UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
POSGRADO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

DISTRIBUCIÓN DE PESOS DE CÓDIGOS CÍCLICOS REDUCIBLES SOBRE CAMPOS FINITOS

TESIS
QUE PARA OPTAR POR EL GRADO DE:
DOCTOR EN CIENCIAS (COMPUTACIÓN)

PRESENTA:
CARLOS ALBERTO VÁZQUEZ FERNÁNDEZ

TUTOR
DR. GERARDO VEGA HERNÁNDEZ
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MÉXICO, D. F. ABRIL 2015

CONTENIDO

RESUMEN

En Teoría de la Información, una familia importante de códigos correctores de error, son los llamados códigos cíclicos. Estos códigos han sido ampliamente estudiados, debido a su rica estructura algebraica, sus enlaces fascinantes a otros objetos tales como polinomios, y a su utilidad en el control de errores en comunicaciones digitales. Por tanto encontrar la distribución de pesos de un código cíclico q-ario C, no sólo es un problema de interés teórico sino también tiene una importancia práctica.

Típicamente, cuando el campo finito F_q es un campo primo, el problema es manejado expresando el peso de Hamming de cada palabra de código en C por medio de cierta combinación de sumas exponenciales. Este método tiene la ventaja de la flexibilidad, en el sentido que puede también ser aplicado a códigos cíclicos sobre campos finitos de orden no primo.

En nuestro proyecto de investigación, estuvimos interesados particularmente en encontrar la distribución de pesos de códigos cíclicos reducibles de N pesos, que son construidos a partir de la suma directa de dos códigos cíclicos irreducibles diferentes, de la misma longitud y dimensión.

Se obtuvieron dos resultados: El primero, es un método que mediante la evaluación de una suma exponencial particular, obtiene la distribución de sus valores, y con ello, se obtiene la distribución de pesos de algunos códigos cíclicos reducibles. El segundo, se apoya en un resultado general presentado en [13],

que evalúa una clase de sumas exponenciales, de las cuales, determinamos la distribución de los valores de una instancia particular de dicha clase, para obtener la distribución de pesos de una familia de códigos cíclicos reducibles no proyectivos. A su vez, pudimos determinar el número exacto de códigos de esa familia, cuando la longitud y la dimensión son conocidas.

Capítulo 1: Introducción

1 INTRODUCCIÓN

La motivación principal que dió origen a la Teoría de Códigos, fue la necesidad de transmitir información, de manera confiable, por medios susceptibles al ruido. Por ruido, podemos entender una amplia gama de factores, podemos considerar como tal a un campo electromagnético presente alrededor del cableado por donde se envía un mensaje, radiaciones de distintas fuentes, masas de aire con cargas eléctricas que pueden afectar las señales inalámbricas, o incluso, el tráfico intenso de información a través de una red de computadoras, teléfonos, o cualquier otro dispositivo de transmisión.

Toda la gente involucrada en el campo de investigación de códigos, coincide en que el punto de orígen, fue la aparición del famoso y clásico articulo de Shannon [17], en 1948. Básicamente lo que se establece ahí, es que existen buenos códigos para transmitir información, y se da un límite o cota dentro del cual deben de permanecer tales códigos para ser considerados buenos u óptimos. Casi a la par, Hamming en [6], retoma la parte teórica del trabajo mencionado, y desde un punto de vista práctico o ingenieril, se avoca a la búsqueda de esos códigos, descubriendo de esta manera a las primeras clases de códigos correctores de error, muchos de ellos cíclicos. De estos últimos, se desprenden los posteriores descubrimientos de Berlekamp, para códigos ne-

gacíclicos [2] y los famosos códigos BCH [3] y de Reed-Solomon [16], los cuales también son cíclicos . Estas cuatro familias, forman una base con la cual se ha estado trabajando desde entonces, refiriéndonos exclusivamente a códigos de bloque lineales cíclicos correctores de error, encontrándose equivalencias, variantes, adecuaciones y aplicaciones de ellos, y se han descubierto otros más, pero muy a menudo se vuelve al origen, pues realmente, no se han encontrado otros códigos que sean mejores a estos, en la mayoría de los casos.

Entonces, tenemos dos ramas dentro del campo de estudio de la Teoría de Códigos: La rama teórica, encabezada por el trabajo de Shannon, que se encarga de trabajar sobre la profundidad matemática, de encontrar formas más convencionales o coloquiales de explicar los códigos y sus algoritmos de decodificación. La rama práctica, encabezada por Hamming, que trata con la ingeniería necesaria para aterrizar las ideas, en implementaciones que sean manejables. Sin embargo, ambas ramas no pueden estar separadas. Se encuentran entrelazadas estrechamente, a menudo no hay distinción entre ellas.

Así pues, con el paso del tiempo, se ha profundizado en el estudio de los antecedentes mencionados, y se ha llegado a una gran diversidad de aplicaciones para los códigos correctores de error, por mencionar brevemente, los encontramos inmersos en las misiones espaciales desde sus inicios, con los satélites o sondas famosas, como las Mariner o las Voyager, cuando se requirió de enviar imágenes a la Tierra desde el espacio, hasta las misiones más recientes, con los robots exploradores de la superficie marciana. Hay una gran variedad de aplicaciones en electrónica

de consumo popular, como en los DVDs y discos compactos, o en la clasificación de objetos, como mercancía mediante códigos de barras bidimensionales, o libros mediante códigos ISBN.

2 Los métodos desarrollados para obtener la distribución de pesos de un código cíclico reducible

Es dentro de la línea de investigación mencionada en parrafos anteriores, donde estamos ubicados. Como ya mencionamos, los códigos cíclicos son una familia importante para el control de errores en comunicaciones digitales, por lo tanto, encontrar la distribución de pesos de un código cíclico q-ario C, no sólo es un problema de interés teórico sino también tiene una importancia práctica. Siendo específicos, la distribución de pesos de un código es un parámetro importante ya que esta juega un rol muy importante en determinar las capacidades de detección y corrección de errores de un código dado. Sin embargo, calcular la distribución de pesos de un código en una computadora, es un trabajo arduo. Para códigos cíclicos este problema es de gran interés, debido a su rica estructura algebraica. Estamos interesados particularmente en encontrar la distribución de pesos de códigos cíclicos reducibles de N pesos.

Nosotros construimos códigos cíclicos reducibles a partir de la suma directa de dos códigos cíclicos irreducibles diferentes, de la misma longitud y dimensión (los códigos cíclicos sobre un campo finito, tienen asociado un polinomio generador y un polinomio de chequeo de paridad; si dicho polinomio de chequeo

es irreducible, el código será irreducible; en el caso contrario, si el polinomio de chequeo es reducible, o sea, el producto de dos o mas factores irreducibles, como en nuestro caso que es el producto de dos, el código es reducible). Ahora, para hallar la distribución de pesos de un código construido por suma directa, nos basamos en una técnica que se ha vuelto muy popular en años recientes:

La técnica de sumas exponenciales, ampliamente utilizada en el estudio de códigos. Estas sumas datan de las epocas de Gauss y Lagrange, quienes las descubrieron en un contexto completamente distinto del nuestro. No imaginarían que en nuestra época, su descubrimiento tendría tales aplicaciones.

Entonces, el trabajo que realizamos es algo muy simple, y consiste en lo siguiente:

Tomamos dos códigos cíclicos irreducibles distintos, C_1 y C_2 respectivamente, construidos sobre un campo finito, ambos de la misma longitud y dimensión. Por ejemplo, sobre F_3, sean C_1 un código cíclico irreducible con polinomio de chequeo de paridad $h(x) = x^2 + x + 2$, y C_2 un código cíclico irreducible con polinomio de chequeo de paridad $h(x) = x^2 + 2x + 2$, ambos códigos de longitud $n = 8$ y dimensión $k = 2$, es decir, contienen 9 palabras, y son de peso 6 (recordemos que el peso de una palabra de código, es el número de símbolos diferentes de cero que contiene):

C_1	C_2
00000000	00000000
11202210	12202110
01120221	01220211
10112022	10122021
21011202	11012202
22101120	21101220
02210112	02110122
20221011	20211012
12022101	22021101

A continuación, se suman de manera directa estos dos códigos, es decir, viendo a las palabras de cada código como vectores, las sumamos coordenada a coordenada, todas contra todas. Por ejemplo, si sumamos la palabra cero de C_1 contra todas las palabras de C_2, claramente obtenemos C_2; de manera similar, si sumamos la palabra cero de C_2 contra todas las palabras de C_1, obtenemos C_1; es decir, tenemos todas las palabras de peso original 6; estos son los casos triviales; pero, si sumamos la palabra 11202210 de C_1 con la palabra 12202110 de C_2, tenemos

$$(11202210 + 12202110) \text{ modulo } 3 = 20101020,$$

la cual es una palabra de peso 4. Ahora, si sumamos la palabra 11202210 de C_1 con la palabra 01220211 de C_2, tenemos

$$(11202210 + 01220211) \text{ modulo } 3 = 12122121,$$

la cual es una palabra de peso 8. Ahora, si sumamos la palabra 11202210 de C_1 con la palabra 21101220 de C_2, tenemos

$$(11202210 + 21101220) \text{ modulo } 3 = 02000100,$$

la cual es una palabra de peso 2. Si continuamos sumando las palabras de C_1 con las de C_2, tendremos el total de palabras obtenidas por suma directa, en el cual existen palabras que contienen el o los pesos originales, pero también palabras de pesos distintos a los originales, En este ejemplo, de manera total tenemos un código $C = C_1 + C_2$, de 81 palabras, cuya distribución de pesos es: 1 palabra de peso 0, 7 palabras de peso 2, 25 palabras de peso 4, 32 palabras de peso 6 y 16 palabras de peso 8. Ahora, este método es útil para códigos pequeños, pero ¿Qué sucede cuando tenemos códigos de mayor longitud y dimensión? ya no es tan inmediato el realizar la suma de esta manera, se vuelve algo impráctico. Entonces lo que se encontró, fueron métodos o algoritmos que nos dan, sin necesidad de construir C, su distribución de pesos, solamente conociendo o proponiendo su longitud y su dimensión.

De esta forma, es mas fácil para alguien el saber, antes siquiera de ponerse a construirlo, la distribución de pesos de un código propuesto, y de esta manera saber si le es útil para un propósito en particular o no, y ahorrarse el tiempo de construir y sumar códigos, si es que al final ni siquiera va a utilizar tal código.

Entonces, los métodos o algoritmos para hallar la distribución de pesos de un código cíclico reducible C sobre un campo finito,

el cual es la suma directa de dos códigos cíclicos irreducibles distintos, de la misma longitud y dimensión, fueron desarrollados gracias al cálculo de la distribución de los valores de sumas exponenciales muy particulares para cada caso. Una manera fácil de ver el comportamiento de una suma exponencial en el contexto de códigos, es la siguiente figura:

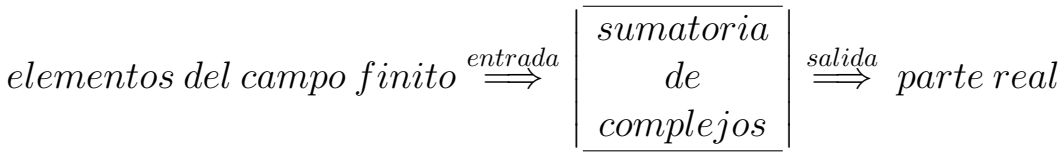

Figura 1: Suma exponencial en el contexto de Códigos

Tenemos como argumentos de entrada a la suma exponencial, a elementos del campo finito, los cuales son mapeados hacia números complejos; se calcula la sumatoria de tales números complejos, correspondientes a todos los argumentos de entrada, y como salida o resultado, obtendremos valores reales enteros. De esta manera se obtiene la distribución de los valores de la suma exponencial. Entonces, en el contexto de códigos, las sumas exponenciales se manipulan de tal forma que, sus valores de salida son totalmente enteros, los cuales corresponden directamente a los pesos del código.

Aplicando el esquema anterior, basado en sumas exponenciales, se obtuvieron dos resultados:

El primer resultado nos da un método, que consiste en la evaluación de una suma exponencial específica, con el objeto de hallar su distribución de valores, y por ende, obtener la distribución de pesos de un grupo particular de códigos cíclicos; la clave en este primer resultado, fué el haber identificado qué suma exponencial en particular nos era útil para el conteo de pesos, la cual es muy parecida a las halladas en [5, 14], y el darnos cuenta que tal suma exponencial requería de precisar dos números enteros a y b, relacionados directamente con dos elementos del campo finito, para su evaluación; estos dos enteros a y b, se encontraron mediante la construcción de tablas de valores para ambos, e identificando los cruces de valores que nos daban el resultado esperado, al momento de realizar la evaluación de la suma exponencial; con lo que pudimos saber en que intervalo de valores enteros debía correr a, y que valor exacto debe tener b, mediante la obtención de una fórmula o relación para su cálculo directo; una vez identificados a y b, la evaluación de la suma exponencial necesita ser programada en cualquier lenguaje o verificada en Maple por ejemplo; a pesar de requerir evaluar una suma exponencial, este método tiene dos puntos a favor: es flexible en cuanto a su aplicación, ya que funciona para todo campo finito, es decir, para campos finitos de orden primo y orden no primo, y los cálculos involucrados se reducen gracias a propiedades inherentes a la suma exponencial utilizada.

El segundo resultado, por una parte, está basado o es motivado por un resultado contemporáneo en [11], trabajo en el cual los autores realizan una búsqueda de distribución de pesos, para un grupo diferente de códigos, y por otra parte, también nos apoyamos en el trabajo presentado en [13], del cual hacemos

uso, y que consiste en la evaluación de una suma exponencial general, a la cual le manipulamos los argumentos, de tal manera que se adaptara a nuestro caso particular. También puede programarse, pero no es necesario, pues no se requiere evaluar la suma exponencial utilizada en este caso, ya que se desarrolló de tal forma la parte matemática, que pudo obtenerse de manera exacta la distribución de los valores de dicha suma exponencial, con lo cual, directamente, se obtiene al final una tabla con la distribución completa de pesos, para una familia de códigos cíclicos en particular. Como un resultado adicional, en este caso, se obtiene también el número exacto de códigos cíclicos en dicha familia, cuando la longitud y dimensión son parámetros conocidos.

De esta manera, con los dos métodos descritos, se le da formalidad a la tarea de calcular la distribución de pesos, de grupos particulares de códigos cíclicos sobre campos finitos, evitando tener datos dispersos en corridas de computadora, al obtener algoritmos precisos que engloban tanto los datos y cálculos involucrados como los resultados obtenidos.

Lo descrito en lineas anteriores es, de un modo muy simple, la explicación del trabajo realizado. Se aterrizó en un par de publicaciones.

Ahora bien, ¿Qué tan útil es el aporte?. Cerca de 1950, comenzó el trabajo sobre códigos, y desde entonces se han estado identificando los mejores códigos que existen, para la mayoría de los propósitos prácticos, y para un amplio abanico de posibilidades teóricas. Han funcionado de manera aceptable hasta el

dia de hoy, entonces, ¿Para qué necesitamos más códigos? y más aún, ¿Para qué necesitamos códigos como los que hemos encontrado, los cuales ni siquiera están cerca de los mejores parámetros buscados para todo código? ¿Realmente abonamos algo al campo de estudio, o sólo nos autocomplacemos?. La respuesta o justificación, en nuestro descargo es la siguiente: Sí, es verdad que al momento los códigos hallados con nuestros métodos, carecen en absoluto de practicidad, es decir, no son óptimos ni se acercan a serlo; de manera similar, en el sentido teórico, aunque en este último caso, el trabajo ha llamado la atención en cierta parte de la comunidad de estudio, tenemos al momento dos citas de terceros [26, 27], para los cuales nuestro aporte les ha servido para saber dónde ya se ha buscado, y por dónde hay que escarbar para encontrar algo más. Aún más, en el segundo resultado dejamos abierta una posible generalización, la cual, los autores de [28] han logrado, apoyándose en nuestro segundo resultado. En resumen, si bien ahora nadie les ha encontrado la aplicación práctica, eso no quiere decir que no la tendrán en un futuro, lejano o cercano, no se puede saber; muchas aportaciones en la historia de la ciencia han surgido de una manera similar: al principio un descubrimiento en particular pareciera no tener sentido, pareciera resultado de una mente febril, por lo que no es tomado en cuenta y es desechado; pasa un tiempo, alguien lo desempolva, lo analiza, y termina descubriendo buenas aportaciones. No decimos que vaya a ser así en nuestro caso, pero alguien le sacará algún provecho en determinado momento, cuándo, no podemos saberlo, sólo nos concretamos a presentar el aporte, esa es nuestra función y no otra.

3 Organización de la tesis

El presente documento se encuentra organizado en un conjunto de 4 capítulos en total, siendo éste el primero de ellos. En el capítulo 2 se realiza una breve revisión de la historia de la Teoría de Códigos, se presentan algunas aplicaciones, y un resumen de sumas exponenciales en el contexto de códigos. En el capítulo 3, se realiza la transcripción del articulo publicado que incluye el primer resultado obtenido en la investigación. El capítulo 4, contiene el segundo resultado, mediante la transcripción ahora, del segundo artículo publicado. Finalmente, se plantea la conclusión del trabajo desarrollado y se listan las referencias bibliográficas.

Capítulo 2: Historia, aplicaciones y sumas exponenciales

1 Teoría de Códigos: Los inicios

Los códigos fueron inventados para corregir errores en canales de comunicación ruidosos. Por ruido, podemos entender una amplia gama de factores, podemos considerar como tal a un campo electromagnético presente alrededor del cableado por donde se envía un mensaje, radiaciones de distintas fuentes, masas de aire con cargas eléctricas que afectan las señales inalámbricas, o incluso, el tráfico intenso de información a través de una red de computadoras, teléfonos, o cualquier otro dispositivo de transmisión. Ahora bien, en Teoría de Códigos, hay mucho que decir cuando de antecedentes históricos se trata, pero sin lugar a dudas, debemos observar que una de las áreas importantes donde la Teoría de Códigos es aplicada, es en telefonía. Por ello no sorprende que los nombres de los pioneros del área, sean los de los miembros del grupo de trabajo inicial de 1948, de los laboratorios de la compañía Bell en USA. Shannon, Hamming, Berlekamp, Gilbert, MacWilliams, Slepian y Sloane, entre otros. Su investigación no sólo es el inicio, sino también un parteaguas en este campo de estudio. Esto, no sólo porque formalizaron ideas esbozadas por algunos de sus contemporáneos, sino que además, desarrollaron la mayor parte de la teoría basica de la que todos nos hemos apoyado, y en la práctica, lograron descubrir una buena cantidad de códigos buenos o útiles que se utilizan hasta el día de hoy. Casi la mayoría de la literatura inicial en Teoría de Códigos puede encontrarse en la Revista Técnica de los Sistemas Bell.

A continuación, hablaremos brevemente del trabajo de algunos de los investigadores aquí mencionados.

1.1 El inicio por C. E. Shannon

El artículo "Una Teoría Matemática de Comunicación" de C. E. Shannon, publicado en 1948, marca el inicio de la Teoría de Códigos. En síntesis, el resultado principal de dicho trabajo nos demuestra que los códigos buenos existen. El paso siguiente es entonces, tratar de construir tales códigos. Dado que estos códigos tienen que ser utilizados pensando en reducir el tamaño de los aparatos electrónicos, debemos estar interesados especialmente en códigos con tal estructura, que permita algoritmos simples de decodificación. Obtener estos códigos es muy difícil.

Para buscar esos códigos buenos, Shannon se enfocó en el problema fundamental de comunicación: reproducir un mensaje seleccionado en un punto dado, exacta o aproximadamente en otro punto.

Desarrolló una Teoría General de Comunicación, en especial se ubicó en la parte matemática, o lo que él llamaba, una Teoría Matemática de Comunicación, obsesionado principalmente por el efecto del ruido en el canal de transmisión, asi como en la estructura que debía tener el mensaje original, basándose en el destino final de la información.

Su investigación comenzó a partir de un enfoque de medición logarítmica, el cual es conveniente por varias razones:

1- Es muy útil en la practica, ya que los parámetros de importancia ingenieril, tales como tiempo, ancho de banda, número de relevadores, tienden a variar linealmente con el logaritmo del número de posibilidades.

2- Es cercano a un enfoque intuitivo de medición.

3- Es matemáticamente manejable.

Por eso es que la elección de una base logarítmica, corresponde a la elección de una unidad de medida de información. Es decir, si se utiliza base 2, las unidades resultantes son llamados dígitos binarios, o más brevemente bits, por lo que dispositivos de información, con dos posiciones estables, tal como los relevadores o un circuito de flip-flop, pueden almacenar un bit de información, entonces N de tales dispositivos pueden almacenar N bits.

