El espectro de códigos cíclicos y grafos asociados

por Lic. Denis Videla

Presentado ante la Facultad de Matemática, Astronomía, Física, y Computación como parte
de los requerimientos para la obtención del grado de Doctor en Matemática de la

Universidad Nacional de Córdoba

Marzo, 2018

Director: Dr. Ricardo Podestá

Agradecimientos

En primer lugar quiero agradecer a mi familia, mis viejos y mis hermanos que los amo mucho, a mi tio Javier y mi Nono que ya no están pero espero que desde allá arriba se hayan alegrado, se los extraña mucho.

También quiero agradecer a mi director Ricardo Podesta por su gran predisposición, por todo el tiempo que me dedicación durante el doctorado y en especial en la escritura de está tesis, gracias por todo.

Quiero agradecer también a FaMAF y al CIEM por haberme brindado el lugar de trabajo. En particular quiero agradecerle a Nancy Moyano por toda su ayuda y muy buena predisposición siempre.

A Roberto Miatello e Isabel Dotti por sus charlas, consejos y predisposición cada vez que necesité una referencia, consejo o recomendación.

A los amigos que he hecho durante este transcurso del doctorado en los pasillos del Famaf, jugando al futbol ó tomando algo en los bares Diego, Oscar, Guille, Gon, Agus, Gabi, Rami, Mauro, Edwin, Ivan A., Maxi, Edu y Angel que nos vinimos juntos desde San Luis. También a mis amigos de la oficina 334 Euge, Meli, Andru, y Marcos que siempre estuvieron y siguen estando para todo.

A Emilio por todos sus consejos y enseanzas durante este trayecto, y también al resto del grupo de teoría de números Juan Pablo y Ariel de los cuales siempre se aprenden cosas buenisimas de matemáticas y futbol en los seminarios.

Al resto de mis compañeros de esta facultad que hicieron mucho más ameno este camino Kari, Fiore, Sonia, Romi, Rocio, Ivan G., Javier, Augusto, Ceci, Mary, Lucia, Juan y Edward.

A todos los profes que tuve en FAMAF, de los cuales aprendí y sigo aprendiendo muchisimo. También agradecer a la UNSL que me formó inicialmente, especialmente a Daniel Jaume que me guió en este camino hermoso que son las matemáticas.

Por último agradecer especialmente a mi novia Andrea por acompañarme siempre y darme la oportunidad de ser Papá de mi hijo Santiago, que llego durante el final del proceso para poner un broche de oro a esta etapa, los amo con todo mi corazón.

Índice general

Introducción

Motivación

Esta tesis se centra en el estudio del espectro o distribución de pesos de códigos cíclicos y de las distintas relaciones que tienen estos espectros con otros objetos que aparecen en el estudio de cuerpos finitos tales como sumas exponenciales, caracteres, curvas algebraicas y grafos de Cayley.

Sea $q = p^s$, donde p es un primo. Un $[n, k, d]$-código lineal sobre $\mathbb{F}_q$ es un subespacio $\mathcal{C}$ de dimensión k de $\mathbb{F}_q^n$, donde d denota la menor distancia de Hamming entre palabras distintas del código $\mathcal{C}$. A los elementos del código le llamaremos las palabras del código (o palabras-código) y su peso, denotado $w(c)$, se define como la cantidad de coordenadas no nulas de él. Notar que como $\mathcal{C}$ es un espacio vectorial se tiene que $d = \text{mín}\{w(c) : c \in \mathcal{C} \setminus \{0\}\}$. Sea

$$A_i = \#\{c \in \mathcal{C} : w(c) = i\}$$

para $i = 0, 1, \ldots, n$. El *enumerador de pesos* del código $\mathcal{C}$ se define como el polinomio

$$W_{\mathcal{C}}(t) = A_0 + A_1 t + \cdots + A_n t^n.$$

La sucesión $(A_0, A_1, \ldots, A_n)$ es llamada *la distribución de pesos* o *el espectro* del código $\mathcal{C}$. Notar que $A_0 = 1$ y $A_1 = A_2 = \cdots = A_{d-1} = 0$.

El estudio de la distribución de pesos de un código lineal es uno de los problemas más importantes en la teoría de códigos ya que permite en algunos casos, calcular el error de probabilidad en el proceso de decodificación vía algunos algoritmos ([29]). El cálculo explícito de distribuciones de pesos es computacionalmente complejo además de ser un problema abierto en general. Incluso, es un problema abierto si nos restringimos a la familia de códigos cíclicos. Aquí, nos concentraremos en calcular explícitamente la distribución de pesos en ciertas familias de códigos cíclicos asociadas a formas cuadráticas.

Un $[n, k]$-código sobre $\mathbb{F}_q$ se dice *cíclico* si cumple que:

$$(c_0, \ldots, c_{n-1}) \in \mathcal{C} \Longleftrightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

En general, podemos identificar al vector $(c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ con el polinomio

$$c_0 + c_1 t + \cdots + c_{n-1} t^{n-1} \in \mathbb{F}_q[t]/(t^n - 1).$$

Cualquier código de longitud n se corresponde a un subconjunto de $\mathbb{F}_q[t]/(t^n - 1)$. Con esta identificación, los códigos cíclicos se corresponden biunívocamente con los ideales de

$\mathbb{F}_q[t]/(t^n-1)$. A su vez, los ideales de $\mathbb{F}_q[t]/(t^n-1)$ se corresponden biunívocamente con los polinomios mónicos que dividen a t^n-1. Por lo tanto, existe un único polinomio mónico $g(t) \in \mathbb{F}_q[t]$ que divide a t^n-1 y genera a $\mathcal{C}$ como un ideal en $\mathbb{F}_q[t]/(t^n-1)$; este g se llama el *polinomio generador* de $\mathcal{C}$. Como $g(t)$ divide a t^n-1, existe $h(t) \in \mathbb{F}_q[t]$ tal que $t^n-1 = g(t)h(t)$. El polinomio $h(t)$ se suele llamar el *polinomio de chequeo* de $\mathcal{C}$. Se dice que $\mathcal{C}$ es *irreducible* si $h(t)$ es irreducible sobre $\mathbb{F}_q$ y si h es reducible también llamamos reducible a $\mathcal{C}$. Los ceros de h se llaman los *ceros del código*.

Hay muchas clases de códigos cíclicos conocidas, como por ejemplo los códigos de Hamming, Golay, BCH, Reed-Solomon, Melas y residuos cuadráticos .

En el survey del 2015 de Dinh, Li y Yue ([11]) se muestran los progresos de estos últimos años en el cálculo explícito de distribuciones de pesos de códigos cíclicos, vía diferentes técnicas que relacionan los pesos del código con sumas de tipo exponencial, como por ejemplo el uso de funciones especiales sobre cuerpos finitos, formas cuadráticas, formas hermitianas, grafos de Cayley, sumas de Gauss y de Kloostermann. Los autores K. Feng y J. Luo ([13]) calcularon explícitamente la distribución de pesos del código cíclico reducible de longitud $n = p^m - 1$ con ceros

$$\alpha^{-1} \quad \text{y} \quad \alpha^{-(p^\ell+1)},$$

donde α es un generador de $\mathbb{F}_{p^m}^*$, $\ell \geq 0$ y $m/(m,\ell)$ impar, usando funciones perfectas no lineales también llamadas funciones planares. En 2008, haciendo uso de formas cuadráticas, los mismos autores calcularon las distribuciones de los códigos cíclicos reducibles con ceros

$$\alpha^{-2}, \alpha^{-(p^\ell+1)} \quad \text{y} \quad \alpha^{-1}, \alpha^{-2}, \alpha^{-(p^\ell+1)},$$

respectivamente, cuando p es un primo impar y $(m,\ell) = 1$ ([14], [15]). Estos métodos introducidos por Feng y Luo permitieron a muchos otros autores calcular explícitamente la distribución de códigos cíclicos sobre $\mathbb{F}_p$, con p un primo impar (ver [49], [50], [51], [52], [53], [54]). Otra forma de estudiar enumeradores de pesos es vía familias de curvas algebraicas de tipo Artin-Schreier como lo hicieron Van der Geer, Van der Vlugt y Schoof ([42], [43], [44]).

La segunda parte de la tesis se trata de la construcción de unos objetos muy importantes para la teoria de números y la combinatoria, llamados grafos de Ramanujan. Los grafos de Ramanujan son una clase de grafos que aparecieron durante la década del 80' para la construcción de unos objetos optimales muy interesantes llamados expanders.

Los primeros en encontrar familias infinitas de grafos de Ramanujan de grado regular fijo fueron Lubotszky, Sarnak y Philips ([32]). Más precisamente, encontraron familias infinitas de grafos de Ramanujan $(p+1)$-regulares, donde p es un primo satisfaciendo $p \equiv 1 \bmod 4$. Luego, Morgenstern pudo encontrar familias infinitas $(p^\ell+1)$-regulares ([37]). Ellos conjeturaron que de haber familias infinitas de grafos de Ramanujan de grado de regularidad fijo k, entonces $k-1$ tendría que ser una potencia de un primo.

En el 2008, Adam Marcus, Daniel Spielman y Nikhil Srivastava ([33]) mostraron que no estaban en lo correcto ya que pudieron probar que existen familias infinitas de grafos de Ramanujan bipartitos de grado fijo k, para todo k. Ellos hicieron uso de herramientas topológicas (2-recubrimientos) y algebraicas (familias entrelazadas) para construir dichos grafos.

Lo interesante, por lo tanto, es ver si de alguna manera uno puede encontrar familias infinitas de grafos de Ramanujan no bipartitos de un grado de regularidad fijo. En esta dirección, aquí vamos a construir muchas familias de grafos de Ramanujan no bipartitos. A futuro, sería muy bueno ver si vía herramientas topológicas (2-levantamientos) u otras herramientas, es posible usar los grafos que vamos a construir aquí para encontrar otras familias infinitas distintas a las ya conocidas.

Resumen y resultados

En el Capítulo 1 se introducirán los conceptos básicos sobre códigos. Veremos las propiedades y parametros más importantes de códigos lineales. Luego, introduciremos los códigos cíclicos y enunciaremos los dos teoremas centrales, estos son la *identidad de MacWilliams* y el *Teorema de Delsarte*. Por último veremos algunos ejemplos muy importantes de códigos cíclicos (Melas, Hamming y BCH).

En el Capítulo 2 veremos en detalle las principales propiedades sobre sumas exponenciales y sobre formas cuadráticas. Una forma cuadrática sobre el cuerpo finito $\mathbb{F}_q$ es un polinomio homogéneo de grado 2 con coeficientes en $\mathbb{F}_q$. Veremos que el estudio de formas cuadráticas sobre cuerpos finitos varía sustancialmente si la característica del cuerpo es 2 o no, ya que cuando la característica es impar, podemos definir las formas cuadráticas de manera matricial; esto permite interpretar los invariantes de la forma cuadrática en invariantes de la matriz asociada, facilitando así su estudio. Específicamente, nos interesan calcular sumas exponenciales relacionadas con formas cuadráticas, estas sumas aparecen naturalmente en la distribución de pesos de los códigos cíclicos que veremos. Por último, veremos en concreto la distribución de rangos y tipos de la forma cuadrática $Q_\lambda(x) = \mathrm{Tr}_{q^m/q}(\lambda x^{q^\ell+1})$ cuando $m/(m,\ell)$ es par.

En el Capítulo 3 calcularemos la distribución de pesos de varias familias de códigos relacionados con la familia de formas cuadráticas $Q_\lambda(x)$ tanto en característica par como en característica impar.

Específicamente, consideraremos los códigos traza $\mathcal{C}_\ell, \mathcal{C}_{\ell,0}, \mathcal{C}_{\ell,1}$ y $\mathcal{C}_{\ell,2}$ definidos de la manera siguiente:

$$\mathcal{C}_\ell = \{c(\lambda) : \lambda \in \mathbb{F}_{q^m}\}, \qquad \mathcal{C}_{\ell,0} = \{c(\lambda) + b : \lambda \in \mathbb{F}_{q^m}, b \in \mathbb{F}_q\},$$
$$\mathcal{C}_{\ell,1} = \{c(\beta,\lambda) : \ \beta,\lambda \in \mathbb{F}_{q^m}\}, \qquad \mathcal{C}_{\ell,2} = \{c(\beta,\lambda) + b : \ \beta,\lambda \in \mathbb{F}_{q^m}, b \in \mathbb{F}_q\},$$

donde

$$c(\lambda) = \left(\mathrm{Tr}_{q^m/q}(\lambda\alpha^{(q^\ell+1)i})\right)_{i=0}^{n-2}, \qquad c(\lambda)+b = \left(\mathrm{Tr}_{q^m/q}(\lambda\alpha^{(q^\ell+1)i}) + b\right)_{i=0}^{n-2},$$
$$c(\beta,\lambda) = \left(\mathrm{Tr}_{q^m/q}(\beta x + \lambda x^{q^\ell+1})\right)_{x\in\mathbb{F}_{q^m}^*}, \quad c(\beta,\lambda)+b = \left(\mathrm{Tr}_{q^m/q}(\beta x + \lambda x^{q^\ell+1}) + b\right)_{x\in\mathbb{F}_{q^m}^*},$$

con α es un elemento primitivo de $\mathbb{F}_{q^m}$ y

$$n = \frac{q^m-1}{(q^m-1, q^\ell+1)}.$$

Para calcular la distribuciones nos organizamos de la siguiente manera:

(i) En un principio vamos a ver que calcular el peso de una palabra es equivalente a calcular ciertas sumas exponenciales.

(ii) Luego, vamos a ver que cuando consideramos códigos cíclicos provenientes de formas cuadráticas el cálculo de dichas sumas exponenciales es equivalente a calcular el rango y el tipo de la forma cuadrática asociada.

Por lo tanto para calcular la distribución de pesos del código, basta calcular la distribución de rangos y tipos de la familia de formas cuadráticas asociadas al código. Veremos que esto se puede plantear de manera general si la familia de formas cuadráticas tienen solamente rangos pares. Finalmente usando distribución de rangos y tipos de la forma cuadrática Q_λ calcularemos el espectro de los códigos cíclicos anteriormente definidos.

En el Capítulo 4 analizaremos los resultados obtenidos en el Capítulo 3 desde el punto de vista de curvas algebraicas. Veremos que, restringiendo los parametros del código, obtenemos curvas optimales en el sentido de Hasse-Weil dentro de la familia de curvas algebraicas parametrizadas

$$C_{\lambda,\beta}: \quad y^p - y = \lambda x^{p^\ell+1} + \beta x \qquad \lambda, \beta \in \mathbb{F}_{p^m}$$

con ℓ fijo.

Por otra parte, cuando m es par y $(m, \ell) = 1$, veremos que en el caso binario ($q = 2$) el dual del código $\mathcal{C}_{\ell,1}$, es decir el código con polinomio generador $m_\alpha(t)m_{\alpha^{2^\ell+1}}(t)$, donde α es un elemento primitivo de $\mathbb{F}_{2^m}$ y m_{α^i} es el polinomio minimal de α^i, satisface una condición de optimalidad en términos de su distancia (es la mayor posible), esto es interesante ya que se conocen pocos códigos con polinomio generador del tipo $m_\alpha(t)m_{\alpha^i}(t)$ satisfaciendo esta condición. De hecho, Van Lint y Wilson probaron que en general casi todos los códigos de este tipo no satisfacen dicha condición de optimalidad ([46]).

Esta propiedad de optimalidad nos permite relacionar el código con una clase especial de función Booleana, llamada función APN, como se ve en [4]. En este caso la función que resulta ser una función APN es la función sobre $\mathbb{F}_{2^m}$ definida por

$$F(x) = x^{2^\ell+1} \quad \text{con} \quad (m, \ell) = 1.$$

Cuando m es impar, se sabe que además la función F pertenece a otra clase especial de funciones Booleanas llamadas funciones AB. Aunque en el capítulo no nos adentraremos en estos temas, en el Capítulo 5 si le daremos mayor importancia.

Finalmente, en el Capítulo 5, veremos distintas construcciones de ciertos objetos muy interesantes, tanto para la teoría de números como para la combinatoria, llamados grafos de Ramanujan. En un principio, veremos la principal propiedad espectral que tienen los grafos de Cayley, que nos permite relacionar los autovalores del grafo con ciertas sumas de caracteres del grupo usado para construir el grafo de Cayley. En nuestro caso, aparecen ciertas sumas de caracteres aditivos de cuerpos finitos, estas resultan ser sumas exponenciales del tipo que veníamos estudiando en los capítulos anteriores, por lo tanto en un principio usaremos las

sumas exponenciales junto con la forma cuadrática $Q_\lambda(x)$ para analizar el espectro del grafo de Cayley

$$\Gamma_{m,\ell} = X(\mathbb{F}_{p^m}, S_\ell) \qquad \text{con} \qquad S_\ell = \{x^{p^\ell+1} : x \in \mathbb{F}_{p^m}^*\}.$$

En el caso binario y ternario ($p = 2, 3$) probaremos que Γ_ℓ es Ramanujan si $(m, \ell) = 1$.

Luego, para el caso binario, veremos qué condiciones tiene que satisfacer una forma cuadrática del tipo $Q_R(x) = \mathrm{Tr}_{2^m/2}(xR(x))$, donde $R(x)$ es un polinomio 2-linealizado, para que el grafo asociado sea Ramanujan. Veremos que hay limitaciones si se quiere generalizar por este camino la construcciones de grafos de Ramanujan. Por lo tanto, se busca generalizar esta construcción de grafos de Ramanujan desde otro punto de vista. Usando el hecho de que la función Booleana $F(x) = x^{2^\ell+1}$ es una función APN, consideramos el grafo

$$\Gamma_F^* = X(F, S_F) \qquad \text{con} \qquad S_F = \{F(x) : x \in \mathbb{F}_{2^m}\}.$$

Este resulta ser un grafo de Ramanujan cuando F es una función APN monomial y m es par. Sin embargo, el grafo considerado resulta ser isomorfo a los grafos $\Gamma_{m,\ell}$. Por lo tanto se considerará otra subfamilia de funciones APN, las llamadas funciones AB. Esta familia satisface muy buenas propiedades con respecto a su transformada de Walsh, lo que permite calcular los autovalores del grafo que vamos a definir, de manera sencilla. Especifícamente, el grafo que consideraremos es

$$\widehat{\Gamma}_F = X(\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}, R_F) \qquad \text{con} \qquad R_F = \{(x, F(x)) : x \in \mathbb{F}_{2^m}^*\},$$

donde F es una función AB y m es un entero impar. Probaremos que este grafo es de Ramanujan. Luego, modificaremos un poco el grafo Γ'_F para obtener otros grafos de Ramanujan. La primer modificación es simplemente considerar el mismo grupo pero tomando como conjunto de conexión a

$$R'_F = \{(x, F(x)) : x \in \mathbb{F}_{2^m}\} \qquad \text{con} \qquad F(0) \neq 0.$$

La otra modificación es considerar el grupo $H = \mathbb{F}_{2^m} \times \mathbb{F}_{2^s}$ con $s \mid m$ y la función

$$F_s(x) = \mathrm{Tr}_{2^m/2^s}(F(x)).$$

Luego,

$$\Gamma_s = X(H, R_{F_s}) \qquad \text{con} \qquad R_{F_s} = \{(x, F_s(x)) : x \in \mathbb{F}_{2^m}^*\}.$$

Por último, veremos una costrucción en característica impar, usando una clase de funciones que también son usadas para el cálculo explícito de distribuciones de pesos de códigos cíclicos. Estas son funciones de $\mathbb{F}_{p^m}$ llamadas funciones planares o funciones PN. Dada F una función planar, sea

$$S_F = \{(x, F(x)) : x \in \mathbb{F}_{p^m}^*\}.$$

Mostraremos que el grafo

$$\Gamma_{F,p} = X(\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, T_F), \qquad \text{donde} \qquad T_F = S_F \cup (-S_F)$$

es de Ramanujan.

Capítulo 1

Preliminares

En esta sección se introducirán los conceptos básicos sobre códigos. Comenzaremos con una introducción rápida a la teoría de códigos, veremos sus propiedades y parametros más importantes. Luego introduciremos los códigos cíclicos y enunciaremos los dos teoremas centrales que van a ayudarnos más adelante, estos son la *identidad de MacWilliams* y el *Teorema de Delsarte*. Por último veremos algunos ejemplos muy importantes de códigos cíclicos cuyo estudio de sus espectros vía sumas exponenciales y curvas algebraicas fueron principal fuente de inspiración para esta Tesis.

Con respecto a la teoría de códigos en general, existe mucho material bibliográfico clásico muy bueno para introducirse en esta teoría, como por ejemplo [35], [41] y [18].

1.1. Generalidades sobre códigos

Un alfabeto es un conjunto finito $\mathcal{A} = \{a_1, \ldots, a_q\}$. A los elementos de $\mathcal{A}$ se los llama símbolos y el número q es la raíz de $\mathcal{A}$. Una n-cadena o palabra de longitud n sobre $\mathcal{A}$ es una sucesión de n elementos de $\mathcal{A}$. En general, escribiremos a las palabras por yuxtaposición de símbolos, es decir $a = a_{i_1} a_{i_2} \cdots a_{i_n}$ con $a_{i_k} \in \mathcal{A}$, y decimos que a tiene longitud n. A veces, sin embargo, será conveniente usar la notación vectorial, y escribir $a = (a_{i_1}, a_{i_2}, \ldots, a_{i_n})$. Denotamos por $\mathcal{A}^n$ el conjunto de todas las n-cadenas y por $\mathcal{A}^*$ el conjunto de todas las palabras sobre $\mathcal{A}$, es decir $\mathcal{A}^* = \bigcup_{n \in \mathbb{N}} \mathcal{A}^n$.

Definición 1.1.1. Si $\mathcal{A} = \{a_1, \ldots, a_q\}$ es un alfabeto, un código q-ario sobre $\mathcal{A}$ es un subconjunto $\mathcal{C}$ de $\mathcal{A}^*$. Los elementos de $\mathcal{C}$ se llaman *palabras-código*. El número $M = |\mathcal{C}|$ es el *tamaño* del código. Si todas las palabras-código tienen longitud fija n decimos que $\mathcal{C}$ es un código *de bloque* de *longitud* n con parámetros (n, M).

Sea $\mathcal{C}$ un código q-ario. Se dice que $\mathcal{C}$ es un código binario, ternario o cuaternario según sea $q = 2$, $q = 3$ ó $q = 4$, respectivamente.

Para codificar y decodificar de manera más práctica y eficiente es útil dotar al alfabeto $\mathcal{A}$ de cierta estructura algebraica. Es común considerar a $\mathcal{A}$ como un cuerpo finito aunque también se lo puede considerar como un anillo. De ahora en adelante, fijamos $\mathcal{A} = \mathbb{F}_q$, el cuerpo finito de q elementos. Recordemos que $\mathbb{F}_q$ es único salvo isomorfismo y que $q = p^r$

para algún primo p y $r \in \mathbb{N}$. Si $q = p$, tenemos $\mathcal{A} = \mathbb{Z}_p$, el cuerpo de enteros módulo p. El conjunto de n-cadenas $\mathcal{A}^n$ es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión n, que identificamos naturalmente con

$$\mathbb{F}_q^n = \{(c_1, \ldots, c_n) : c_i \in \mathbb{F}_q, 1 \leq i \leq n\}$$

mediante la asignación

$$c_1 c_2 \cdots c_n \longleftrightarrow (c_1, c_2, \ldots, c_n).$$

A nosotros nos va a interesar la familia de códigos lineales, que se definen como sigue.

Definición 1.1.2. Un código *lineal* q-ario de *longitud* n y *dimensin* k es un subespacio $\mathcal{C} \subset \mathbb{F}_q^n$ de dimensión k. En este caso decimos que $\mathcal{C}$ es un $[n, k]_q$-código. Cuando $\mathcal{C}$ es un código binario, es usual quitar a $q = 2$ de la notación.

En todo código se puede definir una métrica usando la distancia de Hamming del espacio ambiente. Dada dos palabras c, c' de la misma longitud en el alfabeto $\mathcal{A}$. La *distancia de Hamming* de c a c' denotada por $d(c, c')$ se define como la cantidad de palabras en que difieren c con c', es decir $d : \mathcal{A}^n \times \mathcal{A}^n \to \mathbb{N}_0$, donde

$$d(c, c') = \#\{1 \leq i \leq n : c_i \neq c_i'\}.$$

Se muestra de manera sencilla que d es una métrica en $\mathcal{A}^n$, lo importante de esta distancia es que permite definir un parámetro central en el estudio de códigos autocorrectores, la distancia mínima del código.

Definición 1.1.3. Dado un código $\mathcal{C}$ se define la *distancia mínima* de $\mathcal{C}$, y se la denota por $d(\mathcal{C})$ ó $d_{\mathcal{C}}$, como la menor distancia no nula entre sus palabras código, es decir

$$d = d_{\mathcal{C}} = \text{mín}\{d(c, c') : c, c' \in \mathcal{C}, c \neq c'\}.$$

Un (n, M, d)-*código* es un código de longitud n, tamaño M y distancia mínima d. Cuando $\mathcal{C}$ sea un código lineal sobre $\mathbb{F}_q$ vamos a decir que es un $[n, k, d]_q$-*código* si tiene longitud n, dimensión k y distancia mínima d.

Dado $c \in \mathbb{F}_q^n$ se define el *peso* de c, denotado por $w(c)$, como el número de coordenadas no-nulas de c, es decir

$$w(c) = \#\{1 \leq i \leq n : c_i \neq 0\}.$$

O sea, el peso de c es la distancia de c al $0 = 00 \cdots 0$, esto es $w(c) = d(c, 0)$. Por ejemplo, $w(0120211) = 5$. Si $\mathcal{C}$ es un código, el *peso de* $\mathcal{C}$ se define por

$$w_{\mathcal{C}} = \text{mín}\{w(c) : c \in \mathcal{C} \setminus \{0\}\}.$$

De las definiciones es claro que $d(c, c') = w(c - c')$. Notar además que cuando $\mathcal{C}$ es un código lineal se tiene que $w_{\mathcal{C}} = d_{\mathcal{C}}$. La distancia de un código es clave para detectar y corregir errores. Se sabe que todo código $\mathcal{C}$ con distancia d detecta $d - 1$ errores y corrige $\lfloor \frac{d-1}{2} \rfloor$ errores.

De ahora en más todos los códigos que vamos a considerar van a ser códigos lineales sobre el alfabeto $\mathbb{F}_q$. Cuando consideramos códigos lineales, una ventaja grande de estos códigos es que podemos representarlos por un sistema de generadores.

Definición 1.1.4. Sea $\mathcal{C}$ un $[n,k]$-código lineal. Una *matriz generadora* de $\mathcal{C}$ es una matriz $G \in \mathbb{F}_q^{k\times n}$ cuyas filas forman una base de $\mathcal{C}$. Luego

$$\mathcal{C} = \{uG : u \in \mathbb{F}_q^k\}.$$

Obviamente esta matriz no es única, pero podemos siempre considerar la matriz generadora en forma estándar, es decir $G = (I_k|A)$ donde I_k es la matriz identidad de tamaño $k \times k$ y A de $k \times n-k$. La matriz generadora estándar es más util a la hora de codificar.

