z_2^5 z_3^5 + 15z_0^4 z_1^5 z_2 z_3^5 + 15z_0^4 z_1^5 z_2^5 z_3 \,. \tag{3.3}$$

3.4 Códigos cíclicos óptimos de cinco pesos y dimensión 4

Como resultado secundario de la clase de sumas exponenciales estudiada en la Sección 3.2, ahora extendemos la clase de códigos cíclicos óptimos de cinco pesos presentada recientemente en el [27, Teorema 6] a través del siguiente:

Teorema 15. *Para enteros e_1, e_2 y e_3, sea $\mathcal{C}_{((q+1)e_1,(q+1)e_2,e_3)}$ el código cíclico de longitud $q^2 - 1$, sobre $\mathbb{F}_q$, cuyo polinomio de chequeo de paridad está dado por $h_{(q+1)e_1}(x)h_{(q+1)e_2}(x)h_{e_3}(x)$. Asuma que $q > 2$ y suponga que $\gcd(q + 1, e_3) = 1$, $\gcd(q - 1, e_2 - e_1) = 1$ y $e_3 \equiv e_1 + e_2 \pmod{q-1}$. Entonces:*

(A) *$h_{e_3}(x)$ es el polinomio de chequeo de paridad de un código cíclico de un solo peso, dimensión 2 y longitud $q^2 - 1$, cuyo peso distinto de cero es $q(q - 1)$. Mientras que $h_{(q+1)e_1}(x)$ y $h_{(q+1)e_2}(x)$ son los polinomios de chequeo de paridad de dos códigos cíclicos distintos de dimensión 1 y de un solo peso (equivalentes a un código de repetición).*

(B) *$\mathcal{C}_{((q+1)e_1,(q+1)e_2,e_3)}$ es un $[q^2-1, 4, q(q-1)-2]$ código cíclico óptimo c.r.a Griesmer, de cinco pesos sobre $\mathbb{F}_q$, cuya distribución de pesos está dada por la* Tabla *3.2.*

Peso	**Frecuencia**
0	1
$q(q-1)-2$	$(q-1)^2(q^2-q-1)$
$q(q-1)-1$	$2(q^2-1)(q-1)$
$q(q-1)$	q^2-1
q^2-2	$(q^2-1)(q-1)$
q^2-1	$2(q-1)$

Tabla 3.2: Distribución de pesos de $\mathcal{C}_{((q+1)e_1,(q+1)e_2,e_3)}$.

Demostración. Parte (A): Como $q > 2$, note que $e_1 \not\equiv e_2 \pmod{q-1}$ y, por tanto, $h_{(q+1)e_1}(x) \neq h_{(q+1)e_2}(x)$. Además, $h_{(q+1)e_1}(x)$, $h_{(q+1)e_2}(x)$ y $h_{e_3}(x)$ son los polinomios de chequeo de paridad de tres códigos cíclicos irreducibles distintos de longitudes $\frac{q-1}{\gcd(q-1,e_1)}$, $\frac{q-1}{\gcd(q-1,e_2)}$ y $(q+1)\frac{q-1}{\gcd(q-1,e_3)}$, respectivamente. Por lo tanto, la prueba de este inciso se sigue del [60, Teorema 7].

Parte (B): Claramente, el código cíclico $\mathcal{C}_{((q+1)e_1,(q+1)e_2,e_3)}$ tiene longitud $q^2 - 1$ y su dimensión es 4. Ahora bien, por el Teorema de Delsarte [13], tenemos que

$$\mathcal{C}_{((q+1)e_1,(q+1)e_2,e_3)} := \left\{ \mathbf{c}(a,b,c) \ : \ a,b \in \mathbb{F}_q, c \in \mathbb{F}_{q^2} \right\} ,$$

donde

$$\mathbf{c}(a,b,c) := \left(a\gamma^{(q+1)ie_1} + b\gamma^{(q+1)ie_2} + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(c\gamma^{ie_3}) \right)_{i=0}^{q^2-2} .$$

Entonces, el peso de Hamming de cualquier palabra de código $\mathbf{c}(a,b,c)$, en el código cíclico $\mathcal{C}_{((q+1)e_1,(q+1)e_2,e_3)}$, es igual a $q^2 - 1 - Z_{(e_1,e_2,e_3)}(a,b,c)$, donde

$$Z_{(e_1,e_2,e_3)}(a,b,c) = \sharp\left\{ 0 \le i < q^2-1 : a\gamma^{(q+1)ie_1} + b\gamma^{(q+1)ie_2} + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(c\gamma^{ie_3}) = 0 \right\} .$$

Sean χ' y χ como antes. Entonces, por la relación de ortogonalidad para el caracter χ (ver (1.4)) y utilizando la notación del Lema 8, tenemos que

$$\begin{aligned} Z_{(e_1,e_2,e_3)}(a,b,c) &= \frac{q^2-1}{q} + \frac{1}{q} \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^2}^*} \chi(yax^{(q+1)e_1} + ybx^{(q+1)e_2}) \chi'(ycx^{e_3}) , \\ &= \frac{q^2-1}{q} + \frac{1}{q} T_{(e_1,e_2,e_3)}(a,b,c) . \end{aligned}$$

Así pues, la distribución de pesos de $\mathcal{C}_{((q+1)e_1,(q+1)e_2,e_3)}$ se sigue de la Observación 11.

Por último, como la Tabla 3.2 coincide con el enumerador de pesos del [27, Teorema 6], cualquier código de la forma $\mathcal{C}_{((q+1)e_1,(q+1)e_2,e_3)}$ es óptimo. □

Observación 13. Al fijar $q > 2$, no es difícil verificar que el número, $\mathcal{N}_{(e_1,e_2,e_3)}(q)$, de códigos cíclicos distintos de la forma $\mathcal{C}_{((q+1)e_1,(q+1)e_2,e_3)}$ que satisfacen las condiciones del teorema anterior es $\mathcal{N}_{(e_1,e_2,e_3)}(q) = \frac{(q-1)\phi(q^2-1)}{4}$.

Finalizamos este capítulo mostrando un ejemplo del teorema anterior.

Ejemplo 10. Sea $q = 4$. Entonces, por el Teorema 15 y la Observación 13, tenemos que los 6 códigos: $\mathcal{C}_{(0,5,1)}$, $\mathcal{C}_{(0,10,2)}$, $\mathcal{C}_{(0,5,7)}$, $\mathcal{C}_{(0,10,11)}$, $\mathcal{C}_{(5,10,3)}$ y $\mathcal{C}_{(5,10,6)}$ son $[15,4,10]$ código cíclicos óptimos de cinco pesos sobre $\mathbb{F}_4$, cuyo enumerador de pesos es

$$1 + 99z^{10} + 90z^{11} + 15z^{12} + 45z^{14} + 6z^{15} .$$

Observación 14. Note que los códigos $\mathcal{C}_{(0,10,2)}$, $\mathcal{C}_{(0,5,7)}$, $\mathcal{C}_{(0,10,11)}$, $\mathcal{C}_{(5,10,3)}$ y $\mathcal{C}_{(5,10,6)}$ no pertenecen a la clase de códigos del [27, Teorema 6] a pesar de ser $[15,4,10]$ códigos cíclicos óptimos sobre $\mathbb{F}_4$ cuya distribución de pesos coincide con la del [27, Teorema 6]. De hecho, fijando $q > 2$, se tiene que el [27, Teorema 6] describe tan solo a uno de los $\mathcal{N}_{(e_1,e_2,e_3)}(q)$ códigos cíclicos óptimos descritos por el Teorema 15. Por lo tanto, el Teorema 15 en efecto extiende la clase de códigos cíclicos óptimos de cinco pesos recientemente presentada en el [27, Teorema 6].

Observación 15. Es importante mencionar que los códigos de subcampo para la clase de códigos cíclicos óptimos del [27, Teorema 6] fueron obtenidos en el [27, Teorema 8], donde también se demostró que algunos de los códigos resultantes son óptimos y otros tienen los mejores parámetros conocidos de acuerdo con las tablas de códigos en [21]. Ahora bien, como se mencionó en la observación anterior, el código $\mathcal{C}_{(5,10,3)}$ pertenece al Teorema 15 pero no pertenece a la clase de códigos del [27, Teorema 6].

Con la ayuda de un programa de computadora, no es difícil verificar que el código de subcampo, $\mathcal{C}^{(2)}_{(5,10,3)}$, de $\mathcal{C}_{(5,10,3)}$ es un $[15, 6, 6]$ código cíclico binario de cuatro pesos cuyo enumerador de pesos es $1 + 25z^6 + 30z^8 + 3z^{10} + 5z^{12}$. Más aún, su dual es un $[15, 9, 4]$ código cíclico binario. Por tanto, de acuerdo con [21], el código $\mathcal{C}^{(2)}_{(5,10,3)}$ y su dual son óptimos. Ahora bien, note que $\mathcal{C}^{(2)}_{(5,10,3)}$ es completamente diferente de la clase de códigos de subcampo del [27, Teorema 8]. En consecuencia, este ejemplo muestra que más allá de los [27, Teoremas 6 y 8] aún hay otros códigos cíclicos óptimos de cinco pesos (pertenecientes al Teorema 15) cuyos códigos de subcampo, y sus correspondientes códigos duales, también son óptimos.

Capítulo 4

Obteniendo nuevas clases de códigos lineales óptimos perforando y recortando códigos cíclicos óptimos

En este capítulo utilizamos las técnicas de perforado y recortado (ver Sección 1.3.3) sobre las clases de códigos cíclicos óptimos de los Teoremas 9 y 15 para obtener tres nuevas clases de códigos lineales óptimos c.r.a Griesmer. Las distribuciones de pesos para estos códigos son determinadas. También investigamos sus códigos duales y demostramos que son óptimos o casi óptimos c.r.a Hamming. Más aún, dichos duales contienen clases de códigos AMDS las cuales resultan ser apropiadas para la detección de errores. Además, algunos de los códigos lineales óptimos obtenidos son mínimos y, por tanto, se presentan para construir esquemas de compartición de secretos con buenas estructuras de acceso. Los resultados de este capítulo fueron publicados en [33].