En la siguiente página mostramos el esquema de un sistema general de comunicación:

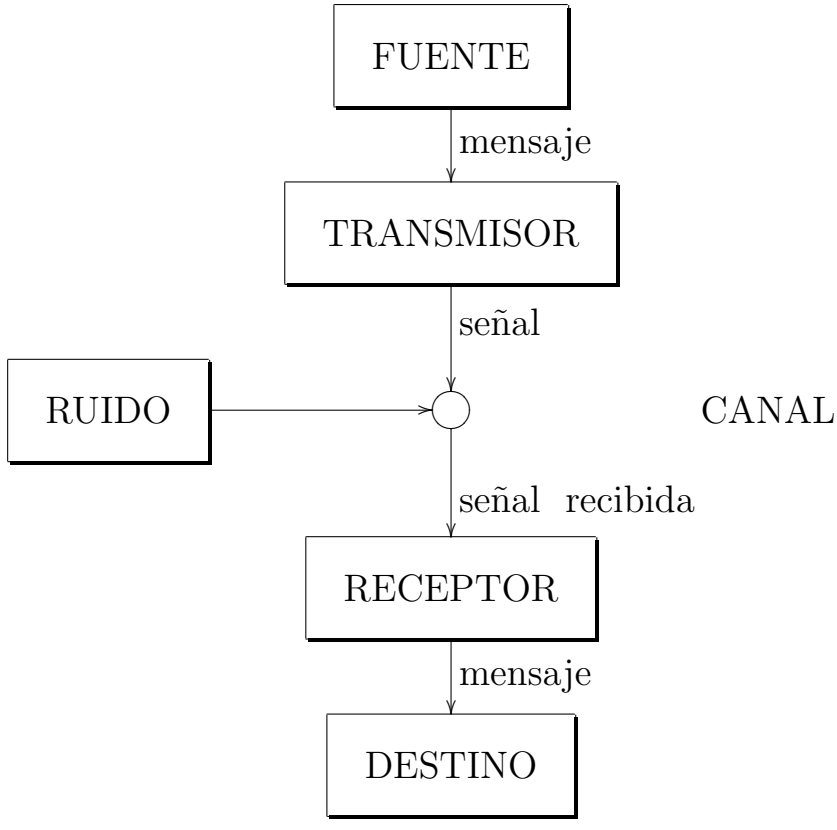

figura 1: Sistema general de comunicación

Una vez que Shannon tuvo claro el enfoque matemático a utilizar, lo aplicó sobre el clásico sistema general de comunicación, indicado en la figura 1, el cual consiste de:

1. Una *fuente de información*, la cual produce un mensaje o secuencia de mensajes a ser comunicados a la terminal receptora. El mensaje puede ser de varios tipos: (a) Una secuencia de letras como en los sistemas de teletipo y telégrafo; (b) Una función de tiempo *f(t)*, como en radio o telefonía; (c) Una

función de tiempo y otras variables, como en televisión blanco y negro, aquí la función es de la forma *f(x,y,t)*, dos coordenadas espaciales y una coordenada de tiempo; (d) Dos o más funciones de tiempo, *f(t), g(t), h(t)*, como es el caso de la transmisión de sonido tridimensional, o en un sistema multiplex de varios canales individuales; (e) Varias funciones de varias variables, como en televisión a color donde el mensaje consiste de tres funciones *f(x,y,t), g(x,y,t), h(x,y,t)* definidas en un sistema contínuo tridimensional, donde tales funciones son vistas como componentes de un campo vectorial definido en dicho espacio o región contínua; (f) Combinaciones de las anteriores, por ejemplo, televisión con un canal de audio asociado.

2. Un *transmisor*, el cual opera sobre el mensaje, de tal forma que produce una señal adecuada para transmitirla sobre el canal. En telefonía, esta operación consiste en cambiar la presión del sonido hacia una corriente eléctrica proporcional. En telegrafía, tenemos una operación de codificación, la cual produce una secuencia de puntos, líneas y espacios, a ser transmitida sobre el canal, lo cual corresponde al mensaje. En un sistema multiplexado, las distintas funciones de voz deben ser muestreadas, compactadas, cuantificadas y codificadas, para finalmente ser intercaladas apropiadamente para construir la señal. Sistemas de televisión y modulación de frecuencia, son otros ejemplos de las operaciones complejas aplicadas al mensaje para obtener la señal.

3. *El canal*, es meramente el medio utilizado para transmitir la señal del transmisor al receptor. Pueden ser un par de alambres, un cable coaxial, una banda de radio frecuencias, un haz

de luz, etc.

4. *El receptor*, de manera ordinaria ejecuta la operación inversa hecha por el transmisor, reconstruyendo el mensaje a partir de la señal.

5. *El destino*, es la persona o cosa a quien se pretende enviar el mensaje.

Entonces, se deben considerar ciertos problemas generales que involucran a los sistemas de comunicación. Lo primero que hizo Shannon en este punto, fue representar los distintos elementos del sistema como entidades matemáticas, idealizadas adecuadamente a partir de sus contrapartes físicas. Y junto con esta representación, hizo una clasificación aproximada de los sistemas de comunicación en tres categorías principales: discretos, contínuos y mezclados. Por sistema discreto, debemos entender un sistema en el cual tanto el mensaje como la señal son secuencias de símbolos discretos. Un caso típico es la telegrafía, donde el mensaje es un secuencia de letras y la señal es una secuencia de puntos, líneas y espacios. Un sistema contínuo es aquel en el cual el mensaje y la señal son ambos tratados como funciones contínuas, como en la radio y la televisión. Un sistema mezclado es aquel en el cual aparecen variables discretas y contínuas, como en los sistemas multiplexados de transmisión de voz.

Entonces, primeramente, consideró el caso discreto, el cual no sólo tiene aplicaciones en Teoría de Comunicación, sino también en Teoría de la Computación, en diseño de telefonía y otros

campos. Además, el caso discreto, es una base para los casos contínuo y mezclado, a los cuales también trató posteriormente.

Shannon analizó el sistema de comunicación completo y principalmente los efectos del ruido sobre el canal de transmisión. También trabajó en algunos precedentes, en cuanto a la generación o naturaleza de una posible fuente de información o generador de mensajes, para que en la siguiente etapa, la del transmisor, se tuviera una codificación aceptable, algo que, si bien en nuestro presente ya no representa una panacea, no deja de ser interesante y digno de una breve mención. Así pues, en el rubro de la codificación, tema que nos compete directamente, Shannon establece que debemos tomar en cuenta el tipo de codificación que es utilizada para transmitir la información, que debemos analizar cómo reduce dicha codificación la capacidad que requiere el canal para la transmisión.

Veamos un caso concreto, tanto de generación del mensaje, como de su codificación: En telegrafía, por ejemplo, los mensajes transmitidos consisten de secuencias de letras. Estas secuencias, sin embargo, no son completamente aleatorias. En general, ellas forman oraciones y tienen la estructura estadística de un lenguaje natural, por ejemplo, el lenguaje Inglés. La letra E ocurre con más frecuencia que la Q, la secuencia TH tiene mayor frecuencia que la secuencia XP, etc. Entonces, la existencia de dicha estructura estadística nos permite un cierto ahorro de tiempo (o de capacidad de canal), si codificamos apropiadamente las secuencias del mensaje en secuencias de señales sobre el canal. Esto se realiza en telegrafía utilizando el símbolo más corto de canal, que es el punto, para la letra más común del

inglés que es la E, mientras que las letras menos frecuentes, tales como Q, X, Z son representadas por secuencias más largas de puntos y rayas. Esta idea también es utilizada en ciertos códigos comerciales, donde palabras y frases comunes son representadas por grupos de cuatro o cinco letras, con considerables ahorros en tiempo promedio. Telegramas de saludos y cumpleaños extienden este procedimiento, de tal forma que codifican de una a dos oraciones, en una secuencia relativamente corta de números.

Ahora bien, podemos pensar en la fuente discreta, como un generador del mensaje, símbolo por símbolo. Esta podrá elegir símbolos sucesivos de acuerdo a ciertas probabilidades, las cuales dependen, en general, de las elecciones precedentes, así como de los símbolos particulares involucrados. Entonces, un sistema físico, o un modelo matemático de un sistema, el cual produce tales secuencias de símbolos, gobernada por un conjunto de probabilidades, es conocido como un proceso estocástico. Por lo tanto, la fuente discreta en cuestión, será representada por un proceso estocástico. A su vez, cualquier proceso estocástico, el cual produce una secuencia discreta de símbolos, elegidos de un conjunto finito, debe ser considerado una fuente discreta. Este proceso podrá incluir casos tales como:

1- Lenguajes naturales como el Inglés, Alemán, Chino, Español.

2- Fuentes de información contínuas que han sido convertidas en discretas, por algún proceso de cuantificación. Por ejemplo, la voz cuantificada de un transmisor, o una señal de televisión cuantificada.

3- Casos matemáticos donde definimos de manera abstracta, un proceso estocástico el cual genera una secuencia de símbolos. Algunos ejemplos son:

(A) Un conjunto de cinco letras, A, B, C, D, E, todas con la misma probabilidad, con elecciones sucesivas e independientes, tal que obtengamos una secuencia, por ejemplo, BDCBCECCCADCBDDAAECEEA. Esta secuencia podría ser construida con el uso de una tabla de números aleatorios.

(B) Utilizando las mismas cinco letras anteriores, pero ahora dándoles las probabilidades .4, .1, .2, .2, .1, respectivamente, con elecciones sucesivas independientes. Un mensaje de esta fuente sería: AAACDCBDCEAADADACEDA.

(C) Una estructura más complicada, es obtenida de símbolos sucesivos que no son elegidos independientemente, pero que sus probabilidades dependen de símbolos precedentes. El caso más simple, es una elección, la cual depende solamente de la letra precedente y de ninguna más. Entonces, tendríamos que manejar probabilidades de transición entre dos letras, o la probabilidad de un "digrama". El siguiente paso, involucraría la elección de una letra en base a las dos letras precedentes, pero no más. En este caso, están involucradas tres letras, o un "trigrama". Continuando de esta manera, obtendríamos procesos más complicados, hasta llegar al caso general, el caso del n-grama, donde se requiere de un conjunto de n probabilidades, para conocer la estructura estadística completa.

(D) Un proceso estocástico que produzca un texto, consis-

tente de una secuencia de “palabras”. Supongamos que tenemos cinco letras, A, B, C, D, E y 16 “palabras” en el lenguaje, con las probabilidades asociadas siguientes:

.10 A	.16 BEBE	.11 CABED	.04 DEB
.04 ADEB	.04 BED	.05 CEED	.15 DEED
.05 ADEE	.02 BEED	.08 DAB	.01 EAB
.01 BADD	.05 CA	.04 DAD	.05 EE

Supongamos “palabras” sucesivas, que son elegidas independientemente y que son separadas por un espacio. Un mensaje típico puede ser:

DAB EE A BEBE DEED DEB ADEE ADEE EE DEB BEBE BEBE BEBE ADEE BED DEED DEED CEED ADEE A DEED DEED BEBE CABED BEBE BED DAB DEED ADEB.

Si todas las palabras son de longitud finita, este proceso es equivalente al de (C), pero la descripción debe ser más simple en términos de estructura de palabra y probabilidades. También se puede generalizar e introducir probabilidades de transición entre palabras, etc.

En síntesis, del análisis anterior, podemos notar lo complejo y aparatoso que podían llegar a ser estos primeros acercamientos teóricos, basados principalmente en probabilidades, a un intento de representar y crear una fuente de información. Y esto solo es parte del problema, ya que posteriormente, una vez que se tienen los mensajes producidos por dicha fuente, se debe tener la codificación para obtener una señal adecuada, que va mas

allá de la codificación por puntos, rayas y números, o sea, llegar al caso práctico de logaritmo en base 2, o lo que es lo mismo, codificación con representación binaria, hay que involucrar al canal y al ruido inherente a él, cosa que el investigador realizó posteriormente, pero que ya no analizamos aquí, pues involucra demasiados aspectos fuera de nuestro alcance.

1.2 Aportaciones de Hamming

Contemporáneo de Shannon, otro de los pioneros en el área fue Hamming, quien cerca de 1950, trabajando en los laboratorios de la compañía Bell, motivado por el cambio tecnológico que involucraba el migrar de sistemas analógicos de comunicación, en aquel entonces ampliamente utilizados, como los sistemas telegráficos, a base de relevadores, hacia los sistemas digitales de comunicación, con la aparición de las primeras computadoras, desarrolló las bases de la Teoría de Códigos que hoy manejamos. Se vivió un momento único en la historia, las comunicaciones ya no serían las mismas, ya que el problema de transmitir información de un lugar a otro, sin errores presentes en el resultado final, ahora se empezaría a resolver por medio de equipos digitales. Un cambio basado en las velocidades de los componentes electrónicos de las computadoras, que resultaron ser elementos básicos mas fiables para las operaciones de transmisión que los relevadores analógicos.

Hamming observa el trabajo teórico de Shannon y, desde un punto de vista práctico, se enfoca en la búsqueda de una buena codificación. Si bien es cierto que, otros investigadores anticiparon algunos códigos en contextos ajenos a la Teoría de Códigos, Hamming dentro de dicha teoría, fue el primero en des-

cubrir por ejemplo, los llamados códigos binarios correctores de un sólo error, que llevan su nombre, los cuales son una familia importante de códigos, ya que presentan una facilidad para su codificación y decodificación.

Asi que, el trabajo de Hamming se centró en darle sentido a la agrupación de símbolos en conjuntos de vectores, para transmisión de información. Tales símbolos eran ceros y unos, basado en la idea de Shannon, sobre el logaritmo base 2, lo cual se acomodaba perfectamente a la situación del momento, ya que cero y uno representan exactamente el comportamiento de un relevador abierto y cerrado respectivamente. Pero como decíamos, no sólo bastaba agruparlos, sino que había que darles un significado para poder realizar la transmisión de información, y al hacer esto, se creó lo que ahora conocemos como códigos binarios. Al darle significado a ese conjunto de vectores binarios, se tuvo que desarrollar necesariamente toda una teoría que respaldara su utilización, y para ello había que jugar con los vectores o palabras de código, con sus parámetros: ampliar y acortar sus longitudes, aumentar y disminuir la cantidad de palabras por código, observar qué sucede cuando se varían parámetros generales. Con ese análisis, al que Hamming dió especial énfasis en su investigación, logró obtener en la práctica, la medida de qué tan bueno es un código para transmitir información. Tal medida es lo que conocemos como la eficiencia de un código, y es lo que había anticipado Shannon en su teorema, pero ahora aterrizado a casos prácticos.

Entonces, para lograr eficiencia, lo que Hamming buscaba era un equilibrio, códigos con la menor redundancia posible (ésta

debe ser vista como la disminución de la capacidad efectiva del canal, para el envío de información), sin descuidar la posibilidad de error en la decodificación. Es decir, lo que se busca es, que para una palabra de código de n dígitos binarios, se transmita la mayor cantidad posible k de dígitos de información, y los restantes bits se desperdicien o utilicen para detectar y corregir errores. De esta forma, una redundancia baja, aumenta la capacidad para envío de información, amén de los errores involucrados.

Lo que logró Hamming en síntesis fue, establecer de manera práctica, los principios para diseñar códigos detectores y correctores de error planteados por Shannon, para resolver condiciones extremas de comunicación, tales como señales desatendidas por largos periodos de tiempo, sistemas grandes y estrechamente relacionados donde una sola falla provoca la incapacidad total del sistema y señales en presencia de ruido, donde es técnicamente difícil reducir el efecto del ruido sobre dichas señales.

Sus resultados nos proporcionan tablas de valores, mediante las cuales encontramos los mejores códigos posibles, para los casos de códigos que detectan un sólo error, códigos que corrigen un sólo error y códigos que detectan dos errores y corrigen uno de ellos, tal que mediante el uso de dichas tablas, nos indican la longitud n mínima necesaria que debe tener el código en cuestión, para transmitir una cantidad k de símbolos de información. También obtuvo otras tablas de valores, que nos indican la posición de cualquier error en un mensaje o palabra de código, por medio de la ubicación que deben tener los símbolos

de chequeo o verificación de error en el mensaje dado.

Otra aportación esencial de Hamming, es el enfoque geométrico del problema, ya que estableció el modelo del cubo de n dimensiones, el cual consiste en relacionar secuencias de ceros y unos, las cuales son las palabras del código, con los vértices de dicho cubo. Gracias a esto, pudo introducir el concepto de distancia o métrica del código, basado en la observación de que un solo error en una palabra de código, cambia una coordenada entre los vértices del cubo, dos errores en una palabra de código, cambian dos coordenadas entre vértices del cubo y en general, d errores en una palabra de código, producen una diferencia en d coordenadas entre los vértices del cubo.

Como consecuencia de lo anterior, se define la distancia de un código lineal, como el número mínimo de dígitos o símbolos en que dos palabras de código cualesquiera son diferentes, o bien, el número de coordenadas distintas entre los vértices del cubo n dimensional, correspondientes a tales palabras. Por ejemplo, notemos que cada una de las siguientes palabras de un código lineal binario cíclico, de longitud 3, colocadas como vértices de un cubo de dimensión 3, están separadas dos unidades o coordenadas, o difieren en dos símbolos, unas de otras:

$$001,\ 010,\ 100,\ 111.$$

Por lo tanto, el número mínimo de separación entre símbolos es 2, lo que nos dice directamente que el código anterior tiene distancia 2. Su representación en un cubo, se muestra en la figura 2:

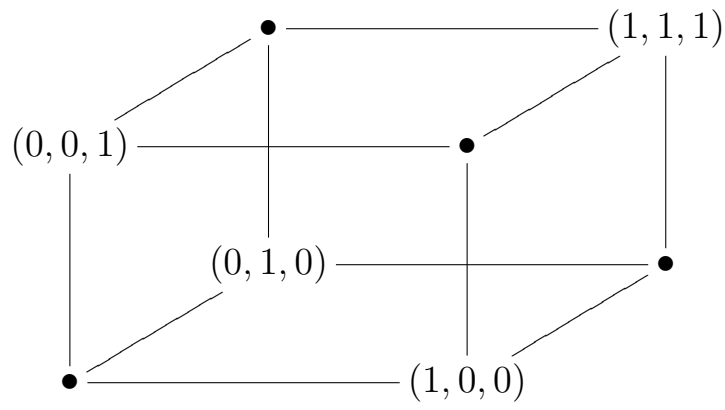

figura 2: representación del código en un cubo

Continuando con el lenguaje geométrico, una esfera de radio r, con respecto a una palabra de código x, se define como todos los vectores que están a una distancia r, con respecto a dicha palabra de código. Así, en el ejemplo anterior, las primeras tres palabras de código están sobre la superficie de una esfera de radio 2, con respecto a la palabra de código 111. De hecho, en el ejemplo, cualquier palabra de código puede ser elegida como centro, ya que las otras tres estarán sobre la superficie de una esfera de radio 2.

Si todas las palabras de código están a una distancia de al menos 2 unas de otras, entonces un sólo error modificará una palabra de código en otro vector que no es palabra del código. Lo que significa que un sólo error o error simple es detectable. Si la distancia entre palabras de código es al menos tres, entonces un error simple, nos dará al vector más cercano a la palabra de código correcta que a cualquier otra, lo que significa

que cualquier error simple podrá ser corregido. Lo anterior se resume en la tabla 1:

Distancia	**Significa**
2	detecta un error
3	corrige un error
4	detecta doble error y corrige uno
5	corrige doble error
	etc

tabla 1: patrón de detección y corrección

Es evidente que, si efectuamos la detección y corrección de la tabla anterior, entonces todas las distancias entre palabras de código, deben ser igual o mayor a la distancia listada. Por lo tanto, el problema de encontrar códigos adecuados, es el mismo que encontrar subconjuntos de vectores en el espacio n dimensional, los cuales mantengan al menos la condición de tal distancia.

De aquí, podemos observar una conexión directa con el trabajo que nosotros realizamos, ya que existe una relación entre la distancia de un código lineal, anteriormente definida, con el peso de dicho código: la distancia de un código lineal es el peso mínimo de cualesquiera de sus palabras, distintas de la palabra cero. De aquí la importancia de obtener la distribución de pesos de los códigos encontrados en nuestra investigación, por los métodos desarrollados que se reportan aquí, ya que esto nos permite saber que tan buenos son tales códigos, con respecto a su

capacidad para detectar y corregir errores, y poder hacer una distinción entre ellos.

1.3 La contribución de Berlekamp

Del trabajo de Shannon y Hamming, hasta el descubrimiento de los códigos correctores de doble error, por Bose y Chaudhuri en 1960 y Hocquenghem en 1959, dando lugar a los códigos BCH, transcurrió aproximadamente una década. La generalización hacia los códigos correctores de t errores, fue inmediatamente lograda, para toda t. Es en ese momento, que el trabajo de Elwyn R. Berlekamp, aparece en escena. El realiza una condensación de los aspectos mas relevantes descubiertos y desarrollados por los investigadores aqui mencionados, de tal manera que esto le permite realizar aportaciones propias, que van desde la mejora en métodos o algoritmos de codificación y decodificación, hasta la generalización de conceptos como la ciclicidad. Su trabajo fue una aportación enorme al campo de estudio, ya que sus descubrimientos son tanto ingenieriles, por medio de los algoritmos y la circuitería necesaria para implementarlos, como matemáticos, al descubrir los polinomios y ecuaciones a resolver para lograr el objetivo [2].

Primeramente, un concepto que juega un rol central en Teoría de Códigos, es, como ya se ha mencionado, el concepto de ciclicidad. Berlekamp, lo generaliza así: si tenemos un código C sobre un campo finito de q elementos, definido como F_q, donde $q = p^m$, con p un número primo y m un entero positivo, entonces, existe $0 \neq a \in F_q$, tal que para cada $c = c_0c_1 \cdots c_{n-1} \in C$, la palabra $(ac_{n-1})c_0c_1 \cdots c_{n-2}$, también pertenece a C. Entonces, podemos identificar códigos cíclicos, si $a = 1$, y con respecto a

la constante $a = -1$, a los llamados códigos negacíclicos. Todos los demás casos para a, nos dan los códigos constacíclicos. De aquí, podemos observar dos cosas: la primera es que, al hacer esta generalización, podemos trabajar automáticamente sobre campos finitos distintos al binario, lo que permite extender el campo de investigación; la segunda cuestión es que, la clase de códigos constacíclicos, incluye como subclases a la clase de códigos cíclicos y a la clase de códigos negacíclicos.

En particular, Berlekamp realizó investigación con respecto a la clase de códigos negacíclicos, sobre todo proponiendo algoritmos para transmisión de la información: Anteriormente, solamente se había considerado el problema de codificación y decodificación para un canal de transmisión binario, cuyas entradas son los símbolos 0 y 1, y cuyas salidas también son los símbolos 0 y 1. En la mayoría de las aplicaciones, la secuencia codificada de ceros y unos se le pasa al bloque modulador, el cual convierte estos símbolos en funciones de tiempo. La función de tiempo resultante es utilizada para controlar la amplitud de la señal transmitida, la cual, por ejemplo, podría ser el voltaje de un cable o la potencia instantánea emitida por un transmisor de radio.