El espacio vectorial $\mathbb{F}_q^n$ tiene un producto interior natural dado por

$$c \cdot c' = c_1c'_1 + c_2c'_2 + \cdots + c_nc'_n.$$

Si $\mathcal{C}$ es un $[n,k]_q$-código, el código dual de $\mathcal{C}$ denotado por $\mathcal{C}^\perp$, es el $[n,n-k]$-código

$$\mathcal{C}^\perp = \{c' \in \mathbb{F}_q^n : c \cdot c' = 0, \forall c \in \mathcal{C}\}.$$

Una matriz generadora H de $\mathcal{C}^\perp$, se llama matriz de paridad de $\mathcal{C}$. En tal caso

$$\mathcal{C} = \{c \in \mathbb{F}_q^n : Hc^\top = 0\}.$$

Por lo visto hasta aquí, podemos ver a un código lineal $\mathcal{C}$ a través de transformaciones lineales: como una imagen, $\mathcal{C} = ImR_G$, donde G es una matriz generadora de $\mathcal{C}$, o como un núcleo, $\mathcal{C} = \ker R_{H^\top}$, donde H es una matriz de paridad de $\mathcal{C}$. Esto da una forma alternativa de definir códigos lineales. Tener un código lineal q-ario de longitud n y rango k es equivalente a tener una sucesión exacta de la forma

$$0 \longrightarrow \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-k} \longrightarrow 0.$$

La distancia mínima de un código se puede caracterizar vía la matriz de paridad, de la siguiente manera. Si H es la matriz de paridad de un $[n,k,d]_q$-código $\mathcal{C}$, entonces

$$d_\mathcal{C} = \text{mín}\{r > 0 : H \text{ tiene } r \text{ columnas linealmente dependientes}\},$$

es decir, si H tiene d columnas linealmente dependientes y todo conjunto de $d-1$ columnas de H es linealmente independiente. Una consecuencia inmediata de este hecho es la famosa cota de Singleton que enuncia que si $\mathcal{C}$ es un $[n,k,d]_q$-código, entonces $d \leq n-k+1$.

1.2. Espectro y enumeradores de pesos

Identidad de MacWilliams

Si $\mathcal{C}$ es un (n,M)-código, para $i = 0,\ldots,n$ denotamos por A_i el número de palabras de peso i en $\mathcal{C}$, es decir

$$A_i = \#\{c \in \mathcal{C} : w(c) = i\}.$$

La sucesión finita $A_0,\ldots,A_n$ se conoce como la *distribución de pesos* o el *espectro* de $\mathcal{C}$ y

$$W_\mathcal{C}(t) = \sum_{i=0}^{n} A_i\, t^i,$$

es llamado el *polinomio enumerador de pesos* de $\mathcal{C}$.

Si $\mathcal{C}$ es un código lineal, denotamos por $A_0^\perp, A_1^\perp, \ldots, A_n^\perp$ al espectro de su código dual $\mathcal{C}^\perp$ y tenemos su enumerador de pesos $W_{\mathcal{C}^\perp}(t) = \sum_I A_i^\perp t^i$. En este caso, existe una relación muy importante entre los enumeradores de pesos de $\mathcal{C}$ y $\mathcal{C}^\perp$, llamada identidad de MacWilliams.

Teorema 1.2.1 (Identidad de MacWilliams)**.** *Sea $\mathcal{C} \subset \mathbb{F}_q^n$ un código lineal, entonces*

$$W_{\mathcal{C}^\perp}(t) = \tfrac{1}{|\mathcal{C}|}\,(1+(q-1)t)^n\, W_{\mathcal{C}}\Big(\tfrac{1-t}{1+(q-1)t}\Big).$$

En término de coeficientes de los polinomios, la identidad de MacWilliams toma la forma

$$A_j^\perp = \tfrac{1}{|\mathcal{C}|}\sum_{i=0}^{n} K_j^{n,q}(i)\, A_i$$

donde $K_k^{n,q}(x)$ es el polinomio q-ario de Krawtchouk de orden n y grado k dado por

$$K_k^{n,q}(x) = \sum_{j=0}^{k}(-1)^j(q-1)^{k-j}\tbinom{x}{j}\tbinom{n-x}{k-j}.$$

Momentos de potencias

Dado un $[n,k]$-código $\mathcal{C}$, el *ℓ-ésimo momento de potencias* de $\mathcal{C}$, que denotamos por P_ℓ, está definido para $\ell = 0, \ldots, n$ por

$$P_\ell = \sum_{i=0}^{n} i^\ell A_i. \tag{1.1}$$

Estos fueron definidos y estudiados por Vera Pless en 1963. Una consecuencia importante de la identidad de MacWilliams, es una formula cerrada para los momentos de potencias i-ésimos de $\mathcal{C}$ en términos de la distribución de pesos de su código dual. En el caso binario, $q = 2$, se tienen las siguientes expresiones (ver [40] o §7.3 en [18])

$$\begin{aligned}
P_0 &= \sum_{j=0}^{n} A_j = 2^{k-1}\\
P_1 &= \sum_{j=0}^{n} jA_j = 2^{k-1}(n - A_1^\perp),\\
P_2 &= \sum_{j=0}^{n} j^2A_j = 2^{k-2}\{n(n+1) - 2nA_1^\perp + 2A_2^\perp\},\\
P_3 &= \sum_{j=0}^{n} j^3A_j = 2^{k-3}\{(n^2(n+3) - (3n^2+3n-2)A_1^\perp + 6(nA_2^\perp - A_3^\perp)\},\\
P_4 &= \sum_{j=0}^{n} j^4A_j = 2^{k-4}\{(n(n+1)(n^2+5n-2) - 4n(n^2+3n-2)A_1^\perp\\
&\qquad + 4(3n^2+3n-4)A_2^\perp - 24nA_3^\perp + 24A_4^\perp\}.
\end{aligned} \tag{1.2}$$

Las fórmulas para el caso general ($q \neq 2$) son mucho más complicadas y no las necesitaremos.

Otros enumeradores

Existen otras variantes del enumerador de pesos. El caso más sencillo es el *enumerador de pesos homogéneo*, que se define como

$$W_{\mathcal{C}}^{h}(t,s) = \sum_{k=0}^{n} A_i \, t^i s^{n-i}.$$

Notar que $W_{\mathcal{C}}^{h}(t,1) = W_{\mathcal{C}}(t)$.

Otra generalización es el enumerador de pesos completo del código. Supongamos que los elementos de $\mathbb{F}_q$ son $\omega_0 = 0, \omega_1, \ldots, \omega_{q-1}$ listados en algún orden fijo. La composición del vector $v = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$ está definida como

$$comp(v) = (t_0, t_1, \ldots, t_{q-1}),$$

donde cada $t_i = t_i(v)$ es el número de componentes v_j de v que son iguales a ω_i, para $0 \leq j \leq n-1$. Claramente, tenemos que

$$\sum_{i=0}^{q-1} t_i = n.$$

Sea $\mathcal{C}$ un $[n,k]$-código lineal sobre $\mathbb{F}_q$ y sea $A(t_0, t_1, \ldots, t_{q-1})$ el número de palabras $c \in \mathcal{C}$ con $comp(c) = (t_0, t_1, ..., t_{q-1})$. El *enumerador de pesos completo* de $\mathcal{C}$ es el polinomio

$$\begin{aligned} W_{\mathcal{C}}(z_0, z_1, \ldots, z_{q-1}) &= \sum_{c \in \mathcal{C}} z_0^{t_0(c)} z_1^{t_1(c)} \cdots z_{q-1}^{t_{q-1}(c)} \\ &= \sum_{(t_0,\ldots,t_{q-1}) \in B_n} A(t_0, t_1, \ldots, t_{q-1}) \, z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}}, \end{aligned}$$

donde

$$B_n = \{(t_0, \ldots, t_{q-1}) \, : \, 0 \leq t_i \leq n, \, t_0 + t_1 + \cdots + t_{q-1} = n\}.$$

Estos enumeradores de pesos también satisfacen identidades de MacWilliams, en el sentido que satisfacen una ecuación funcional junto al enumerador de pesos de su dual. Notar que en el caso binario el enumerador de pesos completo coincide con el enumerador de pesos común homogeneizado. Estos enumeradores de pesos han sido usados en distintos contextos. Por ejemplo, en [17] fueron usados para estudiar las transformadas de Walsh de funciones monomiales sobre cuerpos finitos y en [9] y [10] se usaron para estudiar códigos de autentificación. En particular, en teoría de códigos son relevantes ya que permiten calcular la capacidad de corregir errores del código así como también el error de probabilidad a la hora de decodificar con algunos algoritmos ([29]).

1.3. Códigos cíclicos

1.3.1. Códigos cíclicos y polinomio generador

Sea q una potencia de un primo p y sea n un natural coprimo con q.

Definición 1.3.1. Un código lineal $\mathcal{C}$ sobre $\mathbb{F}_q$ de longitud n se dice *cíclico* si es cerrado por desplazamientos cíclicos de las coordenadas de sus palabras. Esto es

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \quad \Longrightarrow \quad (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

Notar que esto implica que es cerrado por todos los desplazamientos cíclicos.

Si $\mathcal{C} \subseteq \mathbb{F}_q^n$ es un código lineal q-ario, a cada palabra código podemos asignarle un polinomio de la siguiente manera:

$$c_0 c_1 \ldots c_{n-1} \longmapsto c_0 + c_1 t + \cdots + c_{n-1} t^{n-1}.$$

Si llamamos $\phi : \mathcal{C} \to \mathbb{F}_q[t]$ a este mapa, claramente es un isomorfismo de $\mathbb{F}_q$-espacios vectoriales. Vía este isomorfismo podemos identificar al código $\mathcal{C}$ con su imagen $\phi(\mathcal{C})$. De ahora en adelante, ignoraremos el mapa ϕ y pensaremos a las palabras como polinomios, y recíprocamente.

El cociente

$$R_n = \frac{\mathbb{F}_q[t]}{(t^n - 1)}$$

es el álgebra de polinomios de grado menor que n, con la suma usual de polinomios y el producto de polinomios seguido de reducción módulo $t^n - 1$. Notar que el código $\mathcal{C}$ es cíclico si y solo si $\phi(\mathcal{C})$ es un ideal de R_n. El siguiente teorema reune algunos hechos básicos sobre este tipo de códigos.

Teorema 1.3.2. *Sea $\mathcal{C}$ un ideal de R_n, es decir un código cíclico de longitud n. Entonces:*

- *Existe un único polinomio mónico $g(t)$ de grado mínimo en $\mathcal{C}$. Además, este polinomio genera $\mathcal{C}$, es decir $\mathcal{C} = \langle g(t) \rangle$ y por esta razón es llamado el polinomio generador de $\mathcal{C}$.*
- $g(t) \mid t^n - 1$.
- *Si* $\deg(g(t)) = r$, *entonces $\mathcal{C}$ tiene dimensión $n - r$. Más aún*

$$\mathcal{C} = \langle g(t) \rangle = \{r(t)g(t) : gr(g(t)) < n - r\}.$$

- *Si $g(t) = g_0 + g_1 t + \cdots + g_r t^r$, entonces $g \neq 0$ y $\mathcal{C}$ tiene matriz generadora*

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r \end{pmatrix} \tag{1.3}$$

  donde cada fila de G es un desplazamiento cíclico de la fila anterior.

Es importante notar que el código cíclico $\mathcal{C}$ puede estar generado por otros polinomios además del polinomio generador, como lo muestra el siguiente ejemplo.

Ejemplo 1.3.3. Como $1+t$ divide a t^3-1, $\mathcal{C}=\langle 1+t\rangle$ es un código cíclico en $R_3=\mathbb{F}_2[t]/\langle t^3-1\rangle$. Por el teorema anterior, $\dim\mathcal{C}=3-1=2$ y $\mathcal{C}$ está formado por los múltiplos de $1+t$, luego

$$\mathcal{C}=\{0,1+t,1+t^2,t+t^2\}=\{000,110,101,011\}.$$

Se puede verificar que en este caso $1+t^2$ también genera $\mathcal{C}$, aunque $1+t^2$ no es un divisor de t^3-1. $\Diamond$

Una condición necesaria para que $g(t)$ sea el polinomio generador de un código cíclico de longitud n es que divida a t^n-1. Veamos que esta es también una condición suficiente. Sea $p(t)$ un polinomio mónico que divide a t^n-1 y consideremos $g(t)$ el polinomio generador del código $\mathcal{C}=\langle p(t)\rangle$ con $p(t)\neq g(t)$. Como $p(t)$ y $g(t)$ son mónicos, entonces $\deg(g(t))<\deg(p(t))$. Por la elección de $p(t)$ existe un $f(t)\neq 0$ tal que

$$t^n-1=p(t)f(t).$$

Además, existe $a(t)\in R_n$ tal que

$$g(t)\equiv a(t)p(t).$$

Luego, tenemos que

$$g(t)f(t)\equiv a(t)(t^n-1)\equiv 0.$$

Pero $\deg(g(t)f(t))<\deg(p(t)f(t))=n$, por lo tanto $g(t)f(t)=0$ lo cual no puede suceder. Por lo tanto, $p(t)=g(t)$.

Para cada q fijo, sea $\mathcal{D}_n$ el conjunto de todos los divisores mónicos de t^n-1, y sea $\mathcal{I}_n$ el conjunto de todos los ideales de R_n, es decir, todos los códigos cíclicos de longitud n. Por el Teorema 1.3.2, tenemos que el mapa $\Psi:\mathcal{D}_n\to\mathcal{I}_n$ que mapea $g(t)\mapsto\langle g(t)\rangle$, que a cada divisor mónico $g(t)$ de t^n-1 le asocia el código $\langle g(t)\rangle$ generado por $g(t)$, es una correspondencia biunívoca entre $\mathcal{D}_n$ e $\mathcal{I}_n$.

Observación 1.3.4. Esto muestra la importancia de poder factorizar t^n-1 sobre cuerpos finitos. En efecto, si podemos factorizar a t^n-1 completamente sobre $\mathbb{F}_q$, entonces podemos saber cuáles son todos los códigos cíclicos q-arios de longitud n. Podría sin embargo suceder que algunos de estos sean equivalentes entre sí.

Usaremos la siguiente identidad, bien conocida

$$t^n-1=\prod_{d|n}\Phi_d(t)$$

donde $\Phi_d(t)$ es el d-ésimo polinomio ciclotómico de orden n. Por definición $\Phi_d(t)$ es el polinomio cuyas raíces son las raíces n-ésimas de la unidad de grado d. Es decir,

$$\Phi_d(t)=\prod_{(k,n)=1}(t-\omega^k)$$

donde ω es una raíz primitiva n-ésima de la unidad de orden d. Se sabe que $\Phi_d(t)\in\mathbb{Z}[t]$ es irreducible sobre $\mathbb{Q}$, y tiene grado $\phi(d)$. Sin embargo, en general, $\Phi_d(t)$ no es irreducible sobre $\mathbb{F}_q$. Por otra parte, notemos que si $n=p$ es primo, entonces

$$t^p-1=\Phi_1(t)\Phi_p(t).$$

Como $\Phi_1(t) = t - 1$ entonces $\Phi_p(t) = 1 + t + \cdots + t^{p-1}$.

Cuando haya peligro de confusión, adoptaremos la notación $\mathcal{C} = (\!(p(t))\!)$ para denotar el hecho que $\mathcal{C}$ es el ideal generado por $p(t)$ y que $p(t)$ es el polinomio generador de $\mathcal{C}$.

Los códigos cíclicos son cerrados por sumas e intersecciones. En efecto, si $\mathcal{C}_1 = (g(t))$ y $\mathcal{C}_2 = (h(t))$ son códigos cíclicos en R_n, entonces

- $\mathcal{C}_1 \cap \mathcal{C}_2 = (m.c.m\{g(t), h(t)\})$,
- $\mathcal{C}_1 + \mathcal{C}_2 = (m.c.d\{g(t), h(t)\})$.

Además, $\mathcal{C}_1 \subseteq \mathcal{C}_2$ si y sólo si $h(t)$ divide a $g(t)$. Esto último implica que el mapa

$$\Psi : g(t) \mapsto (\!(g(t))\!)$$

es un isomorfismo que invierte el orden en los retículos $(\mathcal{D}_n, |)$ y $(\mathcal{I}_n, \subseteq)$.

1.3.2. Ceros y el polinomio de chequeo de códigos cíclicos

Como el polinomio generador $g(t)$ de un $[n, n-r]$-código cíclico en R_n divide a $t^n - 1$, tenemos

$$t^n - 1 = g(t)h(t)$$

donde $h(t)$ es un polinomio de grado $n-r$ llamado polinomio de chequeo o de control (check polynomial) de $\mathcal{C}$. Tenemos el siguiente resultado que resume las propiedades de $h(t)$.

Teorema 1.3.5. *Sea $h(t)$ el polinomio de chequeo de un código cíclico $\mathcal{C}$ en R_n.*

- *El código $\mathcal{C}$ puede describirse como*

$$\mathcal{C} = \{p(t) \in R_n : p(t)h(t) \equiv 0\}.$$

- *Si $h(t) = h_0 + h_1 t + \cdots + h_{n-r}t^{n-r}$, entonces la matriz de control de paridad de $\mathcal{C}$ está dada por*

$$H = \begin{pmatrix} h_{n-r} & \cdots & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & \cdots & \cdots & h_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & \cdots & h_0 \end{pmatrix}. \tag{1.4}$$

- *El código dual $\mathcal{C}^\perp$ es el código cíclico de dimensión r con polinomio generador*

$$h^\perp(t) = h_0^{-1}t^{n-r}h(t^{-1}) = h_0^{-1}(h_0 t^{n-r} + h_1 t^{n-r+1} + \cdots + h_{n-r}).$$

Existe una forma alternativa de ver a los códigos cíclicos en R_n. Estos pueden ser caracterizados por los ceros del polinomio t^n-1, es decir, por ciertas raíces n-ésimas de la unidad. Sea

$$t^n - 1 = \prod_i m_i(t)$$

la factorización de t^n-1 en factores irreducibles mónicos sobre $\mathbb{F}_q$. Si α es una raíz de $m_i(t)$ en alguna extensión de $\mathbb{F}_q$, entonces $m_i(t)$ es el polinomio minimal de α sobre $\mathbb{F}_q$. Luego, si $f(t) \in \mathbb{F}_q[t]$, entonces $f(\alpha) = 0$ si y sólo si $f(t) = a(t)m_i(t)$ para algún $a(t)$. En particular, si $f(t) \in R_n$, entonces

$$f(\alpha) = 0 \quad \Longleftrightarrow \quad f(t) \in (\!(m_i(t))\!).$$

Generalizando este hecho, obtenemos lo siguiente.

Teorema 1.3.6. *Sea $g(t) = q_1(t)q_2(t)\cdots q_u(t)$ un producto de factores irreducibles de t^n-1, y sean $\{\alpha_1, \ldots, \alpha_s\}$ las raíces de $g(t)$ en el cuerpo de descomposición de t^n-1 sobre $\mathbb{F}_q$. Entonces*

$$(\!(g(t))\!) = \{f(t) \in R_n : f(\alpha_1), \ldots, f(\alpha_s) = 0\}.$$

Más aún, es suficiente tomar una raíz de cada factor irreducible de $g(t)$. Esto es, si β_i es una raíz de $q_i(t)$ para $i = 1, \ldots, u$. Entonces

$$(\!(g(t))\!) = \{f(t) \in R_n : f(\beta_1) = 0, \ldots, f(\beta_u) = 0\}.$$

Las raíces del polinomio generador de un código cíclico se denominan *ceros del código*. La descripción de códigos cíclicos a través de sus ceros permite definir muchas familias famosas de códigos cíclicos, por ejemplo: Hamming binarios, Golay, BCH, Reed-Solomon, QR y Melas, entre otros.

1.3.3. Códigos traza y códigos restringidos

Supongamos que tenemos un código $\mathcal{C}$ sobre $\mathbb{F}_{q^m}$, hay dos formas clásicas de obtener un código sobre $\mathbb{F}_q$ a partir de $\mathcal{C}$: haciendo restricción de coordenadas y tomando trazas.

Códigos restricción

Definición 1.3.7. Sea $\mathcal{C}$ un $[n,k]$-código lineal sobre $\mathbb{F}_{q^m}$. El *código restringido* de $\mathcal{C}$ con respecto a $\mathbb{F}_q$ es

$$\mathcal{C}_{|_{\mathbb{F}_q}} = \mathcal{C} \cap (\mathbb{F}_q)^n = \{c \in \mathcal{C} : c_i \in \mathbb{F}_q, i = 1, \ldots, n\},$$

es decir, el conjunto de palabras en $\mathcal{C}$ donde cada una de sus componentes están en $\mathbb{F}_q$.

Primero describiremos cómo encontrar una matriz de chequeo para $\mathcal{C}_{|_{\mathbb{F}_q}}$ empezando con una matriz de chequeo H de $\mathcal{C}$. Como $\mathbb{F}_{q^m}$ es un espacio vectorial de dimensión m sobre $\mathbb{F}_q$, podemos elegir una $\mathbb{F}_q$-base $\{b_1, b_2, \ldots, b_m\}$ de $\mathbb{F}_{q^m}$ de $\mathbb{F}_{q^m}$. Cada elemento $z \in \mathbb{F}_{q^m}$ puede ser escrito de manera única como $z = z_1b_1 + \cdots + z_mb_m$, donde $z_i \in \mathbb{F}_q$ para $1 \leq i \leq m$. Asociamos a z el vector columna $z' = [z_1 \cdots z_m]^T$. Podemos construir la matriz de chequeo

H' de $\mathcal{C}_{|\mathbb{F}_q}$ a partir de la matriz de chequeo H de $\mathcal{C}$ reemplazando cada entrada h de H por el vector columna h'. Ya que H es una matriz de $(n-k)\times n$ con entradas en $\mathbb{F}_{q^m}$, H' es una matriz de $m(n-k)\times n$ sobre $\mathbb{F}_q$. Las filas de H' podrían ser dependientes. Por lo tanto una matriz de chequeo para $\mathcal{C}_{|\mathbb{F}_q}$ es obtenida a partir de H' borrando sus filas dependientes. Denotamos esta matriz de chequeo por $H_{|\mathbb{F}_q}$.

Esto último implica que si $\mathcal{C}$ es un $[n,k]$-código sobre $\mathbb{F}_{q^m}$ y $\mathcal{C}_{|\mathbb{F}_q}$ es un $[n,k_q]$-código, entonces

$$k \geq k_q \geq n - m(n-k).$$

Notar que si $\mathcal{C}$ es un código cíclico con polinomio generador

$$g(t) = m_{\alpha^{i_1}}(t) m_{\alpha^{i_2}}(t) \cdots m_{\alpha^{i_l}}(t) \in \mathbb{F}_q[t],$$

donde α es un elemento primitivo de $\mathbb{F}_{q^m}$ y $m_{\alpha^{i_k}}(t) \in \mathbb{F}_q[t]$ es el polinomio mínimal de α^{i_k} para $1 \leq k \leq l$, tal que $m_{\alpha^{i_k}}(t) \neq m_{\alpha^{i_j}}(t)$ para $k \neq j$, entonces $\mathcal{C}$ es el código restringido $\tilde{\mathcal{C}}_{|\mathbb{F}_q}$, donde $\tilde{\mathcal{C}}$ es el código cíclico con polinomio generador

$$\tilde{g}(t) = \prod_{k=1}^{l} (t - \alpha^{i_k}) \in \mathbb{F}_{q^m}[t].$$

Por lo tanto, todo código cíclico sobre $\mathbb{F}_q$ cuyo polinomio generador no este factorizado en términos lineales es un código restringido de otro código en alguna extensión de $\mathbb{F}_q$.

Códigos traza

Otra forma natural de definir un código sobre $\mathbb{F}_q$ a partir de un código sobre $\mathbb{F}_{q^m}$ es por medio de la función traza $\mathrm{Tr}_{q^m/q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ definida por

$$\mathrm{Tr}_{q^m/q}(x) = \sum_{i=0}^{m-1} x^{q^i} = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}, \tag{1.5}$$

donde $x \in \mathbb{F}_{q^m}$. Abreviaremos $\mathrm{Tr}_{q^m/q}$ por Tr_m cuando el q está sobreentendido. Dado un vector $c = (c_1, \ldots, c_n) \in \mathbb{F}_{q^m}^n$ podemos definir su traza por

$$\mathrm{Tr}_m(c) = (\mathrm{Tr}_{q^m/q}(c_1), \ldots, \mathrm{Tr}_{q^m/q}(c_n)).$$

Definición 1.3.8. Sea $\mathcal{C}$ un código lineal de longitud n sobre $\mathbb{F}_{q^m}$, el *código traza* de $\mathcal{C}$ es el código sobre $\mathbb{F}_q$ definido por

$$\mathrm{Tr}_m(\mathcal{C}) = \{\mathrm{Tr}_m(c) : c \in \mathcal{C}\}.$$

Notar que si $\mathcal{C}$ es un código cíclico sobre $\mathbb{F}_{q^m}$, entonces $\mathrm{Tr}_m(\mathcal{C})$ es cíclico. El siguiente ejemplo es una clase general de códigos cíclicos que veremos en el próximo capítulo.

Ejemplo 1.3.9. Sea $\mathcal{S}$ un $\mathbb{F}_{q^m}$-subespacio lineal de dimensión finita de $\mathbb{F}_{q^m}[x]$, entonces

$$\mathcal{C}_{\mathcal{S}} = \Big\{ \big(\mathrm{Tr} f(x)\big)_{x\in\mathbb{F}_{q^m}^*} : f \in \mathcal{S} \Big\} \tag{1.6}$$

es un código cíclico. En efecto, si α es un elemento primitivo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, entonces podemos interpretar a la palabra $\big(\mathrm{Tr} f(x)\big)_{x\in\mathbb{F}_{q^m}^*}$ como $\big(\mathrm{Tr} f(\alpha^i)\big)_{i=0}^{q^m-2}$ (salvo permutaciones de coordenadas). En tal caso, si ponemos $g(x) = f(\alpha^{-1}x)$, entonces $g \in S$ y se tiene que

$$\big(g(1), g(\alpha), \ldots, g(\alpha^{q^m-2})\big) = \big(f(\alpha^{q^m-2}), f(1), \ldots, f(\alpha^{q^m-3})\big).$$

De este modo, el código

$$\mathcal{C}'_{\mathcal{S}} = \big\{ (f(x))_{x\in\mathbb{F}_{q^m}^*} : f \in \mathcal{S} \big\}$$

es cerrado por corrimientos cíclicos y su linealidad es consecuencia de la linealidad del espacio S y por lo tanto $\mathcal{C}'_S$ es cíclico. Luego, $\mathrm{Tr}_m(\mathcal{C}'_S) = \mathcal{C}_S$ resulta un código cíclico sobre $\mathbb{F}_q$. $\Diamond$

El siguiente teorema es debido a Delsarte ([8]) y exhibe una relación de dualidad entre los códigos restringidos y los códigos traza.

Teorema 1.3.10 (Delsarte)**.** *Sea $\mathcal{C}$ un código lineal de longitud n sobre $\mathbb{F}_{q^m}$. Entonces*

$$(\mathcal{C}_{|\mathbb{F}_q})^{\perp} = \mathrm{Tr}_m(\mathcal{C}^{\perp}). \tag{1.7}$$

El teorema de Delsarte nos permite dar un código cíclico a partir de conocer cómo se descompone su polinomio de chequeo, de la manera siguiente.

Sea $r = q^m$ y α un generador de $\mathbb{F}_r^*$. Sea $h(t) = h_1(t)\cdots h_u(t) \in \mathbb{F}_q[t]$ donde $h_j(t)$ son polinomios irreducibles distintos sobre $\mathbb{F}_q$.