4.1 Introducción

Es bien sabido que existen distintas formas de construir nuevos códigos lineales a partir de códigos conocidos. Por ejemplo, podemos perforar un código, recortarlo, extenderlo, también podemos concatenar dos códigos o calcular los códigos de subcampo de un código dado. De hecho, muchos códigos importantes e interesantes han surgido al modificar o combinar códigos existentes (ver [26, 27, 32, 41, 55, 57, 63, 64]). Por ejemplo, en [57] los autores estudiaron los códigos de subcampo y los subcódigos de subcampo para una clase de códigos MDS, obteniendo como resultado una clase de códigos LCD y una clase de códigos que puede ser utilizada para construir 3-diseños. Además, en [63] se obtuvieron varias clases nuevas de códigos lineales óptimos perforando algunos códigos lineales binarios. Más aún, al recortar algunos códigos de Hamming, Simplex, Reed-Muller y ovoides, once clases de códigos lineales óptimos fueron presentadas en [41].

En este capítulo utilizamos las técnicas de perforado y recortado sobre las clases de códigos cíclicos óptimos de tres y cinco pesos de los Teoremas 9 y 15 para obtener tres clases de códigos lineales óptimos c.r.a Griesmer. Las distribuciones de pesos para estos códigos son determinadas utilizando el Teorema de Prange (ver Teo-

rema 4). Resulta que los códigos estudiados tienen dos, cuatro, cinco o seis pesos distintos de cero, lo cual es de interés ya que, como se mencionó en la Sección 2.1, los códigos lineales con pocos pesos tienen una amplia gama de aplicaciones en muchos campos de investigación. De hecho, códigos lineales óptimos con pocos pesos fueron reportados en [3, 6, 7, 14, 16, 17, 23, 27–29, 54, 63] y más recientemente en [24, 26, 32, 50, 52, 57, 61, 64, 70]. Así pues, en el contexto de tales códigos, los códigos presentados en este capítulo son nuevos. También investigamos los duales para las tres clases de códigos lineales óptimos y demostramos que son óptimos o casi óptimos c.r.a Hamming. Más aún, dichos duales contienen clases de códigos AMDS las cuales resultan ser apropiadas para la detección de errores. Además, algunos de los códigos lineales óptimos obtenidos son mínimos y, por tanto, se presentan para construir esquemas de compartición de secretos con buenas estructuras de acceso.

Este capítulo está organizado de la siguiente manera: En la Sección 4.2 demostramos que los códigos cíclicos son homogéneos. En las Secciones 4.3 y 4.4 utilizamos las técnicas de perforado y recortado sobre las clases de códigos cíclicos óptimos de los Teoremas 9 y 15 para obtener tres nuevas clases de códigos lineales óptimos cuyos duales son óptimos o casi óptimos. También presentamos ejemplos de los códigos obtenidos.

4.2 Los códigos cíclicos son homogéneos

Sea Sym_n el *grupo simétrico* compuesto por todas las permutaciones del conjunto $\{0, 1, \ldots, n-1\}$. Sea $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$ y $\sigma \in \mathrm{Sym}_n$. Definimos $\sigma(\mathbf{v}) \in \mathbb{F}_q^n$ como

$$\sigma(\mathbf{v}) := \left(v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(n-1)}\right) .$$

Para un código lineal $\mathcal{C}$ de longitud n, el *grupo de automorfismos* de $\mathcal{C}$, $\mathrm{Aut}(\mathcal{C})$, se define como

$$\mathrm{Aut}(\mathcal{C}) := \left\{\sigma \in \mathrm{Sym}_n : \sigma(\mathbf{c}) \in \mathcal{C}, \text{ para todo } \mathbf{c} \in \mathcal{C}\right\} .$$

Más aún, se dice que $\mathrm{Aut}(\mathcal{C})$ es *transitivo* si para cualesquiera dos coordenadas $i, j \in \{0, 1, \ldots, n-1\}$ existe una permutación $\sigma \in \mathrm{Aut}(\mathcal{C})$ tal que $\sigma(i) = j$.

Observación 16. Se sabe que un código lineal $\mathcal{C}$ es homogéneo si $\mathcal{C}$ tiene un grupo de automorfismos transitivo (ver [34, Ejercicio 402]).

Ahora bien, observe que si $\mathcal{C}$ es cíclico de longitud n, entonces por la definición de código cíclico, la permutación $\sigma \in \mathrm{Sym}_n$ definida como

$$\sigma := \begin{pmatrix} 0 & 1 & 2 & \cdots & n-2 & n-1 \\ 1 & 2 & 3 & \cdots & n-1 & 0 \end{pmatrix}$$

es un elemento de $\mathrm{Aut}(\mathcal{C})$. Entonces, note que para cualesquiera dos coordenadas $i, j \in \{0, 1, \ldots, n-1\}$ se cumple que $\sigma^{j-i}(i) = j$, donde la diferencia $j - i$ debe tomarse módulo n. Esto significa que $\mathrm{Aut}(\mathcal{C})$ es transitivo (ver también [43, Sec. II] y [56, Sec. 3.4]), y por lo tanto, en vista de la Observación 16, es importante tener en cuenta que todos los códigos cíclicos son homogéneos.

El hecho de que los códigos cíclicos sean homogéneos es relevante ya que esta propiedad nos permite construir nuevos códigos lineales a partir de ellos, ya sea

mediante las técnicas de perforado o recortado, cuya distribución de pesos puede ser obtenida inmediatamente a través del Teorema de Prange. Esto, por supuesto, siempre que se conozca la distribución de pesos de los códigos cíclicos originales. Además, si los códigos perforados y recortados son construidos a partir de códigos cíclicos con buenos parámetros, entonces existen muchas posibilidades de que los códigos resultantes también tengan buenos parámetros.

4.3 Los códigos perforados y recortados de una clase de códigos cíclicos óptimos de tres pesos

A través del siguiente resultado presentamos dos clases de códigos lineales óptimos cuyos duales son óptimos o casi óptimos.

Teorema 16. *Sea i un entero tal que $0 \leq i \leq n-1$, donde $n = q^m - 1$. Sean $\mathcal{C}^i_{(q,m,e_1,e_2)}$ y $\mathcal{C}_{(q,m,e_1,e_2)i}$ los códigos lineales sobre $\mathbb{F}_q$ obtenidos a partir del código cíclico $\mathcal{C}_{(q,m,e_1,e_2)}$ del Teorema 9 perforando y recortando en la i-ésima coordenada, respectivamente. Si $q > 2$, entonces se cumple lo siguiente:*

(A) *$\mathcal{C}^i_{(q,m,e_1,e_2)}$ es un $[n-1, m+1, n-q^{m-1}-1]$ código lineal óptimo c.r.a Griesmer, de cuatro pesos, con enumerador de pesos*

$$\begin{aligned} &1 + (n-q^{m-1})(q-1)z^{n-q^{m-1}-1} + 2q^{m-1}(q-1)z^{n-q^{m-1}} \\ &+ (q^{m-1}-1)z^{q^{m-1}(q-1)} + (q-1)z^{n-1} \ . \end{aligned} \tag{4.1}$$

Además, el código dual, $\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}$, de $\mathcal{C}^i_{(q,m,e_1,e_2)}$ es un $[n-1, n-m-2, 3]$ código lineal casi óptimo c.r.a Hamming.

(B) *$\mathcal{C}_{(q,m,e_1,e_2)i}$ es un $[n-1, m, n-q^{m-1}]$ código lineal óptimo c.r.a Griesmer, de dos pesos, con enumerador de pesos*

$$1 + q^{m-1}(q-1)z^{n-q^{m-1}} + (q^{m-1}-1)z^{q^{m-1}(q-1)} \ . \tag{4.2}$$

Además, el código dual, $\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}$, de $\mathcal{C}_{(q,m,e_1,e_2)i}$ es un $[n-1, n-m-1, 2]$ código lineal óptimo c.r.a Hamming.

Demostración. Parte (A): Como $\mathcal{C}_{(q,m,e_1,e_2)}$ es cíclico, entonces por el Teorema 3 y la observación posterior, el código perforado $\mathcal{C}^i_{(q,m,e_1,e_2)}$ tiene parámetros $[n-1, m+1, n-q^{m-1}-1]$. En consecuencia, como la distancia mínima de $\mathcal{C}^i_{(q,m,e_1,e_2)}$ es $n - q^{m-1} - 1 = q^{m-1}(q-1) - 2$, obtenemos

$$\begin{aligned} &\left\lceil \frac{q^{m-1}(q-1)-2}{q^0} \right\rceil + \left\lceil \frac{q^{m-1}(q-1)-2}{q^1} \right\rceil + \cdots + \left\lceil \frac{q^{m-1}(q-1)-2}{q^m} \right\rceil \ , \\ &= (q^m - q^{m-1} - 2) + (q^{m-1} - q^{m-2}) + (q^{m-2} - q^{m-3}) + \cdots + (q-1) + 1 \ , \\ &= q^m - 2 = n - 1 \ , \end{aligned}$$

lo cual implica que $\mathcal{C}^i_{(q,m,e_1,e_2)}$ es óptimo c.r.a Griesmer. De nueva cuenta, como $\mathcal{C}_{(q,m,e_1,e_2)}$ es cíclico, es homogéneo (ver Observación 16 y la discusión posterior). Así pues, por el Teorema 4 y (2.2), tenemos que $A_j(\mathcal{C}^i_{(q,m,e_1,e_2)}) = 0$, $0 \leq j \leq n-1$, excepto por los siguientes casos

$$\begin{aligned}
A_0(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= A_0(\mathcal{C}_{(q,m,e_1,e_2)}) = 1 \ , \\
A_{n-q^{m-1}-1}(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= \frac{(n-q^{m-1}-1)+1}{n} A_{n-q^{m-1}}(\mathcal{C}_{(q,m,e_1,e_2)}) \\
&= (n-q^{m-1})(q-1) \ , \\
A_{n-q^{m-1}}(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= \frac{n-(n-q^{m-1})}{n} A_{n-q^{m-1}}(\mathcal{C}_{(q,m,e_1,e_2)}) \\
&\quad + \frac{(n-q^{m-1})+1}{n} A_{q^{m-1}(q-1)}(\mathcal{C}_{(q,m,e_1,e_2)}) \\
&= q^{m-1}(q-1) + q^{m-1}(q-1) = 2q^{m-1}(q-1) \ , \\
A_{q^{m-1}(q-1)}(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= \frac{n-(q^{m-1}(q-1))}{n} A_{q^{m-1}(q-1)}(\mathcal{C}_{(q,m,e_1,e_2)}) \\
&= q^{m-1}-1 \ , \\
A_{n-1}(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= \frac{(n-1)+1}{n} A_n(\mathcal{C}_{(q,m,e_1,e_2)}) = q-1 \ ,
\end{aligned}$$

lo cual coincide con (4.1). Por lo tanto, el enumerador de pesos de $\mathcal{C}^i_{(q,m,e_1,e_2)}$ queda determinado. Ahora bien, debido a (4.1) y las primeras cuatro identidades de Pless, obtenemos que $A_j(\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}) = 0$, para $1 \leq j \leq 2$, y

$$A_3(\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}) = \frac{(q-1)(q-2)(q^m-3)(q^m-4)}{6} \ .$$

Como $q > 2$, $\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}$ es un $[n-1, n-m-2, 3]$ código lineal. Más aún, por la cota de Hamming, no es difícil verificar que para un código de longitud $n-1$ y dimensión $n-m-2$, su distancia mínima puede ser a lo más 4. Por lo tanto, el código $\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}$ es casi óptimo.