Ahora, gracias a la generalización de ciclicidad, pudo trabajar con códigos constacíclicos o negacíclicos, es decir, en un caso no binario, y utilizar algunos esquemas de decodificación para tales casos, por ejemplo, utilizando un alfabeto de cinco símbolos: 0, 1, 2, 3, 4, es decir, sobre F_5. En este caso, Berlekamp trabajó con códigos negacíclicos sobre dicho campo finito, obteniendo valores altos de capacidad de corrección de error, produciendo códigos

buenos sobre alfabetos de orden primo distinto del binario, ya que además de trabajar sobre F_5, también obtuvo códigos negacíclicos con buenos parámetros para corrección de error, sobre F_7, F_{11}, F_{17} y F_{127}. De tal forma que obtuvo una clase amplia de códigos negacíclicos.

En cuanto a los algoritmos de codificación y decodificación, podemos mencionar lo siguiente: El trabajo de Berlekamp en decodificación de códigos cíclicos, que incluyó a los famosos códigos Reed-Solomon [16] y a los códigos BCH [3], fue el esfuerzo brillante de la década. La técnica de Peterson de utilizar inversión matricial para encontrar los coeficientes de error en la transmisión, es demasiado complicada para la decodificación de cantidades grandes de errores. Berlekamp desarrolló un algoritmo brillante, fácilmente mecanizable, que reemplazó al de Peterson. La decodificación de cantidades grandes de errores utilizando códigos Reed-Solomon de longitud grande, se hizo práctico inmediatamente y fue en muchas aplicaciones ya una necesidad. Por ejemplo, uno de los códigos estandar de la NASA, el cual es un código corrector de 16 errores, ha utilizado desde entonces el algoritmo de Berlekamp, en algunas naves espaciales. El ataque de Berlekmap al problema de decodificación, era tan inventivo y original, que requirió de 10 años y un equipo de cuatro matemáticos japonenes (Sugiyama, Kasahara, Hirasawa y Namekawa, en 1975), para ser reconocido como una improvisación de un replanteo o mejora del algoritmo de Euclides [22]. Matemáticamente hablando, James Massey demostró que dicho algoritmo, es un nuevo método para hallar polinomios del menor grado de manera recursiva, dado un conjunto de condiciones iniciales. Berlekamp también contribuyó en la simplificación de los

cálculos de codificación Reed-Solomon, a través de su trabajo en codificación serial de bits. Un circuito decodificador simple para códigos Reed-Solomon, de integración a gran escala (VLSI por sus siglas en inglés), que utiliza el multiplicador serial de bits de Berlekamp, fue implementado en 1984, por Reed, sus estudiantes en USC, y por T.K. Truong de los Laboratorios de Propulsión Reactiva (JPL, siglas en inglés).

Desde un punto de vista práctico, Berlekamp analizó las preguntas más importantes acerca de cualquier código: (1) ¿Qué tan bueno es éste? (2) ¿Qué tan fácil es decodificarlo? y (3) ¿Cuál es su tasa de información?, donde dicha tasa se define como $R = m/n$, con m, el número de símbolos de información del código y n su longitud. Las preguntas (1) y (2) son preguntas de ingeniería, porque las palabras "bueno" y "fácil" pueden ser definidas solamente en términos de la medida de ruido en el canal, el cual nunca es conocido de manera exacta, o del costo de la circuitería, lo cual depende de la tecnología electrónica del momento. Si medimos "bueno" en términos de la distancia del código diseñado, entonces se pueden dar respuestas aproximadas a (1) y (2): para (1), la distancia puede ser especificada arbitrariamente, para (2), La decodificación es relativamente fácil. Estas respuestas son muy alentadoras. Diferente de (1) y (2), la pregunta (3) es una cuestión matemática, y su respuesta es decepcionante en cierto sentido, porque al momento no existen códigos mejores de gran longitud, que tengan una tasa de información más alta, y por lo consiguiente, no podemos hablar de algoritmos de decodificación para ellos.

Entonces para diseñar sus algoritmos, tuvo que considerar

varias cosas: Elegir un conjunto de señales y decidir la regla de demodulación. Esta elección depende de las características detalladas del canal. La potencia de ruido, su espectro, las limitaciones de frecuencia sobre el transmisor, las limitaciones de potencia sobre el transmisor, y posibles interferencias entre símbolos. Entonces lo que hizo, fue asumir que el modulador, el demodulador, y la función de peso del código, estaban dadas, y concentrar la atención en el problema de corregir los errores en la etapa de demodulación del lado del receptor, por medio de codificación y decodificación adecuadas.

Para lograr el objetivo, un método utilizado, fue el decodificar "tachaduras" así como errores: Para algunos canales, resulta muy prudente el no forzar al demodulador a realizar una elección entre alternativas muy cercanas. La mejor estrategia es demodular los símbolos de señales suficientemente débiles o suficientemente ambiguas, no como cualquiera de las q letras del alfabeto en uso, sino como un símbolo o letra adicional, ?, etiquetado como una borradura o tachadura. Además, localizar y corregir cualesquiera errores que pudieran estar presentes; entonces, el decodificador debe intentar determinar los valores de los símbolos en las posiciones tachadas. Así pues, el objetivo del decodificador es corregir todas las erratas, las cuales consisten en dos tipos: tachaduras, cuyas posiciones son conocidas, pero cuyos valores son desconocidos, y los errores, cuyas posiciones y valores son ambos desconocidos. Entonces, para lograr tal corrección, Berlekamp halló tres polinomios localizadores distintos: localizador de tachadura, localizador de error y localizador de errata. Se resuelven mediante un algoritmo o método sencillo, pero tedioso, que aquí no es necesario desarrollar. De esta forma,

Berlekamp encontró varios algoritmos para codificar y decodificar, la mayoría de ellos aplicables a códigos Reed-Solomon.

2 Algunas aplicaciones

2.1 La exploración espacial

La exploración del sistema solar por medio de naves espaciales no tripuladas, es uno de los triunfos humanos desde el siglo pasado. Las dramáticas fotografías de Mercurio, Venus, Marte, Jupiter, Saturno, Urano, y Neptuno transmitidas por naves espaciales, con nombres románticos como *Mariner*, *Voyager*, *Viking*, etc., sobre distancias de cientos de millones, incluso billones, de millas, ha hecho a estos planetas, los cuales eran conocidos previamente como imágenes difusas de un telescopio en libros de texto, tan reales para nosotros, como lo son los Himalayas, el Sahara o la Antártida. Las aplicaciones espaciales con codificación para control de error en general, han sido parte de la tecnología de exploración desde sus inicios, desde los tiempos "prehistóricos" en 1970, hasta el presente, y hacia el futuro.

La misión Mariner 9

Lanzado el 30 de Mayo de 1971, arribando a Marte el 14 de Noviembre del mismo año, y apagado el 27 de octubre de 1972, el Mariner 9 tenía como objetivos, el mapear el 70% de la superficie marciana y estudiar los cambios temporales en la atmósfera. Para el mapeo, fue utilizada una cámara blanco y negro de tv, la cual transmitía "en vivo" fotografías de la superficie. Cada foto receptor en la cámara medía la luminosidad de una sección de la superficie marciana de entre 4 y 5 kilómetros cuadrados,

y producía un valor en escala de grises en el rango de 0 a 63, y a su vez, este valor era representado como un vector binario de longitud 6. De tal manera, que la imagen de televisión era digitalizada por el banco de foto receptores y producía como salida, un flujo de miles de vectores binarios.

La necesidad de codificar

Sin codificación y una probabilidad de fallo $p = 0.05$, el 26% de la imagen sería errónea, una calidad inaceptable para la naturaleza de la misión. Ahora, cualquier codificación aumentaría la longitud del mensaje transmitido. Debido a las restricciones de energía a bordo de la sonda, y a las restricciones en las estaciones receptoras en la Tierra, el mensaje codificado no podría ser mayor a 5 veces la longitud de los datos. Así, un vector binario de 6 bits de datos debía ser codificado como una palabra de código cercana a los 30 bits de longitud. Entonces, la *redundancia* es construida en la señal, es decir, la secuencia transmitida consiste de más que la información necesaria. Estamos familiarizados con el principio de redundancia, gracias a nuestro lenguaje diario. Las palabras de nuestro lenguaje forman una pequeña parte de todas las posibles cadenas de letras o símbolos. En consecuencia, un error de imprenta en una palabra larga es reconocido, porque la palabra es cambiada en algo que se asemeja a la palabra correcta, más de lo que se parece a cualquier otra palabra que conocemos. Esta es la esencia de la codificación.

Otras consideraciones

Una segunda consideración involucra al procedimiento de codificación. El almacenamiento de datos requiere blindaje del medio de almacenamiento, este es peso muerto a bordo de la nave, y la economía exige que haya poco de él. La codificación por lo tanto debía ser realizada "sobre el aire", sin requerimientos de memoria permanente. Por su parte, la decodificación requirió realizarse velozmente. El Laboratorio de Propulsión Reactiva (JPL) en Pasadena California, procesó las señales y las reconvirtió en imágenes de video para la prensa que se dió cita en el JPL. Además de esta prioridad, la decodificación rápida es necesaria, para que la realimentación de la nave sea viable, redireccionando la cámara en función de lo que se ve.

El código

El código seleccionado es un código corrector de 7 errores, el cual reduce la probabilidad de error en la imagen al 0.01%. La decisión sobre cuál código utilizar, se basó principalmente en el algoritmo de decodificación. El algoritmo se llevó a cabo, por una pieza bastante simple de circuitería especializada, llamada "Green Machine" (por el apellido de su creador). El código seleccionado fue un código Reed-Muller, el cual examinamos a continuación.

Definición recursiva de Códigos Reed-Muller

Los códigos Reed-Muller son de los códigos más antiguos conocidos, y han encontrado amplias aplicaciones. Fueron descubier-

tos por Muller y provistos de un algoritmo de decodificación por Reed en 1954.

Definición: Los códigos Reed-Muller de primer orden $\mathcal{R}(1, m)$ son códigos binarios definidos para todo entero $m \geq 1$, de manera recursiva por:

(i) $\mathcal{R}(1, 1) = \{00, 01, 10, 11\} = \mathbb{Z}_2{}^2$.

(ii) para $m > 1$,

$$\mathcal{R}(1, m) = \{(\mathbf{u}, \mathbf{u}), (\mathbf{u}, \mathbf{u} + \mathbf{1}) : \mathbf{u} \in \mathcal{R}(1, m - 1)\}$$

donde $\mathbf{1} =$ vector de unos.

Entonces, para $m > 0$, el código Reed-Muller $\mathcal{R}(1, m)$ es un código lineal binario $[2^m, m + 1, 2^{m-1}]$, en el cual cada palabra de código excepto $\mathbf{0}$ y $\mathbf{1}$ tienen peso 2^{m-1}, es decir, todas las palabras menos $\mathbf{0}$ y $\mathbf{1}$, tienen la mitad de bits en 0 y la mitad de bits en 1. Así, el código tiene distancia 2^{m-1}, por lo tanto, puede corregir $2^{m-2} - 1$ errores.

Ejemplos

Así,

$$\mathcal{R}(1, 2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\},$$

$$\mathcal{R}(1,3) =$$

$$\{00000000, 00001111,$$
$$01010101, 01011010,$$
$$10101010, 10100101,$$
$$11111111, 11110000,$$
$$00110011, 00111100,$$
$$01100110, 01101001,$$
$$10011001, 10010110,$$
$$11001100, 11000011\}.$$

De regreso al Mariner 9

Recordemos que en la misión del Mariner 9, los datos consistían de vectores binarios de longitud 6 (64 niveles de escala de grises), y las restricciones de transmisión requerían que la longitud de las palabras de código fuera de alrededor de 30 bits. Entonces, el código elegido fue el código Reed-Muller $\mathcal{R}(1,5)$, el cual es un código binario $[32, 6, 16]$, es decir, se tienen 64 palabras de longitud 32, y ya que su distancia es 16, puede corregir 7 errores.

Codificación

Como hay 64 palabras de código y 64 tipos de dato, cualquier asignación de palabra de código para el tipo de datos va a funcionar, pero el requisito de que la codificación no debería requerir

memoria, significa que una asignación arbitraria no funcionaría. Puesto que $\mathcal{R}(1,5)$ es un código de dimensión 6 , existe una base con 6 elementos (cualquier combinación lineal la cual nos da una palabra de código). El tipo de dato como vector de 6 bits, se utiliza para proporcionar los coeficientes para la combinación lineal de los vectores de la base, asociando así una palabra de código única para cada tipo de dato. Este cálculo simple puede ser cableado y no requiere memoria.

Como hemos mencionado anteriormente, la verdadera razón para la selección de este código, es que tiene un algoritmo de decodificación muy rápido, ya que los cálculos involucrados pueden acelerarse por un factor de 3, utilizando una Transformada rápida de Fourier sobre grupos Abelianos. Esto es lo que en esencia, hizo la "Green Machine".

Otras misiones

Las naves Voyager 1 y 2, transmitieron fotografías a color de Jupiter y Saturno en 1979 y 1980. La transmisión a color, requiere 3 veces la cantidad de datos, por lo que un código diferente, el código *Golay* (24, 12, 8) fue utilizado [12]. Este sólo corrige 3 errores, pero su tasa de transmisión es mucho más alta. El Voyager 2 viajó hacia Urano y Neptuno, y el código se cambió a un código Reed-Solomon [16], debido a sus capacidades de corrección superiores.

El Estándar CCSDS

Al día de hoy, el uso de codificación en sistemas de telemetría es-

pacial, se ha vuelto una rutina, por lo que no es de sorprenderse que un comité se encargue de escribir el estándar. De hecho, en Mayo de 1984, El Comité Consultivo para Sistemas de Información Espacial (CCSDS, por sus siglas en inglés), que representa a las agencias espaciales de la mayor parte del mundo, incluyendo la NASA y la Agencia Espacial Europea (ESA), emitió una recomendación oficial para un estándar de codificación en telemetría, el cual ha sido adoptado para su uso en numerosas misiones planetarias, incluyendo el malogrado *Mars Observer* de la NASA (a Marte: lanzado en Septiembre de 1992, arribando en Agosto de 1993), *Cassini* (a Saturno: lanzado en 1997, arribando en 2004), la misión conjunta NASA/ESA *Ulysses* (a las regiones polares del sol: lanzado en 1990, arribando en Junio de 1994), y la misión *Giotto* (lanzado el 2 de Julio de 1985, y arribando al cometa Halley en la primavera de 1986, y también transmitiendo imágenes del espacio profundo, como lo hiciera el *Voyager*).

2.2 Códigos Reed-Solomon y el disco compacto

Una de las aplicaciones más espectaculares de la Teoría de Códigos correctores de error, es el Sistema de Audio Digital de Disco Compacto. Este puede ser considerado como un sistema de transmisión que traslada sonido desde el estudio de grabación a la sala de estar. El sonido codificado en bits de datos y modulado en bits de canal, se envía a lo largo del "canal de transmisión", consistente de escritura láser, disco maestro, disco de usuario y lector óptico. Las imperfecciones del disco, producirán errores en los datos recuperados. La naturaleza de los errores conduce, en forma natural, a la adopción de códigos Reed-Solomon. El

sistema de disco compacto fue el primer ejemplo de la introducción de tales códigos en un producto de consumo.

Las ventajas de la grabación de audio y video han sido apreciadas por largo tiempo, y por supuesto, las computadoras han sido operadas durante mucho tiempo en el dominio digital. La aparición de circuitería digital, cada vez más barata y rápida, ha hecho posible la creación de nuevos dispositivos tales como el disco compacto y la grabadora del Cassette Compacto Digital (DCC), una posibilidad no factible, utilizando generaciones previas de circuitería análoga convencional. La principal ventaja que confiere la implementación digital sobre los sistemas análogos, es que en un sistema de grabación digital bien diseñado, la única degradación significativa, toma lugar en la digitalización inicial, y la fidelidad se mantiene hasta el punto final de falla. En un sistema análogo, la fidelidad del sonido se ve disminuida en cada etapa del procesamiento de la señal, y claramente el número de generaciones de grabación está limitado.

La provisión de códigos correctores de error, por la necesidad de trabajar en el dominio digital, ha hecho posible reconstituir casi perfectamente la señal grabada, incluso en la presencia de imperfecciones en el medio de grabación y en el medio de reproducción. No es una exageración decir que, sin códigos correctores de error, el audio digital no es técnicamente posible. Existen dos tipos de errores: aquellos que son distribuidos al azar entre los bits individuales, llamados *errores aleatorios*, y aquellos que ocurren en grupos, y que cubren cientos o incluso miles de bits, llamados *errores de ráfaga*. Los errores de ráfaga, causados por abandonos, son usualmente el resultado de contaminación

en la superficie por huellas dactilares y rasguños en el disco. La caracterización anterior del canal de grabación es por necesidad cualitativa. Cualquier declaración más allá de obviedades como "algunos errores de ráfaga son más grandes que otros" es especulativa y debe ser manejada con gran cuidado.

Las técnicas de codificación son utilizadas en sistemas de comunicación para mejorar la fiabilidad y eficiencia del canal de comunicación. La *fiabilidad* es expresada comúnmente en términos estadísticos, tal como la probabilidad de recibir la información incorrecta, es decir, información que difiere de aquella que fue originalmente transmitida. El control de error se refiere a técnicas de entrega de información de una fuente (el remitente) a un destino (el receptor) con un mínimo de errores. En un sistema de grabación de audio digital, la señal de sonido es digitalizada en la forma de símbolos binarios. El flujo digital de datos así obtenido no es grabado directamente en cinta. Con el fin de hacer posible la grabación de forma fiable de los datos digitales, los datos son, antes de grabar, traducidos en dos pasos sucesivos: (a) código corrector de errores y (b) código de grabación. La salida generada por el código de grabación es colocada en el medio de almacenamiento en la forma de cantidades físicas binarias, por ejemplo, en magnetizaciones positivas y negativas. Durante la lectura de salida, los datos son obtenidos vía los decodificadores, por el código de grabación y por el código corrector de errores. Esquemáticamente, los elementos de los pasos de codificación en un grabador digital, son similares a aquellos de un enlace de comunicación "punto a punto", como en la figura 1. Las cantidades físicas escritas sobre el medio, son generalmente muy pequeñas, y esto significa que los abandonos

causados por huellas dactilares o defectos en el medio, así como los métodos para hacerles frente, son de gran importancia. El control de corrección de errores es realizado mediante la adición de símbolos extra al mensaje transmitido. Estos símbolos extra hacen posible para el receptor, detectar y/o corregir algunos de los errores que pueden ocurrir en el mensaje recuperado. El desafío principal es lograr la protección requerida contra los errores de transmisión inevitables, sin pagar un precio demasiado alto al agregar símbolos extra (la adición de símbolos extra reducirá la capacidad efectiva del medio de almacenamiento). Existen distintas familias de códigos correctores de error. De importancia mayor para aplicaciones de grabación, es la familia de *códigos Reed-Solomon (RS)*. La razón para su preferencia en sistemas de grabación es que pueden combatir combinaciones de errores, aleatorios y de ráfaga. La historia exitosa de los códigos RS inició con esta primera aplicación práctica en grabaciones de audio digital.

Los códigos de Reed-Solomon fueron inventados por Irving S. Reed y Gustave Solomon en los laboratorios Lincoln del MIT. Son una subclase especial de los códigos BCH generalizados [3]. Siendo específicos, un código Reed-Solomon de longitud n y dimensión k sobre un campo finito $\mathbb{F}_q$, con $q = p^m$, donde p es un número primo, y m un entero positivo, es un código cíclico de distancia $d = n - k + 1$, cuya propiedad especial es que su longitud n es igual a $q - 1$. Por supuesto, q nunca es 2.

Para finalizar esta sección, debemos decir que el disco compacto, estandarizado por Sony y Philips en 1980, fue el primer ejemplo de la amplia introducción de códigos Reed-Solomon en

el mercado de consumo. Después de eso, los códigos RS han dominado en productos de almacenamiento de video y audio digital, tales como el grabador DAT, el Cassette Compacto Digital (DCC), y los grabadores de video D1-D2 [22].

Dejamos las aplicaciones de los códigos de bloque correctores de error, para hablar brevemente sobre la herramienta matemática que nos permitió desarrollar el trabajo descrito en los siguientes capítulos.

2.3 La herramienta matemática básica para determinar la distribución de pesos de códigos cíclicos reducibles sobre campos finitos

De entre las diferentes técnicas que existen para determinar la distribución de pesos de códigos cíclicos, podemos mencionar aquella que hace uso de sumas exponenciales, y que, mediante su evaluación, determina la distribución de sus valores, y a su vez, con dicha distribución de valores, podemos obtener la distribución de pesos de los códigos en cuestión. Esta es la técnica que utilizamos en los métodos que desarrollamos, y que reportamos en este trabajo.

En general, las sumas exponenciales son herramientas importantes en teoría numérica para resolver problemas que involucran enteros (y números reales en general) que a menudo son intratables por otros métodos. Sumas análogas pueden ser consideradas en el contexto de campos finitos y resultan ser útiles en varias aplicaciones sobre tales campos, como en nuestro caso, el cálculo de la distribución de pesos de códigos cíclicos sobre dichas estructuras.

Un rol básico en establecer sumas exponenciales para campos finitos, es jugado por un grupo especial de homomorfismos conocidos como *caracteres*. Distinguimos dos tipos de caracteres (caracteres aditivo y multiplicativo) dependiendo de cuando se haga referencia al grupo aditivo o al grupo multiplicativo del campo finito. Estos son mapeos del grupo aditivo o multiplicativo de dicho campo hacia las raíces de la unidad. Y las sumas exponenciales son formadas utilizando los valores de uno o mas caracteres y posiblemente combinando éstos con funciones de pesos o con otras funciones. Si sumamos los valores de un sólo caracter, estamos hablando de una suma de caracter.