Para cada $1 \le j \le u$, sea

$$g_j = \alpha^{-s_j}$$

una raíz de $h_j(t)$, sea n_j el orden de g_j y sea m_j el menor entero positivo tal que

$$q^{m_j} \equiv 1 \pmod{n_j}.$$

Por lo tanto, $\deg(h_j(t)) = m_j$ para todo $j = 1, \ldots, u$. Pongamos

$$n = \tfrac{r-1}{\delta} \qquad \text{con} \qquad \delta = (r-1, s_1, \ldots, s_u)$$

y definamos el código

$$\mathcal{C} = \{c(a_1, \ldots, a_u) : a_j \in \mathbb{F}_{q^{m_j}}\}$$

con

$$c(a_1, \ldots, a_u) = \Big(\sum_{j=1}^{u} \mathrm{Tr}_{q^{m_j}/q}(a_j), \sum_{j=1}^{u} \mathrm{Tr}_{q^{m_j}/q}(a_j g_j), \ldots, \sum_{j=1}^{u} \mathrm{Tr}_{q^{m_j}/q}(a_j g_j^{n-1}) \Big).$$

Por el teorema de Delsarte, $\mathcal{C}$ es un $[n,k]$-código cíclico con polinomio de chequeo $h(t)$ y $k = m_1 + \cdots + m_u$, por lo tanto todo código cíclico puede ser definido dando solamente los ceros del polinomio de chequeo vía esta construcción. Una consecuencia de esto útimo es que todo código cíclico irreducible es traza.

1.3.4. Ejemplos importantes

En esta sección vamos a analizar algunos ejemplos muy importantes de códigos cíclicos.

Códigos de Hamming

Para cada $r \geq 1$, el código de Hamming q-ario $H_{n,q}(r)$ es un $[n, n-r, 3]$-código sobre $\mathbb{F}_q$ con $n = (q^r - 1)/(q-1)$. Su matriz de paridad H tiene la propiedad de que cada columna esta formada por un vector no nulo de cada subespacio 1-dimensional de $\mathbb{F}_q^r$.

Cuando $(n, q-1) = 1$, $H_{n,q}(m)$ puede ser visto como un código cíclico. Por ejemplo, los códigos de Hamming binarios y los ternarios de longitud impar son cíclicos. En efecto, sea α un elemento primitivo en $\mathbb{F}_{q^m}$. Entonces $\beta = \alpha^{q-1}$ es una raíz n-ésima de la unidad. La matriz de chequeo de $H_{q,n}(m)$ es

$$[1 \ \beta \ \beta^2 \ \ldots \ \beta^{n-1}].$$

Notar que su polinomio generador es

$$g(t) = m_\beta(t).$$

Por construcción de la matriz de paridad, la distancia mínima de $H_{n,q}(r)$ es 3, para todo n, q. Como el dual de este código es el código 'simplex', que tiene todas las palabras de peso q^{m-1}, el enumerador de pesos de $H_{n,q}(m)$ puede ser fácilmente obtenido vía la identidad de MacWilliams.

Definición 1.3.11. Sea n un entero positivo coprimo con q. Para $i \in \mathbb{N}_0$, la *coclase q-ciclotómica* módulo n que contiene a i se define como el conjunto

$$C_i = \{i, iq, \ldots, iq^{r-1}\} \pmod{n}$$

donde r es el menor entero positivo tal que $iq^r \equiv i \pmod{n}$.

Nota. La menor extensión de $\mathbb{F}_q$ que contiene a una raíz n-ésima de la unidad es $\mathbb{F}_{q^m}$, donde $m = |C_1|$ es el cardinal de $|\mathcal{C}_1|$ de la coclase q-ciclotómica módulo n que contiene a 1. Si β es una raíz primitiva de la unidad en $\mathbb{F}_{q^m}$, entonces el polinomio minimal de β^i sobre $\mathbb{F}_q$ es

$$m_{\beta^i}(t) = \prod_{j \in C_i} (t - \beta^j).$$

Hay una correspondencia entre los polinomios mónicos irreducibles de $t^n - 1$ y las coclases q-ciclotómicas módulo n. La factorización de $t^n - 1$ en irreducibles está dada por

$$t^n - 1 = \prod_s m_{\beta^s}(t).$$

Definición 1.3.12. Sea β una raíz n-ésima de la unidad en una extensión de $\mathbb{F}_q$. Sea $\mathcal{C}$ un código cíclico sobre $\mathbb{F}_q$ de longitud n con polinomio generador $g(t) \in \mathbb{F}_q[t]$. Entonces existe un conjunto $T \subseteq \{0, 1, \ldots, n-1\}$ tal que las raíces de $g(t)$ son $\{\beta^i : i \in T\}$. A dicho T se lo llama el *conjunto de definición* de $\mathcal{C}$ (con respecto a β).

Nota. Cambiando β cambiará T. Para un β dado, conocer $g(t)$ es equivalente a conocer T, ya que $g(t) = \prod_{i\in T}(t-\beta^i)$. Si $g(\beta^i) = 0$, entonces $g(\beta^{iq}) = 0$, implicando que T es una unión de coclases ciclotómicas módulo n. Recíprocamente, cualquier conjunto $T \subseteq \{0, 1, \ldots, n-1\}$ que es una unión de coclases q-ciclotómicas módulo n tiene la propiedad que

$$\prod_{i\in T}(t-\beta^i) \in \mathbb{F}_q[t]$$

y por lo tanto es el conjunto de definición de un código cíclico de longitud n sobre $\mathbb{F}_q$.

Códigos BCH

Ahora definiremos los códigos BCH (Bose-Chaudhuri,Hocquenghem).

Definición 1.3.13. El código cíclico $BCH_{n,q}(\delta)$ de longitud n y distancia diseñada δ es el código cíclico cuyo polinomio generador es de la forma

$$g(t) = m.c.m\{m_{\beta^a}(t), m_{\beta^{a+1}}(t), \ldots, m_{\beta^{a+\delta-2}}(t)\}$$

para alguna secuencia de elementos $\beta^a, \beta^{a+1}, \ldots, \beta^{a+\delta-2}$, donde β es una raíz n-ésima primitiva de la unidad en alguna extensión de $\mathbb{F}_q$. Alternativamente, $BCH_{n,q}(\delta)$ tiene conjunto de definición $T = C_a \cup C_{a+1} \cup \cdots \cup C_{a+\delta-2}$ relativo a β.

Hay una relación entre la distancia diseñada δ y la verdadera distancia mínima del código. Notar que la matriz de chequeo de $BCH_{n,q}(\delta)$ es

$$H = \begin{pmatrix} 1 & \beta^a & \beta^{2a} & \cdots & \beta^{(n-1)a} \\ 1 & \beta^{a+1} & \beta^{2(a+1)} & \cdots & \beta^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{a+\delta-2} & \beta^{2(a+\delta-2)} & \cdots & \beta^{(n-1)(a+\delta-2)} \end{pmatrix}. \tag{1.8}$$

Esta es una matriz de Vandermonde, por lo tanto cualquier conjunto de $(\delta-1)$ columnas de H son linealmente independientes. Luego el código tiene distancia mínima d satisfaciendo

$$d \geq \delta.$$

Más aún, como las entradas de H están en $\mathbb{F}_{q^m}$, estas pueden ser expresadas como una columna de $m \times 1$ sobre $\mathbb{F}_q$. Entonces, el rango de H es a lo más $m(\delta-1)$ y, por lo tanto, el código $BCH_{n,q}(\delta)$ es un $[n, k, d]_q$-código cíclico con

$$k \leq m(\delta-1) \quad \text{y} \quad d \geq \delta.$$

En el caso particular que $q = 2, a = 1$ y $\delta = 4$ nos referiremos a $BCH_{n,q}(\delta)$ como el código BCH binario 2-corrector de longitud $n = 2^m - 1$. Sea α un elemento primitivo de $\mathbb{F}_{2^m}$, en este caso el polinomio generador de este código es

$$g(t) = m_\alpha(t) m_{\alpha^3}(t)$$

donde $m_{\alpha^i}(t)$ es el polinomio minimal de α^i sobre $\mathbb{F}_2$ con $i = 1, 3$. Su conjunto de definición es $T = C_1 \cup C_3$ donde C_i es la coclase 2-ciclotómica módulo $n = 2^m - 1$ con $i = 1, 3$.

Códigos de Melas

Por último definiremos el código de Melas.

Definición 1.3.14. Sea α un elemento primitivo de $\mathbb{F}_{q^m}$, el código de Melas q-ario $M_n(q)$ de longitud $n = q^m - 1$ es el código cíclico cuyo polinomio generador es de la forma

$$g(t) = m_\alpha(t) m_{\alpha^{-1}}(t)$$

donde $m_{\alpha^i}(t)$ es el polinomio minimal de α^i para $i = \pm 1$ sobre $\mathbb{F}_q$.

Nota. Por el teorema de Delsarte, el dual del código de Melas es el código traza

$$M_n(q)^\perp = \{(\mathrm{Tr}(ax + bx^{-1}))_{x \in \mathbb{F}_{q^m}^*} : \ a, b \in \mathbb{F}_{q^m}\}$$

llamado código de Kloosterman, ya que para calcular los pesos de sus palabras aparecen sumas de Kloosterman. Esto fue probado por Lachaud y Woolfmann independientemente en 1987 y 1989 ([30], [47], [48]). En los años subsiguientes, Schoof y Van der Vlugt se dieron cuenta que existe una relación entre las ecuaciones que aparecen en la identidad de MacWilliams y la traza de operadores de Hecke de ciertas formas modulares. Así pudieron obtener las distribuciones de pesos del código de Melas binario ([42]).

Capítulo 2

Sumas exponenciales y formas cuadráticas

En este capítulo veremos los preliminares algebraicos que nos harán falta para el resto de la tesis. Empezaremos viendo una breve introducción a sumas exponenciales, haciendo hincapié en sumas de caracteres de un cuerpo finito. Luego, veremos formas cuadráticas sobre cuerpos finitos, sus principales propiedades y caracterización. Pero sobre todo, haremos énfasis en la evaluación de sumas exponenciales relacionadas con estas formas cuadráticas, pues estas son necesarias para el cálculo de las distribuciones de pesos de los códigos que aparecerán en el próximo capítulo.

2.1. Sumas exponenciales

En esta sección asumiremos que q es una potencia de un número primo p, digamos $q = p^s$. Todos los resultados de esta sección pueden ser encontrados en [3] (ver también [21] y [36])

Traza y caracteres

Para $\gamma \in \mathbb{F}_{q^m}$, recordemos que la función traza $\mathrm{Tr}_{q^m/q}$ se define como

$$\mathrm{Tr}_{q^m/q}(\gamma) = \sum_{j=0}^{m-1} \gamma^{q^j}.$$

Proposición 2.1.1. *La función $\mathrm{Tr}_{q^m/q}$ es una función $\mathbb{F}_q$-lineal de $\mathbb{F}_{q^m}$ a $\mathbb{F}_q$ sobreyectiva, invariante por el automorfismo de Frobenius, es decir*

$$\mathrm{Tr}_{q^m/q}(\gamma^q) = \mathrm{Tr}_{q^m/q}(\gamma)$$

con $\gamma \in \mathbb{F}_{q^m}$.

A la función traza de q a p la denotaremos simplemente por Tr, es decir $\mathrm{Tr}(\gamma) = \mathrm{Tr}_{q/p}(\gamma)$ para $\gamma \in \mathbb{F}_q$. Además, usaremos las notaciones $\zeta_p = e^{\frac{2\pi i}{p}}$ y $e(\gamma) = \zeta_p^{\mathrm{Tr}(\gamma)}$, es decir

$$e(\gamma) = e^{\frac{2\pi i}{p}\mathrm{Tr}(\gamma)}.$$

Las propiedades de esta función se resumen en la siguiente proposición.

Proposición 2.1.2. *Sean $\gamma_1, \gamma_2 \in \mathbb{F}_q$. Entonces*

- $e(\gamma_1 + \gamma_2) = e(\gamma_1)e(\gamma_2)$.
- *Existe $\gamma \in \mathbb{F}_q$ tal que $e(\gamma) \neq 1$.*
- *Se tiene $\sum_{\gamma \in \mathbb{F}_q} e(\gamma) = 0$.*

Un carácter multiplicativo χ de $\mathbb{F}_q$ es un morfismo de grupos de $\mathbb{F}_q^*$ a $\mathbb{C}^*$, es decir un mapeo $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ tal que

$$\chi(\gamma_1\gamma_2) = \chi(\gamma_1)\chi(\gamma_2),$$

para todo $\gamma_1, \gamma_2 \in \mathbb{F}_q^*$. Se puede ver que la imagen de un carácter siempre está contenida en $\mathbb{S}^1$; más aún, en este caso, la imagen de $\mathbb{F}_q^*$ vía χ está contenida en las raíces $(q-1)$-ésimas de la unidad.

El carácter trivial, usualmente denotado χ_0, es el carácter que satisface $\chi_0(\gamma) = 1$ para todo $\gamma \in \mathbb{F}_q^*$. Es conveniente extender el dominio de definición de un carácter χ de $\mathbb{F}_q^*$ a $\mathbb{F}_q$, haciendo valer $\chi(0) = 1$ si $\chi = \chi_0$, y $\chi(0) = 0$ si χ no es el carácter trivial. Con esta convención tenemos

$$\sum_{a \in \mathbb{F}_q} \chi(a) = \begin{cases} q & \text{si } \chi \text{ es trivial,} \\ 0 & \text{si } \chi \text{ no es trivial.} \end{cases} \tag{2.1}$$

Si denotamos por $\chi_\lambda(\gamma) = e(\lambda\gamma) = \zeta_p^{\mathrm{Tr}(\lambda\gamma)}$, donde $\lambda \in \mathbb{F}_q$. Esta propiedad se puede usar combinatoricamente para contar la cantidad de ceros de funciones $F : \mathbb{F}_{q^m}^* \to \mathbb{F}_q$, más precisamente tenemos

$$q \cdot |\{x \in \mathbb{F}_{q^m}^* : F(x) = 0\}| = \sum_{x \in \mathbb{F}_{q^m}^*} \sum_{a \in \mathbb{F}_q} \chi_{F(x)}(a) = \sum_{x \in \mathbb{F}_{q^m}^*} \sum_{a \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(aF(x))}. \tag{2.2}$$

Nota. Otros autores, por ejemplo Mullen-Panario en [36], suelen suponer que $\chi(0) = 0$ inclusive cuando $\chi = \chi_0$, lo que modifica varias sumas o fórmulas donde influyan caracteres triviales, como la suma anterior por ejemplo.

Sumas de Gauss

Existen varias familias conocidas de sumas exponenciales. Aquí introduciremos las sumas de Gauss, porque éstas aparecen naturalmente en el estudio de códigos cíclicos.

Definición 2.1.3. Dado χ un carácter de $\mathbb{F}_q$ con $q = p^s$ y $\beta \in \mathbb{F}_q$, se define la suma de Gauss por

$$G_s(\beta, \chi) = \sum_{x \in \mathbb{F}_q} \chi(x) e(\beta x).$$

En particular, denotamos $G_s(\chi) = G_s(1, \chi)$, es decir $G_s(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x) e(x)$.

No es muy difícil ver que

$$G_s(\beta, \chi) = \chi(\beta^{-1}) G_s(\chi).$$

Estas sumas de Gauss fueron introducidas por Dirichlet en el estudio de números primos en progresiones aritméticas. En realidad, Gauss estudió otra clases de sumas exponenciales, hoy llamadas k-ésimas sumas de Gauss ó sumas de Gauss de segundo tipo, definidas como sigue.

Definición 2.1.4. Sea $\beta \in \mathbb{F}_q$ con $q = p^s$ y $k \in \mathbb{Z}$.

$$g_s(\beta, k) = \sum_{x \in \mathbb{F}_q} e(\beta x^k) = \sum_{x \in \mathbb{F}_q} e^{\frac{2\pi i}{p} \mathrm{Tr}_{q/p}(\beta x^k)} = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}(\beta x^k)}.$$

Los dos tipos de sumas de Gauss están relacionadas por la siguiente identidad

$$g_s(\beta, k) = \sum_{j=1}^{k-1} G_s(\beta, \chi^j)$$

donde χ es un carácter de orden k sobre $\mathbb{F}_q$ con $q = p^s$ y $\beta \in \mathbb{F}_q^*$. Esta igualdad permite usar las sumas de Gauss de primer tipo para estudiar el espectro de códigos cíclicos irreducibles.

Las sumas de Gauss de segundo tipo aparecen naturalmente cuando queremos calcular la distribución de pesos de códigos irreducibles, pero no se conocen fórmulas generales para este tipo de sumas, salvo en el caso cuadrático (como veremos a continuación).

Teorema 2.1.5 ([21])**.** *Sea q una potencia de un primo impar p y $\beta \in \mathbb{F}_q$. Entonces*

$$g_2(\beta, \chi) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(\beta x^2)} = \begin{cases} \eta(\beta)\sqrt{q} & \text{si } q \equiv 1 \pmod 4, \\ i\eta(\beta)\sqrt{q} & \text{si } q \equiv 3 \pmod 4, \end{cases} \tag{2.3}$$

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

Recordemos que el carácter cuadrático de $\mathbb{F}_q$ se define como el único carácter multiplicativo η de $\mathbb{F}_q$ de orden 2, es decir

$$\eta(x)^2 = 1 \qquad \text{para todo } x \in \mathbb{F}_q^*.$$

Se puede ver de manera sencilla, que $\eta(x) = 1$ si x es el cuadrado de algún elemento de $\mathbb{F}_q^*$ y $\eta(x) = -1$ en caso contrario. En particular, si $q = p$ es un primo impar, entonces

$$\eta(x) = \left(\frac{x}{p}\right)$$

es el símbolo de Legendre módulo p.

Sumas de Jacobi

Otra clase de sumas que suelen aparecer en el contexto de calcular distribuciones de pesos, son las llamadas sumas de Jacobi, ya que estas son útiles para calcular la cantidad de soluciones de ecuaciones diagonales. Dichas ecuaciones son clave para calcular los ceros de ecuaciones donde intervienen formas cuadráticas ya que por ejemplo, en característica impar, toda forma cuadrática se puede "diagonalizar" como veremos en la próxima sección. Las sumas de Jacobi también permiten calcular una clase especial de números, llamados números ciclotómicos, que aparecen en el estudio de distribuciones de cierta clase de códigos cíclicos que no veremos en esta tesis.

Definición 2.1.6. Sean χ, ψ caracteres multiplicativos de $\mathbb{F}_q$, donde $q = p^s$. La *suma de Jacobi* $J_r(\chi, \psi)$ está definida por

$$J_s(\chi, \psi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(1-x). \tag{2.4}$$

Cuando el s esté sobreentendido o no importe en la discusión, quitaremos el subíndice s de la notación.

El *orden* m de la suma $J_s(\chi, \psi)$ se define como el mínimo común múltiplo de los órdenes de los caracteres χ y ψ. Luego, la suma de Jacobi $J_s(\psi, \chi)$ es un entero dentro del cuerpo ciclotómico $\mathbb{Q}(\zeta_m)$, donde $\zeta_m = e^{\frac{2\pi i}{m}}$.

Las sumas de Jacobi son simétricas. En efecto, como la asignación $x \mapsto 1 - x$ es una biyección sobre $\mathbb{F}_q$, se tiene

$$J(\chi, \psi) = J(\psi, \chi).$$

Además, las sumas de Jacobi cumplen las siguientes propiedades, en su mayoría consecuencia de las propiedades de los caracteres multiplicativos del cuerpo $\mathbb{F}_q$.

Proposición 2.1.7. *Sean χ, ψ caracteres multiplicativos de $\mathbb{F}_q$. Luego,*

- *si χ y ψ son ambos triviales, entonces $J(\chi, \psi) = q$,*
- *si exactamente uno de los caracteres ψ ó χ es trivial, entonces $J(\chi, \psi) = 0$,*
- *si χ no es trivial, entonces $J(\chi, \bar{\chi}) = -\chi(-1)$, donde $\bar{\chi}(a) = \overline{\chi(a)}$ para todo a.*

Una relación importante entre las sumas de Jacobi y las de Gauss está dada por el siguiente teorema.

Teorema 2.1.8. *Sean χ, ψ caracteres multiplicativos de $\mathbb{F}_q$, $q = p^s$. Si $\chi\psi$ es no trivial, entonces*

$$J_s(\chi, \psi) = \frac{G_s(\chi)G_s(\psi)}{G_s(\chi\psi)}.$$

Una *ecuación diagonal* es una ecuación polinomial del tipo

$$\alpha_1 x_1^{k_1} + \alpha_2 x_2^{k_2} + \cdots + \alpha_r x_r^{k_r} = \xi \tag{2.5}$$

donde $r, k_1, \ldots, k_r$ son enteros positivos, $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{F}_q^*$ y $\xi \in \mathbb{F}_q$.

Llamaremos $N_r(\xi)$ al número de soluciones de la ecuación de arriba, es decir

$$N_r(\xi) = \#\{(\alpha_1, \ldots, \alpha_r) \in (\mathbb{F}_q^*)^r : \alpha_1 x_1^{k_1} + \alpha_2 x_2^{k_2} + \cdots + \alpha_r x_r^{k_r} = \xi\}. \tag{2.6}$$

Las sumas de Jacobi permiten encontrar la cantidad de soluciones a la ecuación (2.5). Para ello, necesitamos definir primero las sumas de Jacobi generalizadas.

Definición 2.1.9. Sean $\chi_1, \chi_2, \ldots, \chi_r$ caracteres multiplicativos de $\mathbb{F}_q$, con $q = p^s$ y $r \geq 2$. La *suma de Jacobi generalizada* está definida por

$$J_s(\chi_1, \ldots, \chi_r) = \sum_{x_1 + x_2 + \cdots + x_r = 1} \chi_1(x_1)\chi_2(x_2)\cdots\chi_r(x_r) \tag{2.7}$$

donde la suma es tomada sobre todas las r-uplas $(\gamma_1, \ldots, \gamma_r) \in \mathbb{F}_q^r$ con $x_1 + \cdots + x_r = 1$.

Notar que cuando $r = 2$, la suma generalizada de Jacobi coincide con la suma de Jacobi.

Estas sumas de Jacobi generalizadas se pueden expresar como sumas de Jacobi simples, por aplicación reiterada del siguiente teorema de reducción.

Teorema 2.1.10. *Sean $\chi_1, \ldots, \chi_r$ caracteres multiplicativos no triviales de $\mathbb{F}_q$ con $r \geq 2$. Entonces,*

$$J(\chi_1, \ldots, \chi_r) = \begin{cases} -qJ(\chi_1, \ldots, \chi_{r-1}) & \text{si } \chi_1\chi_2\cdots\chi_{r-1} \text{ es trivial,} \\ J(\chi_1\cdots\chi_{r-1}, \chi_r)J(\chi_1, \ldots, \chi_{r-1}) & \text{si } \chi_1\chi_2\cdots\chi_{r-1} \text{ no es trivial.} \end{cases}$$

De particular importancia para nosotros será, en cálculos posteriores, la evaluación de la suma generalizada $J(\eta, \ldots, \eta)$, donde η es el carácter cuadrático de $\mathbb{F}_q$, ya que esta aparece en sumas diagonales cuadráticas.

Proposición 2.1.11. *Para $r \geq 2$, tenemos que*

$$J\underbrace{(\eta, \ldots, \eta)}_{r\text{-veces}} = \begin{cases} -\eta\big((-1)^{\frac{r}{2}}\big)\, q^{\frac{r-2}{2}} & \text{si } r \text{ es par,} \\ \eta\big((-1)^{\frac{r-1}{2}}\big)\, q^{\frac{r-1}{2}} & \text{si } r \text{ es impar,} \end{cases}$$

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

Dado r un entero positivo, denotamos por

$$D_{d_1,\ldots,d_r} = \{(j_1, \ldots, j_r) \in \mathbb{Z}^r : 1 \leq j_i \leq d_i - 1 \text{ para } i = 1, \ldots, r\} \tag{2.8}$$

donde $d_i > 1$ son enteros para $i = 1, \ldots, r$.

Teorema 2.1.12. *Sean $k_1, \dots, k_r$ enteros positivos, $\alpha_1, \dots, \alpha_r \in \mathbb{F}_q^*$ y $\alpha \in \mathbb{F}_q$. Para cada $1 \le i \le r$, sea $d_i = (k_i, q-1)$ y χ_i carácter multiplicativo de $\mathbb{F}_q$ de orden d_i. Si $D = D_{d_1,\dots,d_r}$ es como en (2.8), entonces el número $N_r(\xi)$ de soluciones de la ecuación (2.5) está dado por*

$$N_r(\xi) = \begin{cases} q^{r-1} + \sum\limits_{(j_1,\dots,j_r)\in D} \big(\prod\limits_{i=1}^{r} \chi_i^{j_i}(\xi\alpha_i^{-1}) \big)\, J(\chi_1^{j_1}, \dots, \chi_r^{j_r}) & \text{si } \xi \neq 0, \\ q^{r-1} + (q-1) \sum\limits_{(j_1,\dots j_r)\in D^0} \big(\prod\limits_{i=1}^{r} \chi_i^{j_i}(\alpha_i^{-1}) \big)\, J(\chi_1^{j_1}, \dots, \chi_r^{j_r}) & \text{si } \xi = 0, \end{cases}$$

donde $D^0 = \{(j_1, \dots, j_r) \in D : \chi_1^{j_1} \cdots \chi_r^{j_r} = \chi_0\}$.

Nos interesarán particularmente las ecuaciones diagonales como en (2.5) en las que todos los $k_i = 2$, ya que más adelante estudiaremos la cantidad de soluciones a ecuaciones que involucran formas cuadráticas y que resultarán ser ecuaciones diagonales en característica impar.

Como consecuencia del teorema y la proposición anteriores, en el caso q impar se tiene lo siguiente.

Corolario 2.1.13. *Sea q impar. El número N de soluciones de la ecuación*

$$\alpha_1 x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_r x_r^2 = \xi,$$

donde $\alpha_1, \dots, \alpha_r \in \mathbb{F}_q^*$ y $\xi \in \mathbb{F}_q$, está dado por las siguientes expresiones:

- *Si $\xi \neq 0$, entonces*

$$N = \begin{cases} q^{r-1} - \eta\big((-1)^{\frac{r}{2}}\alpha_1 \cdots \alpha_r\big)\, q^{\frac{r-2}{2}} & \text{si } r \text{ es par}, \\ q^{r-1} + \eta\big((-1)^{\frac{r-1}{2}}\xi\alpha_1 \cdots \alpha_r\big)\, q^{\frac{r-1}{2}} & \text{si } r \text{ es impar}. \end{cases}$$

- *Si $\xi = 0$, entonces*

$$N = \begin{cases} q^{r-1} + \eta\big((-1)^{\frac{r}{2}}\alpha_1 \cdots \alpha_r\big)\big(q^{\frac{r}{2}} - q^{\frac{r-2}{2}}\big) & \text{si } r \text{ es par}, \\ q^{r-1} & \text{si } r \text{ es impar}. \end{cases}$$

2.2. Formas cuadráticas sobre cuerpos finitos

Comenzamos recordando la definición clásica de forma cuadrática sobre cuerpos finitos.

Definición 2.2.1. Una *forma cuadrática* en m variables sobre $\mathbb{F}_q$ es un polinomio homogéneo de grado 2 en m variables con coeficientes en $\mathbb{F}_q$.

Fijada una $\mathbb{F}_q$-base $\mathcal{B}$ de $\mathbb{F}_{q^m}$, como el grado de la extensión de $\mathbb{F}_{q^m}/\mathbb{F}_q$ es m, entonces el vector de coordenadas con respecto a la base $\mathcal{B}$ nos da un isomorfismo de $\mathbb{F}_q$-espacios vectoriales entre $\mathbb{F}_{q^m}$ y $\mathbb{F}_q^m$. Vía este isomorfismo, algunas funciones $Q : \mathbb{F}_{q^m} \to \mathbb{F}_q$ pueden ser identificadas con polinomios de m variables con coeficientes en $\mathbb{F}_q$.