Parte (B): Como $\mathcal{C}^{\perp}_{(q,m,e_1,e_2)}$ es un $[n, n-m-1]$ código lineal entonces, gracias a la Observación 3, el código perforado $(\mathcal{C}^{\perp}_{(q,m,e_1,e_2)})^i$ es un $[n-1, n-m-1]$ código lineal. Por otro lado, debido a la Observación 2, tenemos que $\mathcal{C}_{(q,m,e_1,e_2)i} = ((\mathcal{C}^{\perp}_{(q,m,e_1,e_2)})^i)^{\perp}$. En consecuencia, el código recortado $\mathcal{C}_{(q,m,e_1,e_2)i}$ tiene longitud $n-1$ y dimensión $n-1-(n-m-1) = m$. Más aún, como $\mathcal{C}_{(q,m,e_1,e_2)}$ es homogéneo, por el Teorema 4 y (2.2) obtenemos que $A_j(\mathcal{C}_{(q,m,e_1,e_2)i}) = 0$, $0 \leq j \leq n-1$, excepto por los siguientes casos

$$\begin{aligned}
A_0(\mathcal{C}_{(q,m,e_1,e_2)i}) &= A_0(\mathcal{C}_{(q,m,e_1,e_2)}) = 1 \ , \\
A_{n-q^{m-1}}(\mathcal{C}_{(q,m,e_1,e_2)i}) &= \frac{n-(n-q^{m-1})}{n} A_{n-q^{m-1}}(\mathcal{C}_{(q,m,e_1,e_2)}) \\
&= q^{m-1}(q-1) \ , \\
A_{q^{m-1}(q-1)}(\mathcal{C}_{(q,m,e_1,e_2)i}) &= \frac{n-(q^{m-1}(q-1))}{n} A_{q^{m-1}(q-1)}(\mathcal{C}_{(q,m,e_1,e_2)}) \\
&= q^{m-1}-1 \ ,
\end{aligned}$$

lo cual coincide con (4.2). Por tanto, el enumerador de pesos de $\mathcal{C}_{(q,m,e_1,e_2)i}$ queda determinado. De dicho enumerador podemos ver que la distancia mínima de $\mathcal{C}_{(q,m,e_1,e_2)i}$ es $n - q^{m-1} = q^{m-1}(q-1) - 1$. Entonces, tenemos que

$$\begin{aligned}
&\left\lceil \frac{q^{m-1}(q-1)-1}{q^0} \right\rceil + \left\lceil \frac{q^{m-1}(q-1)-1}{q^1} \right\rceil + \cdots + \left\lceil \frac{q^{m-1}(q-1)-1}{q^{m-1}} \right\rceil , \\
&= (q^m - q^{m-1} - 1) + (q^{m-1} - q^{m-2}) + (q^{m-2} - q^{m-3}) + \cdots + (q^2 - q) + (q-1) , \\
&= q^m - 2 = n - 1 ,
\end{aligned}$$

lo cual implica que $\mathcal{C}_{(q,m,e_1,e_2)i}$ es óptimo c.r.a Griesmer. Además, debido a (4.2) y las tres primeras identidades de Pless, obtenemos que $A_1(\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}) = 0$ y

$$A_2(\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}) = \frac{(q-1)(q-2)(q^m-3)}{2} .$$

Como $q > 2$, $\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}$ es un $[n-1, n-m-1, 2]$ código lineal. Finalmente, por la cota de Hamming, no es difícil verificar que para un código de longitud $n-1$ y dimensión $n-m-1$, su distancia mínima puede ser a lo más 2. Así pues, el código $\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}$ es óptimo. □

Como casos particulares del teorema anterior obtenemos las siguientes dos clases de códigos AMDS.

Corolario 2. *Asuma la misma notación que en el teorema anterior. Si $m = 2$ en el Teorema 16, entonces $\mathcal{C}^{i\perp}_{(q,2,e_1,e_2)}$ es un $[n-1, n-4, 3]$ código AMDS casi óptimo y $\mathcal{C}^{\perp}_{(q,2,e_1,e_2)i}$ es un $[n-1, n-3, 2]$ código AMDS óptimo.*

Demostración. Directo de la definición de un código AMDS. □

Ejemplo 11. Los siguientes son algunos ejemplos del Teorema 16.

(a) Sean $(q, m, e_1, e_2) = (4, 4, 6, 8)$ e i un entero tal que $0 \le i \le q^m - 2$. Como $\gcd(\frac{q^m-1}{q-1}, e_2) = 1$ y $\gcd(q-1, me_1 - e_2) = 1$, $\mathcal{C}_{(4,4,6,8)}$ pertenece a la clase de códigos del Teorema 9. Entonces, por la Parte (A) del Teorema 16, el código perforado $\mathcal{C}^{i}_{(4,4,6,8)}$ es un $[254, 5, 190]$ código lineal óptimo de cuatro pesos sobre $\mathbb{F}_4$ con enumerador de pesos

$$1 + 573z^{190} + 384z^{191} + 63z^{192} + 3z^{254} ,$$

mientras que su código dual $\mathcal{C}^{i\perp}_{(4,4,6,8)}$ es un $[254, 249, 3]$ código lineal casi óptimo c.r.a Hamming. Más aún, por la Parte (B) del Teorema 16, el código recortado $\mathcal{C}_{(4,4,6,8)i}$ es un $[254, 4, 191]$ código lineal óptimo de dos pesos sobre $\mathbb{F}_4$ con enumerador de pesos

$$1 + 192z^{191} + 63z^{192} ,$$

mientras que su código dual $\mathcal{C}^{\perp}_{(4,4,6,8)i}$ es un $[254, 250, 2]$ código lineal óptimo.

(b) Sean $(q, m, e_1, e_2) = (9, 2, 4, 3)$ e i un entero tal que $0 \leq i \leq q^m - 2$. Como $\gcd(\frac{q^m-1}{q-1}, e_2) = 1$ y $\gcd(q-1, me_1 - e_2) = 1$, $\mathcal{C}_{(9,2,4,3)}$ pertenece a la clase de códigos del Teorema 9. Entonces, por la Parte (A) del Teorema 16 y el Corolario 2, el código perforado $\mathcal{C}^i_{(9,2,4,3)}$ es un $[79, 3, 70]$ código lineal óptimo de cuatro pesos sobre $\mathbb{F}_9$ con enumerador de pesos

$$1 + 568z^{70} + 144z^{71} + 8z^{72} + 8z^{79} ,$$

mientras que su código dual $\mathcal{C}^{i\perp}_{(9,2,4,3)}$ es un $[79, 76, 3]$ código lineal AMDS casi óptimo c.r.a Hamming. Más aún, por la Parte (B) del Teorema 16, el código recortado $\mathcal{C}_{(9,2,4,3)i}$ es un $[79, 2, 71]$ código lineal óptimo de dos pesos sobre $\mathbb{F}_9$ con enumerador de pesos

$$1 + 72z^{71} + 8z^{72} ,$$

mientras que su código dual $\mathcal{C}^{\perp}_{(9,2,4,3)i}$ es un $[79, 77, 2]$ código lineal AMDS óptimo.

Los resultados anteriores fueron verificados a través de la calculadora Magma[1].

Observación 17. De acuerdo con las tablas de códigos mantenidas en [21], los códigos duales $[254, 249, 3]$ y $[79, 76, 3]$ obtenidos a través de la Parte (A) del Teorema 16 son óptimos.

Observación 18. Con la notación del Teorema 16, sean $\mathbf{w}_{\min}$ y $\mathbf{w}_{\max}$ los pesos distintos de cero mínimo y máximo de $\mathcal{C}_{(q,m,e_1,e_2)i}$, respectivamente. Es decir, $\mathbf{w}_{\min} = q^{m-1}(q-1) - 1$ y $\mathbf{w}_{\max} = q^{m-1}(q-1)$. Note que

$$\frac{\mathbf{w}_{\min}}{\mathbf{w}_{\max}} > \frac{q-1}{q} .$$

En consecuencia, por el Lema 6, tenemos que cualquier código recortado de dos pesos $\mathcal{C}_{(q,m,e_1,e_2)i}$, obtenido a través de la Parte (B) del Teorema 16, es mínimo. Por tanto, dichos códigos se prestan para construir esquemas de compartición de secretos con buenas estructuras de acceso (ver Proposición 1).

4.4 Los códigos perforados de una clase de códigos cíclicos óptimos de cinco pesos

A través del siguiente resultado presentamos una clase de códigos lineales óptimos cuyos duales no solo son óptimos sino también AMDS.