Debido a la combinación de distintas funciones, para formar a las sumas exponenciales, también existe una clasificación de ellas en familias, podemos mencionar por ejemplo, a la familia de sumas Gaussianas, la cual es posiblemente, el tipo más importante de sumas exponenciales para campos finitos, ya que ellas gobiernan la transición de la estructura aditiva a la estructura multiplicativa y viceversa. Ellas también aparecen en otros contextos en álgebra y teoría numérica.

Las sumas exponenciales se remontan a los primeros trabajos de Lagrange y Gauss, y a la posterior evaluación explícita de ciertas sumas exponenciales básicas, ahora llamadas sumas Gaussianas en su honor. Desde entonces, muchas más sumas exponenciales generales han sido consideradas, pero generalmente, ha sido imposible encontrar evaluaciones explícitas para estas sumas más complicadas. Sin embargo, su evaluación está estrechamente conectada al problema de contar el número de

puntos sobre curvas correspondientes (en general, de las variedades algebraicas), definidas sobre extensiones finitas de $\mathbb{F}_q$ [15], y métodos profundos en geometría algebraica, han sido desarrollados para encontrar buenos límites de valores en tales números. Dos importantes logros de dichos métodos, son el anuncio de Weil en 1940, de la demostración de la hipótesis de Riemann para curvas sobre campos finitos, y la demostración de Deligne de las conjeturas de Weil, para variedades algebraicas. Estos resultados son considerados como grandes logros de las matemáticas del siglo XX, y de ellos, se pueden deducir de manera fácil algunos buenos límites de valores para muchas clases de sumas exponenciales.

En contraste con la profundidad y la sofisticación de las técnicas utilizadas por Weil y Deligne, los límites de valores que ellos encontraron son bastante fáciles de establecerse y utilizarse. Los teóricos de la Codificación y los ingenieros de Comunicaciones, han sido extraordinariamente fecundos en explotar esta facilidad de uso.

Entonces, resumiendo, además de utilizar las sumas exponenciales, para el cálculo de la distribución de pesos de ciertos códigos sobre campos finitos, existen muchas más aplicaciones, como por ejemplo, el estudio de curvas sobre campos finitos, aplicaciones importantes en comunicaciones, como el estudio de acceso múltiple de espectro amplio, o el problema de control de potencia en Multiplexación Ortogonal por División de Frecuencia (OFDM) y el diseño de secuencias de periodo corto, todas ellas analizadas en [1].

Las sumas exponenciales particulares que utilizamos en la investigación, junto con su definición y demás aspectos, se contemplan a detalle en los capítulos 3 y 4 de este trabajo.

Capítulo 3

Sobre la Distribución de Pesos del Dual de algunos Códigos Cíclicos con Dos Ceros No Conjugados

RESUMEN

Una familia importante de códigos para el control de errores en comunicaciones digitales, son los llamados códigos cíclicos. Por lo tanto, encontrar la distribución de pesos de un código cíclico q-ario C, no sólo es un problema de interés teórico sino también tiene una importancia práctica. Típicamente, cuando el campo finito $\mathbb{F}_q$ es un campo primo, el problema es manejado expresando el peso de Hamming de cada palabra de código en C por medio de cierta combinación de sumas exponenciales. En este trabajo, presentaremos un nuevo método para calcular la distribución de pesos del dual de algunos códigos cíclicos con dos ceros no conjugados. Como veremos, tal distribución esta dada también en términos de la evaluación de ciertas sumas exponenciales, sin embargo, tal evaluación será solamente necesaria sobre un subconjunto. Por otra parte, este método tiene la ventaja de la flexibilidad, en el sentido que puede también ser aplicado a códigos cíclicos sobre campos finitos de orden no primo. Este capítulo es la transcripción de [24].

Palabras clave: Distribución de Pesos, sumas exponenciales, secuencias lineales de recurrencia y códigos cíclicos.

1 Introducción

Sea $q = p^m$ donde p es un número primo y m es un entero positivo. Para algún entero positivo k, sea γ un elemento primitivo de $\mathbb{F}_{q^k}$. Sea C el código cíclico sobre $\mathbb{F}_q$ de longitud $n = q^k - 1$. Encontrar la distribución de pesos de C es un problema tanto de interés teórico como práctico. Típicamente, cuando el campo finito $\mathbb{F}_q$ es un campo primo, el problema es manejado expresando el peso de Hamming de cada palabra de código en C por medio de cierta combinación de sumas exponenciales. Para ser más precisos, si C es un código cíclico reducible con polinomio de chequeo de paridad $h(x) = h_1(x)h_2(x)\cdots h_t(x)$ $(t > 1)$, donde $h_i(x)$ $(1 \leq i \leq t)$ son polinomios irreducibles distintos sobre $\mathbb{F}_p[x]$ con el mismo grado k, y si γ^{-a_i} es un cero de $h_i(x)$ $(1 \leq i \leq t)$, entonces la distribución de pesos del código cíclico C puede ser derivada de la distribución de valores de la suma exponencial (ver por ejemplo [5, 14])

$$\sum_{c \in \mathbb{F}_{q^k}} \chi(d_1 c^{a_1} + d_2 c^{a_2} + \cdots + d_t c^{a_t}) \ ,$$

donde χ es el caracter aditivo canonico de $\mathbb{F}_{p^k}$, y $d_1, d_2, \cdots, d_t \in \mathbb{F}_{p^k}$.

En este trabajo, presentamos un nuevo método para calcular la distribución de pesos de algunos códigos cíclicos cuyo código dual tiene dos ceros no conjugados. Esto es, demostraremos que si C es un código cíclico sobre $\mathbb{F}_q$, cuyo código dual tiene ceros γ^{a_1} y γ^{a_2}, donde los enteros a_1 y a_2 satisfacen $a_1 q^i \not\equiv a_2 \pmod{q^k - 1}$, para toda $i \geq 0$ y $\mathrm{mcd}(a_1, (q^k - 1)/(q - 1)) = \mathrm{mcd}(a_2, (q^k - 1)/(q - 1)) = 1$, entonces siempre es posible encontrar un entero ω tal que la distribución de pesos de C puede

ser obtenida completamente por medio de la distribución de los valores de

$$\sum_{c \in \mathbb{F}_{q^k}} \chi(dc^{\omega} - c) \ ,$$

donde $d \in \mathbb{F}_{q^k}^*$. Sin embargo, como veremos, el cálculo de tales valores es necesario solamente sobre un subconjunto de $\mathbb{F}_{q^k}^*$. Además, este método alternativo tiene la ventaja de la flexibilidad, en el sentido de que también puede ser aplicado a códigos cíclicos sobre campos finitos de orden no primo.

Para lograr nuestro propósito, utlizaremos varios resultados relacionados a secuencias lineales de recurrencia y sumas exponenciales. Estos resultados pueden ser encontrados en [10].

Este capítulo está organizado de la siguiente manera: en la sección 2, recordamos la conexión entre códigos cíclicos lineales y secuencias lineales de recurrencia. En la sección 3, utilizamos algunas caracterizaciones para los códigos cíclicos irreducibles de un sólo peso, para poder obtener algunos resultados preliminares. La sección 4 está dedicada a presentar algunos resultados preliminares, pero ahora relacionados a sumas exponenciales y a sumas Gaussianas. El nuevo método para calcular la distribución de pesos es presentado en la sección 5. Finalmente, en la sección 6 se muestran algunos ejemplos y se anexan las conclusiones.

2 Secuencias Lineales de Recurrencia y Códigos Cíclicos

Antes que nada, establecemos, para esta sección y para el resto del capítulo, la siguiente:

Notación: Utilizamos p, q y k, para denotar enteros positivos, tal que p es un número primo y q es una potencia positiva de p. Fijamos $n = q^k - 1$ y $\Delta = (q^k - 1)/(q - 1)$. De aquí en adelante, γ denotará un elemento primitivo fijo de $\mathbb{F}_{q^k}$. Como es usual, $\mathrm{wt}(c(x))$, significa el *peso de Hamming* del polinomio $c(x)$ en el anillo $\mathbb{F}_q[x]/(x^n - 1)$. Además, denotaremos con "Tr", el *mapeo traza absoluta* de $\mathbb{F}_{q^k}$ al campo primo $\mathbb{F}_p$, y con "$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$" el *mapeo traza* de $\mathbb{F}_{q^k}$ a $\mathbb{F}_q$. Finalmente, denotaremos por $\mathcal{C}_b$ la *clase ciclotómica modulo n* sobre el campo primo $\mathbb{F}_p$ el cual contiene a b, donde $0 \leq b < n$. El subíndice b es llamado el *representante de clase modulo n* (ver por ejemplo [12, p.197]).

Sean $h(x)$ y $g(x)$ polinomios mónicos sobre $\mathbb{F}_q$, tal que $h(x)$ es irreducible, grado$(h(x)) = k$ y $h(x)g(x) = x^n - 1$. Sin pérdida de generalidad, podemos suponer que:

$$h(x) = x^k - h_{k-1}x^{k-1} - h_{k-2}x^{k-2} - \cdots - h_0 \ .$$

Dado que los coeficientes del polinomio $g(x)$, se pueden obtener a través de la división sintetica de los polinomios $x^n - 1$ y $h(x)$, entonces, si

$$g(x) = g_0x^{n-1} + g_1x^{n-2} + \cdots + g_{k-1}x^{n-k} + \cdots + g_{n-1} \ , \qquad (1)$$

tenemos $g_i = 0$ para toda $0 \leq i < k - 1$, $g_{k-1} = 1$ y

$$g_{m+k} = h_{k-1}g_{m+k-1} + h_{k-2}g_{m+k-2} + \cdots + h_0g_m \ ,$$

con $0 \leq m < n-k$. Es decir, los n coeficientes de $g(x)$ en (1) son los primeros n términos de la *secuencia de respuesta al impulso de orden k* (ver [10, p.402]), dada por

$$g_{m+k} = h_{k-1}g_{m+k-1} + \cdots + h_0 g_m \text{ para } m = 0, 1, 2, \cdots . \quad (2)$$

De acuerdo con el Teorema 8.27 en [10, p.408], la secuencia anterior es *periódica* (en el sentido de la Definición 8.5 en [10, p.398]), donde tal periodo, r, es igual al *orden* de $h(x)$ (ver por ejemplo la Definición 3.2 en [10, p.84]), es decir, $r = \text{orden}(h(x))$.

Utilizamos la misma notación utilizada en [10, Ch. 8, Secc. 5, p.423]. Así, $S(h(x))$ denotará al conjunto de todas las *secuencias de recurrencia lineal homogéneas* en $\mathbb{F}_q$ con polinomio característico $h(x)$. De manera particular, denotaremos con σ el elemento único en $S(h(x))$, el cual corresponde a la secuencia de respuesta al impulso de orden k cuyo polinomio característico es $h(x)$. Es decir, en el contexto de (2), vemos que $\sigma = g_0, g_1, g_2, \cdots$. Para cualquier secuencia $\tau = t_0, t_1, t_2, \cdots$ en $\mathbb{F}_q$, para cualquier entero $s \geq 0$ y para cualquier elemento del campo finito $d \in \mathbb{F}_q$, denotamos por $d\tau^{(s)}$ la secuencia corrida y pesada $dt_s, dt_{s+1}, dt_{s+2}, \cdots$. Dado que el periodo r, de σ, divide la longitud n, entonces los n coeficientes del polinomio $dx^s g(x)$, en el anillo $\mathbb{F}_q[x]/(x^n - 1)$, son los primeros n términos de la secuencia corrida y pesada $d\sigma^{(s)}$.

Sea $\tau = t_0, t_1, t_2, \cdots$ cualquier secuencia en $\mathbb{F}_q$. Adicionalmente, sea $e \in \mathbb{F}_q$ y sea N un entero positivo. Entonces, denotaremos por $Z(\tau, e, N)$ el número de i, $0 \leq i < N$, con $t_i = e$

(esta notación es similar a la utilizada en [10, p.453]). Dado que $r|n$ entonces, para el caso particular de la secuencia σ, tenemos

$$Z(d\sigma^{(s)}, 0, n) = Z(\sigma, 0, n), \ \forall \ d \in \mathbb{F}_q^* \text{ y enteros } s \geq 0. \qquad (3)$$

Finalizamos esta sección recordando que la secuencia de respuesta al impulso de orden k, llamada σ, puede ser dada por medio de la función traza; es decir, si α es una raíz de $h(x)$, entonces en virtud del Teorema 8.24 de [10, p.406], sabemos que existe $\theta \in \mathbb{F}_{q^k}$ de tal manera que los elementos de la secuencia σ estan dados por

$$g_m = \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\theta\alpha^m) \ \text{ para } m = 0, 1, 2, \cdots . \qquad (4)$$

Una fórmula explícita para θ es presentada en [20, Lema 3].

3 Códigos Cíclicos Irreducibles de un Sólo Peso y algunas de sus consecuencias

La siguiente definición podría ser considerada como una extensión del orden, orden(f), de un polinomio $f(x) \in \mathbb{F}_q[x]$.

Definición 1 *Sea $h(x) \in \mathbb{F}_q[x]$ un polinomio de grado positivo con $h(0) \neq 0$. El entero positivo más pequeño ρ para el cual x^ρ es congruente modulo $h(x)$, con algún elemento de $\mathbb{F}_q$, es llamado el cuasi orden de $h(x)$ y será denotado por* qorden$(h(x))$.

El siguiente conjunto de caracterizaciones para los códigos cíclicos de un sólo peso, que fue presentado en [18], será la herramienta principal de este trabajo.

Teorema 1 *Sean q, k, n, Δ y γ como antes. Para un entero positivo a, sea $h_a(x) \in \mathbb{F}_q[x]$ el polinomio mínimo de γ^a. Establecemos $\rho = \text{qorden}(h_a(x))$ y $g_a(x) = (x^n - 1)/h_a(x)$. Entonces, las siguientes cinco afirmaciones son equivalentes:*

A) $\text{mcd}(a, \Delta) = 1$.

B) $\text{grado}(h_a(x)) = k$ *y* $\rho = \Delta$.

C) $\text{grado}(h_a(x)) = k$ *y* $\text{wt}(g_a(x)) = (q-1)q^{k-1}$.

D) $\text{grado}(h_a(x)) = k$ *y, si σ es la secuencia de respuesta al impulso de orden k con polinomio característico $h_a(x)$, entonces para cada palabra de código distinta de cero $c(x)$ en el código cíclico $< g_a(x) >$ existe un entero único s, $0 \leq s < \Delta$, y un elemento único en el campo $d \in \mathbb{F}_q^*$, tal que los n coeficientes de $c(x)$ son los primeros n términos de la secuencia $\tau = d\sigma^{(s)}$.*

E) *$h_a(x)$ es el polinomio de chequeo de paridad para un código cíclico de un sólo peso sobre $\mathbb{F}_q$, de longitud n y dimensión k.*

Con la misma notación presentamos las siguientes observaciones:

Observación 1 *Observe que si a satisface la afirmación (A) entonces, por la afirmación (B) y la Definición 1, Δ es el entero positivo más pequeño para el cual $(\gamma^a)^\Delta \in \mathbb{F}_q^*$.*

Observación 2 *Observe que si a satisface la afirmación (A) entonces, por la afirmación (B) y la Definición 1, existirá un elemento único en el campo $d_a \in \mathbb{F}_q^*$ tal que $x^\Delta g_a(x) = d_a g_a(x)$ en el anillo $\mathbb{F}_q[x]/(x^n - 1)$, lo cual implica que $\sigma^{(\Delta+m)} = d_a\sigma^{(m)}$ para cualquier entero $m \geq 0$.*

Manteniendo en mente las observaciones anteriores, presentamos los siguientes lemas.

Lema 1 *Asumimos la misma notación que en el teorema previo. También asumimos que el entero a satisface la afirmación (A) y establecemos $\alpha = \gamma^a$. Entonces*

$$\{d\alpha^s \ : \ d \in \mathbb{F}_q^* \ \ y \ \ 0 \leq s < \Delta\} = \mathbb{F}_{q^k}^* \ .$$

Demostración: Es suficiente probar que $|\{d\alpha^s \ : \ d \in \mathbb{F}_q^* \ \text{y} \ 0 \leq s < \Delta\}| = q^k - 1$. Por lo tanto, supondremos la existencia de elementos del campo finito $d_1, d_2 \in \mathbb{F}_q^*$ y enteros $0 \leq s_1, s_2 < \Delta$ tales que $d_1\alpha^{s_1} = d_2\alpha^{s_2}$. Sin pérdida de generalidad, asumimos que $s_1 \geq s_2$, entonces $d_1 d_2^{-1}\alpha^{s_1 - s_2} = 1$, lo cual implica que $\alpha^{s_1-s_2} \in \mathbb{F}_q^*$. Pero $0 \leq s_1 - s_2 < \Delta$, así, por la Observación 1, tenemos $s_1 = s_2$, y en consecuencia, $d_1 = d_2$. □

Lema 2 *Con la misma notación, sean a_1 y a_2 enteros tal que* $\text{mcd}(a_1, \Delta) = \text{mcd}(a_2, \Delta) = 1$ *y* $a_1 q^i \not\equiv a_2 \pmod{q^k - 1}$, *para toda $i \geq 0$. Sea C el código cíclico sobre $\mathbb{F}_q$ de longitud n, cuyo polinomio de chequeo de paridad está dado por $h_{a_1}(x)h_{a_2}(x)$. Sean σ_1 y σ_2 las secuencias de respuesta al impulso de orden km cuyos polinomios característicos son respectivamente $h_{a_1}(x)$ and $h_{a_2}(x)$. Como es usual, sea A_i el número de palabras de código en C, de peso de Hamming i. Si tomamos el siguiente conjunto de secuencias*

$$\mathcal{S} = \{d\sigma_1^{(s)} - \sigma_2 \ : \ d \in \mathbb{F}_q^* \ \ y \ \ 0 \leq s < \Delta\} \ ,$$

entonces $|\mathcal{S}| = q^k - 1$, y si establecemos

$$\mathcal{W} = \{n - Z(\tau, 0, n) \ : \ \tau \in \mathcal{S}\} \cup \{(q-1)q^{k-1}\} \quad y$$

$$F_i = |\{\tau \in \mathcal{S} \ : \ i \in \mathcal{W} \ \ y \ \ n - Z(\tau, 0, n) = i\}| \ ,$$

entonces C es un código cíclico de $|\mathcal{W}|$ pesos de dimensión $2k$, cuya distribución de pesos es la siguiente:

$$A_i = \begin{cases} 1 & si \ \ i = 0 \\ 0 & si \ \ i \neq 0 \ \ e \ \ i \notin \mathcal{W} \\ (q^k - 1)(F_i + 2) & si \ \ i = (q-1)q^{k-1} \\ (q^k - 1)F_i & si \ \ i \neq (q-1)q^{k-1} \ \ e \ \ i \in \mathcal{W} \end{cases} .$$

Demostración: Sean $g_{a_i}(x) = (x^n - 1)/h_{a_i}(x)$ y $C_i =< g_{a_i}(x) >$, con $i = 1, 2$. Dado que $h_{a_1}(x) \neq h_{a_2}(x)$ entonces, por el Teorema 1, sabemos que $|C_1| = |C_2| = q^k$ y $C_1 \cap C_2 = \bar{0}$, por lo tanto la dimensión de C es $2k$. Además, por la afirmación (D), concluimos que $|\mathcal{S}| = q^k - 1$.

Ahora, vamos a mostrar que si $c(x)$ es una palabra de código distinta de cero en C, entonces $\mathrm{wt}(c(x)) \in \mathcal{W}$. Cualquier palabra de código $c(x) \in C$ es de la forma $c(x) = c_1(x) - c_2(x)$, para algunas palabras de código $c_1(x) \in C_1$ y $c_2(x) \in C_2$. La palabra de código $c(x)$ será trivial si al menos una de las palabras de código $c_1(x)$ o $c_2(x)$ es cero, y no trivial si las dos palabras de código $c_1(x)$ y $c_2(x)$ son diferentes de cero. Nuevamente, por el Teorema 1, sabemos que C_1 y C_2 son ambos códigos cíclicos de un sólo peso, con peso distinto de cero igual a $(q-1)q^{k-1}$, entonces si $c(x)$ es una palabra de código trivial distinta de cero,

vemos que $\mathrm{wt}(c(x)) = (q-1)q^{k-1} \in \mathcal{W}$. Ahora, suponemos que $c(x)$ es no trivial; así , por la afirmación (D), existen enteros únicos s_1 y s_2, $0 \leq s_1, s_2 < \Delta$, y elementos únicos del campo $d_1, d_2 \in \mathbb{F}_q^*$, tal que los n coeficientes de $c(x)$ son los primeros n términos de la secuencia $\tau_0 = d_1\sigma_1^{(s_1)} - d_2\sigma_2^{(s_2)}$. Sean s y ϵ dos enteros tales que $s + s_2 = \epsilon\Delta + s_1$, donde $0 \leq s < \Delta$ y $\epsilon = 0$ o 1. Ahora, por la Observación 2, existe un elemento en el campo $d_{a_1} \in \mathbb{F}_q^*$ tal que $\sigma_1^{(\Delta+m)} = d_{a_1}\sigma_1^{(m)}$ para cada entero $m \geq 0$. Así , sea d el elemento del campo en $\mathbb{F}_q^*$ tal que $d_1 = dd_2$ si $\epsilon = 0$ y $d_1 = dd_2d_{a_1}$ si $\epsilon = 1$. Claramente $\tau = d\sigma_1^{(s)} - \sigma_2 \in \mathcal{S}$ y, debido a nuestra elección de d y s, tenemos $d_2\tau^{(s_2)} = \tau_0$ lo cual implica, por (3), que $Z(\tau_0, 0, n) = Z(\tau, 0, n)$, por lo tanto $\mathrm{wt}(c(x)) \in \mathcal{W}$.