Ejemplo 2.2.2. Sea $q = p^m$ con p primo y consideremos $Q(x) = \mathrm{Tr}_{q/p}(\gamma x^2)$ con $\gamma, x \in \mathbb{F}_q$. Fijemos $\mathcal{B} = \{v_1, \ldots, v_m\}$ una $\mathbb{F}_p$-base de $\mathbb{F}_q$.

Escribamos $x = a_1v_1 + \cdots + a_mv_m$ con $a_i \in \mathbb{F}_p$, luego

$$\begin{aligned} Q(a_1v_1 + \cdots + a_mv_m) &= \sum_{i=1}^{m} \mathrm{Tr}_{q/p}\big(\gamma(a_iv_i)^2\big) + \sum_{i\neq j} \mathrm{Tr}_{q/p}\big(\gamma(2a_ia_jv_iv_j)\big) \\ &= \sum_{i=1}^{m} \mathrm{Tr}_{q/p}\big(\gamma(v_i)^2\big)a_i^2 + \sum_{i\neq j} 2\mathrm{Tr}_{q/p}(\gamma v_iv_j)a_ia_j. \end{aligned}$$

Sean $c_i = \mathrm{Tr}_{q/p}(\gamma(v_i)^2)$ y $c_{i,j} = 2\mathrm{Tr}_{q/p}(\gamma v_iv_j)$. El polinomio que representa a $Q(x)$ es el polinomio homogéneo en m variables

$$q(x_1, \ldots, x_m) = \sum_{i=1}^{m} c_ix_i^2 + \sum_{i\neq j} c_{i,j}x_ix_j$$

ya que $q(a_1, \ldots, a_m) = Q(a_1v_1 + \cdots + a_mv_m)$. Notar que en este caso el polinomio que representa a la función es una forma cuadrática. Notar que en característica par, los $c_{i,j} = 0$ para todo $i \neq j$ y por lo tanto $q(x_1, \ldots, x_m)$ es suma de cuadrados. $\lozenge$

Ahora generalizamos un poco la noción de forma cuadrática sobre cuerpos finitos.

Definición 2.2.3. Una función $Q : \mathbb{F}_{q^m} \to \mathbb{F}_q$ se dice *forma cuadrática*, si vía la identificación anterior el polinomio que le corresponde es una forma cuadrática, es decir un polinomio homogéneo de grado 2.

Una manera de probar que una función $Q : \mathbb{F}_{q^m} \to \mathbb{F}_q$ es una forma cuadrática, es considerando la función asociada

$$B(x, y) = Q(x + y) - Q(x) - Q(y) \tag{2.9}$$

ya que en general resulta que

$$Q \text{ es una forma cuadrática} \Leftrightarrow B \text{ es una forma bilineal simétrica}$$

(o sea $B(y, x) = B(x, y)$).

Ejemplo 2.2.4. Sea q cualquier potencia de un primo y consideremos

$$Q(x) = \mathrm{Tr}_{q^m/q}(xR(x)) \tag{2.10}$$

donde $R(x) \in \mathbb{F}_q[x]$ es un polinomio *q-linealizado*, es decir un polinomio de la forma

$$R(x) = \sum_{i=1}^{h} a_i x^{q^{\ell_i}}. \tag{2.11}$$

Notar que R satisface $R(x+y) = R(x) + R(y)$, ya que elevar a la q es un automorfismo de cuerpos en $\mathbb{F}_{q^m}$.

Se puede probar que $Q(x)$ es una forma cuadrática considerando la función asociada $B(x,y)$ como en (2.9). Como $Q(x+y) = Q(x) + Q(y) + \mathrm{Tr}(xR(y)) + \mathrm{Tr}(yR(x))$, tenemos

$$B(x,y) = \mathrm{Tr}_{q^m/q}(xR(y) + yR(x)).$$

Luego,

$$\begin{aligned} B(x+x',y) &= \mathrm{Tr}_{q^m/q}((x+x')R(y) + yR(x+x')) \\ &= \mathrm{Tr}_{q^m/q}(xR(y) + x'R(y) + yR(x) + yR(x')) \\ &= \mathrm{Tr}_{q^m/q}((xR(y) + yR(x)) + (x'R(y) + yR(x'))) \\ &= B(x,y) + B(x',y). \end{aligned}$$

De la misma manera se ve que $B(x, y+y') = B(x,y) + B(x,y')$ y por lo tanto B es bilineal. Además, es claro que $B(y,x) = B(x,y)$. Luego, B es una forma simétrica y por lo tanto $Q(x) = \mathrm{Tr}_{q^m/q}(xR(x))$ es una forma cuadrática. $\Diamond$

Notar que si consideramos dos formas cuadráticas distintas y tomamos dos bases distintas de $\mathbb{F}_{q^m}$, puede suceder que el polinomio que las representa en las bases correspondientes sea el mismo. Por lo tanto, en esencia, son la misma forma cuadrática. En tal caso, la transformación de cambio de base en $\mathbb{F}_{q^m}$ nos permite dar una noción de equivalencia de formas cuadráticas.

Definición 2.2.5. Dos formas cuadráticas Q_1 y Q_2 en m variables sobre $\mathbb{F}_q$ se dicen *equivalentes* si existe un isomorfismo $\mathbb{F}_q$-lineal $S : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, tal que

$$Q_1(x) = Q_2(S(x)).$$

Teniendo en cuenta la última definición, nos interesa saber si hay maneras de decidir cuándo dos formas cuadráticas son equivalentes. Veremos que existen dos invariantes muy importantes, que en algunos casos resultan ser invariantes absolutos, ellos son el *rango* y el *tipo*. Empecemos definiendo el rango de una forma cuadrática.

Definición 2.2.6. Sea Q una forma cuadrática en m variables sobre $\mathbb{F}_q$. El *rango* de Q se define como la mínima cantidad de variables r por la cual Q se puede representar como un polinomio en r variables.

Obviamente $r \leq m$. La siguiente proposición nos da una manera de calcular el rango de una forma cuadrática.

Proposición 2.2.7. *Sea Q una forma cuadrática en m variables sobre $\mathbb{F}_q$. Entonces, el rango de Q es la codimensión del $\mathbb{F}_q$-espacio vectorial*

$$V = \{y \in \mathbb{F}_{q^m} : Q(y) = 0, \quad Q(x+y) = Q(x), \quad \forall x \in \mathbb{F}_{q^m}\}. \tag{2.12}$$

Esto es $|V| = q^{m-r}$, donde r es el rango de Q.

Dada una forma cuadrática Q en m variables sobre $\mathbb{F}_q$, consideremos otra vez la función $B(x,y) = Q(x+y) - Q(x) - Q(y)$. El *radical* de B es el espacio

$$W = W_B = \{y \in \mathbb{F}_{q^m} : B(x,y) = 0, \forall x \in \mathbb{F}_{q^m}\}. \tag{2.13}$$

Claramente $V \subseteq W$. Recordemos que V nos permite calcular el rango de una forma cuadrática vía su codimensión. En algunos casos, la contención anterior es una igualdad y, por lo tanto, podemos usar a W para calcular el rango de una forma cuadrática.

Lema 2.2.8. *Sea Q una forma cuadrática en m variables de rango r sobre $\mathbb{F}_q$ con q impar, y sean V, W como en* (2.12), (2.13) *respectivamente. Entonces, $V = W$ y $r = m - \dim(V)$.*

Luego, en característica impar es posible usar V y W indistintamente. Esto es útil, ya que a V lo definen dos ecuaciones mientras que a W sólo una. En característica par $V \neq W$ en general; pero, sin embargo, en algunos casos se sigue dando la igualdad.

Lema 2.2.9. *Si q es una potencia de dos y Q es una forma cuadrática en m variables sobre $\mathbb{F}_q$ de rango r, entonces $r \geq m - \dim W$. Más precisamente, si Q tiene rango par entonces $r = m - \dim W$ y si Q tiene rango impar entonces $r = m - \dim W + 1$.*

Notar que $m - \dim W$ es siempre par.

Definición 2.2.10. Sea Q una forma cuadrática de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Para $\beta \in \mathbb{F}_{q^m}$y $\xi \in \mathbb{F}_q$ definimos por $N_{Q,\beta}(\xi)$ a la cantidad de soluciones $x \in \mathbb{F}_{q^m}$ de la ecuación

$$Q(x) + \mathrm{Tr}_{q^m/q}(\beta x) = \xi. \tag{2.14}$$

Es decir,

$$N_{Q,\beta}(\xi) = \#\{x \in \mathbb{F}_{q^m} : Q(x) + \mathrm{Tr}_{q^m/q}(\beta x) = \xi\}. \tag{2.15}$$

En particular, usaremos la notación

$$N_Q(\xi) := N_{Q,0}(\xi) = \#\{x \in \mathbb{F}_{q^m} : Q(x) = \xi\}. \tag{2.16}$$

Notar que si Q es de rango r, entonces $N_Q(\xi)$ coincide con $N_r(\xi)$ definido en (2.6).

Las formas cuadráticas sobre cuerpos finitos han sido muy estudiadas. En particular, se las ha clasificado en tres clases no equivalentes. Para ver ésto definamos la forma cuadrática

$$B_{2j}(x) = B_{2j}(x_1, \ldots, x_m) = x_1x_2 + x_3x_4 + \cdots + x_{2j-1}x_{2j}$$

donde j es un entero no negativo y asumimos que B_0=0. Sea $\nu(z)$ la función definida sobre $\mathbb{F}_q$ por

$$\nu(z) = \begin{cases} q-1 & \text{si } z = 0, \\ -1 & \text{si } z \neq 0. \end{cases} \tag{2.17}$$

Teorema 2.2.11. *Sea $q = 2^s$ con $s \in \mathbb{N}$. Toda forma cuadrática $Q(x)$ en m variables sobre $\mathbb{F}_q$ de rango r es equivalente a una de los siguientes tres tipos:*

- *Tipo I: $B_r(x)$, con r par.*
- *Tipo II: $B_{r-1}(x) + x_r^2$, con r impar.*
- *Tipo III: $B_{r-2}(x) + \theta x_{r-1}^2 + x_{r-1}x_r + \theta x_r^2$, con r par y $\theta \in \mathbb{F}_q$ tal que $\mathrm{Tr}_s(\theta) = 1$.*

Además, para cualquier $\xi \in \mathbb{F}_q$, se tiene:

- *Tipo I: $N_Q(\xi) = q^{m-1} + \nu(\xi)q^{m-\frac{r}{2}-1}$.*
- *Tipo II: $N_Q(\xi) = q^{m-1}$.*
- *Tipo III: $N_Q(\xi) = q^{m-1} - \nu(\xi)q^{m-\frac{r}{2}-1}$.*

Teorema 2.2.12. *Sea $q = p^s$ con p primo impar y $s \in \mathbb{N}$. Toda forma cuadrática $Q(x)$ en m variables sobre $\mathbb{F}_q$ de rango r es equivalente a una de los siguientes tres tipos:*

- *Tipo I: $B_r(x)$, con r par.*
- *Tipo II: $B_{r-1}(x) + \mu x_r^2$, con r impar.*
- *Tipo III: $B_{r-2}(x) + x_{r-1}^2 - \rho x_r^2$, con r par y $\mu \in \{1, \rho\}$ con ρ un no cuadrado en $\mathbb{F}_q$.*

Además, para cualquier $\xi \in \mathbb{F}_q$, se tiene:

- *Tipo I: $N_Q(\xi) = q^{m-1} + \nu(\xi)q^{m-\frac{r}{2}-1}$.*
- *Tipo II: $N_Q(\xi) = q^{m-1} + \eta(\mu\xi)q^{m-\frac{r+1}{2}}$.*
- *Tipo III: $N_Q(\xi) = q^{m-1} - \nu(\xi)q^{m-\frac{r}{2}-1}$.*

Aquí, η es el carácter cuadrático multiplicativo de $\mathbb{F}_q$ asumiendo que $\eta(0) = 0$.

Notar que en cualquier característica el tipo de la forma cuadrática de rango par, se hace evidente al analizar la cantidad de soluciones $x \in \mathbb{F}_{q^m}$ a la ecuación $Q(x) = \xi$, pues si Q es de rango par hay una variación de signo en la cantidad de soluciones, por esto definimos

$$\epsilon = \epsilon_Q = \begin{cases} 1 & \text{si } Q \text{ es de tipo I,} \\ -1 & \text{si } Q \text{ es de tipo III.} \end{cases} \tag{2.18}$$

Cuando q es una potencia de un primo impar, el estudio de las formas cuadráticas se simplifica bastante ya que éstas se pueden interpretar de manera matricial, inclusive es posible definir el tipo de una forma cuadrática por cierto invariante matricial como veremos a continuación.

Lema 2.2.13. *Sea Q una forma cuadrática en m variables sobre $\mathbb{F}_q$ con q impar y sea $\mathcal{B}$ una $\mathbb{F}_q$-base de $\mathbb{F}_{q^m}$ fija. Existe una matriz simétrica $H_Q \in M_m(\mathbb{F}_q)$ tal que*

$$XH_QX^t = Q(x)$$

donde X es el vector de coordenadas de $x \in \mathbb{F}_q^m$ en la base $\mathcal{B}$.

En este contexto, el rango de la forma cuadrática Q coincide con el rango de su matriz asociada H_Q. Además, para H_Q existe una matriz $S \in GL_m(\mathbb{F}_q)$ tal que

$$SH_QS^t = \begin{pmatrix} a_1 & & & & & \\ & \ddots & & & & \\ & & a_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}. \tag{2.19}$$

Por lo tanto, en característica impar toda forma cuadrática puede ser dada en forma "diagonal". Es decir, existe una $\mathbb{F}_q$-base de $\mathbb{F}_{q^m}$ tal que la forma cuadrática es representada por un polinomio de la forma

$$q(x_1, x_2, \ldots, x_m) = a_1x_1^2 + \cdots + a_rx_r^2$$

donde r es el rango de la forma cuadrática. Puede suceder que distintas bases diagonalicen una misma forma cuadrática. En tal caso, su expresión diagonal no es única; sin embargo, el valor

$$\Delta = a_1a_2 \cdots a_r \tag{2.20}$$

es invariante por equivalencia diagonal y es llamado el *determinante* de la forma cuadrática.

Cuando q es impar, dos formas cuadráticas Q_1, Q_2 son *equivalentes* si sus matrices correspondientes H_{Q_1}, H_{Q_2} son conjugadas por una matriz inversible.

Definición 2.2.14. Sea q una potencia de un primo impar, y Q una forma cuadrática en m variables sobre $\mathbb{F}_q$. El *tipo* de la forma cuadrática Q se define como $\epsilon_Q = \eta((-1)^{\frac{r}{2}}\Delta)$ donde Δ es el determinante de Q y η es el carácter cuadrático multiplicativo de $\mathbb{F}_q$.

En algunos casos, el tipo permite identificar cúando dos formas cuadráticas son equivalentes.

Lema 2.2.15. *Sean Q_1, Q_2 dos formas cuadráticas en m variables sobre $\mathbb{F}_q$ de igual rango par. Entonces Q_1 y Q_2 son equivalentes si y sólo si $\epsilon_{Q_1} = \epsilon_{Q_2}$.*

Por lo tanto, el rango y el tipo son invariantes absolutos en las formas cuadráticas de rango par en característica impar. Más precisamente, nos permite determinar cuándo una forma de rango par es de tipo I o de tipo III.

Se ha probado hace unos años, que en algunos casos el tipo de una forma cuadrática sólo depende de su rango ([12]).

2.3. Formas cuadráticas y sumas exponenciales

Sea $q = p^s$, con p primo. Recordemos que una forma cuadrática en m variables sobre $\mathbb{F}_q$, es una función de $\mathbb{F}_{q^m}$ a $\mathbb{F}_q$ que, vía el isomorfismo de $\mathbb{F}_q$-espacios vectoriales $\mathbb{F}_{q^m} \simeq \mathbb{F}_q^m$, es un polinomio homogéneo de grado 2 en m variables sobre $\mathbb{F}_q$.

Para $a \in \mathbb{F}_q^*$ y Q una forma cuadrática en m variables sobre $\mathbb{F}_q$ definimos la suma

$$T_{Q,a} = \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(aQ(x))} \tag{2.21}$$

donde $\zeta_p = e^{\frac{2\pi i}{p}}$, como antes. Si $a = 1$, usaremos la notación

$$T_Q = T_{Q,1} = \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(Q(x))}. \tag{2.22}$$

Estas sumas pueden ser calculadas explícitamente en términos del rango y el tipo de Q.

Lema 2.3.1. *Sean Q una forma cuadrática en m variables sobre $\mathbb{F}_q$ de rango r y T_Q como en (2.22). Entonces $|T_Q| = q^{m-\frac{r}{2}}$ ó 0. Mas aún, tenemos:*

(I) Si r es par (con q arbitrario) y $T_Q \neq 0$, entonces para todo $a \in \mathbb{F}_q^*$ se tiene

$$T_{Q,a} = \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(aQ(x))} = \epsilon q^{m-\frac{r}{2}}.$$

(II) Si q es impar (con r arbitrario), entonces

$$T_Q = \begin{cases} \eta(\Delta)\, q^{m-\frac{r}{2}} & \text{si } q \equiv 1 \pmod 4, \\ i^r \eta(\Delta)\, q^{m-\frac{r}{2}} & \text{si } q \equiv 3 \pmod 4. \end{cases}$$

Observación 2.3.2. Sea Q una forma cuadrática de rango r par sobre $\mathbb{F}_q$ con q impar. Luego, el tipo de Q queda en términos del rango y el determinante de Q. En efecto, tomando $a = 1$ en el lema anterior, como las expresiones en (I) y (II) deben coincidir, se tiene que

$$\epsilon_Q = \begin{cases} \eta(\Delta) & \text{si } q \equiv 1 \bmod 4, \\ (-1)^{\frac{r}{2}} \eta(\Delta) & \text{si } q \equiv 3 \bmod 4. \end{cases} \tag{2.23}$$

Cuando consideramos familias de formas cuadráticas de rango par, se puede obtener mayor información a partir de las ecuaciones (2.14). Esto va a ser clave para calcular ciertas sumas exponenciales dobles que aparecen naturalmente en el cálculo de pesos de palabras de ciertos código cíclicos definidos a partir de formas cuadráticas, como veremos en el próximo capítulo.

Lema 2.3.3 ([27], [28]). *Sea Q una forma cuadrática en m variables de rango r par sobre $\mathbb{F}_q$. Entonces, para cada $\xi \in \mathbb{F}_q$, hay una cantidad $q^m - q^r$ de elementos $\beta \in \mathbb{F}_{q^m}$ tales que*

$$N_{Q,\beta}(\xi) = q^{m-1}$$

y una cantidad $q^{r-1} + \epsilon\nu(c)q^{\frac{r}{2}-1}$ de elementos $\beta \in \mathbb{F}_{q^m}$ tales que

$$N_{Q,\beta}(\xi) = q^{m-1} + \epsilon\nu(\xi + c)q^{m-\frac{r}{2}-1}$$

donde ν es como en (2.17) *y $N_{Q,\beta}(\xi)$ como en* (2.15).

Definición 2.3.4. Para Q una forma cuadrática en m variables sobre $\mathbb{F}_q$, $\beta \in \mathbb{F}_{q^m}$ y $b \in \mathbb{F}_q$, definimos las sumas exponenciales

$$S_{Q,b}(\beta) = \sum_{a\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}\left(a(Q(x)+\mathrm{Tr}_{q^m/q}(\beta x)+b)\right)}. \tag{2.24}$$

Cuando $b = 0$, denotamos por $S_Q(\beta)$ a $S_{Q,0}(\beta)$, es decir

$$S_Q(\beta) = \sum_{a\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}\left(a(Q(x)+\mathrm{Tr}_{q^m/q}(\beta x))\right)}. \tag{2.25}$$

Notar que si $\beta = 0$ tenemos

$$S_{Q,b}(0) = \sum_{a\in\mathbb{F}_q^*} \zeta_p^{\mathrm{Tr}_{q/p}(b)} \Big(\sum_{x\in\mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(a(Q(x))} \Big) = \zeta_p^{k_b} \sum_{a\in\mathbb{F}_q^*} T_{Q,a}$$

donde $k_b = \zeta_p^{\mathrm{Tr}_{q/p}(b)}$. Luego, estas sumas pueden ser calculadas por medio del Lema 2.3.1.

A continuación calculamos las sumas $S_{Q,b}(\beta)$ y sus distribuciones, las cuales también quedan en términos del rango y el tipo de Q.

Proposición 2.3.5. *Sea Q una forma cuadrática sobre $\mathbb{F}_q$ de rango r par y $\beta \in \mathbb{F}_{q^m}$. Los valores de $S_Q(\beta)$ tienen la siguiente distribución*

$$S_Q(\beta) = \begin{cases} 0 & q^m - q^r \text{ veces}, \\ \epsilon(q-1)q^{m-\frac{r}{2}} & q^{r-1} + \epsilon(q-1)q^{\frac{r}{2}-1} \text{ veces}, \\ -\epsilon q^{m-\frac{r}{2}} & (q^{r-1} - \epsilon q^{\frac{r}{2}-1})(q-1) \text{ veces}, \end{cases} \tag{2.26}$$

mientras que si $b \in \mathbb{F}_q^*$, los valores de $S_{Q,b}(\beta)$ tienen la siguiente distribución

$$S_{Q,b}(\beta) = \begin{cases} 0 & q^m - q^r \text{ veces}, \\ \epsilon(q-1)q^{m-\frac{r}{2}} & q^{r-1} - \epsilon q^{\frac{r}{2}-1} \text{ veces}, \\ -\epsilon q^{m-\frac{r}{2}} & q^r - q^{r-1} + \epsilon q^{\frac{r}{2}-1} \text{ veces}. \end{cases} \tag{2.27}$$

Demostración. De (2.25), restando la contribución del 0, tenemos

$$S_Q(\beta) = \sum_{x\in\mathbb{F}_{q^m}} \sum_{a\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}\left\{a\left(Q(x)+\mathrm{Tr}_{q^m/q}(\beta x)\right)\right\}} - q^m.$$

Teniendo en cuenta los valores que puede tomar $Q(x) + \mathrm{Tr}_{q^m/q}(\beta x)$, y distinguiendo los casos en que vale 0 o no, tenemos

$$S_Q(\beta) = qN_{Q,\beta}(0) + \sum_{\xi\in\mathbb{F}_q} N_{Q,\beta}(\xi) \sum_{a\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}(a\xi)} - q^m.$$

Usando que los caracteres de $\mathbb{F}_q$ son todos de la forma $\chi_\gamma(x) = \zeta_p^{\mathrm{Tr}_{q/p}(a\gamma)}$ con $\gamma \in \mathbb{F}_q$, y que por la Proposición 2.1.2 la suma de caracteres se anula, llegamos a que

$$S_Q(\beta) = qN_{Q,\beta}(0) - q^m. \tag{2.28}$$

Por el lema anterior $N_{Q,\beta}(0) = q^{m-1}$ para un número $q^m - q^r$ de β's posibles y además

$$N_{Q,\beta}(0) = q^{m-1} + \epsilon\nu(c)q^{m-\frac{r}{2}-1} \tag{2.29}$$

para un número $q^{r-1} + \epsilon\nu(c)q^{\frac{r}{2}-1}$ de β's posibles.

Como $\nu(c) = q - 1$ si $c = 0$ y $\nu(c) = -1$ si $c \in \mathbb{F}_q^*$, hay $q - 1$ elecciones de c tal que $\nu(c) = -1$. Por lo tanto, (2.29) queda

- $N_{Q,\beta}(0) = q^{m-1} + \epsilon(q-1)q^{m-\frac{r}{2}-1}$ para un número $q^{r-1} + \epsilon(q-1)q^{\frac{r}{2}-1}$ de β's,
- $N_{Q,\beta}(0) = q^{m-1} - \epsilon q^{m-\frac{r}{2}-1}$ para un número $(q^{r-1} - \epsilon q^{\frac{r}{2}-1})(q-1)$ de β's,

donde ϵ es como en (2.18). Por todo lo visto, de (2.28) llegamos a que

$$S_Q(\beta) = \begin{cases} 0 & q^m - q^r \text{ veces,} \\ \epsilon(q-1)q^{m-\frac{r}{2}} & q^{r-1} + \epsilon(q-1)q^{\frac{r}{2}-1} \text{ veces,} \\ -\epsilon q^{m-\frac{r}{2}} & (q^{r-1} - \epsilon q^{\frac{r}{2}-1})(q-1) \text{veces.} \end{cases}$$

De manera análoga al caso anterior, si $b \neq 0$ entonces tenemos

$$S_{Q,b}(\beta) = qN_{Q,\beta}(-b) - q^m,$$

y analizando casos de igual manera que antes, se obtiene

$$S_{Q,b}(\beta) = \begin{cases} 0 & q^m - q^r \text{ veces,} \\ \epsilon(q-1)q^{m-\frac{r}{2}} & q^{r-1} - \epsilon q^{\frac{r}{2}-1} \text{ veces,} \\ -\epsilon q^{m-\frac{r}{2}} & q^r - q^{r-1} + \epsilon q^{\frac{r}{2}-1} \text{ veces,} \end{cases}$$

como queríamos mostrar. □

O sea que $S_{Q,b}(\beta)$ y $S_Q(\beta)$ toman exactamente los mismos valores, pero con distintas distribuciones.

Observación 2.3.6. Notar que, por definición, las sumas $T_{Q,a}$ y $S_{Q,b}(\beta)$ están en $\mathbb{Q}(\zeta_p)$. El Lema 2.3.1 y la Proposición 2.3.5 aseguran que, si el rango r de Q es par, en realidad $T_{Q,a}$ y $S_{Q,b}(\beta)$ están en $q^{m-\frac{r}{2}}\mathbb{Z}$.

2.4. La forma cuadrática $Q_{\lambda,\ell}$

Sean $\ell \in \mathbb{N}$ y $\lambda \in \mathbb{F}_{q^m}$ y consideremos la función $Q_{\lambda,\ell} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ definida por

$$Q_{\lambda,\ell}(x) = \mathrm{Tr}_{q^m/q}(\lambda x^{q^\ell+1}) = \mathrm{Tr}_{q^m/q}(xR_\lambda(x)) \tag{2.30}$$

donde $R_\lambda(x) = \lambda x^{q^\ell}$. Por lo visto en secciones anteriores, la función $Q_{\lambda,\ell}(x)$ es una forma cuadrática, ya que $R_\lambda(x)$ es un polinomio q-linealizado sobre $\mathbb{F}_{q^m}$.

Los siguientes teoremas, probados por Klapper en [27] y [28], nos dicen exactamente cómo se distribuyen los rangos y los tipos de la familia de formas cuadráticas $\{Q_{\lambda,\ell}(x)\}_{\lambda,\ell}$ en m variables sobre $\mathbb{F}_q$, parametrizadas por $\lambda \in \mathbb{F}_{q^m}$ y $\ell \in \mathbb{N}$, cuando $m_\ell = \frac{m}{(m,\ell)}$ es par.

En particular, estos resultados aseguran que todas las formas cuadráticas $Q_{\lambda,\ell}$ son de rango par, en característica arbitraria.

Teorema 2.4.1 (Característica par)**.** *Sea q par, $\lambda \in \mathbb{F}_{q^m}^*$ y ℓ tal que $m_\ell = \frac{m}{(m,\ell)}$ es par. Si $Q_{\lambda,\ell}$ es como en* (2.30)*, entonces:*

(a). Si $\frac{1}{2}m_\ell$ es par y λ es una $(q^\ell+1)$-ésima potencia en $\mathbb{F}_{q^m}$, entonces $Q_{\lambda,\ell}$ tiene rango $m - 2(m,\ell)$ y es de tipo III.