Teorema 17. *Sea i un entero tal que $0 \leq i \leq n-1$, donde $n = q^2-1$. Sea $\mathcal{D}_{(q,e_1,e_2,e_3)}$ un código cíclico óptimo de cinco pesos sobre $\mathbb{F}_q$ perteneciente al Teorema 15. Sea $\mathcal{D}^i_{(q,e_1,e_2,e_3)}$ el código obtenido a partir del código cíclico $\mathcal{D}_{(q,e_1,e_2,e_3)}$ perforando en la i-ésima coordenada. Si $q > 2$, entonces $\mathcal{D}^i_{(q,e_1,e_2,e_3)}$ es un $[n-1, 4, n-q-2]$ código lineal óptimo c.r.a Griesmer, sobre $\mathbb{F}_q$, con enumerador de pesos*

[1]Disponible en línea: http://magma.maths.usyd.edu.au/calc/

$$1 + (n-q)(q-1)(q-2)z^{n-q-2} + 3(n-q)(q-1)z^{n-q-1} + 3q(q-1)z^{n-q} + (q-1)z^{q(q-1)} + (n-1)(q-1)z^{n-2} + 3(q-1)z^{n-1} \ . \tag{4.3}$$

Además, el código dual, $\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}$, de $\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}$ es un $[n-1, n-5, 4]$ código lineal AMDS óptimo c.r.a Hamming.

Demostración. Dado que $\mathcal{D}_{(q,e_1,e_2,e_3)}$ es cíclico, entonces por el Teorema 3 y la observación posterior, el código perforado $\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}$ tiene parámetros $[n-1, 4, n-q-2]$. En consecuencia, como la distancia mínima de $\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}$ es $n-q-2 = q(q-1)-3$, obtenemos

$$\begin{aligned} &\left\lceil \frac{q(q-1)-3}{q^0} \right\rceil + \left\lceil \frac{q(q-1)-3}{q^1} \right\rceil + \left\lceil \frac{q(q-1)-3}{q^2} \right\rceil + \left\lceil \frac{q(q-1)-3}{q^3} \right\rceil \ , \\ &= (q^2-q-3) + (q-1) + 1 + 1 = q^2 - 2 = n-1 \ , \end{aligned}$$

lo cual implica que $\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}$ es óptimo c.r.a Griesmer. Más aún, por la Observación 16 y la discusión posterior, el código cíclico $\mathcal{D}_{(q,e_1,e_2,e_3)}$ es homogéneo. Entonces, por el Teorema 4 y la Tabla 3.2, tenemos que $A_j(\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}) = 0$, $0 \le j \le n-1$, excepto por los siguientes casos

$$\begin{aligned} A_0(\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}) &= A_0(\mathcal{D}_{(q,e_1,e_2,e_3)}) = 1 \ , \\ A_{n-q-2}(\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}) &= \frac{(n-q-2)+1}{n} A_{n-q-1}(\mathcal{D}_{(q,e_1,e_2,e_3)}) \\ &= (n-q)(q-1)(q-2) \ , \\ A_{n-q-1}(\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}) &= \frac{n-(n-q-1)}{n} A_{n-q-1}(\mathcal{D}_{(q,e_1,e_2,e_3)}) \\ &\quad + \frac{(n-q-1)+1}{n} A_{n-q}(\mathcal{D}_{(q,e_1,e_2,e_3)}) \\ &= (n-q)(q-1) + 2(n-q)(q-1) = 3(n-q)(q-1) \ , \\ A_{n-q}(\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}) &= \frac{n-(n-q)}{n} A_{n-q}(\mathcal{D}_{(q,e_1,e_2,e_3)}) \\ &\quad + \frac{(n-q)+1}{n} A_{q(q-1)}(\mathcal{D}_{(q,e_1,e_2,e_3)}) \\ &= 2q(q-1) + q(q-1) = 3q(q-1) \ , \\ A_{q(q-1)}(\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}) &= \frac{n-(q(q-1))}{n} A_{q(q-1)}(\mathcal{D}_{(q,e_1,e_2,e_3)}) = q-1 \ , \\ A_{n-2}(\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}) &= \frac{(n-2)+1}{n} A_{n-1}(\mathcal{D}_{(q,e_1,e_2,e_3)}) = (n-1)(q-1) \ , \\ A_{n-1}(\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}) &= \frac{n-(n-1)}{n} A_{n-1}(\mathcal{D}_{(q,e_1,e_2,e_3)}) \\ &\quad + \frac{(n-1)+1}{n} A_{n}(\mathcal{D}_{(q,e_1,e_2,e_3)}) \\ &= (q-1) + 2(q-1) = 3(q-1) \ , \end{aligned}$$

lo cual coincide con (4.3). Por lo tanto, el enumerador de pesos de $\mathcal{D}^{i}_{(q,e_1,e_2,e_3)}$ queda determinado. Ahora bien, debido a (4.3) y las primeras cinco identidades de Pless, obtenemos que $A_j(\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}) = 0$, para $1 \leq j \leq 3$, y

$$A_4(\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}) = \frac{(q-1)(q+2)(q-2)^2(q^2-3)(q^2-5)}{24} .$$

Como $q > 2$, $\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}$ es un $[n-1, n-5, 4]$ código lineal AMDS. Finalmente, por la cota de Hamming, no es difícil verificar que para un código de longitud $n-1$ y dimensión $n-5$, su distancia mínima puede ser a lo más 4. Por tanto, el código $\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}$ es óptimo. □

Observación 19. Con la notación del teorema anterior, sea $\mathcal{D}_{(q,e_1,e_2,e_3)i}$ el código lineal obtenido a partir del código cíclico $\mathcal{D}_{(q,e_1,e_2,e_3)}$ recortando en alguna coordenada $0 \leq i \leq q^2-2$. Así pues, es interesante notar que si $q > 2$, entonces el código recortado $\mathcal{D}_{(q,e_1,e_2,e_3)i}$ tiene los mismos parámetros y la misma distribución de pesos que el código perforado $\mathcal{C}^{i}_{(q,2,e_1,e_2)}$ de la Parte (A) del Teorema 16 (tome en el Teorema $m = 2$).

Ejemplo 12. Los siguientes son algunos ejemplos del teorema anterior.

(a) Sean $(q, e_1, e_2, e_3) = (3, 2, 7, 5)$ e i un entero tal que $0 \leq i \leq q^2-2$. Como $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2-e_1) = 1$, y $e_3 \equiv e_1+e_2 \pmod{q-1}$, $\mathcal{D}_{(3,2,7,5)}$ pertenece a la clase de códigos del Teorema 15. Entonces, por el Teorema 17, el código perforado $\mathcal{D}^{i}_{(3,2,7,5)}$ es un $[7, 4, 3]$ código lineal óptimo de cinco pesos sobre $\mathbb{F}_3$ con enumerador de pesos

$$1 + 10z^3 + 30z^4 + 18z^5 + 16z^6 + 6z^7 ,$$

mientras que su código dual $\mathcal{D}^{i\perp}_{(3,2,7,5)}$ es un $[7, 3, 4]$ código lineal AMDS óptimo.

(b) Sean $(q, e_1, e_2, e_3) = (8, 3, 14, 10)$ e i un entero tal que $0 \leq i \leq q^2-2$. Como $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2-e_1) = 1$, y $e_3 \equiv e_1+e_2 \pmod{q-1}$, $\mathcal{D}_{(8,3,14,10)}$ pertenece a la clase de códigos del Teorema 15. Entonces, por el Teorema 17, el código perforado $\mathcal{D}^{i}_{(8,3,14,10)}$ es un $[62, 4, 53]$ código lineal óptimo de seis pesos sobre $\mathbb{F}_8$ con enumerador de pesos

$$1 + 2310z^{53} + 1155z^{54} + 168z^{55} + 7z^{56} + 434z^{61} + 21z^{62} ,$$

mientras que su código dual $\mathcal{D}^{i\perp}_{(8,3,14,10)}$ es un $[62, 58, 4]$ código lineal AMDS óptimo.

(c) Sean $(q, e_1, e_2, e_3) = (9, 5, 2, 7)$ e i un entero tal que $0 \leq i \leq q^2-2$. Como $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2-e_1) = 1$, y $e_3 \equiv e_1+e_2 \pmod{q-1}$, $\mathcal{D}_{(9,5,2,7)}$ pertenece a la clase de códigos del Teorema 15. Entonces, por el Teorema 17, el código perforado $\mathcal{D}^{i}_{(9,5,2,7)}$ es un $[79, 4, 69]$ código lineal óptimo de seis pesos sobre $\mathbb{F}_9$ con enumerador de pesos

$$1 + 3976z^{69} + 1704z^{70} + 216z^{71} + 8z^{72} + 632z^{78} + 24z^{79} ,$$

mientras que su código dual $\mathcal{D}^{i\perp}_{(9,5,2,7)}$ es un $[79, 75, 4]$ código lineal AMDS óptimo.

Finalizamos este capítulo mostrando que los códigos AMDS obtenidos en este capítulo son apropiados para la detección de errores.

Cuando un $[n,k]$ código lineal q-ario $\mathcal{C}$ con distribución de pesos $(A_j(\mathcal{C}))_{j=0}^n$ es utilizado para la detección de errores en un canal simétrico q-ario con probabilidad de error de símbolo ϵ, la probabilidad de error no detectado está dada por (ver [20, Sec. IV])

$$P_{ue}(\mathcal{C},\epsilon) := \sum_{j=1}^{n} A_j(\mathcal{C}) \left(\frac{\epsilon}{q-1}\right)^j (1-\epsilon)^{n-j} .$$

Si $P_{ue}(\mathcal{C},\epsilon)$ es una función creciente de ϵ en el intervalo $[0,(q-1)/q]$, entonces se dice que $\mathcal{C}$ es *apropiado* para la detección de errores. En [20] se investigó la capacidad de detección de errores de los códigos AMDS y los autores encontraron la siguiente condición suficiente para que un código AMDS sea apropiado para la detección de errores:

Lema 9 ([20, Lemma 4])**.** *Sea $\mathcal{C}$ un $[n,k]$ código AMDS sobre $\mathbb{F}_q$. Entonces, $\mathcal{C}$ es apropiado si*

$$\frac{A_{n-k}(\mathcal{C})}{q-1} \leq \frac{1}{q}\binom{n}{k} .$$

Observación 20. No es difícil verificar que los códigos lineales AMDS $\mathcal{C}^{i\perp}_{(q,2,e_1,e_2)}$, $\mathcal{C}^{\perp}_{(q,2,e_1,e_2)i}$ y $\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}$, del Corolario 2 y el Teorema 17, satisfacen la condición anterior. Por lo tanto, es importante notar que estos códigos son apropiados para la detección de errores.