Finalmente, la distribución de pesos de C viene del hecho de que el número de palabras de código triviales distintas de cero en C es igual a $2(q^k - 1)$ (todas ellas de peso $(q-1)q^{k-1}$), y del hecho de que para cada secuencia $\tau \in \mathcal{S}$, tenemos exactamente $q^k - 1$ pares diferentes (d_2, s_2), de tal manera que los primeros n términos de la secuencia $d_2\tau^{(s_2)}$ son los n coeficientes de alguna palabra de código no trivial $c(x) \in C$. □

4 Algunos resultados sobre Sumas Exponenciales y Gaussianas

Iniciamos esta sección recordando alguna notación sobre caracteres y sumas Gaussianas. Así, conservando nuestra actual notación, definimos el *caracter aditivo canónico* χ de $\mathbb{F}_{q^k}$:

$$\chi(c) := e^{2\pi i \mathrm{Tr}(c)/p} , \qquad \text{para todo } \ c \in \mathbb{F}_{q^k} .$$

Por otra parte, cualquier *caracter multiplicativo* de $\mathbb{F}_{q^k}$ se define como

$$\psi_j(\gamma^l) := e^{2\pi ijl/(q^k-1)} , \qquad \text{para } \; j,l = 0,1,\cdots q^k-2 .$$

Para cualquier caracter multiplicativo ψ de $\mathbb{F}_{q^k}$ y para el caracter aditivo canónico χ de $\mathbb{F}_{q^k}$, *la suma Gaussiana* $G(\psi,\chi)$ se define como

$$G(\psi,\chi) := \sum_{c\in\mathbb{F}^*_{q^k}} \psi(c)\chi(c) .$$

Para cualesquiera dos enteros ω e i, definimos la siguiente suma exponencial:

$$\mathrm{E}^{(\omega)}_{q^k}(i) := \sum_{c\in\mathbb{F}_{q^k}} \chi(\gamma^i c^\omega - c) .$$

Los siguientes dos lemas son propiedades de $\mathrm{E}^{(\omega)}_{q^k}(i)$.

Lema 3 *Sean ω e i dos enteros, entonces*

$$\mathrm{E}^{(\omega p)}_{q^k}(i) = \mathrm{E}^{(\omega)}_{q^k}(i) \qquad y \qquad \mathrm{E}^{(\omega)}_{q^k}(ip) = \mathrm{E}^{(\omega)}_{q^k}(i) .$$

Demostración: Primeramente, observemos que

$$\mathrm{E}^{(\omega)}_{q^k}(i) = 1 + \sum_b \overline{\chi}(\gamma^b) \sum_{j\in\mathcal{C}_b} \chi(\gamma^i\gamma^{j\omega}) ,$$

donde b corre a través de un conjunto de representantes de clase modulo n. Así, el resultado se obtiene de las siguientes identidades:

$$\sum_{j\in\mathcal{C}_b}\chi(\gamma^i\gamma^{j\omega p}) \;=\; \sum_{j\in\mathcal{C}_b}\chi(\gamma^i\gamma^{j\omega})$$
$$\sum_{j\in\mathcal{C}_b}\chi(\gamma^{ip}\gamma^{j\omega}) = \sum_{j\in\mathcal{C}_b}\chi(\gamma^{ip}\gamma^{j\omega p}) \;=\; \sum_{j\in\mathcal{C}_b}\chi((\gamma^i\gamma^{j\omega})^p) = \sum_{j\in\mathcal{C}_b}\chi(\gamma^i\gamma^{j\omega})\ .$$

□

Lema 4 *Sean ω e i dos enteros, entonces*

$$\sum_{i=0}^{q^k-2}\mathrm{E}_{q^k}^{(\omega)}(i) = q^k\ .$$

Demostración: Dado que $\chi(0)=1$, tenemos

$$\sum_{i=0}^{q^k-2}\sum_{c\in\mathbb{F}_{q^k}}\chi(\gamma^i c^\omega - c) = q^k - 1 + \sum_{c\in\mathbb{F}_{q^k}^*}\sum_{i=0}^{q^k-2}\chi(\gamma^i c^\omega - c)\ .$$

Pero $\sum_{i=0}^{q^k-2}\chi(\gamma^i c^\omega - c) = \chi(-c)\sum_{i=0}^{q^k-2}\chi(\gamma^i c^\omega)$ y dado que, para todo $c\neq 0$, sabemos que $\sum_{i=0}^{q^k-2}\chi(\gamma^i c^\omega) = \sum_{i=0}^{q^k-2}\chi(\gamma^i) = -1$, por lo que concluimos que

$$\sum_{i=0}^{q^k-2}\sum_{c\in\mathbb{F}_{q^k}}\chi(\gamma^i c^\omega - c) = q^k - 1 - \sum_{c\in\mathbb{F}_{q^k}^*}\chi(-c) = q^k - 1 - \sum_{i=0}^{q^k-2}\chi(\gamma^i) = q^k\ .$$

□

Lema 5 *Sean ν y ζ dos enteros tal que $\nu\zeta = (q-1)$. Entonces, para cualesquiera enteros ω y y, tenemos*

$$\sum_{t=1}^{\Delta\nu-1}\psi_{\zeta t}(\gamma^y)G(\overline{\psi_{\zeta t}},\chi)G(\psi_{\zeta t}^{\omega},\overline{\chi}) = -q^k + \Delta\nu\sum_{j=0}^{\zeta-1}\mathrm{E}_{q^k}^{(\omega)}(y+j\Delta\nu)\ .$$

Demostración: Utilizando la definición de suma Gaussiana, se obtiene

$$\begin{aligned} G(\overline{\psi_{\zeta t}},\chi)G(\psi_{\zeta t}^{\omega},\overline{\chi}) &= \sum_{c_1\in\mathbb{F}_{q^k}^*}\sum_{c\in\mathbb{F}_{q^k}^*}\overline{\psi_{\zeta t}}(c_1)\chi(c_1)\psi_{\zeta t}^{\omega}(c)\overline{\chi}(c) \\ &= \sum_{c\in\mathbb{F}_{q^k}^*}\sum_{c_1\in\mathbb{F}_{q^k}^*}\psi_{\zeta t}(c^{\omega}c_1^{-1})\chi(c_1-c)\ . \end{aligned}$$

En la suma interior sustituimos $d^{-1}=c^{\omega}c_1^{-1}$. Entonces

$$\begin{aligned} G(\overline{\psi_{\zeta t}},\chi)G(\psi_{\zeta t}^{\omega},\overline{\chi}) &= \sum_{c\in\mathbb{F}_{q^k}^*}\sum_{d\in\mathbb{F}_{q^k}^*}\psi_{\zeta t}(d^{-1})\chi(dc^{\omega}-c) \\ &= \sum_{d\in\mathbb{F}_{q^k}^*}\psi_{\zeta t}(d^{-1})(\sum_{c\in\mathbb{F}_{q^k}}\chi(dc^{\omega}-c)-\chi(0)) \\ &= \sum_{d\in\mathbb{F}_{q^k}^*}\psi_{\zeta t}(d^{-1})\sum_{c\in\mathbb{F}_{q^k}}\chi(dc^{\omega}-c) \\ &= \sum_{i=0}^{q^k-2}\psi_{\zeta t}(\gamma^{-i})\mathrm{E}_{q^k}^{(\omega)}(i)\ , \end{aligned}$$

por lo tanto,

$$\begin{aligned} \sum_{t=1}^{\Delta\nu-1}\psi_{\zeta t}(\gamma^{y})G(\overline{\psi_{\zeta t}},\chi)G(\psi_{\zeta t}^{\omega},\overline{\chi}) &= \sum_{i=0}^{q^k-2}\mathrm{E}_{q^k}^{(\omega)}(i)\sum_{t=1}^{\Delta\nu-1}\psi_{\zeta}(\gamma^{t(y-i)}) \\ &= -\sum_{i=0}^{q^k-2}\mathrm{E}_{q^k}^{(\omega)}(i)+\Delta\nu\sum_{j=0}^{\zeta-1}\mathrm{E}_{q^k}^{(\omega)}(y+j\Delta\nu)\ , \end{aligned}$$

dado que ψ_ζ tiene orden $\Delta\nu$. Entonces el resultado se obtiene por el Lema 4. □

Finalizamos esta sección con el siguiente:

Lema 6 *Sean a_1 y a_2 enteros tal que $\nu = \mathrm{mcd}(a_1 - a_2, q-1)$, $\zeta = (q-1)/\nu$, $\alpha_1 = \gamma^{a_1}$ y $\alpha_2 = \gamma^{a_2}$. Asumimos que a_2 es una unidad en el anillo $\mathbb{Z}_\Delta$, donde $\tilde{a}_2$ es su inverso en dicho anillo. Sea $\omega = 1 + \tilde{a}_2(a_1 - a_2)$, donde las operaciones aritméticas en la definición de ω son tomadas en $\mathbb{Z}$. Sea B un conjunto de pares de caracteres multiplicativos de $\mathbb{F}_{q^k}$. Para $d, \theta_1, \theta_2 \in \mathbb{F}_{q^k}^*$ establecemos*

$$\mathcal{F}(d) = \sum_{(\psi,\varphi)\in B} \psi(\theta_1)G(\bar{\psi},\chi)\varphi(\theta_2)G(\bar{\varphi},\bar{\chi})\psi(d)\sum_{m=0}^{n-1}\psi(\alpha_1)^m\varphi(\alpha_2)^m \ .$$

$$\textit{Si } B = \{(\psi_{u_1}, \psi_{u_2(q-1)-u_1}) \mid 0 \le u_1 < q^k - 1,\ 0 \le u_2 < \Delta\}$$

entonces, para cualquier entero y, tenemos

$$\mathcal{F}(\theta_1^{-1}\theta_2^{\omega}\gamma^y) = -n^2 + \frac{n^2}{\zeta}\sum_{j=0}^{\zeta-1} \mathrm{E}_{q^k}^{(\omega)}(y + j\Delta\nu) \ .$$

Demostración: Utilizando B tenemos

$$\begin{aligned}\mathcal{F}(d) &= \sum_{u_1=0}^{q^k-2}\psi_{u_1}(\theta_1)G(\overline{\psi}_{u_1},\chi)\sum_{u_2=0}^{\Delta-1}\psi_{u_2(q-1)-u_1}(\theta_2)G(\overline{\psi}_{u_2(q-1)-u_1},\bar{\chi})\psi_{u_1}(d)\\ &\quad\times\sum_{m=0}^{n-1}\psi_{u_1}(\alpha_1)^m\psi_{u_2(q-1)-u_1}(\alpha_2)^m \ .\end{aligned}$$

La suma interior en la última expresión es una serie geométrica finita que se desvanece si $\psi_{u_1}(\alpha_1)\psi_{u_2(q-1)-u_1}(\alpha_2) \neq 1$, debido a que

$$\psi_{u_1}(\alpha_1)^n\psi_{u_2(q-1)-u_1}(\alpha_2)^n = \psi_{u_1}(\alpha_1^n)\psi_{u_2(q-1)-u_1}(\alpha_2^n) = \psi_{u_1}(1)\psi_{u_2(q-1)-u_1}(1) = 1 \ .$$

Por otro lado,

$$\psi_{u_1}(\alpha_1)\psi_{u_2(q-1)-u_1}(\alpha_2) = 1 \Leftrightarrow \psi_1(\gamma^{a_1u_1+a_2(u_2(q-1)-u_1)}) = 1 \ ,$$

y claramente

$$\psi_1(\gamma^{a_1u_1+a_2(u_2(q-1)-u_1)}) = 1 \Leftrightarrow a_2u_2(q-1) \equiv (a_2-a_1)u_1 \pmod{q^k-1} \ ,$$

pero la última congruencia implica que $(q-1)|(a_2-a_1)u_1$, y dado que $\mathrm{mcd}(a_1-a_2, q-1) = \nu$, entonces $u_1 = \zeta t$ para $t = 0, 1, \cdots, \Delta\nu - 1$. Ahora, también de la congruencia previa, tenemos $\tilde{a}_2a_2u_2(q-1) \equiv \tilde{a}_2(a_2-a_1)u_1 \pmod{q^k-1}$, pero $\tilde{a}_2a_2 = 1+\ell\Delta$ para algún entero ℓ, así $u_2(q-1) \equiv \tilde{a}_2(a_2-a_1)u_1 \pmod{q^k-1}$ y por lo tanto, para cada t, existe un entero único $0 \leq u_2 < \Delta$ tal que $u_2 \equiv \tilde{a}_2bt \pmod{\Delta}$, donde $b = (a_2-a_1)/\nu$. Con esto concluimos que $\psi_{u_1} = \psi_{\zeta t}$ y $\psi_{u_2(q-1)-u_1} = \psi_{\tilde{a}_2(a_2-a_1)\zeta t-\zeta t} = \overline{\psi^{\omega}_{\zeta t}}$. Así

$$\mathcal{F}(\theta_1^{-1}\theta_2^{\omega}\gamma^y) = n+n\sum_{t=1}^{\Delta\nu-1} \psi_{\zeta t}(\theta_1)G(\overline{\psi_{\zeta t}}, \chi)\overline{\psi^{\omega}_{\zeta t}}(\theta_2)G(\psi^{\omega}_{\zeta t}, \overline{\chi})\psi_{\zeta t}(\theta_1^{-1}\theta_2^{\omega}\gamma^y) \ .$$

Pero $\psi_{\zeta t}(\theta_1)\overline{\psi^{\omega}_{\zeta t}}(\theta_2)\psi_{\zeta t}(\theta_1^{-1}\theta_2^{\omega}) = 1$, y dado que $\Delta\nu = n/\zeta$ entonces, por medio del lema previo, obtenemos el resultado deseado. □

5 La Distribución de Pesos de algunos Códigos Cíclicos cuyo Código Dual tiene Dos Ceros No Conjugados

El resultado siguiente muestra que para algunos códigos cíclicos C cuyo código dual tiene dos ceros no conjugados, es siempre

posible encontrar un entero ω tal que la distribución de pesos de C puede ser obtenida completamente por medio de la distribución de los valores de $\sum_{c\in\mathbb{F}_{q^k}} \chi(dc^\omega - c)$, donde $d \in \mathbb{F}_{q^k}^*$.

Teorema 2 *Para un entero positivo a, sea $h_a(x) \in \mathbb{F}_q[x]$ el polinomio mínimo de γ^a. Sean a_1 y a_2 dos enteros de tal manera que* $\mathrm{mcd}(a_1, \Delta)$=$\mathrm{mcd}(a_2, \Delta) = 1$ *y* $a_1 q^i \not\equiv a_2 \pmod{q^k - 1}$, *para toda $i \geq 0$. Sean α_1, α_2, ν, ζ, $\tilde{a}_2$ y ω como en el Lema 6. Sea C el código cíclico sobre $\mathbb{F}_q$ de longitud n, cuyo polinomio de chequeo de paridad está dado por $h_{a_1}(x)h_{a_2}(x)$. Como es usual, sea A_i el número de palabras de código en C, de peso de Hamming i. Sea*

$$\mathcal{Y} = \{0, 1, 2, \cdots, q^k - 2\} ,$$

y si establecemos

$$\mathcal{W}' = \{(q-1)q^{k-1} - \frac{\nu}{q}\sum_{j=0}^{\zeta-1} \mathrm{E}_{q^k}^{(\omega)}(y + j\Delta\nu) \ : y \in \mathcal{Y}\} \cup \{(q-1)q^{k-1}\} \quad \text{y}$$

$$F_i' = |\{y \in \mathcal{Y} \ : \ i \in \mathcal{W}' \text{ y } \ (q-1)q^{k-1} - \frac{\nu}{q}\sum_{j=0}^{\zeta-1} \mathrm{E}_{q^k}^{(\omega)}(y + j\Delta\nu) = i\}| \ ,$$

entonces C es un código cíclico de $|\mathcal{W}'|$ pesos de dimensión $2k$ cuya distribución de pesos es la siguiente:

$$A_i = \begin{cases} 1 & si \ \ i = 0 \\ 0 & si \ \ i \neq 0 \ \ e \ \ i \notin \mathcal{W}' \\ (q^k - 1)(F_i' + 2) & si \ \ i = (q-1)q^{k-1} \\ (q^k - 1)F_i' & si \ \ i \neq (q-1)q^{k-1} \ \ e \ \ i \in \mathcal{W}' \end{cases} .$$

Demostración: Sean σ_1 y σ_2, respectivamente, las secuencias de respuesta al impulso de orden k cuyos polinomios característicos son, respectivamente, $h_{a_1}(x)$ y $h_{a_2}(x)$. Sean $\mathcal{S}$, $\mathcal{W}$ y F_i como en el Lema 2. Así, en el contexto de la demostración del Lema 2, es suficiente mostrar la existencia de una biyección Φ, de $\mathcal{S}$ sobre $\mathcal{Y}$, de tal manera que si $\Phi(\tau) = y$ entonces

$$(q-1)q^{k-1} - \frac{\nu}{q}\sum_{j=0}^{\zeta-1} \mathrm{E}_{q^k}^{(\omega)}(y + j\Delta\nu) = n - Z(\tau, 0, n)\ . \qquad (5)$$

Para esto, asumiremos que $\sigma_i = g_0^{(i)}, g_1^{(i)}, g_2^{(i)}, \ldots$, para valores de $i = 1, 2$. Adicionalmente, utilizando (4), tomamos θ_i tal que $g_m^{(i)} = \mathrm{Tr}_{F/K}(\theta_i \alpha_i^m)$, para $i = 1, 2$ y $m = 0, 1, 2, \cdots$. Dado que $h_{a_i}(x) \neq 1$, para $i = 1, 2$, tenemos $\theta_1^{-1}\theta_2^{\omega} \neq 0$. Con esto, utilizamos ahora el Lema 1 para definir la biyección Φ de la siguiente manera:

$$\Phi(\tau = d\sigma_1^{(s)} - \sigma_2) = y \iff d\alpha_1^s = \theta_1^{-1}\theta_2^{\omega}\gamma^y\ .$$

De este modo, sólo nos resta calcular $Z(\tau, 0, n)$. Para esto, sea χ' el caracter aditivo canónico de $\mathbb{F}_q$, entonces, por la propiedad ortogonal de χ', tenemos

$$\frac{1}{q}\sum_{c\in\mathbb{F}_q} \chi'(c(dg_{m+s}^{(1)} - g_m^{(2)})) = \begin{cases} 1 & \text{si } \ dg_{m+s}^{(1)} = g_m^{(2)} \\ 0 & \text{de otra manera} \end{cases}\ .$$

Así,

$$Z(\tau, 0, n) = \frac{1}{q}\sum_{m=0}^{n-1}\sum_{c\in\mathbb{F}_q} \chi'(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(dc\theta_1\alpha_1^{m+s}))\chi'(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(-c\theta_2\alpha_2^m))\ .$$

Si χ denota el caracter aditivo canónico de $\mathbb{F}_{q^k}$, entonces χ' y χ están relacionados por $\chi'(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta)) = \chi(\beta)$ para toda $\beta \in \mathbb{F}_{q^k}$. Por lo tanto,

$$\begin{aligned} Z(\tau,0,n) &= \frac{1}{q}\sum_{c\in\mathbb{F}_q}\sum_{m=0}^{n-1}\chi(dc\,\theta_1\alpha_1^{m+s})\bar{\chi}(c\,\theta_2\alpha_2^m) \\ &= \frac{n}{q}+\frac{1}{q}\sum_{c\in\mathbb{F}_q^*}\sum_{m=0}^{n-1}\chi(dc\,\theta_1\alpha_1^{m+s})\bar{\chi}(c\,\theta_2\alpha_2^m)\ . \quad (6) \end{aligned}$$

Ahora, por medio de la expansión de la restricción de χ a $\mathbb{F}_{q^k}^*$ en términos de los caracteres multiplicativos de $\mathbb{F}_{q^k}$, con sumas Gaussianas como coeficientes de Fourier (ver por ejemplo [10, p. 195]), sabemos que $\chi(dc\,\theta_1\alpha_1^{m+s})\ \bar{\chi}(c\,\theta_2\alpha_2^m)$ es igual a

$$\frac{1}{(q^k-1)^2}\sum_{\psi}\sum_{\varphi}\psi(dc\,\theta_1\alpha_1^{m+s})G(\bar{\psi},\chi)\varphi(c\,\theta_2\alpha_2^m)G(\bar{\varphi},\bar{\chi})\ ,$$

donde las sumas son extendidas sobre todos los caracteres multiplicativos ψ y φ de $\mathbb{F}_{q^k}$. Dado que $n = q^k - 1$ entonces, sustituyendo la última expresión en (6), obtenemos

$$\begin{aligned} Z(\tau,0,n) &= \frac{n}{q}+\frac{1}{qn^2}\sum_{\psi}\psi(\theta_1)G(\bar{\psi},\chi)\sum_{\varphi}\varphi(\theta_2)G(\bar{\varphi},\bar{\chi})\psi(d\alpha_1^s) \\ &\quad\times\sum_{m=0}^{n-1}\psi(\alpha_1)^m\varphi(\alpha_2)^m\sum_{c\in\mathbb{F}_q^*}(\psi\varphi)(c)\ . \end{aligned}$$

Si la restricción de $\psi\varphi$ a $\mathbb{F}_q^*$ es no trivial, entonces, por la propiedad ortogonal de $\psi\varphi$, tenemos $\sum_{c\in\mathbb{F}_q^*}(\psi\varphi)(c) = 0$. En consecuencia, es suficiente extender la suma previa sobre el conjunto B de pares de caracteres ψ y φ para los cuales $\psi\varphi$ es trivial en $\mathbb{F}_q^*$, de modo que $Z(\tau,0,n)$ es igual a

$$\frac{n}{q}+\frac{q-1}{qn^2}\sum_{(\psi,\varphi)\in B}\psi(\theta_1)G(\bar{\psi},\chi)\varphi(\theta_2)G(\bar{\varphi},\bar{\chi})\psi(d\alpha_1^s)\sum_{m=0}^{n-1}\psi(\alpha_1)^m\varphi(\alpha_2)^m\ .$$

Dado que $\mathbb{F}_q^* = \{\gamma^{s\Delta} \mid 0 \leq s < (q-1)\}$, entonces tenemos $B = \{(\psi_{u_1}, \psi_{u_2(q-1)-u_1}) \mid 0 \leq u_1 < q^k - 1, 0 \leq u_2 < \Delta\}$. Pero, por la biyección Φ, sabemos que $d\alpha_1^s = \theta_1^{-1}\theta_2^{\omega}\gamma^y$, así una aplicación directa del Lema 6 prueba (5). □

6 Algunos Ejemplos

La clave principal para la determinación de la distribución de pesos, en el contexto del Teorema 2, es la evaluación de la suma exponencial $\mathrm{E}_{q^k}^{(\omega)}(i)$, para una ω fija, y para $i = 0, 1, \cdots, q^k - 2$. Sin embargo, gracias a la segunda igualdad en el Lema 3, dicha evaluación sólo es necesario realizarla para un conjunto de representantes de clase modulo $q^k - 1$. Tomando esto en consideración, y utilizando nuestra notación actual, presentamos los siguientes ejemplos.