(b). Si $\frac{1}{2}m_\ell$ es par y λ no es una $(q^\ell+1)$-ésima potencia en $\mathbb{F}_{q^m}$, entonces $Q_{\lambda,\ell}$ tiene rango m y es de tipo I.

(c). Si $\frac{1}{2}m_\ell$ es impar y λ es una $(q^\ell+1)$-ésima potencia en $\mathbb{F}_{q^m}$, entonces $Q_{\lambda,\ell}$ tiene rango $m - 2(m,\ell)$ y es de tipo I.

(d). Si $\frac{1}{2}m_\ell$ es impar y λ no es una $(q^\ell+1)$-ésima potencia en $\mathbb{F}_{q^m}$, entonces $Q_{\lambda,\ell}$ tiene rango m y es de tipo III.

Teorema 2.4.2 (Característica impar)**.** *Sea q impar y ℓ tal que $m_\ell = \frac{m}{(m,\ell)}$ es par y escribimos $\lambda = \alpha^t$ donde α un elemento primitivo de $\mathbb{F}_{q^m}$. Entonces:*

(a). Si $\frac{1}{2}m_\ell$ es par y $t \equiv 0 \ mod\ (q^{(m,\ell)}+1)$ entonces $Q_{\lambda,\ell}$ tiene rango $m - 2(m,\ell)$ y es de tipo III.

(b). Si $\frac{1}{2}m_\ell$ es par y $t \not\equiv 0 \ mod\ (q^{(m,\ell)}+1)$ entonces $Q_{\lambda,\ell}$ tiene rango m y es de tipo I.

(c). Si $\frac{1}{2}m_\ell$ es impar y $t \equiv \frac{q^{(m,\ell)}+1}{2} \ mod\ (q^{(m,\ell)}+1)$ entonces $Q_{\lambda,\ell}$ tiene rango $m - 2(m,\ell)$ y es de tipo I.

(d). Si $\frac{1}{2}m_\ell$ es impar y $t \not\equiv \frac{q^{(m,\ell)}+1}{2} \ mod\ (q^{(m,\ell)}+1)$ entonces $Q_{\lambda,\ell}$ tiene rango m y es de tipo III.

Por lo tanto, si consideramos las sumas exponenciales $S_{Q_{\lambda,\ell}}(\beta)$ y $S_{Q_{\lambda,\ell},b}(\beta)$, definidas en la sección anterior, obtenemos su distribución cuando λ varía en $\mathbb{F}_{q^m}$ y ℓ en $\mathbb{N}$. Como veremos en el capítulo siguiente esta es la clave para poder calcular la distribución de pesos de códigos cíclicos que se definen a partir de formas cuadráticas del estilo $Q_R(x) = \mathrm{Tr}_{q^m/q}(xR(x))$ donde $R(x)$ es un polinomio q-linealizado sobre $\mathbb{F}_{q^m}$.

Ahora fijamos notaciones que necesitaremos en los siguientes capítulos. Definamos el subconjunto de elementos no nulos de $\mathbb{F}_{q^m}$ que son potencias $(q^\ell+1)$-ésimas, es decir

$$T = T_{m,\ell} = \{\beta^{(q^\ell+1)} : \beta \in \mathbb{F}_{q^m}^*\} \tag{2.31}$$

y los subconjuntos de enteros positivos

$$\begin{aligned} T_1 = T_1(m,\ell) &= \big\{i \in \{1,\dots,q^m-1\} : i \equiv 0 \,(\text{mód } q^{(m,\ell)}+1)\big\}, \\ T_2 = T_2(m,\ell) &= \big\{i \in \{1,\dots,q^m-1\} : i \equiv \tfrac{q^{(m,\ell)}+1}{2} \,(\text{mód } q^{(m,\ell)}+1)\big\}. \end{aligned} \tag{2.32}$$

Además, denotaremos a sus cardinales por

$$M = \#T, \qquad M_1 = \#T_1, \qquad M_2 = \#T_2. \tag{2.33}$$

Por último, denotaremos de la siguiente manera a los cardinales de sus complementos con respecto a $\mathbb{F}_{q^m}^*$

$$M' = q^m - 1 - M, \qquad M_1' = q^m - 1 - M_1, \qquad M_2' = q^m - 1 - M_2. \tag{2.34}$$

A continuación calculamos estos números.

Lema 2.4.3. *Sean M, M_1 y M_2 como en* (2.33)*. Entonces*

$$M = \frac{q^m-1}{(q^m-1, q^\ell+1)}. \tag{2.35}$$

Si además $q^{(m,\ell)}+1 \mid q^m-1$ se tiene

$$M_1 = M_2 = \frac{q^m-1}{q^{(m,\ell)}+1}. \tag{2.36}$$

Demostración. Notar que si α es un elemento primitivo de $\mathbb{F}_{q^m}$, entonces $T = \langle \alpha^{q^\ell+1} \rangle$, y por lo tanto $M = \frac{q^m-1}{(q^m-1,q^\ell+1)}$.

Por otro lado, si k, N, s_1, s_2 son enteros no negativos tales que $k \mid N$ y $0 \le s_1, s_2 \le k-1$, entonces

$$\#\{i \in \{1,\dots,N\} : i \equiv s_1 \bmod k\} = \#\{i \in \{1,\dots,N\} : i \equiv s_2 \bmod k\} = \tfrac{N}{k}.$$

Por lo tanto, si $q^{(m,\ell)}+1 \mid q^m-1$, usando (2.32) con $N = q^m-1$ tenemos

$$M_1 = M_2 = \frac{q^m-1}{q^{(m,\ell)}+1},$$

como queríamos ver. □

Capítulo 3

Distribuciones de pesos

Sea α un elemento primitivo de $\mathbb{F}_{q^m}$ y ℓ un entero no negativo. En el año 2009 K. Feng y J. Luo ([13]) calcularon explícitamente la distribución de pesos del código cíclico reducible de longitud $n = p^m - 1$ con ceros

$$\alpha^{-1} \quad \text{y} \quad \alpha^{-(p^\ell+1)}$$

con $m/(m,\ell)$ un entero impar, usando sumas exponenciales asociadas a funciones planares (también llamadas funciones perfectas no lineales o PN). En 2008, los mismos autores, usando sumas exponenciales asociadas a formas cuadráticas, pudieron calcular la distribuciones de los códigos cíclicos reducibles con ceros

$$\alpha^{-2},\, \alpha^{-(p^\ell+1)} \quad \text{y} \quad \alpha^{-1},\, \alpha^{-2},\, \alpha^{-(p^\ell+1)}$$

cuando $(m,\ell) = 1$ y p es un primo impar ([14], [15]).

Estos métodos introducidos por Feng y Luo permitieron luego, a muchos otros autores, calcular explícitamente la distribución de pesos de códigos cíclicos sobre $\mathbb{F}_p$, cuando p es un primo impar (ver [49], [50], [51], [52], [53], [54]). En este capítulo, usaremos los resultados de formas cuadráticas y sumas exponenciales del Capítulo 2 para encontrar la distribución de pesos de varios códigos cíclicos que tienen en común el cero $\alpha^{-(p^\ell+1)}$, en el caso $m/(m,\ell)$ par.

3.1. Pesos de códigos definidos por formas cuadráticas

Los códigos cíclicos $\mathcal{C}_\mathcal{L}$, $\mathcal{C}_{\mathcal{L},0}$, $\mathcal{C}_{\mathcal{L},1}$ y $\mathcal{C}_{\mathcal{L},2}$

Consideremos $\mathcal{L} \subset \mathbb{F}_{q^m}[x]$ un $\mathbb{F}_{q^m}$-subespacio de dimensión finita formado por polinomios q-linealizados, es decir

$$\mathcal{L} = \langle x^{q^{\ell_1}}, x^{q^{\ell_2}}, \ldots, x^{q^{\ell_s}} \rangle \subset \mathbb{F}_{q^m}[x]$$

para ciertos enteros no negativos $\ell_1, \ldots, \ell_s$. Definimos el código

$$\mathcal{C}_\mathcal{L} = \left\{ c_R = \left(\mathrm{Tr}_{q^m/q}(xR(x)) \right)_{x \in \mathbb{F}_{q^m}^*} : R \in \mathcal{L} \right\} \subset \mathbb{F}_q^n \tag{3.1}$$

con $n = q^m - 1$ y los siguientes códigos sobre $\mathbb{F}_q$ relacionados

$$\begin{aligned}
\mathcal{C}_{\mathcal{L},0} &= \left\{ c_{R,b} = \left(\mathrm{Tr}_{q^m/q}\big(xR(x)\big) + b\right)_{x\in\mathbb{F}_{q^m}^*} : R \in \mathcal{L},\ b \in \mathbb{F}_q \right\}, \\
\mathcal{C}_{\mathcal{L},1} &= \left\{ c_R(\beta) = \left(\mathrm{Tr}_{q^m/q}(xR(x) + \beta x)\right)_{x\in\mathbb{F}_{q^m}^*} : R \in \mathcal{L},\ \beta \in \mathbb{F}_{q^m} \right\}, \\
\mathcal{C}_{\mathcal{L},2} &= \left\{ c_{R,b}(\beta) = \left(\mathrm{Tr}_{q^m/q}(xR(x) + \beta x) + b\right)_{x\in\mathbb{F}_{q^m}^*} : R \in \mathcal{L},\ \beta \in \mathbb{F}_{q^m},\ b \in \mathbb{F}_q \right\}.
\end{aligned} \tag{3.2}$$

Notar que $c_{R,b} = c_R + b$ y $c_{R,b}(\beta) = c_R(\beta) + b$ y que además se tiene $c_{R,0} = c_R(0) = c_R$, $c_{R,b}(0) = c_{R,b}$ y $c_{R,0}(\beta) = c_R(\beta)$. De aquí, claramente tenemos

$$\mathcal{C}_{\mathcal{L}} \subset \mathcal{C}_{\mathcal{L},0}\,,\, \mathcal{C}_{\mathcal{L},1} \subset \mathcal{C}_{\mathcal{L},2}.$$

Ya vimos en el capítulo anterior (Ejemplo 2.2.4) que si R es un polinomio q-linealizado, entonces $Q_R(x) = \mathrm{Tr}_{q^m/q}(xR(x))$ es una forma cuadrática. Además, todos estos códigos resultan cíclicos ya que son un caso particular de los códigos cíclicos (1.6) presentados en el Ejemplo 1.3.9.

En esta sección encontraremos los pesos de códigos cíclicos $\mathcal{C}_{\mathcal{L}}$ para ciertos conjuntos $\mathcal{L}$. Además, encontraremos los pesos de otros códigos relacionados con $\mathcal{C}_{\mathcal{L}}$. Un problema desafiante y más complicado es encontrar la *distribución* de pesos de estos códigos.

A continuación damos una lista de códigos de tipo $\mathcal{C}_{\mathcal{L}}$ donde la distribución de pesos está resuelta completamente. Sea p un primo, q una potencia de un primo y $m, \ell \in \mathbb{N}$.

LISTA DE CÓDIGOS $\mathcal{C}_{\mathcal{L}}$ CON $Spec(\mathcal{C}_{\mathcal{L}})$ CONOCIDO.

(a) $\mathcal{L} = \langle x^{2^\ell} \rangle \subset \mathbb{F}_{2^m}[x]$ donde $\frac{m}{(m,\ell)}$ es impar ([26], 1971).

(b) $\mathcal{L} = \langle x^{p^\ell} \rangle \subset \mathbb{F}_{p^m}[x]$ donde p es impar y $\frac{m}{(m,\ell)}$ es impar ([13], 2007).

(c) $\mathcal{L} = \langle x^{p^i} \rangle_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} \subset \mathbb{F}_{p^m}[x]$ con $p = 2$ ([43], 1992).

(d) $\mathcal{L} = \langle x, x^{p^\ell} \rangle \subset \mathbb{F}_{p^m}[x]$ donde p es impar y $(m, \ell) = 1$, $m \geq 3$ ([14], [15], 2007 y 2008).

(e) $\mathcal{L} = \langle x^{p^\ell}, x^{p^{3\ell}} \rangle \subset \mathbb{F}_{p^m}[x]$ donde p es impar ([50], [51], 2013 y 2014).

(f) $\mathcal{L} = \langle x^{q^{(2i-1)}} \rangle_{i=1}^{\frac{m}{4}} \subset \mathbb{F}_{q^m}[x]$ con $m \geq 4$, tal que $v_2(m) \geq 2$ ([53], 2013).

(g) $\mathcal{L} = \langle x^{q^{(2i-1)}}, x^{q^{\frac{m}{2}}} \rangle_{i=1}^{\lfloor \frac{m}{4} \rfloor} \subset \mathbb{F}_{q^m}[x]$ con m tal que $v_2(m) = 1$ ([53], 2013).

(h) $\mathcal{L} = \langle x, x^3, x^{3^2} \rangle \subset \mathbb{F}_{3^m}[x]$ ([31], 2014).

En general, el cálculo de la distribución de pesos no es un proceso "hereditario", en el sentido que conocer la distribución de un código no nos dice nada sobre la distribución de

pesos de sus subcódigos. Por lo tanto, es factible considerar otros subconjuntos $\mathcal{L}$ contenidos en algunos de los ya conocidos.

En las próximas secciones vamos a trabajar con un subespacio particular de polinomios linealizados, a saber $\mathcal{L} = \langle x^{q^\ell} \rangle$, con q potencia de un primo, y resolveremos el problema de la distribución de pesos de $\mathcal{C}_\mathcal{L}$, $\mathcal{C}_{\mathcal{L},0}$, $\mathcal{C}_{\mathcal{L},1}$ y $\mathcal{C}_{\mathcal{L},2}$ cuando $\frac{m}{(m,\ell)}$ es par, en todas las características. Esto completa el caso de los items (a) y (b) de la lista anterior.

A continuación, vamos a calcular la expresión de los pesos de los códigos $\mathcal{C}_\mathcal{L}$, $\mathcal{C}_{\mathcal{L},0}$, $\mathcal{C}_{\mathcal{L},1}$ y $\mathcal{C}_{\mathcal{L},2}$ con $\mathcal{L}$ arbitrario y veremos que, en algunos casos favorables, es posible encontrar expresiones de las distribuciones de pesos de otros códigos cíclicos relacionados con $\mathcal{C}_\mathcal{L}$, en términos de invariantes de las formas cuadráticas usadas para definir dichos códigos.

3.1.1. Característica impar, códigos $C_\mathcal{L}$ y $C_{\mathcal{L},0}$

Como vimos en el Capítulo 2, si $\mathbb{F}_q$ tiene característica impar el estudio de formas cuadráticas de m variables sobre $\mathbb{F}_q$ se facilita, ya que en este caso toda forma cuadrática Q se puede "diagonalizar", en el siguiente sentido: existe una $\mathbb{F}_q$-base $\mathcal{B}$ de $\mathbb{F}_{q^m}$ y constantes $\alpha_1, \ldots, \alpha_r \in \mathbb{F}_q$, donde r es el rango de Q, tal que si $x \in \mathbb{F}_{q^m}$ tiene vector de coordenadas $[x]_\mathcal{B} = (x_1, \ldots, x_m)$, entonces

$$Q(x) = \alpha_1 x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_r x_r^2.$$

Recordemos que denotamos por $\Delta = \alpha_1 \cdots \alpha_r$ al determinante de la forma cuadrática Q.

El siguiente teorema nos dice cómo son los pesos de $\mathcal{C}_\mathcal{L}$.

Teorema 3.1.1. *Sea q una potencia de un primo impar. Consideremos $\mathcal{C}_\mathcal{L}$ como en* (3.1)*, donde $\mathcal{L} \subset \mathbb{F}_{q^m}[x]$ es un subespacio de dimensión finita de polinomios q-linealizados. El peso de $c_R \in \mathcal{C}_\mathcal{L}$ está dado por*

$$w(c_R) = \begin{cases} q^m - q^{m-1} - \eta(-1)^{\frac{r}{2}}\eta(\Delta)(q^{m-\frac{r}{2}} - q^{m-\frac{r}{2}-1}) & \text{si } r \text{ es par,} \\ q^m - q^{m-1} & \text{si } r \text{ es impar,} \end{cases} \tag{3.3}$$

donde $r = r_R$ es el rango de la forma cuadrática $Q_R(x) = \mathrm{Tr}_{q^m/q}(xR(x))$ y η es el carácter cuadrático de $\mathbb{F}_q$. En particular, $q - 1 \mid w(c_R)$ para todo $c_R \in \mathcal{C}_\mathcal{L}$.

Nota. Un código tal que todas sus palabras son divisibles por un entero positivo d, es llamado *d-divisible*. En este caso, el código $\mathcal{C}_\mathcal{L}$ es $(q-1)$-divisible.

Demostración. Sea $c_R = (\mathrm{Tr}_{q^m/q}(xR(x)))_{x \in \mathbb{F}_{q^m}^*}$ una palabra de $\mathcal{C}_\mathcal{L}$. Como q es impar y R es un polinomio q-linealizado, entonces $Q_R(x) = \mathrm{Tr}_{q^m/q}(xR(x))$ es una forma cuadrática diagonalizable. Supongamos que Q_R tiene rango $r \leq m$, entonces existe una $\mathbb{F}_q$-base $\mathcal{B}$ de $\mathbb{F}_{q^m}$ y constantes $\alpha_1, \ldots \alpha_r \in \mathbb{F}_q$ tales que si $x \in \mathbb{F}_{q^m}$ tiene vector de coordenadas $[x]_\mathcal{B} = (x_1, \ldots, x_m)$ entonces

$$Q_R(x) = \alpha_1 x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_r x_r^2.$$

Luego

$$w(c_R) = \#\{x \in \mathbb{F}_{q^m}^* : Q_R(x) \neq 0\} = q^m - 1 - \#\{x \in \mathbb{F}_{q^m}^* : Q_R(x) = 0\}.$$

Notar que $Q_R(0) = 0$, por lo tanto si denotamos $Z_R = \#\{x \in \mathbb{F}_{q^m} : Q_R(x) = 0\}$, entonces

$$w(c_R) = q^m - Z_R.$$

Denotemos por N a la cantidad de soluciones $(x_1, \ldots, x_r) \in \mathbb{F}_q^r$ de la ecuación diagonal

$$\alpha_1 x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_r x_r^2 = 0.$$

Por el Corolario 2.1.13, tenemos que

$$N = \begin{cases} q^{r-1} + \eta((-1)^{\frac{r}{2}}\alpha_1 \cdots \alpha_r)(q^{\frac{r}{2}} - q^{\frac{r-2}{2}}) & \text{si } r \text{ es par,} \\ q^{r-1} & \text{si } r \text{ es impar,} \end{cases}$$

donde η es el carácter cuadrático de $\mathbb{F}_q$. Notar que

$$Z_R = \#\{(x_1, \ldots, x_m) \in \mathbb{F}_q^m : \alpha_1 x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_r x_r^2 = 0\},$$

entonces

$$Z_R = q^{m-r}N = \begin{cases} q^{m-1} + \eta(-1)^{\frac{r}{2}}\eta(\Delta)(q^{m-\frac{r}{2}} - q^{m-\frac{r}{2}-1}) & \text{si } r \text{ es par,} \\ q^{m-1} & \text{si } r \text{ es impar.} \end{cases}$$

Por lo tanto, como $w(c_R) = q^m - Z_R$, se obtiene (3.3) como queríamos demostrar. La última afirmación del enunciado es evidente de (3.3). □

De manera análoga es posible encontrar los pesos de las palabras del código $\mathcal{C}_{\mathcal{L},0}$.

Teorema 3.1.2. *Sea q una potencia de un primo impar. Consideremos $\mathcal{C}_{\mathcal{L},0}$ como en* (3.2)*, donde $\mathcal{L} \subset \mathbb{F}_{q^m}[x]$ es un subespacio de dimensión finita de polinomios q-linealizados. El peso de $c_{R,b} \in \mathcal{C}_{\mathcal{L},0}$ con $b \neq 0$ está dado por*

$$w(c_{R,b}) = \begin{cases} q^m - 1 & \text{si } R = 0, \\ q^m - q^{m-1} - \eta(-1)^{\frac{r+1}{2}}\,\eta(b\Delta)\,q^{m-\frac{r+1}{2}} - 1 & \text{si } r \text{ es impar y } R \neq 0, \\ q^m - q^{m-1} + \eta(-1)^{\frac{r}{2}}\,\eta(\Delta)\,q^{m-\frac{r}{2}-1} - 1 & \text{si } r \text{ es par y } R \neq 0, \end{cases}$$

donde $r = r_R$ es el rango de la forma cuadrática $Q_R(x) = \mathrm{Tr}_{q^m/q}(xR(x))$ y η es el carácter cuadrático de $\mathbb{F}_q$.

3.1.2. Rangos pares

En esta subsección, analizaremos la distribución de pesos de todos códigos relacionados con $\mathcal{C}_{\mathcal{L}}$ para familias de polinomios linealizados que cumplen un cierta propiedad de paridad.

Definición 3.1.3. Una familia $\mathcal{L} \subset \mathbb{F}_{q^m}[x]$ de polinomios q-linealizados se dice que *satisface la propiedad de paridad* (o simplemente que *es de paridad*) si la forma cuadrática $Q_R(x) = \mathrm{Tr}_{q^m/q}(xR(x))$ es de rango par para todo $R \in \mathcal{L}$.

Notar que si $\mathcal{L}$ es de paridad, entonces toda subfamilia $\mathcal{L}' \subset \mathcal{L}$ también lo es. Veremos que algunas familias $\mathcal{L}$ de la lista anterior satisfacen esta propiedad de paridad.

En los siguientes ejemplos, q es una potencia de un primo y m, ℓ son enteros positivos.

Ejemplo 3.1.4. Consideremos la familia $\mathcal{L}_\ell = \langle x^{q^\ell} \rangle \subset \mathbb{F}_{q^m}[x]$.
(i) Si $m/(m,\ell)$ es par (luego m es par), los Teoremas 2.4.1 y 2.4.2 aseguran que $Q_\gamma(x) = \mathrm{Tr}_{q^m/q}(\gamma x^{q^\ell})$ tiene rango m ó $m - 2(m,\ell)$, lo que implica que $\mathcal{L}_\ell$ es de paridad.
(ii) Si $m/(m,\ell)$ es impar, la familia $\mathcal{L}_\ell$ no es necesariamente de paridad, ya que las formas cuadráticas inducidas tiene siempre rango m. Sin embargo, $\mathcal{L}_\ell$ resulta de paridad cuando $1 \leq v_2(m) \leq v_2(\ell)$ ([27], [28]). ◊

Ejemplo 3.1.5. Consideremos $\mathcal{L}_{\ell,3\ell} = \langle x^{p^\ell}, x^{p^{3\ell}} \rangle \subset \mathbb{F}_{p^m}[x]$ tal que $m/(m,\ell)$ es par y p es un primo impar. En [51] los autores probaron que Q_R tiene rango par para todo $R \in \mathcal{L}_{\ell,3\ell}$ y por lo tanto este conjunto satisface la propiedad de paridad. ◊

Ejemplo 3.1.6. Consideremos $\mathcal{L}_{\ell,(2k-1)\ell} = \langle x^{p^\ell}, x^{p^{(2k-1)\ell}} \rangle \subset \mathbb{F}_{p^m}[x]$ con $k \in \mathbb{N}$ tal que $m/(m,\ell)$ es par y p es un primo impar. Usando métodos análogos a los usados en [51], se puede probar que este conjunto satisface la propiedad de paridad. ◊

El siguiente ejemplo generaliza a los anteriores con q potencia del primo p, cuando el entero ℓ que aparece en dichos ejemplos es impar.

Ejemplo 3.1.7. Consideremos $\mathcal{L}_{\ell_1,\ldots,\ell_u} = \langle x^{q^{\ell_1}}, \ldots, x^{q^{\ell_u}} \rangle \subset \mathbb{F}_{q^m}[x]$ con m par tal que los enteros

$$1 \leq \ell_1 < \ell_2 < \cdots < \ell_u \leq 2\lfloor \tfrac{m}{4} \rfloor - 1$$

son todos impares. En [53] se prueba que Q_R tiene rango par para todo $R \in \mathcal{L}_{\ell_1,\ldots,\ell_u}$ y por lo tanto $\mathcal{L}_{\ell_1,\ldots,\ell_u}$ satisface la propiedad de paridad. En particular,

$$\mathcal{L}_{1,3,5,\ldots,2t-1} = \langle x^q, x^{q^3}, x^{q^5}, \ldots, x^{q^{2t-1}} \rangle \subset \mathbb{F}_{q^{4t}}[x]$$

resulta una familia de paridad para todo $t \in \mathbb{N}$. ◊

Sea $\mathcal{L}$ una familia de polinomios q-linealizados que satisface la propiedad de paridad. Los Teoremas 2.2.11 y 2.2.12, que dan la clasificación de formas cuadráticas, nos dicen que

$Q_R(x) = \mathrm{Tr}_{q/p}(xR(x))$ es de tipo I ó de tipo III para todo $R \in \mathcal{L}$. Por lo tanto, para $r \in \mathbb{N}$, definimos los conjuntos

$$\begin{aligned} K_r &= \{R \in \mathcal{L} : Q_R \text{ tiene rango } r\}, \\ K_{r,1} &= \{R \in \mathcal{L} \setminus \{0\} : Q_R \text{ tiene rango } r \text{ y es de tipo I}\}, \\ K_{r,2} &= \{R \in \mathcal{L} \setminus \{0\} : Q_R \text{ tiene rango } r \text{ y es de tipo III}\}. \end{aligned} \tag{3.4}$$

Obviamente se tiene que $K_0 = \{0\}$ y por otro lado $K_r = K_{r,1} \sqcup K_{r,2}$ cuando $r > 0$. Denotaremos a sus cardinales respectivamente con

$$M_{r,1} = \#K_{r,1}, \qquad M_{r,2} = \#K_{r,2}, \tag{3.5}$$

donde además ponemos

$$M_r = \#K_r.$$

Notar que $M_0 = 1$ y además cuando $r > 0$ tenemos que

$$M_r = M_{r,1} + M_{r,2}. \tag{3.6}$$

También necesitaremos el conjunto

$$R_{\mathcal{L}} = \{r \in \mathbb{Z}_{\geq 0} : \text{existe } R \in \mathcal{L} \text{ con } Q_R \text{ de rango } r\} \tag{3.7}$$

y $R^*_{\mathcal{L}} = R_{\mathcal{L}} \setminus \{0\}$. Estos conjuntos son claves para encontrar las distribuciones de pesos de los códigos cíclicos $\mathcal{C}_{\mathcal{L}}$, $\mathcal{C}_{\mathcal{L},0}$, $\mathcal{C}_{\mathcal{L},1}$ y $\mathcal{C}_{\mathcal{L},2}$.

Distribución de pesos de $\mathcal{C}_{\mathcal{L}}$

Para $c_R \in \mathcal{C}_{\mathcal{L}}$ y $c \in \mathbb{F}_q^*$, consideremos los números

$$N_R(c) = \#\left\{x \in \mathbb{F}_{q^m}^* : Q_R(x) = c\right\} \tag{3.8}$$

donde $\ell \in \mathbb{N}$, $\lambda \in \mathbb{F}_{q^m}$ y $c \in \mathbb{F}_q^*$. Notar que $N_R(c)$ es igual a $N_{Q_R}(c)$, definido en (2.16) para la forma cuadrática Q_R. Luego, el peso de c_R está dado por

$$w(c_R) = \sum_{c \in \mathbb{F}_q^*} N_R(c). \tag{3.9}$$

A continuación calculamos los números $N_R(c)$ y también los pesos de $\mathcal{C}_{\mathcal{L}}$.