Capítulo 5

Conclusiones

Sea q una potencia de un número primo y $m \geq 2$ un entero. En este trabajo se presentaron los resultados derivados de una profundización en el estudio de la clase de códigos cíclicos óptimos q-arios de tres pesos del Teorema 9.

En el Capítulo 2 estudiamos los códigos de subcampo q_0-arios (con $q = q_0^r$) para una subclase de los códigos cíclicos óptimos del Teorema 9 cuando $m = 2$. Demostramos que algunos de estos códigos de subcampo son códigos cíclicos óptimos de tres pesos, de longitud $q^2 - 1$ y dimensión $2r + 1$, que pertenecen de nueva cuenta a la clase de códigos cíclicos óptimos del Teorema 9 (Parte (A) del Teorema 10). Para los otros códigos de subcampo estudiados, probamos que son códigos cíclicos de tres pesos y longitud $q^2 - 1$ cuya dimensión es $3r$ (Parte (B) del Teorema 10). Para estos últimos códigos de subcampo también determinamos la distancia mínima para sus códigos duales y con esto concluimos que dichos duales son casi óptimos c.r.a Hamming. Más aún, se demostró que algunos de los códigos de subcampo de la Parte (B) del Teorema 10 son óptimos y otros tienen los mejores parámetros conocidos de acuerdo con las tablas de códigos mantenidas en [21] (Ejemplo 5 y Observación 8). Sin embargo, como se señaló al final de la Sección 2.3, existen códigos cíclicos pertenecientes al Teorema 9 cuyos códigos de subcampo no pueden describirse a través del Teorema 10 y los cuales tienen buenos parámetros. Por lo tanto, como trabajo futuro sería interesante estudiar a dichos códigos.

Como una aplicación de los códigos lineales con pocos pesos, se determinó la estructura de cobertura para los códigos de subcampo del Teorema 10 (Teorema 11) y se utilizó para presentar un ejemplo específico de un esquema de compartición de secretos basado en uno de estos códigos al final de la Sección 2.4 (Ejemplo 6).

Más aún, al extender algunos de los códigos cíclicos óptimos de tres pesos del Teorema 9, presentamos una clase de códigos lineales óptimos c.r.a Griesmer, de dos pesos sobre $\mathbb{F}_q$, cuyos duales son casi óptimos c.r.a Hamming (Teorema 12). A través del análisis de varios ejemplos se sugiere que dichos duales son óptimos (Ejemplo 7 y Observación 10). También utilizamos los códigos extendidos del Teorema 12 para construir grafos fuertemente regulares (Teorema 13 y Ejemplo 8). Es importante notar que los parámetros y la distribución de pesos de los códigos en el Teorema 12 coinciden con los de una clase de códigos en el Ejemplo SU1 en [8] (tome $l = k + 1$ y $t = k$). Además, como se señaló en la Observación 9, también coinciden con los de la clase de códigos del [24, Teorema 6.3]. Por lo tanto, como trabajo futuro sería interesante demostrar si estos códigos son equivalentes entre sí.

En el Capítulo 3 estudiamos una clase de sumas exponenciales y obtuvimos su

distribución de valores (Lema 8, Corolario 1 y Observación 11). Luego utilizamos esta distribución de valores para determinar el enumerador de pesos completo para una subclase de los códigos cíclicos óptimos de tres pesos (Teorema 14) del Teorema 9 cuando $m = 2$. Como resultado secundario de la clase de sumas exponenciales estudiada en la Sección 3.2, extendimos la clase de códigos cíclicos óptimos de cinco pesos (Teorema 15) presentada recientemente en [27]. Como se señaló en la Observación 15, aparte de los [27, Teoremas 6 y 8], hay evidencia de la existencia de otros códigos cíclicos óptimos de cinco pesos cuyos códigos de subcampo, y sus duales, son óptimos. Por tanto, como trabajo futuro sería interesante obtener una descripción para dichos códigos de subcampo.

Es importante notar que, como se muestra en el [58, Ejemplo 2], hay exactamente 12 códigos cíclicos óptimos de tres pesos sobre $\mathbb{F}_4$ de longitud 15 y dimensión 3. Por otro lado, como se señala en el Ejemplo 9, al menos 4 de estos 12 códigos tienen el mismo enumerador de pesos completo dado por (3.3). Más precisamente, con la notación del Teorema 14, los códigos $\mathcal{C}_{(0,1)}$ y $\mathcal{C}_{(5,3)}$ son códigos cíclicos óptimos de tres pesos sobre $\mathbb{F}_4$ de longitud 15 y dimensión 3, cuyos enumeradores de pesos completos son

$$\begin{aligned} &z_0^{15} + z_1^{15} + z_2^{15} + z_3^{15} + 15z_0^3z_1^4z_2^4z_3^4 + \\ &15z_0^4z_1^3z_2^4z_3^4 + 15z_0^4z_1^4z_2^3z_3^4 + 15z_0^4z_1^4z_2^4z_3^3 \,, \end{aligned} \tag{5.1}$$

y

$$\begin{aligned} &z_0^{15} + 3z_1^5z_2^5z_3^5 + 5z_0^3z_2^6z_3^6 + 5z_0^3z_1^6z_3^6 + 5z_0^3z_1^6z_2^6 + \\ &15z_0^4z_1^5z_2^3z_3^3 + 15z_0^4z_1^3z_2^5z_3^3 + 15z_0^4z_1^3z_2^3z_3^5 \,, \end{aligned} \tag{5.2}$$

respectivamente. Lo anterior muestra que no todos los códigos cíclicos óptimos de tres pesos del Teorema 9 (con $m = 2$) tienen el mismo enumerador de pesos completo. De hecho, (3.3), (5.1) y (5.2) parecen ser los tres posibles enumeradores de pesos completos para estos 12 códigos. Así pues, como complemento de este trabajo, creemos que podría ser interesante determinar el enumerador de pesos completo para la parte restante de códigos cíclicos óptimos de tres pesos que se encuentra más allá del Teorema 14. Más aún, creemos que hay exactamente $q-1$ posibles enumeradores de pesos completos que un código cíclico óptimo de tres pesos y dimensión 3, sobre $\mathbb{F}_q$, puede tomar.

Sea $q > 2$. En el Capítulo 4 utilizamos las técnicas de perforado y recortado sobre las clases de códigos cíclicos óptimos de los Teoremas 9 y 15 para obtener:

(i) Una clase de $[q^m - 2, m + 1, q^{m-1}(q - 1) - 2]$ códigos lineales óptimos c.r.a Griesmer, de cuatro pesos sobre $\mathbb{F}_q$, cuyos duales son $[q^m - 2, q^m - m - 3, 3]$ códigos lineales casi óptimos c.r.a Hamming (Parte (A) del Teorema 16). A través del análisis de varios ejemplos se sugiere que dichos duales son óptimos (Observación 17).

(ii) Una clase de $[q^m-2, m, q^{m-1}(q-1)-1]$ códigos lineales óptimos c.r.a Griesmer, de dos pesos sobre $\mathbb{F}_q$, cuyos duales son $[q^m - 2, q^m - m - 2, 2]$ códigos lineales óptimos c.r.a Hamming (Parte (B) del Teorema 16). Más aún, estos códigos de dos pesos son mínimos (Observación 18) y, por tanto, se prestan para construir esquemas de compartición de secretos con buenas estructuras de acceso.

(iii) Una clase de $[q^2-2, 4, q(q-1)-3]$ códigos lineales óptimos c.r.a Griesmer, sobre $\mathbb{F}_q$, cuyos duales son $[q^2-2, q^2-6, 4]$ códigos lineales AMDS óptimos c.r.a Hamming (Teorema 17).

Las distribuciones de pesos para estas tres clases de códigos fueron determinadas explícitamente. Además, si $m = 2$, entonces los códigos duales en (i) y (ii) son AMDS (Corolario 2). Más aún, todos los códigos AMDS presentados en el Capítulo 4 son apropiados para la detección de errores (Observación 20). También, como se señaló al inicio de dicho capítulo, las tres clases de códigos lineales óptimos en (i),(ii) y (iii) parecen ser nuevas.

Finalmente, como resultado del presente trabajo de investigación fueron publicados dos capítulos de libro [31, 62] y tres artículos en revistas indexadas [32, 33, 61], cuyas primeras páginas se encuentran en el Anexo A. También se presentaron tres ponencias cuyas constancias se incluyen, de igual forma, en dicho Anexo. Es importante señalar que el proyecto de investigación [62], que fue presentado en el congreso internacional "WAIFI 2024: International Workshop on the Arithmetic of Finite Fields", no fue incluido en esta tesis pues fue un trabajo que se realizó durante el último semestre de mis estudios de doctorado.

Anexo A

Participaciones y publicaciones

El Comité Organizador otorga la presente

C O N S T A N C I A

A: *Félix Hernández*

por haber impartido la conferencia con título

Los códigos de subcampo de una subclase de códigos cíclicos óptimos y sus estructuras de cobertura

en el 14º Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas, celebrado del 26 al 28 de junio de 2023, de forma remota desde CDMX, México

Dr. Noé Gutiérrez Herrera
Por el Comité Organizador
UAM-Iztapalapa

Dra. Gina Gallegos García
Por el Comité Organizador
IPN- CIC

The Organizing Committee of the

15th Latin American Theoretical Informatics Symposium
LATIN 2022

Certified that

Félix Hernández

Has participated as a Speaker with the talk

On the subfield codes of a subclass of optimal cyclic codes and their covering structures

in the **15 Latin American Theoretical Informatics Symposium LATIN 2022**

november 7th-11th, 2022.

CIMAT, Guanajuato, México

Dr. Francisco Rodríguez Henríquez
General Chair
Cryptography Research Centre, TII
Abu Dhabi, United Arab Emirates.