1) Sean $q = 4$, $k = 2$, $a_1 = 6$ y $a_2 = 3$, entonces $\Delta = 5$, $\nu = 3$, $\zeta = 1$, $\tilde{a}_2 = 2$ y $\omega = 7$. Si elegimos $\mathbb{F}_{16} = \mathbb{F}_2(\gamma)$, con $\gamma^4 + \gamma + 1 = 0$, encontramos que $\mathrm{E}_{16}^{(7)}(0) = \mathrm{E}_{16}^{(7)}(1) = 0$, $\mathrm{E}_{16}^{(7)}(3) = 4$, $\mathrm{E}_{16}^{(7)}(5) = 8$ y $\mathrm{E}_{16}^{(7)}(7) = -4$. Dado que $|\mathcal{C}_b| = 4$ para $b = 1, 3, 7$, $|\mathcal{C}_5| = 2$ y $|\mathcal{C}_0| = 1$ entonces, por el Teorema 2 tenemos $\mathcal{W}' = \{12, 9, 6, 15\}$, $F'_{12} = 5$, $F'_9 = F'_{15} = 4$ y $F'_6 = 2$. Por lo tanto $h_6(x)h_3(x) \in \mathbb{F}_4[x]$, es el polinomio de chequeo de paridad para un código cíclico

de cuatro pesos sobre $\mathbb{F}_4$, de longitud 15, dimensión 4 y polinomio enumerador de pesos: $A(z) = 1 + 30z^6 + 60z^9 + 105z^{12} + 60z^{15}$.

2) Sean $q = 4$, $k = 2$, $a_1 = 6$ y $a_2 = 2$, entonces $\Delta = 5$, $\nu = 1$, $\zeta = 3$, $\tilde{a}_2 = 3$ y $\omega = 13$. Debido a la primera igualdad en el Lema 3, tenemos $\mathrm{E}_{16}^{(13)}(i) = \mathrm{E}_{16}^{(7)}(i)$ para toda i $(0 \leq i < 15)$. Así, utilizando el ejemplo previo, tenemos

$$\sum_{j=0}^{2} \mathrm{E}_{16}^{(13)}(y + 5j) = \begin{cases} 16 & \text{si } \ y \in \mathcal{C}_0 \cup \mathcal{C}_5 \\ 0 & \text{en otro caso} \end{cases} ,$$

lo que implica que $\mathcal{W}' = \{8, 12\}$, $F_8' = 3$ y $F_{12}' = 12$. Por lo tanto $h_6(x)h_2(x) \in \mathbb{F}_4[x]$, es el polinomio de chequeo de paridad para un código cíclico de doble peso sobre $\mathbb{F}_4$, de longitud 15, dimensión 4 y polinomio enumerador de pesos: $A(z) = 1 + 45z^8 + 210z^{12}$.

3) Sean $q = 2$, $k = 4$, $a_1 = 7$ y $a_2 = 1$, entonces $\Delta = 15$, $\nu = \zeta = 1$, $\tilde{a}_2 = 1$ y $\omega = 7$. Así, utilizando el ejemplo 1), tenemos $\mathcal{W}' = \{8, 6, 4, 10\}$, $F_8' = 5$, $F_6' = F_{10}' = 4$ y $F_4' = 2$. Por lo tanto $h_1(x)h_7(x) \in \mathbb{F}_2[x]$, es el polinomio de chequeo de paridad para un código cíclico binario de cuatro pesos de longitud 15, dimensión 8 y polinomio enumerador de pesos: $A(z) = 1 + 30z^4 + 60z^6 + 105z^8 + 60z^{10}$.

4) Sean $q = 3$, $k = 3$, $a_1 = 4$ y $a_2 = 2$, entonces $\Delta = 13$, $\nu = 2$, $\zeta = 1$, $\tilde{a}_2 = 7$ y $\omega = 15$. Si elegimos $\mathbb{F}_{27} = \mathbb{F}_3(\gamma)$, con $\gamma^3 + 2\gamma + 1 = 0$, encontramos que para $i \in \{0, 2, 4, 7, 13, 14, 17\}$, $\mathrm{E}_{27}^{(15)}(i) = 0$, $\mathrm{E}_{27}^{(15)}(1) = \mathrm{E}_{27}^{(15)}(8) = 9$ y $\mathrm{E}_{27}^{(15)}(5) = -9$. Dado que $|\mathcal{C}_b| = 3$ para $b = 1, 2, 4, 5, 7, 8, 14, 17$ y $|\mathcal{C}_b| = 1$ para $b = 0, 13$ entonces, por el Teorema 2 tenemos $\mathcal{W}' = \{18, 12, 24\}$,

$F'_{18} = 17$, $F'_{12} = 6$ y $F'_{24} = 3$. Por lo tanto $h_4(x)h_2(x) \in \mathbb{F}_3[x]$, es el polinomio de chequeo de paridad para un código cíclico de tres pesos sobre $\mathbb{F}_3$, de longitud 26, dimensión 6 y polinomio enumerador de pesos: $A(z) = 1 + 156z^{12} + 494z^{18} + 78z^{24}$.

Conclusión

En general, el problema de determinar la distribución de pesos de un código cíclico sobre un campo finito, tiende a ser difícil. Típicamente, cuando el campo finito es un campo primo, el problema es manejado expresando el peso de Hamming de cada palabra de código, por medio de cierta combinación de sumas exponenciales. En este trabajo, presentamos un método alternativo para calcular la distribución de pesos de algunos códigos cíclicos cuyo código dual tiene dos ceros no conjugados (Teorema 2). Este método también necesita la evaluación de algunas sumas exponenciales, sin embargo, como vimos en la sección anterior, tal evaluación solamente es necesaria sobre un conjunto de representantes de clase modulo n. Adicionalmente, este método tiene la ventaja de la flexibilidad, en el sentido de que también puede ser aplicado a códigos cíclicos sobre campos finitos de orden no primo.

Capítulo 4

La Distribución de Pesos de una Familia de Códigos Cíclicos Reducibles

RESUMEN

Un resultado general sobresaliente el cual nos brinda la evaluación de una familia de sumas exponenciales fue presentado por Marko J. Moisio (*Acta Arithmetica*, 93 (2000) 117-119). En este trabajo, utilizamos una instancia particular de este resultado general, para poder determinar la distribución de los valores de una suma exponencial particular. Entonces, motivados por algunas nuevas ideas frescas y originales de Changli Ma, Liwei Zeng, Yang Liu, Dengguo Feng y Cunsheng Ding (*IEEE Trans. Inf. Theory,* 57-1 (2011) 397-402), utilizamos esta distribución de valores, para obtener la distribución de pesos de una familia de códigos cíclicos reducibles. Como veremos mas adelante, todos los códigos en esta familia son códigos cíclicos no proyectivos. Más aún, ellos pueden ser identificados en una forma muy fácil. De hecho, como un subproducto de esta fácil identificación, podemos determinar el número exacto de códigos cíclicos en una familia, cuando la longitud y dimensión son conocidas. Este capítulo es la transcripción de [25].

Palabras clave: Distribución de pesos, códigos cíclicos reducibles y sumas exponenciales.

1 Introducción

Una familia importante de códigos para control de errores en comunicaciones digitales, son los llamados códigos cíclicos. Por tanto, encontrar la distribución de pesos de un código cíclico q-ario C, no solamente es un problema de interes teórico, sino también es de importancia práctica. Siendo más específicos, la distribución de pesos de un código es importante porque esta juega un rol determinante en determinar las capacidades de detección y corrección de un código dado. Sin embargo, calcular la distribución de pesos de un código, mediante una computadora, puede ser una tarea formidable. Para códigos cíclicos este problema es de especial interés, debido a su rica estructura algebraica. Muchos autores han trabajado en el problema de determinar la distribución de pesos de códigos cíclicos no irreducibles, utilizando diferentes técnicas (ver por ejemplo [7], [21], [5], [20] y [11]). Para una familia particular de códigos cíclicos, es bastante común que una de esas técnicas consista en calcular la distribución de valores de una suma exponencial específica. Sin embargo, en la mayoría de los casos, la evaluación de una suma exponencial es también un problema arduo. Un resultado general extraordinario que nos da la evaluación de una familia de sumas exponenciales fue presentado en [13]. En este trabajo, determinamos la distribución de valores de una instancia particular de este resultado general. Entonces, basados en algunas nuevas ideas originales en [11], tomamos esta distribución de valores para obtener la distribución de pesos de una familia de códigos cíclicos reducibles. Como veremos posteriormente, todos los códigos en esta familia son códigos cíclicos no proyectivos. Además, los códigos en esta familia pueden ser identificados en una forma fácil. De hecho, como un subproducto de esta fácil

identificación, podemos determinar el número exacto de códigos cíclicos en una familia, cuando la longitud y dimensión son conocidas.

Este trabajo está organizado de la siguiente manera: En la Sección 2 establecemos alguna notación, recordamos algunas definiciones y establecemos nuestra suposición principal, la cual será considerada en todo este capítulo. También recordamos, para esta sección, algunos resultados ya conocidos. En particular, presentamos la evaluación de una suma exponencial específica, la cual puede ser derivada como una instancia de un resultado general que fue presentado originalmente en [8]. La Sección 3 está dedicada a presentar algunos resultados generales. En la Sección 4, utilizamos estos resultados para obtener la distribución de pesos de una familia de códigos cíclicos reducibles no proyectivos. También presentamos, en la Sección 4, una fórmula explícita para el número de códigos cíclicos que pertenecen a una de estas familias, cuando la longitud y dimensión son conocidas. Además, algunos ejemplos de esta fórmula son incluidos al final de esta sección. Finalmente, la Sección 5 presenta las conclusiones.

2 Definiciones, notación, preliminares y suposición principal

Primeramente, establecemos, para esta sección y para el resto del capítulo, la siguiente:

Notación. Para p, t, q, k y Δ, denotamos cinco enteros posi-

tivos tal que p es un número primo, $q = p^t$ y $\Delta = (q^k - 1)/(q-1)$. De aquí en adelante, γ denotará un elemento primitivo fijo de $\mathbb{F}_{q^k}$. Para cualesquiera dos enteros i y j, definimos $\mathcal{D}_i^{(j)} = \gamma^i \langle \gamma^j \rangle$, donde $\langle \gamma^j \rangle$ denota el subgrupo de $\mathbb{F}_{q^k}^*$ generado por γ^j. Para cualquier entero a, el polinomio $h_a(x) \in \mathbb{F}_q[x]$ denotará el polinomio mínimo de γ^{-a}. Además, denotamos con "Tr", el mapeo traza absoluta de $\mathbb{F}_{q^k}$ al campo primo $\mathbb{F}_p$, y con "$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$" el mapeo traza de $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$.

Las siguientes definiciones son importantes para nosotros:

Un código cíclico es *irreducible* si su polinomio de chequeo de paridad es irreducible (su representación polinomial es un ideal mínimo).

Un código de N-pesos es un código tal que la cardinalidad del conjunto de sus pesos distintos de cero es N.

Un código proyectivo es un código lineal tal que el peso mínimo de su código dual es al menos tres (o de manera equivalente, si cualesquiera dos columnas de su matriz generadora son linealmente independientes).

Para este trabajo, estamos interesados particularmente en códigos cíclicos no irreducibles, cuyos polinomios de chequeo de paridad son factorizables en forma exacta en dos factores irreducibles diferentes, es decir, estamos interesados en códigos cíclicos cuyos códigos duales tienen dos ceros no conjugados.

Ahora, continuamos con esta sección recordando la definición, y una propiedad básica del caracter o sumas exponenciales (ver, por ejemplo, [10]). Para hacer esto, sean p, q, k y γ como antes, entonces el caracter aditivo canónico χ, de $\mathbb{F}_{q^k}$, se define como

$$\chi(y) = \zeta_p^{\mathrm{Tr}(y)} , \qquad \text{for all } y \in \mathbb{F}_{q^k} ,$$

donde $\zeta_p = \exp(\frac{2\pi\sqrt{-1}}{p})$. Para el caracter aditivo canónico χ', de $\mathbb{F}_q$, la siguiente propiedad ortogonal nos será de utilidad:

$$\sum_{y \in \mathbb{F}_q} \chi'(y) = 0 . \tag{1}$$

El siguiente es un resultado preliminar sencillo:

Lema 1 . *Sean u y v dos enteros positivos tal que u es impar. Si 4 divide $u+1$ entonces 4 divide $\frac{u^{2v}-1}{(u-1)}$.*

Demostración: Dado que $u \equiv 3 \pmod 4$ entonces, si v es un entero impar, tenemos que $u^v \equiv 3 \pmod 4$, por tanto 4 divide $\frac{u^{2v}-1}{(u-1)} = (u^v+1)\frac{u^v-1}{(u-1)}$. Po otra parte, si v es par, entonces $2|(u^{v/2}+1)$, por tanto 4 divide $\frac{u^{2v}-1}{(u-1)} = (u^v+1)(u^{v/2}+1)\frac{u^{v/2}-1}{(u-1)}$. □

Ahora, establecemos, para esta sección y para el resto del capítulo, la siguiente:

Suposición principal. De aquí en adelante, estamos suponiendo que q es un entero impar mayor que 3 tal que 4 divide $q+1$. Además, siempre asumimos que k es un entero par.

Observación 1 . *Como una consecuencia de la suposición principal, observemos que* $\frac{q-1}{2}$ *es un entero impar. Además, debido al lema anterior, observemos que* 4 *divide* Δ.

Con la suposición principal en mente, sea χ el caracter aditivo canónico de $\mathbb{F}_{q^k}$, e i cualquier entero. Ahora, debido a la Observación 1, y dado que $(q^k - 1) = \Delta(q-1)$, tenemos que $4|(q^k-1)$, por tanto, $\sum_{x\in\mathbb{F}_{q^k}} \chi(\gamma^i x^4) = 1 + 4\sum_{z\in\mathcal{D}_i^{(4)}} \chi(z)$. Considerando este hecho, y dado que $4|(q+1)$, entonces el siguiente resultado es una instancia particular de un resultado general que fue probado en [13] (ver Teorema 1):

Teorema 1 . *Con nuestra notación y la suposición principal, sean* i *y* w *dos enteros de tal manera que* w *esta dada por*

$$w = \begin{cases} 0 & si\ \ (2 \mid \frac{k}{2}) \quad o \quad (2 \nmid \frac{k}{2}\ y\ 2 \mid \frac{q+1}{4}) \ , \\ \\ 2 & en\ otro\ caso \end{cases} .$$

También sean η_0 *y* η_1 *dos enteros dados por*

$$\begin{aligned} \eta_0 &= \frac{(-1)^{\frac{k}{2}-1}3q^{\frac{k}{2}}-1}{4} \ , \\ \eta_1 &= \frac{(-1)^{\frac{k}{2}}q^{\frac{k}{2}}-1}{4} \ . \end{aligned}$$

Entonces

$$\sum_{z\in\mathcal{D}_i^{(4)}} \chi(z) = \begin{cases} \eta_0 & si\ i \equiv w \pmod 4 \ , \\ \\ \eta_1 & en\ otro\ caso \end{cases} . \qquad (2)$$

Como veremos más adelante, el teorema previo será fundamental en determinar la distribución de pesos de una familia de códigos cíclicos reducibles.

3 Algunos Resultados Generales

Lema 2 . *Sean q, k y Δ como antes. Considerando nuestra suposición principal, tenemos que Δ no divide $2(q^s-1)$ para cualquier entero s tal que $1 \leq s < k$.*

Demostración: Por el contrario, supongamos que $\Delta | 2(q^s-1)$ para algún entero s tal que $1 \leq s < k$. Así, debe existir un entero positivo l tal que $2(q^s-1) = l(q^{k-1}+q^{k-2}+\cdots+q+1)$. Claramente, si $s < k-1$ o $l > 1$ entonces $2(q^s-1) < l(q^{k-1}+q^{k-2}+\cdots+q+1)$. Por otro lado, observemos que la igualdad $2(q^{k-1}-1) = (q^{k-1}+q^{k-2}+\cdots+q+1)$ es imposible si $q > 3$. □

Lema 3 . *Sean q, k y Δ como antes. Considerando nuestra suposición principal, también tomamos λ como un divisor de $q-1$, y definimos $n = \lambda\Delta$. Sea a_2 un entero tal que $a_2 n \equiv 0 \pmod{q^k-1}$. Si $\mathrm{mcd}(\frac{\Delta}{2}, a_2) = 2$, entonces $\mathrm{mcd}(q^k-1, a_2) = 2^d\frac{q-1}{\lambda'}$ para algunos enteros d y λ', tal que $d = 0, 1$ o 2, y λ' es el divisor de $q-1$ que satisface $\mathrm{mcd}(q-1, a_2) = \frac{q-1}{\lambda'}$. Además, si tenemos que $d = 2$ en la afirmación previa, entonces $\mathrm{mcd}(q^k-1, a_2+\frac{q^k-1}{2}) = 2^{d'}\frac{q-1}{\lambda'}$, para algún entero d' tal que $d' = 0$ o 1.*

Demostración: Dado que $a_2 n \equiv 0 \pmod{q^k-1}$ entonces observemos que $a_2 = \frac{q-1}{\lambda}u$ para algún entero u. Ahora, dado que estamos suponiendo que $\mathrm{mcd}(\frac{\Delta}{2}, a_2) = 2$, entonces tendremos que $\mathrm{mcd}(q^k-1, a_2) = \mathrm{mcd}(2(q-1)\frac{\Delta}{2}, a_2) = \mathrm{mcd}(4(q-$

$1), a_2)$=mcd$(4(q-1), \frac{q-1}{\lambda}u)$=$2^d\frac{q-1}{\lambda'}$, para algunos enteros d y λ', tal que $d = 0, 1$ o 2, y λ' es el divisor de $q-1$ que satisface mcd$(q-1, a_2) = \frac{q-1}{\lambda'}$ (recordemos que $\frac{q-1}{2}$ es un entero impar, y observemos que $\lambda'|\lambda$).

Para la segunda afirmación, debemos primero observar que mcd$(\frac{\Delta}{2}, a_2 + \frac{q^k-1}{2})$=mcd$(\frac{\Delta}{2}, a_2 + \frac{\Delta}{2}(q-1))$=mcd$(\frac{\Delta}{2}, a_2) = 2$, y también que mcd$(q-1, a_2 + \frac{q^k-1}{2})$ =mcd$(q-1, a_2 + \frac{\Delta}{2}(q-1))$ =mcd$(q-1, a_2) = \frac{q-1}{\lambda'}$. Así, para la primera afirmación de este lema, sabemos que debe existir un número entero d' de tal manera que mcd$(q^k-1, a_2+\frac{q^k-1}{2}) = 2^{d'}\frac{q-1}{\lambda'}$ y $d' = 0, 1$ o 2. Ahora, si $d = 2$, entonces $2|a_2$, lo cual implica que $\frac{q-1}{\lambda'}$ =mcd$(q-1, a_2)$ es un entero par. Por lo tanto 8 divide a $2^d\frac{q-1}{\lambda'}$, lo cual implica que $8|a_2$. Así, suponiendo que $d' = d = 2$, obtenemos que mcd$(q^k - 1, a_2 + \frac{q^k-1}{2})$ =mcd$(\Delta(q-1), a_2 + \frac{\Delta}{2}(q-1)) = 2^d\frac{q-1}{\lambda'}$, y esto implicará que $4|\frac{\Delta}{2}$. En consecuencia, tenemos que mcd$(\frac{\Delta}{2}, a_2) \geq 4$, una contradicción. Por lo tanto mcd$(q^k - 1, a_2 + \frac{q^k-1}{2}) = 2^{d'}\frac{q-1}{\lambda'}$, para algún entero d' tal que $d' = 0$ o 1. □

Como una consecuencia directa del lema anterior tenemos el siguiente:

Corolario 1 . *Consideremos la misma notación e hipótesis del lema anterior, entonces* mcd$(q^k - 1, a_2) = 2^d\frac{q-1}{\lambda'}$ *o* mcd$(q^k - 1, a_2 + \frac{q^k-1}{2}) = 2^d\frac{q-1}{\lambda'}$, *para algunos enteros* d *y* λ' *tal que* $d = 0$ *o* 1, *y* λ' *es el divisor de* $q-1$ *que satisface* mcd$(q-1, a_2) = \frac{q-1}{\lambda'}$.