Lema 3.1.8. *Sea $\mathcal{L}$ una familia de polinomios q-linealizados con la propiedad de paridad. Si $R \in \mathcal{L}$ y Q_R es la forma cuadrática asociada a R, entonces para $c \in \mathbb{F}_q^*$ se tiene*

$$N_R(c) = q^{m-1} - \epsilon q^{m-\frac{r}{2}-1}, \tag{3.10}$$

donde r y ϵ son el rango y el tipo de Q_R. Los pesos del código $\mathcal{C}_{\mathcal{L}}$ definido en (3.1) *son*

$$w(c_R) = q^m - q^{m-1} - \epsilon(q-1)q^{m-\frac{r}{2}-1}. \tag{3.11}$$

Demostración. Como $\mathcal{L}$ satisface la propiedad de paridad, Q_R debe tener rango r par y por los Teoremas 2.2.11 y 2.2.12 de clasificación de formas cuadráticas, tenemos que

$$N_R(c) = q^{m-1} + \epsilon\nu(c)q^{m-\frac{r}{2}-1}$$

donde $\nu(c)$ es la función que vale -1 si $c \in \mathbb{F}_q^*$ y $q-1$ si $c = 0$, por lo tanto obtenemos (3.10) como queríamos demostrar.

Notar que los valores $N_R(c)$ no dependen de c cuando $c \neq 0$ y, como $w_H(c_R) = \sum_{c\in\mathbb{F}_q^*} N_R(c)$, entonces

$$w(c_R) = (q-1)N_R(c) = q^m - q^{m-1} - \epsilon(q-1)q^{m-\frac{r}{2}-1}$$

como queríamos demostrar. □

Este último lema nos permite calcular el enumerador de pesos completo de $\mathcal{C}_\mathcal{L}$ y por lo tanto su espectro.

Teorema 3.1.9. *Sean q una potencia de un primo, $\mathcal{L} \subset \mathbb{F}_{q^m}[x]$ un $\mathbb{F}_{q^m}$-subespacio de dimensión finita conteniendo solamente polinomios q-linealizados que satisfacen la propiedad de paridad y $\mathcal{C}_\mathcal{L}$ el código cíclico definido en* (3.1)*. El enumerador de pesos completo de $\mathcal{C}_\mathcal{L}$ está dado por*

$$W_\mathcal{L}(z_0, \ldots, z_{q-1}) = z_0^n + \sum_{i=1,2}\sum_{r\in R_\mathcal{L}} M_{r,i}\, z_0^{a_0(r,i)} z_1^{a_1(r,i)} \cdots z_{q-1}^{a_1(r,i)}$$

donde $M_{r,i}$ y $R_\mathcal{L}$ están definidos en (3.5) *y* (3.7) *y además*

$$a_0(r,i) = q^{m-1} + (-1)^{i+1}(q-1)q^{m-\frac{r}{2}-1} - 1 \qquad y \qquad a_1(r,i) = q^{m-1} + (-1)^i q^{m-\frac{r}{2}-1}.$$

En particular, evaluando el polinomio $W_\mathcal{L}$ en $(1, t, \ldots, t)$ obtenemos la distribución de pesos del código $\mathcal{C}_\mathcal{L}$ (ver Tabla 3.1) y por lo tanto $\mathcal{C}_\mathcal{L}$.

Demostración. Sea $R \in \mathcal{L}$. Notar que los monomios del enumerador de pesos completos no nulos son o bien de la forma

$$z_0^{N_R(0)} \prod_{j=1}^{q-1} z_j^{N_R(c)}$$

cuando $R \neq 0$ con c algún elemento no nulo de $\mathbb{F}_q$, ya que los valores $N_R(c)$ no dependen de c; o bien son el monomio z_0^n correspondiente a la palabra cero. Usando la definición de los números $M_{r,i}$ y el lema anterior obtenemos el enumerador de pesos completo de $\mathcal{C}_\mathcal{L}$. □

Tabla 3.1: Distribución de pesos de $\mathcal{C}_\mathcal{L}$.

Pesos posibles	Frecuencias
0	1
$q^m - q^{m-1} + (-1)^i(q-1)q^{m-\frac{r}{2}-1}$	$M_{r,i}$

En la tabla, r varía en $R_\mathcal{L}$ e $i = 1, 2$.

Distribución de pesos de $\mathcal{C}_{\mathcal{L},0}$

Ahora consideremos el código cíclico $\mathcal{C}_{\mathcal{L},0}$ definido en (3.2) con $\mathcal{L}$ una familia de polinomios linealizados satisfaciendo la propiedad de paridad.

Para calcular la distribución de pesos de $\mathcal{C}_{\mathcal{L},0}$ consideremos $c_{R,b} \in \mathcal{C}_{\mathcal{L},0}$ con $R \in \mathcal{L}$ y $b \in \mathbb{F}_q$. Si $R = 0$, entonces tenemos que

$$w(c_{R,b}) = \begin{cases} 0 & \text{si } b = 0, \\ q^m - 1 & \text{si } b \neq 0. \end{cases}$$

Supongamos entonces que $R \neq 0$. Notar que si $b = 0$, entonces

$$c_{R,b} = c_R \in \mathcal{C}_{\mathcal{L}}$$

y por lo tanto su peso está dado por (3.11) del Lema 3.1.8, en este caso. Para encontrar los pesos restantes, notar que

$$w(c_{R,b}) = q^m - 1 - N_R(-b)$$

donde $N_R(-b)$ es como en (3.8). Por el Lema 3.1.8, obtenemos que

$$w(c_{R,b}) = q^m - q^{m-1} + \epsilon q^{m-\frac{r}{2}-1} - 1 \qquad \text{si } b \neq 0,$$

donde ϵ y r son el tipo y el rango de la forma cuadrática Q_R.

Por lo tanto obtenemos que los pesos posibles para $c_{R,b}$ estan dados por

$$w(c_{R,b}) = \begin{cases} 0 & \text{si } R = 0,\ b = 0, \\ q^m - 1 & \text{si } R = 0,\ b \neq 0, \\ q^m - q^{m-1} - \epsilon(q-1)q^{m-\frac{r}{2}-1} & \text{si } R \neq 0,\ b = 0, \\ q^m - q^{m-1} + \epsilon q^{m-\frac{r}{2}-1} - 1 & \text{si } R \neq 0,\ b \neq 0, \end{cases} \tag{3.12}$$

donde ϵ y r son el tipo y el rango de la forma cuadrática Q_R. Luego, tenemos el siguiente resultado.

Teorema 3.1.10. *Sea q una potencia de un primo. Sea $\mathcal{L} \subset \mathbb{F}_{q^m}[x]$ un $\mathbb{F}_{q^m}$-subespacio de dimensión finita conteniendo solamente polinomios q-linealizados que satisfacen la propiedad de paridad y $\mathcal{C}_{\mathcal{L},0}$ es el código cíclico definido en* (3.2)*. Entonces, la distribución de pesos del código $\mathcal{C}_{\mathcal{L},0}$ está dado por la Tabla 3.2, donde $M_{r,i}$ y $R_{\mathcal{L}}$ son como en* (3.5) *y* (3.7)*.*

Demostración. Sea $c_{R,b}$ una palabra de $\mathcal{C}_{\mathcal{L},0}$. Supongamos que la forma cuadrática asociada Q_R tiene rango r y tipo ϵ_R respectivamente, y sean $K_{r,1}$ y $K_{r,2}$ como en (3.4). Por definición $M_{r,i} = \#K_{r,i}$ y como $\mathcal{L}$ satisface la propiedad de paridad, obtenemos que

$$\epsilon_R = \begin{cases} 1 & \text{si } R \in K_{r,1}, \\ -1 & \text{si } R \in K_{r,2}. \end{cases}$$

Entonces $\epsilon_R = (-1)^{i+1}$ si $R \in K_{r,i}$, $i = 1, 2$. Luego, por la igualdad (3.12), obtenemos

$$w(c_{R,b}) = \begin{cases} 0 & \text{si } b = 0,\ R = 0, \\ q^m - 1 & \text{si } b \neq 0,\ R = 0, \\ q^m - q^{m-1} + (-1)^i (q-1) q^{m-\frac{r}{2}-1} & \text{si } b = 0,\ R \in K_{r,i}, \\ q^m - q^{m-1} + (-1)^{i+1} q^{m-\frac{r}{2}-1} - 1 & \text{si } b \neq 0,\ R \in K_{r,i}, \end{cases}$$

con $i = 1, 2$. Contando la cantidad de posibilidades en cada caso, obtenemos la Tabla 3.2. □

Tabla 3.2: Distribución de pesos de $\mathcal{C}_{\mathcal{L},0}$.

Pesos posibles	Frecuencias
0	1
$q^m - q^{m-1} + (-1)^i (q-1) q^{m-\frac{r}{2}-1}$	$M_{r,i}$
$q^m - 1$	$q - 1$
$q^m - q^{m-1} + (-1)^{i+1} q^{m-\frac{r}{2}-1} - 1$	$M_{r,i}(q-1)$

En la tabla, r varía en $R_{\mathcal{L}}$ e $i = 1, 2$.

Distribución de pesos de $\mathcal{C}_{\mathcal{L},1}$ y $\mathcal{C}_{\mathcal{L},2}$

Veamos la expresión de los pesos de las palabras de $\mathcal{C}_{\mathcal{L},1}$ definido en (3.2). Por la ortogonalidad de los caracteres (ver (2.1), (2.2)), se tiene que

$$\begin{aligned} w(c_R(\beta)) &= q^m - 1 - \#\{x \in \mathbb{F}_{q^m}^* : Q_R(x) + \mathrm{Tr}_{q^m/q}(\beta x) = 0\} \\ &= q^m - 1 - \tfrac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\mathrm{Tr}_{q/p}(a(Q_R(x) + \mathrm{Tr}_{q^m/q}(\beta x)))} \\ &= q^m - 1 - \tfrac{1}{q} \Big\{ \sum_{a \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(a(Q_R(x) + \mathrm{Tr}_{q^m/q}(\beta x)))} - q \Big\} \\ &= q^m - 1 - \tfrac{1}{q} \Big\{ \sum_{a \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(a(Q_R(x) + \mathrm{Tr}_{q^m/q}(\beta x)))} + q^m - q \Big\}. \end{aligned}$$

Por lo tanto,

$$w(c_R(\beta)) = q^m - q^{m-1} - \tfrac{1}{q} S_{Q_R}(\beta), \tag{3.13}$$

donde S_{Q_R} es como en (2.25). De la misma forma, cuando $b \neq 0$, tenemos

$$w(c_{R,b}(\beta)) = q^m - q^{m-1} - 1 - \tfrac{1}{q} S_{Q_R,b}(\beta). \tag{3.14}$$

Notar que si $R = 0$, entonces $Q_R = 0$ y por lo tanto

$$w(c_0(\beta)) = q^m - q^{m-1}$$

para todo $\beta \neq 0$.

Por último, cuando R y β son nulos entonces $w(c_{0,b}(0)) = q^m - 1$ si $b \neq 0$, ya que en este caso la palabra no tiene ninguna coordenada nula.

La discusión anterior y la Proposición 2.3.5, nos permiten calcular explícitamente las distribuciones de pesos de los códigos $\mathcal{C}_{\mathcal{L},1}$ y $\mathcal{C}_{\mathcal{L},2}$.

Teorema 3.1.11. *Sea $\mathcal{L} \subset \mathbb{F}_{q^m}[x]$ un $\mathbb{F}_{q^m}$-subespacio de dimensión finita conteniendo solamente polinomios q-linealizados que satisfacen la propiedad de paridad. Sean $M_{r,1}$, $M_{r,2}$, M_r y $R_{\mathcal{L}}$ como en* (3.5) *y* (3.7)*. Entonces, la distribución de pesos de los códigos cíclicos $\mathcal{C}_{\mathcal{L},1}$ y $\mathcal{C}_{\mathcal{L},2}$, definidos en* (3.2)*, están dados por las Tablas 3.3 y 3.4, respectivamente.*

Demostración. Sea $c_{R,b}(\beta) \in \mathcal{C}_{\mathcal{L}_2}$, cuando $b = 0$ denotemos $c_R(\beta) = c_{R,0}(\beta)$. Supongamos que la forma cuadrática asociada Q_R tiene rango r y tipo ϵ_R respectivamente, y sean $K_{r,1}$ y $K_{r,2}$ como en (3.4). Luego $\epsilon_R = (-1)^{i+1}$ si $R \in K_{r,i}$, $i = 1, 2$. Por la discución previa al teorema y la Proposición 2.3.5 obtenemos que

$$w(c_{R,b}(\beta)) = \begin{cases} 0 & \text{si } b = 0,\ R = 0, \\ q^m - q^{m-1} & \text{si } b = 0,\ R \in K_{r,i},\ \text{para } q^m - q^r\ \beta's \\ q^m - q^{m-1} + (-1)^i(q-1)q^{m-\frac{r}{2}-1} & \text{si } b = 0,\ R \in K_{r,i},\ \text{para } q^{r-1} + (-1)^{i+1}(q-1)q^{\frac{r}{2}-1}\ \beta's \\ q^m - q^{m-1} + (-1)^{i+1}q^{m-\frac{r}{2}-1} & \text{si } b = 0,\ R \in K_{r,i},\ \text{para } (q^{r-1} + (-1)^i q^{\frac{r}{2}-1})(q-1)\ \beta's \\ q^m - 1 & \text{si } b \neq 0,\ R = 0,\ \beta = 0 \\ q^m - q^{m-1} - 1 & \text{si } b \neq 0,\ R \in K_{r,i},\ \text{para } q^m - q^r\ \beta's \\ q^m - q^{m-1} + (-1)^i(q-1)q^{m-\frac{r}{2}-1} - 1 & \text{si } b \neq 0,\ R \in K_{r,i},\ \text{para } q^{r-1} + (-1)^i q^{\frac{r}{2}-1}\ \beta's \\ q^m - q^{m-1} + (-1)^{i+1}q^{m-\frac{r}{2}-1} - 1 & \text{si } b \neq 0,\ R \in K_{r,i},\ \text{para } q^r - q^{r-1} + (-1)^{i+1}q^{\frac{r}{2}-1}\ \beta's \end{cases}$$

con $i = 1, 2$. Contando la cantidad de posibilidades obtenemos las distribuciones de pesos buscadas. □

Tabla 3.3: Distribución de pesos de $\mathcal{C}_{\mathcal{L},1}$.

Pesos posibles	Frecuencias
0	1
$q^m - q^{m-1}$	$\sum_{r \in R_{\mathcal{L}}} M_r(q^m - q^r)$
$q^m - q^{m-1} + (-1)^i(q-1)q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^{i+1}(q-1)q^{\frac{r}{2}-1})$
$q^m - q^{m-1} + (-1)^{i+1}q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^i q^{\frac{r}{2}-1})(q-1)$

Tabla 3.4: Distribución de pesos de $\mathcal{C}_{\mathcal{L},2}$.

Pesos posibles	Frecuencias
0	1
$q^m - q^{m-1}$	$\sum_{r\in R_\mathcal{L}} M_r(q^m - q^r)$
$q^m - q^{m-1} + (-1)^i(q-1)q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^{i+1}(q-1)q^{\frac{r}{2}-1})$
$q^m - q^{m-1} + (-1)^{i+1}q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^i q^{\frac{r}{2}-1})(q-1)$
$q^m - 1$	$q-1$
$q^m - q^{m-1} - 1$	$(q-1)\sum_{r\in R_\mathcal{L}} M_r(q^m - q^r)$
$q^m - q^{m-1} - 1 + (-1)^i(q-1)q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^i q^{\frac{r}{2}-1})(q-1)$
$q^m - q^{m-1} - 1 + (-1)^{i+1}q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^r - q^{r-1} + (-1)^{i+1}q^{\frac{r}{2}-1})(q-1)$

En ambas tablas, r varía en $R_\mathcal{L}$ e $i = 1, 2$.

Nota. Las primeras filas de las Tablas 3.2 y 3.4 coinciden con las Tablas 3.1 y 3.3, respectivamente. Además si $k_\mathcal{L}$ denota la dimensión de $\mathcal{C}_\mathcal{L}$ y $k_{\mathcal{L},i}$ para $i = 0, 1, 2$ y tenemos las siguientes relaciones

$$k_{\mathcal{L},0} = k_\mathcal{L} + 1, \qquad k_{\mathcal{L},1} = k_\mathcal{L} + m, \qquad k_{\mathcal{L},2} = k_{\mathcal{L},1} + 1$$

3.2. El código $\mathcal{C}_\ell$ y su espectro

El código irreducible $\mathcal{C}_\ell$

Consideremos $\mathcal{C}_\ell$ el código cíclico irreducible sobre $\mathbb{F}_q$, cuyo polinomio de chequeo $h_\ell(x)$ es el polinomio minimal de $\alpha^{-(q^\ell+1)}$.

Por el Teorema de Delsarte, éste es el código

$$\mathcal{C}_\ell = \left\{ c(\lambda) = \left(\mathrm{Tr}_{q^m/q}(\lambda\alpha^{(q^\ell+1)i})\right)_{i=0}^{n-1} : \lambda \in \mathbb{F}_{q^m} \right\} \tag{3.15}$$

de longitud n con

$$n = \frac{q^m - 1}{(q^m - 1, q^\ell + 1)}.$$

Para conocer explícitamente la longitud del código $\mathcal{C}_\ell$ necesitamos saber el valor de $(q^m - 1, q^\ell + 1)$. Los siguientes lemas calculan exactamente este valor dependiendo de la paridad de q. Sus pruebas son elementales. Denotaremos por v_2 a la valuación 2-ádica.

Lema 3.2.1. *Sea $q = p^s$ con p primo impar, entonces*

$$(q^m - 1, q^\ell + 1) = \begin{cases} q^{(m,\ell)} + 1 & \text{si} \quad v_2(m) > v_2(\ell), \\ 2 & \text{si} \quad v_2(m) \leq v_2(\ell). \end{cases}$$

Lema 3.2.2. *Sea b un entero par, entonces*

$$(b^m - 1, b^\ell + 1) = \begin{cases} b^{(m,\ell)} + 1 & \text{si} \quad v_2(m) > v_2(\ell), \\ 1 & \text{si} \quad v_2(m) \leq v_2(\ell). \end{cases}$$

Por lo tanto, si suponemos que $m_\ell = m/(m,\ell)$ es par, entonces $n = \frac{q^m-1}{q^{(m,\ell)}+1}$, ya que la condición $v_2(m) > v_2(\ell)$ es equivalente a pedir que m_ℓ sea par.

Notar además que en este caso $q^{(m,\ell)}+1 \mid q^m-1$, por el Lema 2.4.3 tenemos que

$$\begin{aligned} M &= n && \text{en característica par,} \\ M_1 = M_2 &= n && \text{en característica impar,} \end{aligned} \tag{3.16}$$

donde M, M_1 y M_2 son los cardinales de los conjuntos T, T_1 y T_2 definidos en (2.31) y (2.32).

El siguiente Lema nos será utíl para ver que ciertas expresiones que aparecerán son enteros.

Lema 3.2.3. *Sea q una potencia de un primo y sean m, ℓ enteros positivos tales que $m_\ell = m/(m,\ell)$ sea par. Entonces*

$$q^{(m,\ell)}+1 \mid q^{\frac{m}{2}} + (-1)^{\frac{1}{2}m_\ell+1}, \qquad q^{(m,\ell)}+1 \mid q^{\frac{m}{2}+(m,\ell)} + (-1)^{\frac{1}{2}m_\ell}$$

Demostración. Notar que como $m_\ell = \frac{m}{(m,\ell)}$ es par, entonces $(m,\ell) = (\frac{m}{2},\ell)$. Por lo tanto $(m,\ell) \mid \frac{m}{2}$. Sean k, t enteros positivos tales que $k \mid t$. Luego, como $q^k \equiv -1 \pmod{q^k+1}$ entonces $(q^k)^{\frac{t}{k}} \equiv (-1)^{\frac{t}{k}} \pmod{q^k+1}$ y por lo tanto

$$q^t \equiv (-1)^{\frac{t}{k}} \pmod{q^k+1}.$$

Tomando $t = \frac{m}{2}$ y $k = (m,\ell)$ obtenemos que

$$q^{\frac{m}{2}} + (-1)^{\frac{1}{2}m_\ell+1} \equiv 0 \pmod{q^{(m,\ell)}+1}$$

como queríamos demostrar. Teniendo en cuenta que $q^{(m,\ell)} \equiv -1 \pmod{q^{(m,\ell)}+1}$, entonces

$$q^{\frac{m}{2}+(m,\ell)} + (-1)^{\frac{1}{2}m_\ell} \equiv 0 \pmod{q^{(m,\ell)}+1}.$$

Concluyendo así la demostración. □

Hay una estrecha relación entre el código irreducible $\mathcal{C}_\ell$ y el código $\mathcal{C}_{\mathcal{L}_\ell}$ definido a partir de la familia de polinomios linealizados $\mathcal{L}_\ell = \langle x^{q^\ell} \rangle$ como en (3.1). Resulta que $\mathcal{C}_{\mathcal{L}_\ell}$ se obtiene tomando $(q^m-1, q^\ell+1) = q^{(m,\ell)}+1$ copias de $\mathcal{C}_\ell$, por lo tanto si $R_{\lambda,\ell}(x) = \lambda x^{q^\ell}$ con $\lambda \in \mathbb{F}_{q^m}$, entonces

$$w(c(\lambda)) = \frac{w(c_{R_{\lambda,\ell}})}{q^{(m,\ell)}+1}.$$

Del mismo modo, podemos considerar los números

$$N_{\lambda,\ell}(c) = \#\left\{0 \le i \le n-1 : \mathrm{Tr}_{q^m/q}(\lambda\alpha^{(q^\ell+1)i}) = c\right\}$$

donde $c \in \mathbb{F}_q^*$, y obtenemos que

$$N_{\lambda,\ell}(c) = \frac{N_{R_{\lambda,\ell}}(c)}{q^{(m,\ell)}+1}.$$

Los Teoremas 2.4.1 y 2.4.2 implican que la familia $\mathcal{L}_\ell$ satisface la propiedad de paridad y como consecuencia del Teorema 3.1.8 obtenemos el siguiente resultado.

Teorema 3.2.4. *Sea q una potencia de un primo. Sean m y ℓ enteros positivos tales que $m_\ell = \frac{m}{(m,\ell)}$ es par. Entonces, $\mathcal{C}_\ell$ es un $[n, m, d]$-código con $n = \frac{q^m-1}{q^{(m,\ell)}+1}$ y $d = n(q-1)d'$ con*

$$d' = \begin{cases} 1 - q^{-\frac{m}{2}} & \text{si } \frac{1}{2}m_\ell \text{ es par,} \\ 1 - q^{(m,\ell)-\frac{m}{2}} & \text{si } \frac{1}{2}m_\ell \text{ es impar.} \end{cases}$$

El enumerador de pesos completo de $\mathcal{C}_\ell$ está dado por:

$$W_{\mathcal{C}_\ell}(z_0, \ldots, z_{q-1}) = z_0^n + n z_0^{a_0} z_1^{a_1} \cdots z_{q-1}^{a_1} + (q^m - 1 - n) z_0^{a'_0} z_1^{a'_1} \cdots z_{q-1}^{a'_1}$$

donde

$$a_0 = n - \tfrac{(q-1)q^{m-1}}{q^{(m,\ell)}+1}(1 + (-1)^{\frac{1}{2}m_\ell} q^{(m,\ell)-\frac{m}{2}}), \qquad a_1 = \tfrac{q^{m-1}}{q^{(m,\ell)}+1}(1 + (-1)^{\frac{1}{2}m_\ell} q^{(m,\ell)-\frac{m}{2}}),$$
$$a'_0 = n - \tfrac{(q-1)q^{m-1}}{q^{(m,\ell)}+1}(1 + (-1)^{\frac{1}{2}m_\ell+1} q^{-\frac{m}{2}}), \qquad a'_1 = \tfrac{q^{m-1}}{q^{(m,\ell)}+1}(1 + (-1)^{\frac{1}{2}m_\ell+1} q^{-\frac{m}{2}}),$$

En particular, $\mathcal{C}_\ell$ tiene enumerador de pesos

$$W_{\mathcal{C}_\ell}(x) = 1 + n x^{(q-1)a_1} + (q^m - 1 - n) x^{(q-1)a'_1}.$$

Por lo tanto el código $\mathcal{C}_\ell$ es $(q-1)$-divisible.

Sabemos que por definición a_i, a'_i deben ser enteros, sin embargo esto no es claro de sus expresiones. Veamos, pues, que este es el caso. Notemos que $a_0 = n - (q-1)a_1$ y $a'_0 = n - (q-1)a'_1$. Por lo tanto, basta probar que a_1 y a'_1 son enteros.

Primero consideremos

$$a'_1 = \tfrac{q^{m-1}}{q^{(m,\ell)}+1}(1 + (-1)^{\frac{1}{2}m_\ell+1} q^{-\frac{m}{2}}) = \tfrac{q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1} q^{\frac{m}{2}-1}}{q^{(m,\ell)}+1} = q^{\frac{m}{2}-1} \tfrac{q^{\frac{m}{2}} + (-1)^{\frac{1}{2}m_\ell+1}}{q^{(m,\ell)}+1}$$

Por Lema 3.2.3, tenemos que $a'_1 \in \mathbb{N}$.

Ahora consideremos

$$a_1 = \tfrac{q^{m-1}}{q^{(m,\ell)}+1}(1 + (-1)^{\frac{1}{2}m_\ell} q^{(m,\ell)-\frac{m}{2}}) = q^{\frac{m}{2}-1} \tfrac{q^{\frac{m}{2}} + (-1)^{\frac{1}{2}m_\ell} q^{(m,\ell)}}{q^{(m,\ell)}+1}$$

Notemos que

$$q^{\frac{m}{2}} + (-1)^{\frac{1}{2}m_\ell} q^{(m,\ell)} = (q^{\frac{m}{2}} + (-1)^{\frac{1}{2}m_\ell+1}) + (-1)^{\frac{1}{2}m_\ell}(q^{(m,\ell)} + 1).$$

Por lo tanto, $q^{(m,\ell)} + 1 \mid q^{\frac{m}{2}} + (-1)^{\frac{1}{2}m_\ell} q^{(m,\ell)}$, mostrando así que a_1 es entero también.

El código $\mathcal{C}_{\ell,0}$

Ahora consideremos el código $\mathcal{C}_{\ell,0}$, cuyo polinomio de chequeo es

$$h_0(x) = (x-1)\, m_{\alpha^{-(2^\ell+1)}}(x)$$

Tabla 3.5: Distribución de pesos de $\mathcal{C}_\ell$.

Pesos posibles	Frecuencias
0	1
$\dfrac{q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1}}{q^{(m,\ell)}+1}$	n
$\dfrac{q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1}}{q^{(m,\ell)}+1}$	$q^m - 1 - n$

donde $m_{\alpha^{-(2^\ell+1)}}(x)$ es el polinomio minimal de $\alpha^{-(2^\ell+1)}$. En este caso, por el Teorema de Delsarte, $\mathcal{C}_{\ell,0}$ es el código traza siguiente

$$\mathcal{C}_{\ell,0} = \left\{ c(\lambda, b) = \left(\mathrm{Tr}_{q^m/q}(\lambda\alpha^{i(q^\ell+1)}) + b\right)_{i=0}^{n-2} : \lambda \in \mathbb{F}_{q^m}, b \in \mathbb{F}_q \right\} \tag{3.17}$$

con

$$n = \frac{q^m - 1}{\delta} \qquad \text{y} \qquad \delta = (q^m - 1, q^\ell + 1).$$

Notar que el código $\mathcal{C}_\ell$ es un subcódigo de $\mathcal{C}_{\ell,0}$, ya que $c(\lambda, b) = c(\lambda)+b$. Si nos restringimos al caso $m_\ell = m/(m,\ell)$ par, obtenemos que $n = \frac{q^m-1}{q^{(m,\ell)}+1}$, por los Lemas 3.2.1 y 3.2.2.