Dr. Armando Castañeda
Program Committee Chair
UNAM, México

Dr. Mariano Rivera Meraz
Organizing Committee Chair
CIMAT, Guanajuato, México

Prof. Qiang Wang
School of Mathematics and Statistics
Carleton University
1125 Colonel By Drive
Ottawa, Ontario
Canada K1S 5B6
wang@math.carleton.ca

June 22, 2024

Félix Hernández
Universidad Nacional Autónoma de México,
Mexico

Dear Félix Hernández:

Thank you very much for attending WAIFI 2024: The internationl workshop on the Arithmetic of Finite Fields, at Carleton Dominion-Chalmers Center located in downtown Ottawa, June 10-12, 2024. The webpage of the workshop is http://www.waifi.org

The talk Determining the complete weight distributions of some families of cyclic codes was presented by you and it was well received. Please let us know if you have any question.

Sincerely,

Prof. Qiang Wang
For the General co-chairs of WAIFI 2024

School of Mathematics and Statistics
Carleton University
Ottawa, ON
CANADA K1S 5B6

On the Subfield Codes of a Subclass of Optimal Cyclic Codes and Their Covering Structures

Félix Hernández[1(✉)] and Gerardo Vega[2]

[1] Posgrado en Ciencia e Ingeniería de la Computación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, Mexico
felixhdz@ciencias.unam.mx

[2] Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, Mexico
gerardov@unam.mx

Abstract. A class of optimal three-weight $[q^k-1, k+1, q^{k-1}(q-1)-1]$ cyclic codes over $\mathbb{F}_q$, with $k \geq 2$, achieving the Griesmer lower bound, was presented by Heng and Yue [IEEE Trans. Inf. Theory, 62(8) (2016) 4501–4513]. In this paper we study some of the subfield codes of this class of optimal cyclic codes when $k = 2$. The weight distributions of the subfield codes are settled. It turns out that some of these codes are optimal and others have the best known parameters. The duals of the subfield codes are also investigated and found to be almost optimal with respect to the sphere-packing bound. In addition, the covering structure for the studied subfield codes is determined. Some of these codes are found to have the important property that any nonzero codeword is minimal. This is a desirable property which is useful in the design of a secret sharing scheme based on a linear code. Moreover, we present a specific example of a secret sharing scheme based on one of these subfield codes.

Keywords: Subfield codes · Optimal cyclic codes · Secret sharing schemes · Covering structure · Sphere-packing bound

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. An $[n, l, d]$ linear code, $\mathcal{C}$, over $\mathbb{F}_q$ is a l-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. It is called *optimal* if there is no $[n, l, d']$ code with $d' > d$, and *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.

Recently, a class of optimal three-weight $[q^k-1, k+1, q^{k-1}(q-1)-1]$ cyclic codes over $\mathbb{F}_q$ achieving the Griesmer lower bound was presented in [11], which generalizes a result in [20] from $k = 2$ to arbitrary positive integer $k \geq 2$. Further, the q_0-ary subfield codes of two families of q-ary optimal linear codes were studied

F. Hernández - PhD student, manuscript partially supported by CONACyT, México.

A. Castañeda and F. Rodríguez-Henríquez (Eds.): LATIN 2022, LNCS 13568, pp. 255–270, 2022.
https://doi.org/10.1007/978-3-031-20624-5_16

Algorithmica
https://doi.org/10.1007/s00453-023-01173-5

The Subfield and Extended Codes of a Subclass of Optimal Three-Weight Cyclic Codes

Félix Hernández[1] · Gerardo Vega[2]

Received: 23 February 2023 / Accepted: 4 September 2023

Abstract
A class of optimal three-weight $[q^k - 1, k + 1, q^{k-1}(q - 1) - 1]$ cyclic codes over $\mathbb{F}_q$, with $k \geq 2$, achieving the Griesmer bound, was presented by Heng and Yue (IEEE Trans Inf Theory 62(8):4501–4513, 2016. https://doi.org/10.1109/TIT.2016.2550029). In this paper we study some of the subfield codes of this class of optimal cyclic codes when $k = 2$. The weight distributions of the subfield codes are settled. It turns out that some of these codes are optimal and others have the best known parameters. The duals of the subfield codes are also investigated and found to be almost optimal with respect to the sphere-packing bound. In addition, the covering structure for the studied subfield codes is determined. Some of these codes are found to have the important property that any nonzero codeword is minimal, which is a desirable property that is useful in the design of a secret sharing scheme based on a linear code. Moreover, a specific example of a secret sharing scheme based on one of these subfield codes is given. Finally, a class of optimal two-weight linear codes over $\mathbb{F}_q$, achieving the Griesmer bound, whose duals are almost optimal with respect to the sphere-packing bound is presented. Through a different approach, this class of optimal two-weight linear codes was reported very recently by Heng (IEEE Trans Inf Theory 69(2):978–994, 2023. https://doi.org/10.1109/TIT.2022.3203380). Furthermore, it is shown that these optimal codes can be used to construct strongly regular graphs.

A short version of this paper appeared in the Proceedings of LATIN 2022 [1].

✉ Félix Hernández
felixhdz@ciencias.unam.mx

Gerardo Vega
gerardov@unam.mx

[1] Posgrado en Ciencia e Ingeniería de la Computación, Universidad Nacional Autónoma de México, Mexico City 04510, Mexico

[2] Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, Mexico City 04510, Mexico

Published online: 25 September 2023

Cryptography and Communications
https://doi.org/10.1007/s12095-022-00601-7

The complete weight distribution of a subclass of optimal three-weight cyclic codes

Gerardo Vega[1] · **Félix Hernández**[2]

Received: 16 February 2022 / Accepted: 29 June 2022

Abstract
The weight distribution of a code is usually investigated on the basis of Hamming weight, under which all the nonzero components of a codeword are regarded as identical. To describe the structure of nonbinary codes in more detail, each nonzero component should be distinguished from the other and this is done by means of the complete weight distribution. However, obtaining the complete weight distribution for nonbinary codes is an even harder problem than obtaining the ordinary weight distribution. Therefore, the complete weight distribution is unknown for most codes. The complete weight distributions of two classes of p-ary cyclic codes were recently reported by Heng and Yue (Cryptogr. Commun. **9**, 323–343, 8). The purpose of this work is to present the complete weight distribution of a subclass of optimal three-weight cyclic codes over any finite field.

Keywords Complete weight enumerator of a code · Weight distribution · Optimal three-weight cyclic codes

Mathematics Subject Classification (2010) 94B15 · 11T71

1 Introduction

The complete weight distribution of a code enumerates the codewords by the number of symbols of each kind contained in each codeword. Therefore, the complete weight distribution of a code contains much more information than the ordinary weight distribution. In fact, the complete weight distribution has a wide range of applications in many research fields as the information it contains is of vital use in practical applications. For example, as pointed out in [2] the complete weight enumerator of Reed-Solomon codes could be

✉ Gerardo Vega
gerardov@unam.mx

Félix Hernández
felixhdz@ciencias.unam.mx

[1] Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, Mexico

[2] Posgrado en Ciencia e Ingeniería de la Computación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, Mexico

Published online: 01 August 2022

Applicable Algebra in Engineering, Communication and Computing
https://doi.org/10.1007/s00200-024-00653-7

ORIGINAL PAPER

Obtaining new classes of optimal linear codes by puncturing and shortening optimal cyclic codes

Félix Hernández[1] · **Gerardo Vega**[2]

Received: 19 October 2023 / Revised: 20 February 2024 / Accepted: 24 February 2024

Abstract
In this paper we use the puncturing and shortening techniques on two already-known classes of optimal cyclic codes in order to obtain three new classes of optimal linear codes achieving the Griesmer bound. The weight distributions for these codes are settled. We also investigate their dual codes and show that they are either optimal or almost optimal with respect to the sphere-packing bound. Moreover, these duals contain classes of almost maximum distance separable codes which are shown to be proper for error detection. Further, some of the obtained optimal linear codes are suitable for constructing secret sharing schemes with nice access structures.

Keywords Optimal linear codes · Almost MDS codes · Punctured codes · Shortened codes · Griesmer bound

1 Introduction

Let q be a power of a prime number. Denote by $\mathbb{F}_q$ the finite field with q elements. An $[n, k, d]$ linear code, $\mathcal{C}$, over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. In this context, the vectors of $\mathcal{C}$ are called *codewords*. We index the coordinates of the codewords in $\mathcal{C}$ with the elements in $\{0, 1, \ldots, n-1\}$. The linear code $\mathcal{C}$ is called *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. In addition, $\mathcal{C}$ is called *optimal* if there is no $[n, k, d']$ code over $\mathbb{F}_q$ with $d' > d$ or its parameters meet a bound on linear codes. On the other hand, $\mathcal{C}$ is called *almost*

✉ Félix Hernández
felixhdz@ciencias.unam.mx

Gerardo Vega
gerardov@unam.mx

[1] Posgrado en Ciencia e Ingeniería de la Computación, Universidad Nacional Autónoma de México, 04510 Mexico City, Mexico

[2] Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, 04510 Mexico City, Mexico

Published online: 06 April 2024

Determining the complete weight distributions of some families of cyclic codes*

Gerardo Vega[1][0000−0002−4957−6575] and Félix Hernández[2][0000−0002−4791−485X]

[1] Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, MEXICO
gerardov@unam.mx

[2] Posgrado en Ciencia e Ingeniería de la Computación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, MEXICO
felixhdz@ciencias.unam.mx

Abstract. Obtaining the complete weight distributions for nonbinary codes is an even harder problem than obtaining their Hamming weight distributions. In fact, obtaining these distributions is a problem that usually involves the evaluation of sophisticated exponential sums, which leaves this problem open for most of the linear codes. In this work we present a method that uses the known complete weight distribution of a given cyclic code, to determine the complete weight distributions of other cyclic codes. In addition we also obtain the complete weight distributions for a particular kind of one- and two-weight irreducible cyclic codes, and use these distributions and the method, in order to determine the complete weight distributions of infinite families of cyclic codes. As an example, and as a particular instance of our results, we determine in a simple way the complete weight distribution for one of the two families of reducible cyclic codes studied by Bae, Li and Yue [Discrete Mathematics, 338 (2015) 2275–2287].