Lema 4 . *Sean* q, k, Δ *y* γ *como antes. Considerando nuestra suposición principal, también tomamos* λ *como un divisor de* $q-1$, *y definimos* $n = \lambda\Delta$. *Sea* a_2 *un entero tal que* $a_2 n \equiv 0 \pmod{q^k - 1}$. *Supongamos que* mcd$(q^k - 1, a_2) = 2^d\frac{q-1}{\lambda'}$ *para algunos enteros* d *y* λ', *tal que* $d = 0$ *o* 1, *y* λ' *es el divisor de* $q-1$ *que satisface* mcd$(q-1, a_2) = \frac{q-1}{\lambda'}$. *Si* $n' = \lambda'\frac{\Delta}{2^d}$ *entonces*

$$\{(\gamma^{a_2 m}, (-1)^m) \mid 0 \leq m < n\} = \frac{2^d \lambda}{\lambda'} * \{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\} ,$$

donde $\frac{2^d \lambda}{\lambda'} * \{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\}$ *es el multiconjunto en el cual cada elemento de* $\{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\}$ *aparece con multiplicidad* $\frac{2^d \lambda}{\lambda'}$.

Demostración: Dado que $0 \leq d \leq 1$ y $\mathrm{mcd}(q^k - 1, a_2) = 2^d \frac{q-1}{\lambda'}$, entonces n' es el entero positivo mas pequeño que satisface $2^d \frac{q-1}{\lambda'} n' \equiv 0 \pmod{q^k - 1}$. Además, deben existir enteros i y j tales que $ia_2 + j(q^k - 1) = 2^d \frac{q-1}{\lambda'}$. Observemos que i es necesariamente un entero impar, porque si no, entonces $2^{d+1} \frac{q-1}{\lambda'} | (ia_2)$, y dado que $2^{d+1} \frac{q-1}{\lambda'} | (q^k - 1)$ (recordemos que $0 \leq d \leq 1$ y $q^k - 1 = \Delta(q-1)$), entonces podemos concluir que $2^{d+1} \frac{q-1}{\lambda'} | 2^d \frac{q-1}{\lambda'}$, y claramente esta última condición es imposible. Así, dado que $\langle \gamma^{a_2} \rangle = \langle \gamma^{2^d \frac{q-1}{\lambda'}} \rangle$, $|\langle \gamma^{a_2} \rangle| = n'$, y dado que i es un entero impar, entonces

$$\{(\gamma^{a_2 m}, (-1)^m) \mid 0 \leq m < n'\} = \{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\} .$$

El resultado se sigue ahora del hecho de que $\frac{n}{n'} = \frac{2^d \lambda}{\lambda'}$. □

La siguiente es una versión modificada del Lema 3 en [11].

Lema 5 . *Con nuestra notación y suposición principal, sea* λ' *y* d *enteros tales que* λ' *es un divisor de* $(q-1)$ *y* d *es igual a cero o a uno. Si* $\mathrm{mcd}(\frac{\Delta}{2}, \frac{2^d(q-1)}{\lambda'}) = 2$, *entonces, para cualquier entero* i, *tenemos*

$$\{xy \mid x \in \mathcal{D}_i^{(\frac{2^{d+1}(q-1)}{\lambda'})} \text{ con } y \in \mathbb{F}_q^*\} = \frac{2\lambda'}{2^d} * \mathcal{D}_i^{(4)} ,$$

donde $\frac{2\lambda'}{2^d} * \mathcal{D}_i^{(4)}$ *es el multiconjunto en el cual cada elemento de* $\mathcal{D}_i^{(4)}$ *aparece con multiplicidad* $\frac{2\lambda'}{2^d}$.

Demostración: Dado que $\mathcal{D}_i^{(j)} = \gamma^i \mathcal{D}_0^{(j)}$, para todos los enteros i y j, entonces, sin pérdida de generalidad, podemos suponer simplemente que $i = 0$. Por hipótesis, podemos ver que $\frac{2^{d-1}(q-1)}{\lambda'}$ es un entero positivo, y también que $\mathrm{mcd}(\Delta, \frac{2^{d+1}(q-1)}{\lambda'}) = 4$. Ahora, dado que $4|\Delta$ y $d = 0$ o 1, entonces observemos que $(\frac{2^{d+1}(q-1)}{\lambda'})|(q^k - 1)$. Así, para cada $x \in \mathcal{D}_0^{(\frac{2^{d+1}(q-1)}{\lambda'})}$ y $y \in \mathbb{F}_q^*$, existen enteros únicos l_1 y l_2, con $0 \leq l_1 < \lambda' \frac{\Delta}{2^{d+1}}$ y $0 \leq l_2 < (q-1)$, tal que

$$\begin{aligned} xy &= \gamma^{\frac{2^{d+1}(q-1)}{\lambda'} l_1 + \Delta l_2} , \\ &= (\gamma^4)^{\frac{2^{d-1}(q-1)}{\lambda'} l_1 + \frac{\Delta}{4} l_2} . \end{aligned}$$

Por lo tanto $xy \in \mathcal{D}_0^{(4)}$. Ahora, trivialmente, tenemos que $\frac{\Delta}{4} | \lambda' \frac{\Delta}{2^{d+1}}$ y $\frac{2^{d-1}(q-1)}{\lambda'} | (q-1)$. Así, dado que $\mathrm{mcd}(\frac{\Delta}{4}, \frac{2^{d-1}(q-1)}{\lambda'}) = 1$, y dado que $|\langle \gamma^4 \rangle| = \frac{q^k-1}{4}$, concluimos que cada elemento xy aparecerá con multiplicidad dada por $\lambda' \frac{\Delta}{2^{d+1}}(q-1)/(\frac{q^k-1}{4}) = \frac{2\lambda'}{2^d}$. □

El siguiente resultado será importante para poder determinar la distribución de pesos de la clase de códigos cíclicos no irreducibles en la que estamos interesados.

Lema 6 . *Para enteros i y j, con $0 \leq i, j \leq 3$, sea*

$$\mathcal{E}_{(i,j)} = \{(\alpha, \alpha) \mid \alpha \in \mathcal{D}_i^{(4)}\} \cup \{(\alpha, -\alpha) \mid \alpha \in \mathcal{D}_j^{(4)}\} ,$$

y

$$\mathcal{G}_{(i,j)} = \{(\alpha, \beta) \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \mid (\beta + \alpha) \in \mathcal{D}_i^{(4)} \ y \ \ (\beta - \alpha) \in \mathcal{D}_j^{(4)}\} .$$

También, sea w como en el Teorema 1, y para cualquier entero par r definimos los seis conjuntos siguientes:

$$
\begin{aligned}
\mathcal{S}_1 &= \{\ (0,0)\} \\
\mathcal{S}_2 &= \begin{cases} \mathcal{E}_{(w,w+2)} & si\ r/2\ es\ impar \\ \mathcal{E}_{(w,w)} & si\ r/2\ es\ par \end{cases}, \\
\mathcal{S}_3 &= \begin{cases} \mathcal{E}_{(w+2,w)} \quad \cup \mathcal{E}_{(1,1)} \cup \mathcal{E}_{(3,3)} & si\ r/2\ es\ impar \\ \mathcal{E}_{(w+2,w+2)} \cup \mathcal{E}_{(1,1)} \cup \mathcal{E}_{(3,3)} & si\ r/2\ es\ par \end{cases}, \\
\mathcal{S}_4 &= \begin{cases} ((\cup_{i=0}^{3}\mathcal{G}_{(i,w+2)}) \cup (\cup_{j=0}^{3}\mathcal{G}_{(w,j)})) \setminus \mathcal{G}_{(w,w+2)} & si\ r/2\ es\ impar \\ ((\cup_{i=0}^{3}\mathcal{G}_{(i,w)}) \quad \cup (\cup_{j=0}^{3}\mathcal{G}_{(w,j)})) \setminus \mathcal{G}_{(w,w)} & si\ r/2\ es\ par \end{cases}, \\
\mathcal{S}_5 &= \begin{cases} \mathcal{G}_{(w,w+2)} & si\ r/2\ es\ impar \\ \mathcal{G}_{(w,w)} & si\ r/2\ es\ par \end{cases}, \\
\mathcal{S}_6 &= (\cup_{i=0}^{3} \cup_{j=0}^{3} \mathcal{G}_{(i,j)}) \setminus (\mathcal{S}_4 \cup \mathcal{S}_5)\ ,
\end{aligned}
$$

donde el subíndice $w+2$ es tomado modulo 4 (así, si $w = 2$ entonces, por ejemplo, $\mathcal{E}_{(w,w+2)} = \mathcal{E}_{(2,0)}$). Entonces, los conjuntos $\mathcal{S}_l$, $l = 1,2,3,4,5,6$, son disjuntos en pares, y $\mathbb{F}_{q^k} \times \mathbb{F}_{q^k} = \cup_{l=1}^{6}\mathcal{S}_l$. Sus cardinalidades son: $|\mathcal{S}_1| = 1$, $|\mathcal{S}_2| = \frac{q^k-1}{2}$, $|\mathcal{S}_3| = \frac{3(q^k-1)}{2}$, $|\mathcal{S}_4| = \frac{6(q^k-1)^2}{16}$, $|\mathcal{S}_5| = \frac{(q^k-1)^2}{16}$ y $|\mathcal{S}_6| = \frac{9(q^k-1)^2}{16}$. Más aún, sean η_0 y η_1 como en el Teorema 1, así, si $\alpha, \beta \in \mathbb{F}_{q^k}$ entonces

$$
\sum_{m=0}^{1} \sum_{z \in \mathcal{D}_{rm}^{(4)}} \chi(z(\beta + (-1)^m \alpha)) = \begin{cases} \frac{q^k-1}{2} & si\ (\alpha,\beta) \in \mathcal{S}_1 \\ \frac{q^k-1}{4} + \eta_0 & si\ (\alpha,\beta) \in \mathcal{S}_2 \\ \frac{q^k-1}{4} + \eta_1 & si\ (\alpha,\beta) \in \mathcal{S}_3 \\ \eta_0 + \eta_1 & si\ (\alpha,\beta) \in \mathcal{S}_4 \\ 2\eta_0 & si\ (\alpha,\beta) \in \mathcal{S}_5 \\ 2\eta_1 & si\ (\alpha,\beta) \in \mathcal{S}_6 \end{cases}.
$$

Observación 2 . *Dado que $4|\Delta$, entonces $\mathbb{F}_q^* \subset \mathcal{D}_0^{(4)}$. Por lo tanto, para cualquier entero i, observemos que $\alpha \in \mathcal{D}_i^{(4)}$ si y sólo*

si $2\alpha \in \mathcal{D}_i^{(4)}$. *Además, si* i *y* l *son enteros y si* $\rho \in \mathcal{D}_l^{(4)}$, *entonces observemos que*

$$\sum_{z \in \mathcal{D}_i^{(4)}} \chi(z\rho) = \sum_{z \in \mathcal{D}_{i+l}^{(4)}} \chi(z) \, .$$

Demostración: Dado que $-1 \neq 1$, sobre el campo finito $\mathbb{F}_{q^k}$, entonces la primera afirmación viene de una inspección directa de los conjuntos $\mathcal{S}_l$, $l = 1, 2, 3, 4, 5, 6$.

Trivialmente, $|\mathcal{S}_1| = 1$. Por otro lado, dado que $4|(q^k - 1)$, entonces observemos que $|\mathcal{D}_i^{(4)}| = \frac{q^k-1}{4}$, para toda $0 \leq i \leq 3$, y esto implica que $|\mathcal{E}_{(i,j)}| = 2|\mathcal{D}_0^{(4)}| = \frac{q^k-1}{2}$, para $0 \leq i, j \leq 3$. Por lo tanto, $|\mathcal{S}_2| = \frac{q^k-1}{2}$ y $|\mathcal{S}_3| = \frac{3(q^k-1)}{2}$. Ahora, sea

$$M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \, .$$

Claramente, la matriz M es invertible sobre $\mathbb{F}_{q^k}$. Así, la transformación lineal $T_M : \mathbb{F}_{q^k}^2 \to \mathbb{F}_{q^k}^2$, dada por la regla

$$T_M(\alpha, \beta) = \begin{pmatrix} \beta + \alpha \\ \beta - \alpha \end{pmatrix} \, ,$$

es una biyección entre los vectores en $\mathbb{F}_{q^k}^2$. Así, si $(\delta_i, \delta_j) \in \mathcal{D}_i^{(4)} \times \mathcal{D}_j^{(4)}$ entonces, debe existir un vector único $(\alpha, \beta) \in \mathbb{F}_{q^k}^2$ tal que $\beta + \alpha = \delta_i$ y $\beta - \alpha = \delta_j$. Por lo tanto, $|\mathcal{G}_{(i,j)}| = |\mathcal{D}_i^{(4)} \times \mathcal{D}_j^{(4)}| = \frac{q^k-1}{4} \cdot \frac{q^k-1}{4} = \frac{(q^k-1)^2}{16}$, para $0 \leq i, j \leq 3$. Así $|\mathcal{S}_4| = \frac{6(q^k-1)^2}{16}$, $|\mathcal{S}_5| = \frac{(q^k-1)^2}{16}$ y $|\mathcal{S}_6| = \frac{9(q^k-1)^2}{16}$.

Observemos que

$$\sum_{m=0}^{1}\sum_{z\in\mathcal{D}_{rm}^{(4)}}\chi(z(\beta+(-1)^m\alpha))=\begin{cases}\sum\limits_{z\in\mathcal{D}_0^{(4)}}\chi(z(\beta+\alpha))+\sum\limits_{z\in\mathcal{D}_2^{(4)}}\chi(z(\beta-\alpha)), & \text{si } r/2 \text{ es impar}\\ \\ \sum\limits_{z\in\mathcal{D}_0^{(4)}}\chi(z(\beta+\alpha))+\sum\limits_{z\in\mathcal{D}_0^{(4)}}\chi(z(\beta-\alpha)), & \text{si } r/2 \text{ es par}\end{cases},$$

y que $\sum_{z\in\mathcal{D}_i^{(4)}}\chi(0)=|\mathcal{D}_0^{(4)}|=\frac{q^k-1}{4}$, para $0\leq i\leq 3$. Por otro lado, recordemos que w puede tomar solamente los valores 0 o 2. Por lo tanto, invocando la observación 2, podemos ver que la última afirmación se sigue de (2) y de la definición de los conjuntos $\mathcal{S}_l$, $l=1,2,3,4,5,6$. □

Observación 3 . *Como una consecuencia directa del lema anterior observemos que, sin importar el valor del entero par r, la suma exponencial $\sum_{m=0}^{1}\sum_{z\in\mathcal{D}_{rm}^{(4)}}\chi(z(\beta+(-1)^m\alpha))$ tendrá la siguiente distribución de valores:*

Tabla 1. Distribución de valores de
$$\sum_{m=0}^{1}\sum_{z\in\mathcal{D}_{rm}^{(4)}}\chi(z(\beta+(-1)^m\alpha)),$$
donde r es cualquier entero par.

Valor	**Frecuencia**
$\frac{q^k-1}{2}$	1
$\frac{q^k-1}{4}+\eta_0$	$\frac{q^k-1}{2}$
$\frac{q^k-1}{4}+\eta_1$	$\frac{3(q^k-1)}{2}$
$\eta_0+\eta_1$	$\frac{6(q^k-1)^2}{16}$
$2\eta_0$	$\frac{(q^k-1)^2}{16}$
$2\eta_1$	$\frac{9(q^k-1)^2}{16}$

Como veremos en la siguiente sección, la distribución de los valores de la suma exponencial anterior, determinará la distribución de pesos de una familia de códigos cíclicos no irreducibles.

4 La Distribución de Pesos de una Familia de Códigos Cíclicos no Irreducibles

Iniciamos esta sección recordando la siguiente identidad bastante conocida:

Sea $\mathcal{C}$ un código lineal de N pesos, sobre $\mathbb{F}_q$, de longitud n y dimensión $2k$. Supongamos que $w_1, w_2, \cdots, w_N$ son los pesos distintos a cero de $\mathcal{C}$. Para $1 \leq i \leq N$, sea A_i el número de palabras de peso w_i en $\mathcal{C}$ y sea B_j el número de palabras de peso j en $\mathcal{C}^{\perp}$ (el código dual de $\mathcal{C}$). Entonces, la tercera identidad de Pless (ver [8, p.259] para el resultado general), para $\mathcal{C}$, es

$$\sum_{i=1}^{N} w_i^2 A_i = [n(q-1)(n(q-1)+1) - B_1(q+2(n-1)(q-1)) + 2B_2]q^{2k-2} \ . \quad (3)$$

En el contexto de la identidad anterior, observemos que un código lineal es proyectivo si y sólo si B_1 y B_2 son cero en (3).

Manteniendo en mente esta identidad, estamos listos para obtener la distribución de pesos de una familia de códigos cíclicos no irreducibles.

Teorema 2 . *Sean q, k y Δ como antes. Considerando nuestra suposición principal, también tomamos a λ como un divisor de $(q-1)$ y definimos $n = \lambda\Delta$. Sean a_1 y a_2 dos enteros tal que $a_2 n \equiv 0 \pmod{q^k - 1}$ y $a_2 q^{\jmath} - a_1 \equiv \frac{q^k-1}{2} \pmod{q^k-1}$, para algún entero $\jmath$ con $1 \leq q^{\jmath} < q^k$. Sea $\mathcal{C}_{(a_1,a_2)}$ el código cíclico con*

polinomio de chequeo de paridad $h_{a_1}(x)h_{a_2}(x)$. *Si* $\mathrm{mcd}(\frac{\Delta}{2}, a_2) = 2$, *entonces las siguientes tres afirmaciones son ciertas:*

(A) $\mathrm{grado}(h_{a_1}(x)) = \mathrm{grado}(h_{a_2}(x)) = k$ *y* $h_{a_1}(x) \neq h_{a_2}(x)$.

(B) $\mathcal{C}_{(a_1,a_2)}$ *es un código cíclico* $[n, 2k]$ *con distribución de pesos dada por*

Tabla 2. Distribución de pesos de $\mathcal{C}_{(a_1,a_2)}$.

Peso	**Frecuencia**
0	1
$\frac{\lambda}{2}(q^{k-1} - 3(-q)^{(k-2)/2})$	$\frac{q^k-1}{2}$
$\frac{\lambda}{2}(q^{k-1} + (-q)^{(k-2)/2})$	$\frac{3(q^k-1)}{2}$
$\lambda(q^{k-1} - (-q)^{(k-2)/2})$	$\frac{6(q^k-1)^2}{16}$
$\lambda(q^{k-1} - 3(-q)^{(k-2)/2})$	$\frac{(q^k-1)^2}{16}$
$\lambda(q^{k-1} + (-q)^{(k-2)/2})$	$\frac{9(q^k-1)^2}{16}$

(C) *Si* B_1 *y* B_2 *son, respectivamente, el número de palabras de peso* 1 *y* 2 *en el código dual de* $\mathcal{C}_{(a_1,a_2)}$, *entonces* $B_1 = 0$ *y* $B_2 = \frac{n(q-1)(2\lambda-1)}{2}$. *Por lo tanto* $\mathcal{C}_{(a_1,a_2)}$ *es un código cíclico no proyectivo.*

Demostración: Primero observemos que, para cualquier entero $\jmath$, tenemos que γ^{-a_2} y $\gamma^{-a_2 q^\jmath}$ son conjugados. Así, sin pérdida de generalidad, podemos suponer simplemente que $a_1 = a_2 + \frac{q^k-1}{2}$.

Parte (A): Sea s el entero positivo mas pequeño tal que $a_2 q^s \equiv a_2 \pmod{n}$. Entonces $\lambda\Delta | a_2(q^s - 1)$. Pero $\mathrm{mcd}(\Delta, 2a_2) = 4$; así, la condición $\lambda\Delta | (2a_2 \frac{q^s-1}{2})$ implica que $\Delta | 2(q^s - 1)$. Sin embargo, gracias al Lema 2, sabemos que esta última condición es imposible si $s < k$, por lo tanto, $\mathrm{grado}(h_{a_2}(x)) = k$. Por

otro lado, $\mathrm{mcd}(\frac{\Delta}{2}, a_1) = \mathrm{mcd}(\frac{\Delta}{2}, a_2 + \frac{q^k-1}{2}) = \mathrm{mcd}(\frac{\Delta}{2}, a_2 + \frac{\Delta}{2}(q-1)) = \mathrm{mcd}(\frac{\Delta}{2}, a_2) = 2$, así podemos concluir similarmente que $\mathrm{grado}(h_{a_1}(x)) = k$.

Ahora, supongamos que $h_{a_1}(x) = h_{a_2}(x)$. Entonces, existirá un entero $0 \leq s < k$ tal que $a_2 q^s \equiv a_1 \pmod{q^k - 1}$. Pero $a_1 = a_2 + \frac{q^k-1}{2}$, así la última congruencia implica que $a_2(q^s - 1) \equiv \frac{q^k-1}{2} \pmod{q^k - 1}$, lo cual a su vez implica que $a_2(q^s - 1) \equiv 0 \pmod{\frac{q^k-1}{2}}$. En consecuencia, $(q^k - 1) | 2a_2(q^s - 1)$, y por lo tanto $\Delta | 2a_2((q^s - 1)/(q - 1))$. Ahora, dado que $\mathrm{mcd}(\Delta, 2a_2) = 4$, tendremos que $\Delta | 4((q^s - 1)/(q - 1))$, y por lo tanto $(q^k - 1) | 4(q^s - 1)$. Pero tal condición es imposible si $s < k$ y $q \geq 5$, así, $h_{a_1}(x) \neq h_{a_2}(x)$.

Parte (B): Dado que $a_1 n = a_2 n + (q^k - 1)\lambda\frac{\Delta}{2} \equiv 0 \pmod{q^k - 1}$, entonces el código cíclico, $\mathcal{C}_{(a_1,a_2)}$, tiene longitud n y su dimensión es $2k$, debido a la Parte (A).