Al igual que sucede con $\mathcal{C}_\ell$ y $\mathcal{C}_{\mathcal{L}_\ell}$, existe la misma relación entre $\mathcal{C}_{\ell,0}$ y $\mathcal{C}_{\mathcal{L}_\ell,0}$ en el sentido que $\mathcal{C}_{\mathcal{L}_\ell,0}$ se obtiene con $(q^m - 1, q^\ell + 1) = q^{(m,\ell)} + 1$ copias de $\mathcal{C}_{\ell,0}$.

Por razonamientos análogos al caso de $\mathcal{C}_\ell$, podemos encontrar la distribución de pesos de $\mathcal{C}_{\ell,0}$ como consecuencia del Teorema 3.1.10.

Teorema 3.2.5. *Sea q una potencia de algún primo. Sean m y ℓ enteros positivos tales que $m_\ell = \frac{m}{(m,\ell)}$ es par. Entonces $\mathcal{C}_{\ell,0}$ es un $[n, m+1, d]$-código, donde*

$$n = \frac{q^m - 1}{q^{(m,\ell)} + 1} \qquad y \qquad d = \frac{q^m - q^{m-1} - d'}{q^{(m,\ell)} + 1}$$

con $d' = q^{\frac{m}{2}+(m,\ell)-1} + 1$ ó $d' = (q-1)q^{\frac{m}{2}+(m,\ell)-1}$ dependiendo si $\frac{1}{2}m_\ell$ es par ó impar, respectivamente. La distribución de pesos de $\mathcal{C}_{\ell,0}$ está dada por la Tabla 3.6.

Demostración. Sean $c(\lambda, b) = c(\lambda) + b$ y $c_{R_{\lambda,b}}$ palabras de $\mathcal{C}_{\ell,0}$ y $\mathcal{C}_{\mathcal{L}_\ell,0}$, respectivamente, donde $\lambda \in \mathbb{F}_{q^m}$, $b \in \mathbb{F}_q$, $R_\lambda(x) = \lambda x^{q^\ell}$ y $\mathcal{L}_\ell = \langle x^{q^\ell} \rangle \subset \mathbb{F}_{q^m}[x]$. Como $\mathcal{C}_{\mathcal{L}_\ell,0}$ se obtiene con $(q^m - 1, q^\ell + 1)$ copias de $\mathcal{C}_{\ell,0}$, tenemos que

$$w(c(\lambda) + b) = \frac{w(c_{R_{\lambda,b}})}{(q^m - 1, q^\ell + 1)},$$

como m_ℓ es par por hipótesis, por los Lemas 3.2.1 y 3.2.2 tenemos que

$$w(c(\lambda) + b) = \frac{w(c_{R_{\lambda,b}})}{q^{(m,\ell)} + 1}.$$

Notar que la forma cuadrática asociada a R_λ es exactamente

$$Q_{R_\lambda}(x) = \mathrm{Tr}_{q^m/q}(\lambda x^{q^\ell+1}) = Q_\lambda(x)$$

donde $Q_{\lambda,\ell}$ es la forma cuadrática (2.30), por lo tanto los Teoremas 2.4.1 y 2.4.2 implican que $\mathcal{L}_\ell$ satisface la propiedad de paridad, por lo tanto el Teorema 3.1.10 implica que para encontrar la distribución de pesos de $\mathcal{C}_{\ell,0}$, sólo basta encontrar el conjunto $R_{\mathcal{L}_\ell}$ así como también los números $M_{r,i}$.

Los Teoremas 2.4.1 y 2.4.2, implican que

$$R_{\mathcal{L}_\ell} = \{m,\, m - 2(m,\ell)\}.$$

Si M, M', M_1, M_1' M_2 y M_2' son los números definidos en (2.33) y (2.34), tenemos que

$$\begin{array}{llll}
M_{m,2} = M_{m-2(m,\ell),1} = 0, & M_{m,1} = M', & M_{m-2(m,\ell),2} = M & \text{si } q \text{ par, } \frac{1}{2}m_\ell \text{ par,} \\
M_{m,1} = M_{m-2(m,\ell),2} = 0, & M_{m-2(m,\ell),1} = M, & M_{m,2} = M' & \text{si } q \text{ par, } \frac{1}{2}m_\ell \text{ impar,} \\
M_{m,2} = M_{m-2(m,\ell),1} = 0, & M_{m,1} = M_1', & M_{m-2(m,\ell),2} = M_1 & \text{si } q \text{ impar, } \frac{1}{2}m_\ell \text{ par,} \\
M_{m,1} = M_{m-2(m,\ell),2} = 0, & M_{m-2(m,\ell),1} = M_2, & M_{m,2} = M_2' & \text{si } q \text{ impar, } \frac{1}{2}m_\ell \text{ impar.}
\end{array}$$

Como m_ℓ es par, entonces $(q^m-1, q^\ell+1) = q^{(m,\ell)}+1$. Como además $q^{(m,\ell)}+1 \mid q^m-1$, el Lema 2.4.3 implica que $M = n$ en característica par y además $M_1 = M_2 = n$ en característica impar.

Teniendo en cuenta que la variación de los tipos de las formas cuadráticas $Q_{\lambda,\ell}$ depende de la paridad de $\frac{1}{2}m_\ell$, esto en términos de la variable i que aparece en las Tablas 3.3 y 3.4 es

$$(-1)^i = \begin{cases} (-1)^{\frac{1}{2}m_\ell} & \text{si } r = m - 2(m,\ell) \\ (-1)^{\frac{1}{2}m_\ell+1} & \text{si } r = m. \end{cases} \tag{3.18}$$

Notar que estas últimas igualdades se dan en cualquier característica. Luego, usando el Teorema 3.1.10 obtenemos la tabla buscada.

Con respecto a los parámetros del código $\mathcal{C}_{\ell,0}$, la longitud del código ya la sabíamos por el Teorema de Delsarte y la dimensión se encuentra calculando el grado del polinomio de chequeo, el cual tiene grado $m+1$. Por último, la distancia del código se encuentra observando la Tabla 3.5. Esto concluye la demostración. □

3.3. La distribución de pesos de $\mathcal{C}_{\ell,1}$ y $\mathcal{C}_{\ell,2}$

Sea α un elemento primitivo de $\mathbb{F}_{q^m}$. Consideremos los polinomios

$$h_1(x)h_2(x) \qquad \text{y} \qquad (x-1)h_1(x)h_2(x),$$

Tabla 3.6: Distribución de pesos de $\mathcal{C}_{\ell,0}$.

Pesos posibles	Frecuencias
0	1
$\frac{q^m-1}{q^{(m,\ell)}+1}$	$q-1$
$\frac{q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1}}{q^{(m,\ell)}+1}$	n
$\frac{q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1}}{q^{(m,\ell)}+1}$	q^m-1-n
$\frac{q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}+(m,\ell)-1}-1}{q^{(m,\ell)}+1}$	$n(q-1)$
$\frac{q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1}-1}{q^{(m,\ell)}+1}$	$(q^m-1-n)(q-1)$

donde $h_1(x)$ y $h_2(x)$ son los polinomios minimales de α^{-1} y $\alpha^{-(q^\ell+1)}$ sobre $\mathbb{F}_q$, respectivamente. Por el Teorema de Delsarte, el código con polinomio de chequeo $h_1(x)h_2(x)$ es

$$\mathcal{C}_{\ell,1}=\left\{c(\beta,\lambda)=\left(\mathrm{Tr}_{q^m/q}(\beta x+\lambda x^{q^\ell+1})\right)_{x\in\mathbb{F}_{q^m}^*}\right\}_{\beta,\lambda\in\mathbb{F}_{q^m}} \tag{3.19}$$

y el código con polinomio de chequeo $(x-1)h_1(x)h_2(x)$ es

$$\mathcal{C}_{\ell,2}=\left\{c(\beta,\lambda)+b=\left(\mathrm{Tr}_{q^m/q}(\beta x+\lambda x^{q^\ell+1})+b\right)_{x\in\mathbb{F}_{q^m}^*}\right\}_{\beta,\lambda\in\mathbb{F}_{q^m},b\in\mathbb{F}_q}. \tag{3.20}$$

Notar que $\mathcal{C}_{\ell,1}=\mathcal{C}_{\mathcal{L}_\ell,1}$ y $\mathcal{C}_{\ell,2}=\mathcal{C}_{\mathcal{L}_\ell,2}$ donde

$$\mathcal{L}_\ell=\langle x^{q^\ell}\rangle\subset\mathbb{F}_{q^m}[x].$$

Por los Teoremas 2.4.1 y 2.4.2 tenemos que $\mathcal{L}_\ell$ satisface la propiedad de paridad cuando $m/(m,\ell)$ es par. Por lo tanto, es posible usar el Teorema 3.1.11 para calcular la distribución de pesos de los códigos $\mathcal{C}_{\ell,1}$ y $\mathcal{C}_{\ell,2}$.

Teorema 3.3.1. *Sea q una potencia de un primo y sean m,ℓ enteros positivos tales que $m_\ell=m/(m,\ell)$ es par. Entonces, las distribuciones de pesos de los códigos $\mathcal{C}_{\ell,1}$ y $\mathcal{C}_{\ell,2}$ están dadas por las Tablas 3.7 y 3.8, donde $n=\frac{q^m-1}{q^{(m,\ell)}+1}$.*

Demostración. Por el Teorema 3.1.11, sólo basta calcular los valores $M_{r,1}$, $M_{r,2}$ y el conjunto $R_{\mathcal{L}_\ell}$ definidos en (3.5) y (3.7). Por el Teorema 2.4.1 y 2.4.2 si m_ℓ es par, entonces

$$R_{\mathcal{L}_\ell}=\{m,\, m-2(m,\ell)\}.$$

Sean T, T_1 y T_2 como en (2.31) y (2.32), sean M, M_1 ,M_2, M', M_1' y M_2' los cardinales de T, T_1 y T_2 y de sus respectivos complementos con respecto a $\mathbb{F}_{q^m}^*$ (ver (2.33) – (2.34)).

En característica par, el Teorema 2.4.1, implica que si $\frac{1}{2}m_\ell$ es par, entonces

$$M_{m,2} = M_{m-2(m,\ell),1} = 0, \quad M_{m,1} = M', \quad M_{m-2(m,\ell),2} = M \quad \text{si } \tfrac{1}{2}m_\ell \text{ es par},$$
$$M_{m,1} = M_{m-2(m,\ell),2} = 0, \quad M_{m-2(m,\ell),1} = M, \quad M_{m,2} = M' \quad \text{si } \tfrac{1}{2}m_\ell \text{ es impar}.$$

Por otro lado, en característica impar, el Teorema 2.4.2 implica que

$$M_{m,2} = M_{m-2(m,\ell),1} = 0, \quad M_{m,1} = M_1', \quad M_{m-2(m,\ell),2} = M_1 \quad \text{si } \tfrac{1}{2}m_\ell \text{ es par},$$
$$M_{m,1} = M_{m-2(m,\ell),2} = 0, \quad M_{m-2(m,\ell),1} = M_2, \quad M_{m,2} = M_2' \quad \text{si } \tfrac{1}{2}m_\ell \text{ es impar}.$$

Por Lema 2.4.3, tenemos que $M = \frac{q^m-1}{(q^m-1,q^\ell+1)}$ y por el Lema 3.2.2, tenemos que

$$M = \frac{q^m-1}{q^{(m,\ell)}+1} = n$$

y además

$$M' = q^m - 1 - \tfrac{q^m-1}{q^{(m,\ell)}+1} = nq^{(m,\ell)}.$$

Por otro lado el Lema 3.2.1, implica que $M_1 = M_2 = n$, ya que en este caso $q^{(m,\ell)}+1 \mid q^m-1$ en característica impar. Además

$$M_1' = M_2' = q^m - 1 - \tfrac{q^m-1}{q^{(m,\ell)}+1} = nq^{(m,\ell)}.$$

Teniendo en cuenta que la variación de los tipos de las formas cuadráticas $Q_{\lambda,\ell}$ depende de la paridad de $\frac{1}{2}m_\ell$, esto en términos de la variable i que aparece en la Tabla 3.2 significa que $(-1)^i$ es como en (3.18). Notar que estas igualdades se dan en cualquier característica. Usando las Tablas 3.3 y 3.4, obtenemos la distribución de pesos de los códigos $\mathcal{C}_{\ell,1}$ y $\mathcal{C}_{\ell,2}$. □

Notar que los pesos del código $\mathcal{C}_{\ell,1}$ sólo dependen de (m,ℓ). Por lo tanto, si $(m,\ell) = 1$, los pesos del código $\mathcal{C}_{\ell,1}$ son exactamente los pesos tomando $\ell = 1$. En el caso binario ($q = 2$), este código es el dual del código BCH 2-corrector.

Corolario 3.3.2. *Sea $q = 2$ y sean m, ℓ enteros positivos tales que m es par y $(m,\ell) = 1$. Entonces la distribución de pesos del código binario $\mathcal{C}_{\ell,1}$ es igual a la distribución de pesos del dual del código BCH 2-corrector.*

Tabla 3.7: La distribución de pesos de $\mathcal{C}_{\ell,1}$.

Pesos posibles	Frecuencias
0	1
$q^m - q^{m-1}$	$n(q^m - q^{m-2(m,\ell)}) + q^m - 1$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1}$	$nq^{(m,\ell)}(q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}-1})$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1}$	$n(q^{m-1-2(m,\ell)} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-(m,\ell)-1})$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1}$	$nq^{(m,\ell)}(q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}-1})(q-1)$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}+(m,\ell)-1}$	$n(q^{m-1-2(m,\ell)} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-(m,\ell)-1})(q-1)$

Tabla 3.8: La distribución de pesos de $\mathcal{C}_{\ell,2}$.

Pesos posibles	Frecuencias
0	1
$q^m - q^{m-1} - 1$	$n(q^m - q^{m-2(m,\ell)})(q-1) + (q^m-1)(q-1)$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1} - 1$	$nq^{(m,\ell)}(q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}-1})(q-1)$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1} - 1$	$n(q^{m-1-2(m,\ell)} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-(m,\ell)-1})(q-1)$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1} - 1$	$nq^{(m,\ell)}(q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1})(q-1)$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}+(m,\ell)-1} - 1$	$n(q^{m-2(m,\ell)} - q^{m-1-2(m,\ell)} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}-(m,\ell)-1})(q-1)$
$q^m - 1$	$q-1$
$q^m - q^{m-1}$	$n(q^m - q^{m-2(m,\ell)}) + q^m - 1$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1}$	$nq^{(m,\ell)}(q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}-1})$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1}$	$n(q^{m-1-2(m,\ell)} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-(m,\ell)-1})$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1}$	$nq^{(m,\ell)}(q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}-1})(q-1)$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}+(m,\ell)-1}$	$n(q^{m-1-2(m,\ell)} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-(m,\ell)-1})(q-1)$

3.4. Otras distribuciones de pesos

En esta sección veremos como aplicar los resultados sobre códigos definidos a partir de familias de polinomios linealizados satisfaciendo la propiedad de paridad, analizando las papers [50] y [51].

3.4.1. Códigos a partir de $\mathcal{L}_{\ell,3\ell}$

Consideremos la familia

$$\mathcal{L}_{\ell,3\ell} = \langle x^{p^\ell}, x^{p^{3\ell}} \rangle \subset \mathbb{F}_{p^m}[x]$$

con p primo impar y $m_\ell = m/(m,\ell)$ par.

En el siguiente teorema resumimos en nuestra notación resultados probados en [50]. Éste nos dice exactamente cómo se distribuyen los rangos y los tipos de las formas cuadráticas definidas a partir de los polinomios linealizados de $\mathcal{L}_{\ell,3\ell}$.

Teorema 3.4.1 ([50]). *Sea p un primo impar y sean m, ℓ enteros, tales que $m_\ell = m/(m,\ell)$ es par con $m > 6\ell$. Consideremos $R_{\mathcal{L}_{\ell,3\ell}}$ como en (3.7) y denotemos $\delta = (m,\ell)$, entonces*

$$R_{\mathcal{L}_{\ell,3\ell}} = \{m, m-2\delta, m-4\delta, m-6\delta\} \tag{3.21}$$

Por lo tanto $\mathcal{L}_{\ell,3\ell}$ es una familia de paridad. Además los $M_{r,i}$ tienen las siguientes expresiones dependiendo de la paridad de $\frac{1}{2}m_\ell$:

- *Si* $\frac{1}{2}m_\ell$ *es impar. Entonces* $M_{m,1} = M_{m-2\delta,2} = M_{m-4\delta,1} = M_{m-6\delta,2} = 0$ *y*

$$M_{m,2} = \frac{p^{2m+6\delta}-p^{2m+4\delta}-p^{2m+\delta}+p^{m+4\delta}+p^{m+\delta}-p^{6\delta}-p^{\frac{3m}{2}+5\delta}+p^{\frac{3m}{2}+4\delta}+p^{\frac{m}{2}+5\delta}-p^{\frac{m}{2}+4\delta}}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

$$M_{m-2\delta,1} = \frac{p^{2m-2\delta}(p^{7\delta}-p^{2\delta}-1)+p^{m-2\delta}(p^{5\delta}-p^{6\delta}+p^{2\delta}+1)-p^{3\delta}(p^{2\delta}-p^{\delta}+1)+(p^{\frac{3m}{2}}-p^{\frac{m}{2}})(\sum_{i=0}^{5}(-1)^{i+1}p^{i\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

$$M_{m-4\delta,2} = \frac{p^{2m-3\delta}(p^{5\delta}+p^{\delta}-1)-p^{m-3\delta}(p^{6\delta}+p^{4\delta}+p^{\delta}-1)+p^{\delta}(p^{2\delta}-p^{\delta}+1)-(p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-2\delta})(\sum_{i=0}^{5}(-1)^{i+1}p^{i\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

$$M_{m-6\delta,1} = \frac{p^{2m-3\delta}-p^{m}-p^{m-3\delta}+1+p^{\frac{3m}{2}-\delta}-p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-\delta}+p^{\frac{m}{2}-2\delta}}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

- *Si* $\frac{1}{2}m_\ell$ *es par. Entonces* $M_{m,2} = M_{m-2\delta,1} = M_{m-4\delta,2} = M_{m-6\delta,1} = 0$ *y*

$$M_{m,2} = \frac{p^{2m+6\delta}-p^{2m+4\delta}-p^{2m+\delta}+p^{m+4\delta}+p^{m+\delta}-p^{6\delta}+p^{\frac{3m}{2}+5\delta}-p^{\frac{3m}{2}+4\delta}-p^{\frac{m}{2}+5\delta}+p^{\frac{m}{2}+4\delta}}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

$$M_{m-2\delta,2} = \frac{p^{2m-2\delta}(p^{7\delta}-p^{2\delta}-1)+p^{m-2\delta}(p^{5\delta}-p^{6\delta}+p^{2\delta}+1)-p^{3\delta}(p^{2\delta}-p^{\delta}+1)-(p^{\frac{3m}{2}}-p^{\frac{m}{2}})(\sum_{i=0}^{5}(-1)^{i+1}p^{i\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

$$M_{m-4\delta,1} = \frac{p^{2m-3\delta}(p^{5\delta}+p^{\delta}-1)-p^{m-3\delta}(p^{6\delta}+p^{4\delta}+p^{\delta}-1)+p^{\delta}(p^{2\delta}-p^{\delta}+1)+(p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-2\delta})(\sum_{i=0}^{5}(-1)^{i+1}p^{i\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

$$M_{m-6d,2} = \frac{p^{2m-3\delta}-p^{m}-p^{m-3\delta}+1-p^{\frac{3m}{2}-\delta}+p^{\frac{3m}{2}-2\delta}+p^{\frac{m}{2}-\delta}-p^{\frac{m}{2}-2\delta}}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

En el mencionado trabajo [50], las distribuciones de rangos del teorema anterior fueron usadas para calcular los espectros de los códigos $\mathcal{C}_{\mathcal{L}_{\ell,3\ell}}$ y $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},1}$. Sin embargo, como ya vimos en la primera sección del capítulo, esta información es suficiente también para calcular el espectro de $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},0}$ y $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},2}$.

Para calcular dichos espectros, será conveniente usar las siguientes notaciones

$$R_0 = \frac{p^{2m+6\delta}-p^{2m+4\delta}-p^{2m+\delta}+p^{m+4\delta}+p^{m+\delta}-p^{6\delta}+(-1)^{\frac{m_\ell}{2}}(p^{\frac{3m}{2}+5\delta}-p^{\frac{3m}{2}+4\delta}-p^{\frac{m}{2}+5\delta}+p^{\frac{m}{2}+4\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

$$R_1 = \frac{p^{2m-2\delta}(p^{7\delta}-p^{2\delta}-1)+p^{m-2\delta}(p^{5\delta}-p^{6\delta}+p^{2\delta}+1)-p^{3\delta}(p^{2\delta}-p^{\delta}+1)+(-1)^{\frac{m_\ell}{2}+1}(p^{\frac{3m}{2}}-p^{\frac{m}{2}})(\sum_{i=0}^{5}(-1)^{i+1}p^{i\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

$$R_2 = \frac{p^{2m-3\delta}(p^{5\delta}+p^{\delta}-1)-p^{m-3\delta}(p^{6\delta}+p^{4\delta}+p^{\delta}-1)+p^{\delta}(p^{2\delta}-p^{\delta}+1)+(-1)^{\frac{m_\ell}{2}}(p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-2\delta})(\sum_{i=0}^{5}(-1)^{i+1}p^{i\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

$$R_3 = \frac{p^{2m-3\delta}-p^{m}-p^{m-3\delta}+1+(-1)^{\frac{m_\ell}{2}+1}(p^{\frac{3m}{2}-\delta}-p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-\delta}+p^{\frac{m}{2}-2\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}$$

Teorema 3.4.2. *Sea* p *un primo impar y sean* m, ℓ *enteros positivos tales que* $m_\ell = m/(m,\ell)$ *es par con* $m > 6\ell$*. Entonces, las distribuciones de pesos de los códigos* $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},0}$ *y* $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},2}$ *están dadas por las Tablas 3.9 y 3.10, donde los* R_i*,* $i = 0, \ldots, 3$*, son como arriba.*

Nota. La distribución de los códigos $\mathcal{C}_{\mathcal{L}_{\ell,3\ell}}$ y $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},1}$ pueden ser encontradas en las tablas 3.9 y 3.10. Más precisamente la distribución de pesos de $\mathcal{C}_{\mathcal{L}_{\ell,3\ell}}$ son las primeras 5 filas de la tabla 3.9, mientras que el espectro de $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},1}$ está dado por las primeras 10 filas de la tabla 3.10.

Tabla 3.9: Distribución de pesos de $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},0}$.

Pesos posibles	Frecuencias
0	1
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}-1}$	R_0
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}+(m,\ell)-1}$	R_1
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}+2(m,\ell)-1}$	R_2
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}+3(m,\ell)-1}$	R_3
$p^m - 1$	$p-1$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-1} - 1$	$(p-1)R_0$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}+(m,\ell)-1} - 1$	$(p-1)R_1$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}+2(m,\ell)-1} - 1$	$(p-1)R_2$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}+3(m,\ell)-1} - 1$	$(p-1)R_3$

Tabla 3.10: Distribución de pesos de $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},2}$.

Pesos posibles	Frecuencias
0	1
$p^m - p^{m-1}$	$p^m - 1 + \sum_{i=0}^{3} R_i(p^m - p^{m-i(m,\ell)})$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}-1}$	$(p^{m-1} + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}-1})R_0$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}+(m,\ell)-1}$	$(p^{m-2(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}-(m,\ell)-1})R_1$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}+2(m,\ell)-1}$	$(p^{m-4(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}-2(m,\ell)-1})R_2$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}+3(m,\ell)-1}$	$(p^{m-6(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}-3(m,\ell)-1})R_3$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-1}$	$(p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}-1})(p-1)R_0$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}+(m,\ell)-1}$	$(p^{m-2(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-(m,\ell)-1})(p-1)R_1$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}+2(m,\ell)-1}$	$(p^{m-4(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}-2(m,\ell)-1})(p-1)R_2$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}+3(m,\ell)-1}$	$(p^{m-6(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-3(m,\ell)-1})(p-1)R_3$
$p^m - 1$	$p-1$
$p^m - p^{m-1} - 1$	$(p-1)(p^m - 1 + \sum_{i=0}^{3} R_i(p^m - p^{m-i(m,\ell)}))$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}-1}$	$(p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}-1})(p-1)R_0$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}+(m,\ell)-1}$	$(p^{m-2(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-(m,\ell)-1})(p-1)R_1$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}+2(m,\ell)-1}$	$(p^{m-4(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}-2(m,\ell)-1})(p-1)R_2$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}+3(m,\ell)-1}$	$(p^{m-6(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-3(m,\ell)-1})(p-1)R_3$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-1}$	$(p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-1})(p-1)R_0$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}+(m,\ell)-1}$	$(p^{m-2(m,\ell)} - p^{m-2(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}-(m,\ell)-1})(p-1)R_1$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}+2(m,\ell)-1}$	$(p^{m-4(m,\ell)} - p^{m-4(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-2(m,\ell)-1})(p-1)R_2$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}+3(m,\ell)-1}$	$(p^{m-6(m,\ell)} - p^{m-6(m,\ell)-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}-3(m,\ell)-1})(p-1)R_3$

Capítulo 4

Optimalidad

En este capítulo vamos a ver que el código $\mathcal{C}_{\ell,1}$ introducido anteriormente, permite construir objetos optimales en diferentes sentidos. Por una parte, veremos que en el caso binario el código dual de $\mathcal{C}_{\ell,1}$ es óptimo, en el sentido que su distancia mínima es la mayor distancia posible dentro de la clase de códigos con ceros α^{-1}, α^{-i} ([6]). Por otra parte, usando los pesos del código $\mathcal{C}_{\ell,1}$ veremos que cuando $\ell \mid m$, la curva algebraica definida sobre $\mathbb{F}_{p^m}$ con ecuación afín

$$y^p - y = \lambda x^{p^\ell+1} + \beta x$$

es optimal en el sentido de Hasse-Weil, es decir que la curva satisface la igualdad en la cota de Hasse-Weil.

4.1. Optimalidad de $\mathcal{C}_{\ell,1}^\perp$ en términos de distancia

En esta sección vamos a suponer que $p = q = 2$ y $n = 2^m - 1$. Sea α un elemento primitivo de $\mathbb{F}_{2^m}$. Definimos como $\mathcal{C}(r,s)$ al código cíclico binario con polinomio generador

$$m(x) = m_{\alpha^r}(x) m_{\alpha^s}(x),$$

donde r y s son enteros positivos con $m_{\alpha^r} \neq m_{\alpha^s}$. Notar que el dual de este código, por el teorema de Delsarte, es

$$\mathcal{C}' = \mathcal{C}(r,s)^\perp = \left\{ c(\lambda,\beta) = \left(\mathrm{Tr}_{2^m/2}(\lambda x^r + \beta x^s)\right)_{x \in \mathbb{F}_{2^m}^*} : \lambda, \beta \in \mathbb{F}_{2^m} \right\},$$

si suponemos que $(r, s, 2^m - 1) = 1$. El siguiente Lema nos dice cuáles son los valores de la distancia mínima de estos códigos.

Lema 4.1.1. *Sea $\mathcal{C}(r,s)$ el código cíclico binario con polinomio generador $m_{\alpha^r}(x) m_{\alpha^s}(x)$ con $r, s \in \mathbb{N}$ y sea d su distancia mínima. Entonces,*

$$2 \leq d \leq 5.$$

Además, $d = 2$ si y sólo si $(r, s, 2^m - 1) > 1$.