Keywords: Complete weight enumerator · Weight distribution · One- and two-weight irreducible cyclic codes · Cyclic codes · Gauss sums.

1 Introduction

The complete weight distribution of a code enumerates the codewords by the number of symbols of each kind contained in each codeword. Therefore, the complete weight distribution of a code contains much more information than the Hamming weight distribution. In fact, the complete weight distribution has a wide range of applications in many research fields as the information it contains is of vital use in practical applications. For example, as pointed out in [2] the complete weight distribution of Reed-Solomon codes could be helpful in soft decision decoding. As another example, the complete weight distribution is useful in the computation of the Walsh transform of monomial functions over

* This manuscript is partially supported by PAPIIT-UNAM IN107423. The second author has also received research support from CONAHCyT, México.

Bibliografía

[1] Ashikhmin, A., Barg, A.: Minimal vectors in linear codes. IEEE Trans. Inf. Theory **44**(5), 2010–2017 (1998). doi:10.1109/18.705584

[2] Bae, S., Li, C., Yue, Q.: On the complete weight enumerators of some reducible cyclic codes. Discrete Math. **338**(12), 2275–2287 (2015). doi:10.1016/j.disc.2015.05.016

[3] Ball, S., Montanucci, E.: Affine blocking sets, three-dimensional codes and the Griesmer bound. Discrete Math. **307**(13), 1600–1608 (2007). doi:10.1016/j.disc.2006.09.011

[4] Becerra, D.: Esquema de compartición de secretos con detección eficiente de trampas. Tesis de maestría. Posgrado en Ciencia e Ingeniería de la Computación, UNAM (2019), disponible en línea: `http://132.248.9.195/ptd2019/agosto/0794968/Index.html`

[5] Blake, I.F., Kith, K.: On the complete weight enumerator of Reed-Solomon codes. SIAM J. Discrete Math. **4**(2), 164–171 (1991). doi:10.1137/0404016

[6] Bouyukliev, I.G.: Classification of Griesmer codes and dual transform. Discrete Math. **309**(12), 4049–4068 (2009). doi:10.1016/j.disc.2008.12.002

[7] Calderbank, A.R., Goethals, J.M.: Three-weight codes and association schemes. Philips J. Res. **39**(4-5), 143–152 (1984)

[8] Calderbank, A.R., Kantor, W.M.: The geometry of two-weight codes. Bull. London Math. Soc. **18**(2), 97–122 (1986). doi:10.1112/blms/18.2.97

[9] Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inf. Theory **51**(6), 2089–2102 (2005). doi:10.1109/TIT.2005.847722

[10] Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**, 125–156 (1998). doi:10.1023/A:1008344232130

[11] Chan, C.H., Xiong, M.: On the complete weight distribution of subfield subcodes of algebraic-geometric codes. IEEE Trans. Inf. Theory **65**(11), 7079–7086 (2019). doi:10.1109/TIT.2019.2922630

[12] Choudhari, S.P., Chakole, M.B.: Reed-Solomon code for WiMAX network. In: 2017 International Conference on Communication and Signal Processing (ICCSP). pp. 0176–0179 (2017). doi:10.1109/ICCSP.2017.8286801

[13] Delsarte, P.: On subfield subcodes of modified Reed-Solomon codes (corresp.). IEEE Trans. Inf. Theory **21**(5), 575–576 (1975). doi:10.1109/TIT.1975.1055435

[14] Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015). doi:10.1109/TIT.2015.2420118

[15] Ding, C., Heng, Z.: The subfield codes of ovoid codes. IEEE Trans. Inf. Theory **65**(8), 4715–4729 (2019). doi:10.1109/TIT.2019.2907276

[16] Ding, C., Luo, J., Niederreiter, H.: Two-weight codes punctured from irreducible cyclic codes. In: Li, Y., Ling, S., Niederreiter, H., Wang, H., Xing, C., Zhang, S. (eds.) Proc. 1st Int. Workshop Coding Theory Cryptogr. pp. 119–124. World Scientific, Singapore (2008). doi:10.1142/9789812832245_0009

[17] Ding, C., Niederreiter, H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory **53**(6), 2274–2277 (2007). doi:10.1109/TIT.2007.896886

[18] Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**(1), 81–99 (2005). doi:10.1016/j.tcs.2004.09.011

[19] Ding, C., Yin, J.: Sets of optimal frequency-hopping sequences. IEEE Trans. Inf. Theory **54**(8), 3741–3745 (2008). doi:10.1109/TIT.2008.926410

[20] Dodunekova, R., Dodunekov, S., Klove, T.: Almost-MDS and near-MDS codes for error detection. IEEE Trans. Inf. Theory **43**(1), 285–290 (1997). doi:10.1109/18.567708

[21] Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. `http://www.codetables.de`, último acceso el 12 de junio de 2023

[22] Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006). doi:10.1109/TIT.2006.872854

[23] Hellesth, T.: Projective codes meeting the Griesmer bound. Discrete Math. **106-107**, 265–271 (1992). doi:10.1016/0012-365X(92)90553-R

[24] Heng, Z.: Projective linear codes from some almost difference sets. IEEE Trans. Inf. Theory **69**(2), 978–994 (2023). doi:10.1109/TIT.2022.3203380

[25] Heng, Z., Ding, C.: The subfield codes of hyperoval and conic codes. Finite Fields Their Appl. **56**, 308–331 (2019). doi:10.1016/j.ffa.2018.12.006

[26] Heng, Z., Ding, C.: The subfield codes of some $[q+1, 2, q]$ MDS codes. IEEE Trans. Inf. Theory **68**(6), 3643–3656 (2022). doi:10.1109/TIT.2022.3151721

[27] Heng, Z., Wang, Q., Ding, C.: Two families of optimal linear codes and their subfield codes. IEEE Trans. Inf. Theory **66**(11), 6872–6883 (2020). doi:10.1109/TIT.2020.3006846

[28] Heng, Z., Wang, W., Wang, Y.: Projective binary linear codes from special Boolean functions. Appl. Algebra Eng. Commun. **32**, 521–552 (2021). doi:10.1007/s00200-019-00412-z

[29] Heng, Z., Yue, Q.: Several classes of cyclic codes with either optimal three weights or a few weights. IEEE Trans. Inf. Theory **62**(8), 4501–4513 (2016). doi:10.1109/TIT.2016.2550029

[30] Heng, Z., Yue, Q.: Complete weight distributions of two classes of cyclic codes. Cryptogr. Commun. **9**, 323–343 (2017). doi:10.1007/s12095-015-0177-y

[31] Hernández, F., Vega, G.: On the subfield codes of a subclass of optimal cyclic codes and their covering structures. In: Castañeda, A., Rodríguez-Henríquez, F. (eds.) LATIN 2022: Theoretical Informatics. Lecture Notes in Computer Science, vol. 13568, pp. 255–270. Springer, Cham (2022). doi:10.1007/978-3-031-20624-5_16

[32] Hernández, F., Vega, G.: The subfield and extended codes of a subclass of optimal three-weight cyclic codes. Algorithmica **85**, 3973–3995 (2023). doi:10.1007/s00453-023-01173-5

[33] Hernández, F., Vega, G.: Obtaining new classes of optimal linear codes by puncturing and shortening optimal cyclic codes. AAECC (2024). doi:10.1007/s00200-024-00653-7

[34] Huffman, W.C., Pless, V.: Fundamentals of error-correcting codes. Cambridge Univ. Press, Cambridge, U.K. (2003)

[35] Kong, X., Yang, S.: Complete weight enumerators of a class of linear codes with two or three weights. Discrete Math. **342**(11), 3166–3176 (2019). doi:10.1016/j.disc.2019.06.025

[36] Li, C., Qu, L., Ling, S.: On the covering structures of two classes of linear codes from perfect nonlinear functions. IEEE Trans. Inf. Theory **55**(1), 70–82 (2009). doi:10.1109/TIT.2008.2008145

[37] Li, C., Bae, S., Ahn, J., Yang, S., Yao, Z.A.: Complete weight enumerators of some linear codes and their applications. Des. Codes Cryptogr. **81**, 153–168 (2016). doi:10.1007/s10623-015-0136-9

[38] Li, C., Ding, C., Li, S.: LCD cyclic codes over finite fields. IEEE Trans. Inf. Theory **63**(7), 4344–4356 (2017). doi:10.1109/TIT.2017.2672961

[39] Li, C., Yue, Q., Fu, F.W.: Complete weight enumerators of some cyclic codes. Des. Codes Cryptogr. **80**, 295–315 (2015). doi:10.1007/s10623-015-0091-5

[40] Lidl, R., Niederreiter, H.: Finite fields. Cambridge Univ. Press, Cambridge, U.K. (1983)

[41] Liu, Y., Ding, C., Tang, C.: Shortened linear codes over finite fields. IEEE Trans. Inf. Theory **67**(8), 5119–5132 (2021). doi:10.1109/TIT.2021.3087082

[42] Luo, J., Feng, K.: Cyclic codes and sequences from generalized Coulter–Matthews function. IEEE Trans. Inf. Theory **54**(12), 5345–5353 (2008). doi:10.1109/TIT.2008.2006394

[43] Luo, Y., Xing, C., Yuan, C.: Optimal locally repairable codes of distance 3 and 4 via cyclic codes. IEEE Trans. Inf. Theory **65**(2), 1048–1053 (2019). doi:10.1109/TIT.2018.2854717

[44] MacWilliams, F.J., Mallows, C., Sloane, N.J.A.: Generalizations of Gleason's Theorem on weight enumerators of self-dual codes. IEEE Trans. Inf. Theory **18**(6), 794–805 (1972). doi:10.1109/TIT.1972.1054898

[45] MacWilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. North-Holland, Amsterdam, The Netherlands (1977)

[46] Marelli, A., Micheloni, R.: BCH codes for solid-state-drives. In: Micheloni, R., Marelli, A., Eshghi, K. (eds.) Inside Solid State Drives (SSDs). Springer Series in Advanced Microelectronics, vol. 37, pp. 369–406. Springer, Singapore (2018). doi:10.1007/978-981-13-0599-3_11