Ahora, para cada $\alpha, \beta \in \mathbb{F}_{q^k}$, definimos $c(n, a_1, a_2, \alpha, \beta)$ como el vector de longitud n sobre $\mathbb{F}_q$, el cual está dado por:

$$(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha(\gamma^{a_1})^0 + \beta(\gamma^{a_2})^0), \cdots, \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha(\gamma^{a_1})^{n-1} + \beta(\gamma^{a_2})^{n-1})) \ .$$

Gracias al Teorema de Delsarte (ver, por ejemplo, [4]), es bien sabido que

$$\mathcal{C}_{(a_1,a_2)} = \{c(n, a_1, a_2, \alpha, \beta) \mid \alpha, \beta \in \mathbb{F}_{q^k}\} \ .$$

Así el peso Hamming de cualquier palabra de código de la forma $c(n, a_1, a_2, \alpha, \beta) \in \mathcal{C}_{(a_1,a_2)}$ es igual a $n - Z(\alpha, \beta)$, donde

$$Z(\alpha, \beta) = \sharp\{m \mid 0 \leq m < n, \text{ y } \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha\gamma^{a_1 m} + \beta\gamma^{a_2 m}) = 0\} \ .$$

Ahora, si χ' es el caracter aditivo canónico de $\mathbb{F}_q$, entonces,

por la propiedad ortogonal en (1), sabemos que para cada $c \in \mathbb{F}_q$ tenemos

$$\sum_{y \in \mathbb{F}_q} \chi'(yc) = \begin{cases} q & \text{si } c = 0 \\ \\ 0 & \text{si } c \neq 0 \end{cases} ,$$

así

$$Z(\alpha, \beta) = \frac{1}{q} \sum_{m=0}^{n-1} \sum_{y \in \mathbb{F}_q} \chi'(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(y(\alpha\gamma^{a_1 m} + \beta\gamma^{a_2 m}))) \; .$$

Si χ denota el caracter aditivo canónico de $\mathbb{F}_{q^k}$, entonces χ' y χ estan relacionados por $\chi'(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\varepsilon)) = \chi(\varepsilon)$ para toda $\varepsilon \in \mathbb{F}_{q^k}$. Por lo tanto, tenemos que

$$\begin{aligned} Z(\alpha, \beta) &= \frac{n}{q} + \frac{1}{q} \sum_{m=0}^{n-1} \sum_{y \in \mathbb{F}_q^*} \chi(y(\alpha\gamma^{a_1 m} + \beta\gamma^{a_2 m})) \\ &= \frac{n}{q} + \frac{1}{q} \sum_{m=0}^{n-1} \sum_{y \in \mathbb{F}_q^*} \chi(\gamma^{a_2 m} y((-1)^m \alpha + \beta)), \end{aligned}$$

donde la ultima igualdad surge porque $a_1 = a_2 + \frac{q^k-1}{2}$ y $\gamma^{\frac{q^k-1}{2}} = -1$. Ahora, dado que $\mathrm{mcd}(\frac{\Delta}{2}, a_2) = 2$ y $\mathcal{C}_{(a_1,a_2)} = \mathcal{C}_{(a_2,a_1)}$, entonces, gracias al Corolario 1, podemos asumir sin pérdida de generalidad que $\mathrm{mcd}(q^k - 1, a_2) = 2^d \frac{q-1}{\lambda'}$ para algunos enteros d y λ' tal que $d = 0$ o 1, y λ' es el divisor de $(q-1)$ que satisface $\mathrm{mcd}(q-1, a_2) = \frac{q-1}{\lambda'}$. Pero estas condiciones son la hipótesis en el Lema 4, así

$$Z(\alpha, \beta) = \frac{n}{q} + \frac{2^d \lambda}{q\lambda'} \sum_{m=0}^{n'-1} \sum_{y \in \mathbb{F}_q^*} \chi(\gamma^{2^d \frac{q-1}{\lambda'} m} y((-1)^m \alpha + \beta)) \; ,$$

donde $n' = \lambda' \frac{\Delta}{2^d}$. Pero sabemos que $d = 0$ o 1, entonces tendremos que $|\mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})}| = n' = \lambda' \frac{\Delta}{2^d}$ es un entero par, así observamos que

$$\{\gamma^{2^d \frac{q-1}{\lambda'} m} \mid 0 \leq m < n'\} = \mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})} = \mathcal{D}_0^{(\frac{2^{d+1}(q-1)}{\lambda'})} \cup \mathcal{D}_{2^d \frac{q-1}{\lambda'}}^{(\frac{2^{d+1}(q-1)}{\lambda'})} .$$

Por lo tanto,

$$Z(\alpha, \beta) = \frac{n}{q} + \frac{2^d \lambda}{q\lambda'} \sum_{m=0}^{1} \sum_{x \in \mathcal{D}_{2^d \frac{q-1}{\lambda'} m}^{(\frac{2^{d+1}(q-1)}{\lambda'})}} \sum_{y \in \mathbb{F}_q^*} \chi(xy((-1)^m \alpha + \beta)) . \quad (4)$$

Dado que $\text{mcd}(\frac{\Delta}{2}, a_2) = 2$, entonces $2^d \frac{q-1}{\lambda'} = \text{mcd}(q^k - 1, a_2)$ es un entero par tal que $2^d \frac{q-1}{\lambda'} | a_2$, por lo tanto tendremos que $2 \leq \text{mcd}(\frac{\Delta}{2}, 2^d \frac{q-1}{\lambda'}) \leq \text{mcd}(\frac{\Delta}{2}, a_2) = 2$. Así, la conclusión es que $\text{mcd}(\frac{\Delta}{2}, 2^d \frac{q-1}{\lambda'}) = 2$. Por lo tanto, después de aplicar el Lema 5 a (4), obtenemos

$$Z(\alpha, \beta) = \frac{n}{q} + \frac{2\lambda}{q} \sum_{m=0}^{1} \sum_{z \in \mathcal{D}_{2^d \frac{q-1}{\lambda'} m}^{(4)}} \chi(z(\beta + (-1)^m \alpha)) .$$

Dado que el peso de Hamming de toda palabra de código $c(n, a_1, a_2, \alpha, \beta) \in \mathcal{C}_{(a_1,a_2)}$ es igual a $n - Z(\alpha, \beta)$, y dado que $2^d \frac{q-1}{\lambda'}$ es un entero par, entonces el resultado se sigue de la Observación 3.

Parte (C): Es bien sabido que no existen palabras de peso 1 en el dual de cualquier código cíclico (ver, por ejemplo, [23]), por lo tanto $B_1 = 0$. Dado que $q > 3$ y $B_1 = 0$, la afirmación acerca de B_2, se sigue directamente de la Tabla 2 y de (3). Finalmente, dado que $n(q-1) \neq 0$ y $\lambda \neq \frac{1}{2}$, entonces $B_2 \neq 0$. Por lo tanto $\mathcal{C}_{(a_1,a_2)}$ es un código cíclico no proyectivo. □

El siguiente ejemplo es una aplicación directa del teorema

anterior.

Ejemplo 1 . Si $q = 7$, $k = 2$, $\lambda = 1$ y $a_2 = 6$, entonces $\Delta = 8$ y $\mathrm{mcd}(\frac{\Delta}{2}, a_2) = 2$. Además, observemos que $\frac{\lambda}{2}(q^{k-1} + (-q)^{(k-2)/2}) = \lambda(q^{k-1} - 3(-q)^{(k-2)/2}) = 4$. Por lo tanto, $\mathcal{C}_{(30,6)}$ es un código cíclico proyectivo de 4 pesos, sobre $\mathbb{F}_7$, de longitud 8, dimensión 4 y polinomio enumerador de pesos $A(z) = 1 + 24z^2 + 216z^4 + 864z^6 + 1296z^8$.

Observemos que, para un divisor λ de $(q-1)$ y para cualquier entero a_2, el Teorema 2 básicamente establece que si a_2 satisface la condición $\mathrm{mcd}(\frac{\Delta}{2}, a_2) = 2$, entonces, para cada entero $\jmath$, el código $\mathcal{C}_{(a_2 q^\jmath \pm \frac{q^k-1}{2}, a_2)}$ debe ser descrito por medio de las tres afirmaciones en dicho teorema. Gracias a esta condición de fácil verificación, podemos dar el número exacto de códigos cíclicos diferentes $\mathcal{C}_{(a_1,a_2)}$, que satisfacen la hipótesis en el Teorema 2, pero antes de eso, apuntemos la siguiente:

Observación 4 . *Si ϕ denota la función ϕ de Euler (ver, por ejemplo, [9, p. 20]) y si ζ y $\frac{\Delta}{4}$ son dos enteros positivos, entonces el número de enteros entre 1 y $\zeta\frac{\Delta}{4}$, primos relativos a $\frac{\Delta}{4}$, es $\zeta\phi(\frac{\Delta}{4})$.*

Teorema 3 . *Sean q, k y Δ como antes. Considerando nuestra suposición principal, también tomamos a λ como un divisor de $(q-1)$ y definimos $n = \lambda\Delta$. Para cualesquiera enteros a_1 y a_2, sea $\mathcal{C}_{(a_1,a_2)}$ el código cíclico con polinomio de chequeo de paridad $h_{a_1}(x)h_{a_2}(x)$. Sea $\mathcal{N}_{(q,k,\lambda)}$ el número de códigos cíclicos, $\mathcal{C}_{(a_1,a_2)}$ de longitud n y dimensión $2k$ que satisfacen las condiciones en el Teorema 2. Entonces*

$$\mathcal{N}_{(q,k,\lambda)} = \begin{cases} 0 & \text{si } \mathrm{mcd}(\frac{\Delta}{2}, \frac{q-1}{\lambda}) > 2 \\ \\ \frac{2\lambda\phi(\frac{\Delta}{4})}{mcd(\lambda,2)k} & \text{en otro caso} \end{cases} .$$

Demostración: Un código cíclico $\mathcal{C}_{(a_1,a_2)}$ pertenece a la familia de códigos descrita por el Teorema 2, si $a_2 n \equiv 0 \pmod{q^k-1}$, $\mathrm{mcd}(\frac{\Delta}{2}, a_2) = 2$ y $a_1 = a_2 q^\jmath \pm \frac{q^k-1}{2}$, para algún entero $\jmath$ con $1 \leq q^\jmath < q^k$. Entonces $a_2 = \frac{q-1}{\lambda} u$, para algún entero u. Si suponemos que $\mathrm{mcd}(\frac{\Delta}{2}, \frac{q-1}{\lambda}) > 2$ entonces, claramente, $\mathrm{mcd}(\frac{\Delta}{2}, a_2) > 2$. Por lo tanto $\mathcal{N}_{(q,k,\lambda)} = 0$, si $\mathrm{mcd}(\frac{\Delta}{2}, \frac{q-1}{\lambda}) > 2$. Así supondremos que $\mathrm{mcd}(\frac{\Delta}{2}, \frac{q-1}{\lambda}) \leq 2$. Ahora, dado que cada uno de los polinomios mínimos $h_{a_1}(x)$ y $h_{a_2}(x)$ tiene exactamente k raíces conjugadas diferentes, y dado que tenemos que $\mathrm{mcd}(\frac{\Delta}{2}, a_1) = \mathrm{mcd}(\frac{\Delta}{2}, a_2 q^\jmath \pm \frac{q^k-1}{2}) = \mathrm{mcd}(\frac{\Delta}{2}, a_2 q^\jmath \pm \frac{\Delta}{2}(q-1)) = \mathrm{mcd}(\frac{\Delta}{2}, a_2 q^\jmath) = \mathrm{mcd}(\frac{\Delta}{2}, a_2)$ para cualquier entero $\jmath$, entonces

$$\begin{aligned} \mathcal{N}_{(q,k,\lambda)} &= \frac{\sharp\{a_2 \mid a_2 n \equiv 0 \,(\mathrm{mod}\ q^k-1),\ \mathrm{mcd}(\frac{\Delta}{2}, a_2) = 2 \text{ y } 0 \leq a_2 < (q^k-1)\}}{2k} \\ &= \frac{\sharp\{u \mid \mathrm{mcd}(\frac{\Delta}{2}, \frac{q-1}{\lambda} u) = 2 \text{ y } 0 \leq u < n\}}{2k} \,. \end{aligned}$$

Pero $\frac{q-1}{2}$ es un entero impar, y dado que estamos suponiendo que $\mathrm{mcd}(\frac{\Delta}{2}, \frac{q-1}{\lambda}) \leq 2$, así

$$\mathcal{N}_{(q,k,\lambda)} = \frac{\sharp\{u \mid \mathrm{mcd}(\frac{\Delta}{4}, u) = 1 \text{ y } 0 \leq u < \frac{n}{\mathrm{mcd}(\lambda,2)}\}}{2k} \,.$$

Claramente $\frac{n}{\mathrm{mcd}(\lambda,2)} = \frac{4\lambda}{\mathrm{mcd}(\lambda,2)} \frac{\Delta}{4}$, por lo tanto el resultado se sigue directamente de la Observación 4. □

Los siguientes ejemplos son aplicaciones directas del Teorema 3.

Ejemplo 2 . Si $q = 7$, $k = 2$ y $\lambda = 3$, entonces $\Delta = 8$ y $\mathcal{N}_{(7,2,3)} = 3$. De hecho, si $q = 7$, $k = 2$ y $\lambda = 3$, entonces la familia de códigos cíclicos $\mathcal{C}_{(a_1,a_2)}$ descrita por el Teorema 2 es

$\mathcal{C}_{(2,26)}$, $\mathcal{C}_{(6,30)}$ y $\mathcal{C}_{(10,34)}$. Estos tres códigos son códigos cíclicos no proyectivos de 4 pesos, de longitud 24, dimensión 4 y polinomio enumerador de pesos $A(z) = 1+24z^6+216z^{12}+864z^{18}+1296z^{24}$.

Ejemplo 3 . Si $q = 11$, $k = 2$ y $\lambda = 10$, entonces $\Delta = 12$ y $\mathcal{N}_{(11,2,10)} = 10$. Estos diez códigos son códigos cíclicos no proyectivos de 5 pesos, de longitud 120, dimensión 4 y polinomio enumerador de pesos $A(z) = 1 + 60z^{40} + 180z^{60} + 900z^{80} + 5400z^{100} + 8100z^{120}$.

5 Conclusión

En este trabajo presentamos la evaluación de una suma exponencial específica, la cual puede ser derivada directamente como una instancia particular de un resultado general que fue originalmente presentado en [13]. Continuamos determinando la distribución de valores de dicha suma exponencial específica, y la utilizamos con el objetivo de presentar la distribución de pesos de una familia de códigos cíclicos reducibles. Como mostramos aquí, todos los códigos en esta familia son códigos cíclicos no proyectivos. Mas aún, mostramos que los códigos en esta familia pueden ser identificados de forma fácil, y como un subproducto de dicha identificación, pudimos determinar el número exacto de códigos cíclicos en una familia, cuando la longitud y dimensión son conocidas.

Finalmente, es interesante darnos cuenta que la familia de códigos estudiados en este trabajo es completamente diferente a la familia de códigos estudiados en [19]. Sin embargo, las técnicas que fueron utilizadas para estudiar ambas familias, son muy similares. Así, tal vez es posible desarrollar una teoría más general que incluya a estas dos familias de códigos.

Conclusiones Generales

En general, el problema de determinar la distribución de pesos de un código cíclico sobre un campo finito es difícil. Típicamente, cuando el campo finito es un campo primo, el problema es manejado expresando el peso de Hamming de cada palabra de código por medio de cierta combinación de sumas exponenciales. En este proyecto de investigación, encontramos dos métodos alternativos para determinar la distribución de pesos de códigos cíclicos reducibles sobre un campo finito, los cuales son la suma directa de dos códigos cíclicos irreducibles distintos.

Con el primer método, calculamos la distribución de pesos de algunos códigos cíclicos reducibles. Este método necesita la evaluación de algunas sumas exponenciales, sin embargo, como se descubrió, tal evaluación sólo requiere realizarse unas cuantas veces. Además, este método tiene la ventaja de ser flexible, en el sentido de que también puede aplicarse a códigos cíclicos sobre campos finitos de orden no primo.

Por su parte, el segundo método nos proporciona la distribución de pesos de una familia de códigos cíclicos reducibles, y en este caso, ya no se requiere la evaluación de sumas exponenciales para obtener su distribución de valores, con lo cual el cálculo de la distribución de pesos del código es directa. Todos los códigos en esta familia son códigos cíclicos no proyectivos.

El hecho de que ellos pueden identificarse de manera fácil, nos permitió como un resultado adicional, el poder determinar el número exacto de códigos cíclicos en una familia, cuando la longitud y la dimensión son dadas.

La conclusión final es que, el método de calcular o encontrar la distribución de valores de una suma exponencial, es una poderosa herramienta para hallar la distribución de pesos de códigos cíclicos en general, por lo que es posible que con el uso de tal herramienta, se pueda desarrollar una teoría más amplia, que incluya varias familias de códigos, con el objetivo de hallar generalizaciones.

Referencias

1. Alard, M. and Lasalle R., Principles of modulation and channel coding for digital broadcasting for mobile receivers, EBU Review, No. 224 Aug. 1987, pp. 47-69.

2. Berlekamp, E. R., Algebraic Coding Theory, McGraw-Hill Book Company, 1968.

3. Bose, R. C. and Ray-Chaudhuri, D. K., On a class of error-correcting binary group codes, Information and Control No. 3, 1960, pp. 68-79.

4. Delsarte P., On subfield subcodes of Reed-Solomon codes, IEEE Trans. Inform. Theory 21 No. 5, 1975, pp. 575-576.

5. Feng, K. and Luo J., Weight distribution of some reducible cyclic codes, Finite Fields and Their Applications, Vol. 14, No. 2, 2008, pp. 390-409.

6. Hamming, R., Error detecting and error correcting codes, The Bell System Technical Journal, Vol. 29, 1950, pp. 147-160.

7. Helleseth, T., Some two-weight codes with composite parity-check polynomials, IEEE Trans. Inform. Theory 22, 1976, pp. 631-632.

8. Huffman, W. and Pless, V., Fundamental of Error-Correcting Codes, Cambridge University Press, Cambridge UK, 2003.

9. Ireland, K. and Rosen, M., A Classical Introduction to Modern Number Theory, Springer- Verlag New York, 1990.

10. Lidl, R. and Niederreiter, H., Finite Fields, Cambridge Univ. Press, Cambridge, 1983, pp. 755.

11. Ma, C., Zeng, L., Liu, Y., Feng, D. and Ding, C., The Weight Enumerator of a Class of Cyclic Codes, IEEE Trans. Inf. Theory 57 No. 1, 2011, pp. 397-402.

12. MacWilliams, F.J. and Sloane, N.J.A., The Theory of Error-Correcting Codes, Amsterdam, North-Holland, The Netherlands, 1977, pp. 762.

13. Moisio, M., A note on evaluations of some exponential sums, Acta Arith. 93, 2000, pp.117-119.

14. Moisio, M., Exponential sums, Gauss sums and cyclic codes, Dissertation, Acta Univ. Oul. A 306, 1998, pp. 33.

15. Paterson, Kenneth G., Applications of Exponential Sums in Communications Theory, Extended Enterprise Laboratory, HP Laboratories Bristol, HPL-1999-101, 1999.

16. Reed, Irving S. and Solomon, Gustave, Polynomial Codes over Certain Finite Fields, Journal of the Society for Industrial and Applied Mathematics (SIAM) Vol. 8, No. 2, 1960, pp. 300-304.

17. Shannon, C. E., A Mathematical Theory of Communication, The Bell System Technical Journal, Vol. 27, July, October, 1948, pp. 379423, 623656.

18. Vega, G., Determining the Number of One-weight Cyclic Codes when Length and Dimension are Given, International Workshop on the Arithmetic of Finite Fields 2007, Lecture Notes in Computer Science, vol. 4547, 2007, pp. 284-293.

19. Vega, G., The Weight Distribution of an Extended Class of Reducible Cyclic Codes, IEEE Trans. Inform. Theory 58 No.7, 2012, pp. 4862-4869.

20. Vega, G., Two-weight cyclic codes constructed as the direct sum of two one-weight cyclic codes, Finite Fields and Their Applications, Vol. 14, No. 3, 2008, pp. 785-797.

21. Vega, G. and Wolfmann, J., New classes of 2-weight cyclic codes, Des. Codes Crypt. no.42, 2007, pp. 327-334.

22. Wicker, S. and Bhargava, V., Reed-Solomon codes and their applications, IEEE Information Theory Society, 1994.

23. Wolfmann, J., Are 2-Weight Projective Cyclic Codes Irreducible?, IEEE Trans. Inform. Theory 51 No. 2, 2005, pp. 733-737.

24. Vázquez-Fernández C.A. and Vega-Hernández G., On the Weight Distribution of the Dual of some Cyclic Codes with Two Non Conjugated Zeros, Journal of Applied Research and Technology, Centro de Ciencias Aplicadas y Desarrollo Tecnológico, Universidad Nacional Autónoma de México, vol. 9, no. 1, April 2011, pp. 36-48.

25. Vega, G. and Vázquez, C.A., The weight distribution of a family of reducible cyclic codes, in: Arithmetic of Finite Fields, Lecture Notes in Computer Science 7369, Springer-Verlag, 2012, pp. 16-28.

26. Ding, C., Gao, Y. and Zhou, Z., Five Families of Three-Weight Ternary Cyclic Codes and Their Duals, IEEE Trans. Inform. Theory 59 No. 12, 2013, pp. 7940-7946.

27. Zhengchun, Z. and Cunsheng, D., Seven Classes of Three-Weight Cyclic Codes, IEEE Trans. on Communications 61 No. 10, 2013, pp. 4120-4126.

28. Vega, G. and Morales Luis B., A General Description for the Weight Distribution of Some Reducible Cyclic Codes, IEEE Trans. Inform. Theory 59 No. 9, 2013, pp. 5994-6001.