[47] Massey, J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory. pp. 276–279 (1993)

[48] Massey, J.L.: Some applications of coding theory in cryptography. In: Codes and Ciphers: Cryptography and Coding IV. pp. 33–47 (1995)

[49] McEliece, R.J., Swanson, L.: Reed-solomon codes and the exploration of the solar system. In: Wicker, S.B., Bhargava, V.K. (eds.) Reed-Solomon Codes and Their Applications. pp. 25–40. Wiley-IEEE Press (1994). doi:10.1109/9780470546345.ch3

[50] Mesnager, S., Qian, L., Cao, X., Yuan, M.: Several families of binary minimal linear codes from two-to-one functions. IEEE Trans. Inf. Theory **69**(5), 3285–3301 (2023). doi:10.1109/TIT.2023.3236955

[51] Moisio, M.: On relations between certain exponential sums and multiple Kloosterman sums and some applications to coding theory. Preprint (1997), disponible en línea: https://lipas.uwasa.fi/~mamo/gauss.pdf

[52] Ouyang, J., Liu, H., Wang, X.: Several classes of p-ary linear codes with few weights. Appl. Algebra Eng. Commun. Comput. **34**, 691–715 (2023). doi:10.1007/s00200-021-00527-2

[53] Schmidt, B., White, C.: All two-weight irreducible cyclic codes? Finite Fields Their Appl. **8**(1), 1–17 (2002). doi:10.1006/ffta.2000.0293

[54] Shi, M., Solé, P.: Three-weight codes, triple sum sets, and strongly walk regular graphs. Des. Codes Cryptogr. **87**, 2395–2404 (2019). doi:10.1007/s10623-019-00628-7

[55] Solomon, G., Stiffler, J.: Algebraically punctured cyclic codes. Inf. Control. **8**(2), 170–179 (1965). doi:10.1016/S0019-9958(65)90080-X

[56] Tan, P., Fan, C., Ding, C., Tang, C., Zhou, Z.: The minimum locality of linear codes. Des. Codes Cryptogr. **91**, 83–114 (2023). doi:10.1007/s10623-022-01099-z

[57] Tang, C., Wang, Q., Ding, C.: The subfield codes and subfield subcodes of a family of MDS codes. IEEE Trans. Inf. Theory **68**(9), 5792–5801 (2022). doi:10.1109/TIT.2022.3163813

[58] Vega, G.: A characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field. Finite Fields Their Appl. **42**, 23–38 (2016). doi:10.1016/j.ffa.2016.07.001

[59] Vega, G.: An extended characterization of a class of optimal three-weight cyclic codes over any finite field. Finite Fields Their Appl. **48**, 160–174 (2017). doi:10.1016/j.ffa.2017.07.010

[60] Vega, G.: A characterization of all semiprimitive irreducible cyclic codes in terms of their lengths. AAECC **30**(5), 441–452 (2019). doi:10.1007/s00200-019-00385-z

[61] Vega, G., Hernández, F.: The complete weight distribution of a subclass of optimal three-weight cyclic codes. Cryptogr. Commun. **15**, 317–330 (2023). doi:10.1007/s12095-022-00601-7

[62] Vega, G., Hernández, F.: Determining the complete weight distributions of some families of cyclic codes. In: Nikova, S., Panario, D. (eds.) Arithmetic of Finite Fields. Lecture Notes in Computer Science, Springer, Cham (2024), *(en prensa)*.

[63] Wang, X., Zheng, D., Ding, C.: Some punctured codes of several families of binary linear codes. IEEE Trans. Inf. Theory **67**(8), 5133–5148 (2021). doi:10.1109/TIT.2021.3088146

[64] Xiang, C., Tang, C., Ding, C.: Shortened linear codes from APN and PN functions. IEEE Trans. Inf. Theory **68**(6), 3780–3795 (2022). doi:10.1109/TIT.2022.3145519

[65] Yang, S.: Complete weight enumerators of a class of linear codes from Weil sums. IEEE Access **8**, 194631–194639 (2020). doi:10.1109/ACCESS.2020.3034110

[66] Yang, S., Yao, Z.A.: Complete weight enumerators of a class of linear codes. Discrete Math. **340**(4), 729–739 (2017). doi:10.1016/j.disc.2016.11.029

[67] Yang, S., Yao, Z.A.: Complete weight enumerators of a family of three-weight linear codes. Des. Codes Cryptogr. **82**, 663–674 (2017). doi:10.1007/s10623-016-0191-x

[68] Yang, S., Yao, Z.A., Zhao, C.A.: A class of three-weight linear codes and their complete weight enumerators. Cryptogr. Commun. **9**, 133–149 (2017). doi:10.1007/s12095-016-0187-4

[69] Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**(1), 206–212 (2006). doi:10.1109/TIT.2005.860412

[70] Zhang, X., Du, X., Jin, W.: Weight distributions of two classes of linear codes with five or six weights. Discrete Math. **345**(7), 112881 (2022). doi:10.1016/j.disc.2022.112881

[71] Zheng, D., Zhao, Q., Wang, X., Zhang, Y.: A class of two or three weights linear codes and their complete weight enumerators. Discrete Math. **344** (2021). doi:10.1016/j.disc.2021.112355

[72] Zhou, Z., Ding, C.: A class of three-weight cyclic codes. Finite Fields Their Appl. **25**, 79–93 (2014). doi:10.1016/j.ffa.2013.08.005

[73] Zhu, C., Liao, Q.: Complete weight enumerators for several classes of two-weight and three-weight linear codes. Finite Fields Their Appl. **75** (2021). doi:10.1016/j.ffa.2021.101897

Lista de símbolos

Nota. Los símbolos que aparecen solo en un contexto restringido no se encuentran listados. Se proporciona una referencia de página para la primera aparición del símbolo.

Símbolo	Descripción	Página
$\sharp A$	el número de elementos del conjunto finito A	4
$a \mid b$	a divide a b	20
$a \nmid b$	a no divide a b	20
x^T	el vector transpuesto del vector x	3
$\gcd(a, b)$	el máximo común divisor de a y b	9
$a \equiv b \pmod{n}$	a es congruente con b módulo n	9
$\lceil x \rceil$	el menor entero mayor o igual a x	6
$\lfloor x \rfloor$	el mayor entero menor o igual a x	6
$\binom{n}{j}$	coeficiente binomial	6
$e^{2\pi\sqrt{-1}/p}$	la p-ésima raíz compleja de la unidad	11
$\deg(f(x))$	el grado del polinomio $f(x)$	17
$g \circ f$	la composición de la función f con la función g	35
$\phi(\cdot)$	la función de Euler	41
$w_H(\cdot)$	la función peso de Hamming	3
$\mathcal{C}^\perp$	el código dual de $\mathcal{C}$	5
$\mathcal{C}^{(q_0)}$	el código de subcampo de $\mathcal{C}$ sobre $\mathbb{F}_{q_0}$	6
$\widehat{\mathcal{C}}$	el código extendido de $\mathcal{C}$	7
$\mathcal{C}^i$	el código obtenido a partir de $\mathcal{C}$ al perforar en la i-ésima coordenada	7
$\mathcal{C}_i$	el código obtenido a partir de $\mathcal{C}$ al recortar en la i-ésima coordenada	8
$A_j(\mathcal{C})$	el número de palabras de código con peso de Hamming j en $\mathcal{C}$	4
$\mathrm{CWE}_{\mathcal{C}}$	el enumerador de pesos completo de $\mathcal{C}$	4
$\langle\gamma\rangle$	el grupo cíclico generado por γ	2
$\langle\gamma^d\rangle$	el subgrupo cíclico de $\langle\gamma\rangle$ generado por γ^d	13
$\mathbb{C}$	el campo de los números complejos	11
$\mathbb{Z}_n$	el anillo de enteros módulo n	9
C_s	la clase q-ciclotómica de s módulo n	9
$\Omega_{(n,q)}$	el conjunto de todos los representantes de las clases q-ciclotómicas módulo n	9
$\mathbb{F}_q, \mathrm{GF}(q)$	el campo finito de orden q	1
$\mathbb{F}_{q^m}$	la extensión finita de grado m de $\mathbb{F}_q$	2
$\mathbb{F}_q(\gamma)$	la extensión de $\mathbb{F}_q$ obtenida al agregar la raíz γ	9
$\mathbb{F}_q^*$	el grupo multiplicativo de elementos distintos de cero de $\mathbb{F}_q$	2

$\mathbb{F}_q^n$	el conjunto de vectores de longitud n con entradas en $\mathbb{F}_q$	3
$\langle \cdot, \cdot \rangle$	el producto escalar usual en el espacio vectorial $\mathbb{F}_q^n$	5
$\mathbb{F}_q[x]$	el anillo de polinomios con indeterminada x sobre $\mathbb{F}_q$	2
$\langle f(x) \rangle$	el ideal principal generado por el polinomio $f(x)$	10
$\mathbb{F}_q[x]/\langle x^n - 1 \rangle$	el anillo de polinomios con indeterminada x sobre $\mathbb{F}_q$ de grado a lo más $n-1$	10
$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a)$	la traza de $a \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$	2
$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a)$	la norma de $a \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$	2
$M_a(x)$	el polinomio mínimo de $a \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$	2
χ	el caracter aditivo canónico de $\mathbb{F}_q$	11
$\bar{\chi}$	el conjugado del caracter aditivo canónico χ	12
ψ, ψ_j	un caracter multiplicativo de $\mathbb{F}_q$	11
$\bar{\psi}$	el conjugado del caracter multiplicativo ψ	12
ψ_0	el caracter multiplicativo trivial de $\mathbb{F}_q$	11
η	el caracter cuadrático de $\mathbb{F}_q$ (q impar)	12
$\widehat{\mathbb{F}}_q$	el grupo de caracteres multiplicativos de $\mathbb{F}_q$	12
$G_{\mathbb{F}_q}(\psi, \chi)$	la suma Gaussiana de ψ y χ sobre $\mathbb{F}_q$	12
Sym_n	el grupo simétrico sobre un conjunto de n símbolos	46
$\mathrm{Aut}(\mathcal{C})$	el grupo de automorfismos de $\mathcal{C}$	46

Índice alfabético