Por lo tanto, si consideramos el código $\mathcal{C}(1,i)$ con polinomio generador

$$m(x) = m_\alpha(x)\, m_{\alpha^i}(x)$$

con $i \in \mathbb{N}$, su distancia mínima d satisface que $3 \leq d \leq 5$.

Van Lint y Wilson probaron que si $(i,m) > 1$ y m es impar entonces la distancia de $\mathcal{C}(1,i)$ es a lo más 4. Ellos, además, probaron que en general la mayoría de los códigos de este tipo tienen distancia menor o igual a 4 ([45], [46]).

Se conocen pocas familias de códigos $\mathcal{C}(1,i)$ con distancia 5. Entre las más conocidas se encuentran los códigos de Melas, que se obtienen al tomar $i = -1$. Otras clases conocidas se deben a Kasami ([25], [26]). Kasami probó que si m es impar y $(m,\ell) = 1$ entonces $\mathcal{C}(1,i)$ tiene distancia mínima 5 para

$$i = 2^\ell + 1 \qquad \text{e} \qquad i = 2^{2\ell} - 2^\ell + 1.$$

Luego, Janwa ([24], [23]) extendió el resultado de Kasami para m par, en el caso en que $i = 2^{2\ell} - 2^\ell + 1$.

Veamos que si m par e $i = 2^\ell + 1$, el código $\mathcal{C}(1,i)$ tiene distancia mínima 5. Para ello, consideramos el Teorema 3.3.1. En dicho teorema calculamos la distribución de pesos del código dual de $\mathcal{C}(1,i)$ con $i = 2^\ell + 1$ cuando $m_\ell = m/(m,\ell)$ es par. Notar que en este caso la Tabla 3.6 es independiente de la paridad de $\frac{1}{2}m_\ell$.

Cuando $(m,\ell) = 1$, la tabla de pesos y frecuencias de $\mathcal{C}_{\ell,1}$ es:

Pesos posibles	Frecuencias
0	1
2^{m-1}	$(2^m-1)(2^{m-2}+1)$
$2^{m-1} - 2^{\frac{m}{2}-1}$	$\frac{2}{3}(2^m-1)(2^{m-1}+2^{\frac{m}{2}-1})$
$2^{m-1} + 2^{\frac{m}{2}}$	$\frac{1}{3}(2^m-1)(2^{m-3}-2^{\frac{m}{2}-2})$
$2^{m-1} + 2^{\frac{m}{2}-1}$	$\frac{2}{3}(2^m-1)(2^{m-1}+2^{\frac{m}{2}-1})$
$2^{m-1} - 2^{\frac{m}{2}}$	$\frac{1}{3}(2^m-1)(2^{m-3}+2^{\frac{m}{2}-2})$

Se puede probar que el código $\mathcal{C}_{\ell,1}$ tiene dimensión $k = 2m$ cuando $\ell \neq \frac{m}{2}$, viendo que el tamaño de la 2-coclase ciclotómica de $2^\ell + 1$ tiene tamaño m, en este caso.

Por lo tanto, si suponemos que $(m,\ell) = 1$, tenemos que $k = 2m$.

Sea P_i el i-ésimo momento de potencia de $\mathcal{C}_{\ell,1}$ definido en (1.1). Como $A_1^\perp = A_2^\perp = 0$, de

(1.2) tenemos

$$\begin{aligned}
P_1 &= \sum_{j=0}^{n} jA_j = 2^{k-1}n, \\
P_2 &= \sum_{j=0}^{n} j^2A_j = 2^{k-2}n(n+1), \\
P_3 &= \sum_{j=0}^{n} j^3A_j = 2^{k-3}\{(n^2(n+3) - 6A_3^{\perp}\}, \\
P_4 &= \sum_{j=0}^{n} j^4A_j = 2^{k-4}\{(n(n+1)(n^2+5n-2) - 24(nA_3^{\perp} + A_4^{\perp})\}.
\end{aligned} \tag{4.1}$$

Se puede verificar que los pesos w, y la cantidad A_w de palabras de peso w en $\mathcal{C}_{\ell,1}$ satisfacen la igualdad en los primeros dos momentos. Veamos qué sucede con los momentos tercero y cuarto. Luego

$$\begin{aligned}
P_3 &= (2^m-1)(2^{4m-5}+2^{3m-3}) \\
&\quad +\tfrac{(2^m-1)}{3}(2^{2m-1}-2^{m-1})\{(2^{m-1}-2^{\frac{m}{2}-1})^2+(2^{m-1}+2^{\frac{m}{2}-1})^2\} \\
&\quad +\tfrac{(2^m-1)}{3}(2^{4m-5}-2^{2m-1}) \\
&= (2^m-1)(2^{4m-5}+2^{3m-3}) + \tfrac{(2^m-1)}{3}(2^{2m-1}-2^{m-1})(2^{2m-1}+2^{m-1}) \\
&\quad +\tfrac{(2^m-1)}{3}(2^{4m-5}-2^{2m-1}) \\
&= (2^m-1)(2^{4m-5}+2^{3m-3}+\tfrac{2^{4m-2}}{3}-\tfrac{2^{2m-2}}{3}+\tfrac{2^{4m-5}}{3}-\tfrac{2^{2m-1}}{3}) \\
&= (2^m-1)(2^{4m-3}+2^{3m-3}-2^{2m-2}) \\
&= 2^{k-3}n^2(n+3).
\end{aligned}$$

Por lo tanto, $A_3^{\perp} = 0$.

Ahora sólo resta ver qué sucede con el cuarto momento. Tenemos

$$\begin{aligned}
P_4 &= (2^m-1)(2^{5m-6}+2^{4m-4}) \\
&\quad +\tfrac{(2^m-1)}{3}(2^{2m-1}-2^{m-1})\{(2^{m-1}-2^{\frac{m}{2}-1})^3+(2^{m-1}+2^{\frac{m}{2}-1})^3\} \\
&\quad +\tfrac{(2^m-1)}{3}(2^{5m-6}+2^{4m-3}-3\cdot 2^{3m-2}) \\
&= (2^m-1)(2^{5m-6}+2^{4m-4}) + \tfrac{(2^m-1)}{3}(2^{2m-1}-2^{m-1})(2^{3m-2}+3\cdot 2^{2m-2}) \\
&\quad +\tfrac{(2^m-1)}{3}(2^{5m-6}+2^{4m-3}-3\cdot 2^{3m-2}) \\
&= (2^m-1)(2^{5m-6}+2^{4m-4}+\tfrac{2^{5m-3}}{3}+\tfrac{2^{5m-6}}{3}+2^{4m-3}-2^{3m-3}-2^{3m-2}) \\
&= (2^m-1)(2^{5m-4}+3\cdot 2^{4m-4}-3\cdot 2^{3m-3}) \\
&= 2^m 2^{2m-4}(2^m-1)(2^{2m}+3\cdot 2^m-6).
\end{aligned}$$

Por otro lado, se puede verificar que

$$2^{k-4}n(n+1)(n^2+5n-2) = 2^m 2^{2m-4}(2^m-1)(2^{2m}+3\cdot 2^m-6),$$

de donde sale que $A_4^{\perp} = 0$.

De este modo, llegamos al siguiente resultado.

Teorema 4.1.2. *Sean m y ℓ enteros positivos tales que $(m, \ell) = 1$. Entonces el código dual del código cíclico binario $\mathcal{C}_{\ell,1}$ es optimal.*

Este último teorema implica que la función $F(x) = x^{2^\ell+1}$, usada para construir el cero $\alpha^{-(2^\ell+1)}$ del código, es una función Booleana especial llamada APN ([4]). En el Capítulo 5 veremos en más profundidad este tipo de funciones y las usaremos para construir grafos de Ramanujan, que son objetos optimales en otro sentido.

4.2. Curvas optimales a partir de $\mathcal{C}_{\ell,1}$

En esta sección, veremos cómo encontrar curvas optimales por medio de $\mathcal{C}_{\ell,1}$. En [34] se pueden encontrar los principales resultados de curvas algebraicas sobre cuerpos finitos que usaremos, tales como la clásica cota de Hasse Weil, el operador de Frobenius y la fórmula de género de Riemann-Hurwitz-Zeuthen.

Puntos racionales de curvas asociadas a $\mathcal{C}_{\ell,1}$

Consideremos el código cíclico

$$\mathcal{C}_{\ell,1} = \left\{ c(\lambda, \beta) = \left(\mathrm{Tr}_{p^m/p}(\lambda x^{p^\ell+1} + \beta x)\right)_{x \in \mathbb{F}_{p^m}^*} : \lambda, \beta \in \mathbb{F}_{p^m} \right\}$$

El Teorema 90 de Hilbert nos dice que en general

$$\mathrm{Tr}_{p^m/p}(z) = 0 \quad \Longleftrightarrow \quad \exists y \in \mathbb{F}_{p^m} : \; y^p - y = z.$$

Sea

$$f(x) = \lambda x^{p^\ell+1} + \beta x,$$

con $\lambda \neq 0$, como el grado de $f(x)$ es coprimo con p, entonces el polinomio en dos variables

$$y^p - y - f(x) \in \mathbb{F}_{p^m}[x, y]$$

es absolutamente irreducible y por lo tanto el conjunto algebraico con ecuación afín

$$C_{\lambda,\beta}^{\ell} : \; y^p - y = \lambda x^{p^\ell+1} + \beta x, \tag{4.2}$$

es irreducible y, en consecuencia, define una curva algebraica. A este tipo de curvas se las conoce como curvas de Artin-Schreier. El Teorema 90 de Hilbert nos da una relación directa entre los pesos del códigos $\mathcal{C}_{\ell,1}$ y la cantidad de puntos $\mathbb{F}_{p^m}$-racionales de $C_{\lambda,\beta}^{\ell}$. Más precisamente, se tiene el siguiente resultado.

Lema 4.2.1. *Sea $c(\lambda,\beta)$ una palabra de $\mathcal{C}_{\ell,1}$ tal que $\lambda \neq 0$ y sea $\#C^{\ell}_{\lambda,\beta}(\mathbb{F}_{p^m})$ la cantidad de puntos $\mathbb{F}_{p^m}$-racionales de la curva $C^{\ell}_{\lambda,\beta}$ definida en (4.2). Entonces,*

$$w(c(\lambda,\beta)) = p^m - \frac{\#C^{\ell}_{\lambda,\beta}(\mathbb{F}_{p^m}) - 1}{p}.$$

Demostración. Supongamos que $\lambda \neq 0$. Luego, por definición

$$w(c(\lambda,\beta)) = p^m - 1 - \#\{x \in \mathbb{F}^*_{p^m} : \mathrm{Tr}_{p^m/p}(\lambda x^{p^\ell+1} + \beta x) = 0\}.$$

Por Teorema 90 de Hilbert se tiene

$$\mathrm{Tr}_{p^m/p}(\lambda x^{p^\ell+1} + \beta x) = 0 \quad \Longleftrightarrow \quad \exists y \in \mathbb{F}_{p^m} : y^p - y = \lambda x^{p^\ell+1} + \beta x.$$

Ahora, analicemos la ecuación $y^p - y = \lambda x^{p^\ell+1} + \beta x$. Como $\deg(\lambda x^{p^\ell+1} + \beta x) = p^\ell + 1$ es coprimo con p, el polinomio $y^p - y - (\lambda x^{p^\ell+1} + \beta x)$ define una curva de Artin-Schreier (ver (4.2)). Se sabe que estas curvas son un cubrimiento de p-hojas de $\mathbb{P}^1$. Esto quiere decir que dado x, existen o bien p-valores de y o bien ningún valor de y satisfaciendo

$$y^p - y = \lambda x^{p^\ell+1} + \beta x.$$

Si consideramos $x = 0$ en la ecuación, entonces obtenemos que $y^p - y = 0$. Como elevar a la p es exactamente el automorfismo de Frobenius, obtenemos que $y^p = y$ en $\mathbb{F}_{p^m}$ si y sólo si $y \in \mathbb{F}_p$.

Teniendo en cuenta que esta curva tiene a ∞ como punto racional y este no se corresponde a ningún x satisfaciendo

$$\mathrm{Tr}_{p^m/p}(\lambda x^{p^\ell+1} + \beta x) = 0,$$

luego, el Teorema 90 de Hilbert implica que

$$\#C^{\ell}_{\lambda,\beta}(\mathbb{F}_{p^m}) = p(\#\{x \in \mathbb{F}^*_{p^m} : \mathrm{Tr}_{p^m/p}(\lambda x^{p^\ell+1} + \beta x) = 0\}) + p + 1.$$

Por lo tanto

$$w(c(\lambda,\beta)) = p^m - \frac{\#C^{\ell}_{\lambda,\beta}(\mathbb{F}_{p^m}) - 1}{p},$$

como queríamos demostrar. □

Como consecuencia del Teorema 3.3.1 obtenemos

Teorema 4.2.2. *Sea p primo y m, ℓ enteros positivos tales que $m_\ell = m/(m,\ell)$ sea par. Consideremos la curva $C^{\ell}_{\lambda,\beta}$ como en (4.2), donde $\lambda \in \mathbb{F}^*_{p^m}, \beta \in \mathbb{F}_{p^m}$. Escribimos $\lambda = \alpha^t$, donde α es un elemento primitivo de $\mathbb{F}_{p^m}$. Luego*

- *Si $p > 2$, $\frac{1}{2}m_\ell$ es par y $t \equiv 0 \pmod{p^{(m,\ell)}+1}$, entonces*

$$\#C^{\ell}_{\lambda,\beta}(\mathbb{F}_{p^m}) = \begin{cases} p^m + 1 & \text{para } p^m - p^{m-2(m,\ell)} \ \beta'\text{s}, \\ p^m + 1 - p^{(m,\ell)}(p-1)\sqrt{p^m} & \text{para } p^{m-2(m,\ell)-1} - (p-1)p^{\frac{m}{2}-(m,\ell)-1} \ \beta'\text{s}, \\ p^m + 1 + p^{(m,\ell)}\sqrt{p^m} & \text{para } (p^{m-2(m,\ell)-1} + p^{\frac{m}{2}-(m,\ell)-1})(p-1)\beta'\text{s}. \end{cases}$$

- *Si* $p > 2$, $\frac{1}{2}m_\ell$ *es par y* $t \not\equiv 0 \pmod{p^{(m,\ell)}+1}$, *entonces*

$$\#C^\ell_{\lambda,\beta}(\mathbb{F}_{p^m}) = \begin{cases} p^m + 1 + (p-1)\sqrt{p^m} & \text{para } p^{m-1} + (p-1)p^{\frac{m}{2}} \ \beta'\text{s}, \\ p^m + 1 - \sqrt{p^m} & \text{para } (p-1)(p^{m-1} - p^{\frac{m}{2}-1}) \ \beta'\text{s}. \end{cases}$$

- *Si* $p > 2$, $\frac{1}{2}m_\ell$ *es impar y* $t \equiv \frac{p^{(m,\ell)}+1}{2} \pmod{p^{(m,\ell)}+1}$, *entonces*

$$\#C^\ell_{\lambda,\beta}(\mathbb{F}_{p^m}) = \begin{cases} p^m + 1 & \text{para } p^m - p^{m-2(m,\ell)} \ \beta'\text{s}, \\ p^m + 1 + p^{(m,\ell)}(p-1)\sqrt{p^m} & \text{para } p^{m-2(m,\ell)-1} + (p-1)p^{\frac{m}{2}-(m,\ell)-1} \ \beta'\text{s}, \\ p^m + 1 - p^{(m,\ell)}\sqrt{p^m} & \text{para } (p^{m-2(m,\ell)-1} - p^{\frac{m}{2}-(m,\ell)-1})(p-1)\beta'\text{s}. \end{cases}$$

- *Si* $p > 2$, $\frac{1}{2}m_\ell$ *es impar y* $t \not\equiv \frac{p^{(m,\ell)}+1}{2} \pmod{p^{(m,\ell)}+1}$ *entonces*

$$\#C^\ell_{\lambda,\beta}(\mathbb{F}_{p^m}) = \begin{cases} p^m + 1 - (p-1)\sqrt{p^m} & \text{para } p^{m-1} - (p-1)p^{\frac{m}{2}-1} \ \beta'\text{s}, \\ p^m + 1 + \sqrt{p^m} & \text{para } (p^{m-1} + p^{\frac{m}{2}-1})(p-1) \ \beta'\text{s}. \end{cases}$$

- *Si* $p = 2$ *y* λ *es una potencia* $(2^\ell+1)$*-ésima en* $\mathbb{F}_{2^m}$, *entonces*

$$\#C^\ell_{\lambda,\beta}(\mathbb{F}_{2^m}) = \begin{cases} 2^m + 1 & \text{para } 2^m - 2^{m-2(m,\ell)} \ \beta'\text{s}, \\ 2^m + 1 - 2^{(m,\ell)}\sqrt{2^m} & \text{para } 2^{m-2(m,\ell)-1} - 2^{\frac{m}{2}-(m,\ell)-1} \ \beta'\text{s}, \\ 2^m + 1 + 2^{(m,\ell)}\sqrt{2^m} & \text{para } 2^{m-2(m,\ell)-1} + 2^{\frac{m}{2}-(m,\ell)-1}\beta'\text{s}. \end{cases}$$

- *Si* $p = 2$ *y* λ *no es una potencia* $(2^\ell+1)$*-ésima en* $\mathbb{F}_{2^m}$ *entonces*

$$\#C^\ell_{\lambda,\beta}(\mathbb{F}_{2^m}) = \begin{cases} 2^m + 1 + \sqrt{2^m} & \text{para } 2^{m-1} + 2^{\frac{m}{2}-1} \ \beta'\text{s}, \\ 2^m + 1 - \sqrt{2^m} & \text{para } 2^{m-1} - 2^{\frac{m}{2}-1} \ \beta'\text{s}. \end{cases}$$

Demostración. Es inmediata del Lema 4.2.1 anterior, de la tabla dada por el Teorema 3.3.1 tomando en estos $q = p$, y por último de los Lemas 2.4.1 y 2.4.2 para conocer la forma que debe tener λ en cada caso. □

Traza del operador de Frobenius

De la teoría de curvas de Artin-Schreier las cantidades $\#C^\ell_{\lambda,\beta}(\mathbb{F}_{p^m})$ se pueden poner en término de la traza del operador de Frobenius tr_F actuando en los grupos de cohomología étale $H^1_{et}(C^\ell_{\lambda,\beta}, \mathbb{Q}_j)$ con $j \neq p$ primo, esto es

$$\#C^\ell_{\lambda,\beta}(\mathbb{F}_{p^m}) = p^m + 1 + tr_F.$$

Por lo tanto, se obtienen los valores y las frecuencias de la traza de Frobenius.

Corolario 4.2.3. *Sea tr_F la traza del operador de Frobenius actuando en los grupos de cohomología $H^1_{et}(C^\ell_{\lambda,\beta}, \mathbb{Q}_j)$ con $j \neq p$ primo, donde $C^\ell_{\lambda,\beta}$ es como en (4.2), $\lambda \neq 0$ y escribimos $\lambda = \alpha^t$ con α un elemento primitivo de $\mathbb{F}_{p^m}$. Si $m_\ell = m/(m,\ell)$ es par, entonces tr_F tiene los siguientes valores:*

- *Si $p > 2$ y $\frac{1}{2}m_\ell$ es par, entonces*

$$tr_F = \begin{cases} -(p-1)p^{\frac{m}{2}+(m,\ell)} & \text{si } t \equiv 0 \pmod{p^{(m,\ell)}+1}, \\ (p-1)p^{\frac{m}{2}} & \text{si } t \not\equiv 0 \pmod{p^{(m,\ell)}+1}. \end{cases}$$

- *Si $p > 2$ y $\frac{1}{2}m_\ell$ es impar, entonces*

$$tr_F = \begin{cases} (p-1)p^{\frac{m}{2}+(m,\ell)} & \text{si } t \equiv \frac{p^{(m,\ell)}+1}{2} \pmod{p^{(m,\ell)}+1}, \\ -(p-1)p^{\frac{m}{2}} & \text{si } t \not\equiv \frac{p^{(m,\ell)}}{2} \pmod{p^{(m,\ell)}+1}. \end{cases}$$

- *Si $p = 2$ y $\frac{1}{2}m_\ell$ es par, entonces*

$$tr_F = \begin{cases} -2^{\frac{m}{2}+(m,\ell)} & \text{si } \lambda \in T, \\ 2^{\frac{m}{2}} & \text{si } \lambda \notin T. \end{cases}$$

- *Si $p = 2$ y $\frac{1}{2}m_\ell$ es impar, entonces*

$$tr_F = \begin{cases} 2^{\frac{m}{2}+(m,\ell)} & \text{si } \lambda \in T, \\ -2^{\frac{m}{2}} & \text{si } \lambda \notin T. \end{cases}$$

Aquí, T es el conjunto de potencias $(2^\ell+1)$-ésimas de $\mathbb{F}_{2^m}$ definido en (2.31).

Una familia de curvas optimales

La fórmula del género de Riemann-Hurwitz, nos dice que el género de la curva de Artin-Schreier con ecuación afín

$$C_f : \quad y^p - y = f(x)$$

donde $f(x) \in \mathbb{F}_{p^m}[x]$ y $(\deg f, p) = 1$ es

$$g = \tfrac{1}{2}(\deg f - 1)(p-1).$$

Por lo tanto, el género de la curva $C^\ell_{\lambda,\beta}$ es

$$g = \tfrac{1}{2}p^\ell(p-1)$$

para todo $\lambda \neq 0$ y $\beta \in \mathbb{F}_{p^m}$. Analizando la cantidad de puntos $\mathbb{F}_{p^m}$-racionales dados por el teorema anterior es posible encontrar curvas maximales y minimales, es decir curvas que cumplen la igualdad en la cota de la desigualdad de Hasse-Weil. Recordemos que esta nos dice que

$$p^m + 1 - 2g\sqrt{p^m} \leq \#C^\ell_{\lambda,\beta}(\mathbb{F}_{p^m}) \leq p^m + 1 + 2g\sqrt{p^m}. \tag{4.3}$$

Teorema 4.2.4. *Sea p primo y ℓ un divisor de m tal que m/ℓ es par. Para $\lambda \in \mathbb{F}_{p^m}^*$, escribamos $\lambda = \alpha^t$, donde α es un elemento primitivo de $\mathbb{F}_{p^m}$. Luego, se tiene lo siguiente*

- *Si $p > 2$ entonces:*
  - *(a) La curva $C_{\lambda,\beta}^{\ell}$ es minimal si $m/2\ell$ es par y $t \equiv 0 \pmod{p^{(m,\ell)}+1}$ para un número $p^{m-2\ell-1} - (p-1)p^{\frac{m}{2}-\ell-1}$ de β's posibles.*
  - *(b) La curva $C_{\lambda,\beta}^{\ell}$ es maximal si $m/2\ell$ es impar $t \equiv \frac{p^{(m,\ell)}+1}{2} \pmod{p^{(m,\ell)}+1}$ para un número $p^{m-2\ell-1} + (p-1)p^{\frac{m}{2}-\ell-1}$ de β's posibles.*
- *Si $p = 2$ y λ es una potencia $(2^\ell+1)$-ésima de $\mathbb{F}_{2^m}$, entonces:*
  - *(a) Hay una cantidad $2^{m-2\ell-1} - 2^{\frac{m}{2}-\ell-1}$ de elementos β tales que $C_{\lambda,\beta}^{\ell}$ es minimal.*
  - *(b) Hay una cantidad $2^{m-2\ell-1} + 2^{\frac{m}{2}-\ell-1}$ de elementos β tales que $C_{\lambda,\beta}^{\ell}$ es maximal.*

Ejemplo 4.2.5. Veamos qué sucede cuando $\beta = 0$ y $p = 2$. Para ello, consideremos el código irreducible $\mathcal{C}_\ell$ y T el conjunto de potencias $(2^\ell+1)$-ésimas de $\mathbb{F}_{2^m}$. Si α es un elemento primitivo de $\mathbb{F}_{2^m}$ y $\lambda \in \mathbb{F}_{2^m}^*$, al igual que antes, el peso de la palabra $c(\lambda) = (\mathrm{Tr}_{2^m/2}(\lambda\alpha^{(2^\ell+1)i}))_{i=1}^n$ está relacionado con la cantidad de puntos $\mathbb{F}_{2^m}$-racionales de la curva algebraica

$$C_\lambda^\ell : y^2 + y = \lambda x^{2^\ell+1},$$

razonando de manera similar al Lema 4.2.1, pero teniendo en cuenta la multiplicidad obtenida de pasar de la palabra $c(\lambda)$ a la palabra $c'(\lambda) = (\mathrm{Tr}_{2^m/2}(\lambda x^{2^\ell+1}))_{x\in\mathbb{F}_{2^m}^*}$, resulta que

$$w(c(\lambda)) = \tfrac{1}{2^{(m,\ell)}+1}(2^m - \tfrac{\#C_\lambda^\ell(\mathbb{F}_{2^m})-1}{2}).$$

Por Teorema 3.2.4, si $p = 2$, $\beta = 0$, $\lambda \in T$ y $\ell \mid m$, entonces C_λ^ℓ es una curva maximal ó minimal cuando $m/2\ell$ es impar ó par, respectivamente.

Capítulo 5

Grafos de Ramanujan

En este capítulo veremos distintas maneras de construir grafos relevantes para la teoría de números y la combinatoria llamados grafos de Ramanujan. Estos grafos empezaron a tener más relevancia durante las décadas del 80 y del 90, ya que permiten construir otros objetos combinatóricos importantes llamados expanders o expansores.

Empezaremos el capítulo introduciendo la teoría espectral de grafos. Luego, veremos que la forma cuadrática $Q_\gamma(x)$ nos permite calcular el espectro del grafo de Cayley $\Gamma_\ell = X(\mathbb{F}_{q^m}, S_\ell)$, donde $S_\ell = \{x^{q^\ell+1} : x \in \mathbb{F}_{q^m}^*\}$ cuando q es una potencia de un primo impar. Más aún, probaremos que el grafo Γ es un grafo de Ramanujan no bipartito cuando $q = 2, 3$ y $(\ell, m) = 1$ con m par.

Veremos que intentar generalizar la construcción vía formas cuadráticas se limita bastante. Por ende, se buscará hacer construcciones prestando más atención a las propiedades que tiene la función $F(x) = x^{p^\ell+1}$. Sucede que, para $p = 2$ con las hipótesis anteriormente asumidas, ésta resulta ser una clase especial de función Booleana, por lo tanto contruiremos otros grafos de Ramanujan considerando otras funciones booleanas especiales de la misma clase. Al final, consideraremos el caso no Booleano y veremos que es posible también construir otros grafos de Ramanujan.

5.1. Teoría espectral de grafos

Un *grafo* Γ es un triple que consta de un conjunto de vértices $V = V(\Gamma)$, un conjunto de lados o aristas $E = E(\Gamma)$ y un mapa que asocia a cada lado dos vértices (no necesariamente distintos), llamandos puntos finales o vértices del lado. Un *lazo* ó *loop* es un lado cuyos puntos finales son iguales. Lados múltiples son lados que tienen el mismo par de puntos finales. Un *grafo simple* es un grafo que no tiene lados múltiples ni lazos. Si un grafo tiene lados múltiples o lazos, es llamado un *multigrafo*. Cuando dos vértices u, v son puntos finales de un mismo lado, decimos que son *adyacentes* ó *vecinos* y escribimos $u \sim v$ para indicar esto.

A cualquier grafo, le podemos asociar la matriz de adyacencia A, que es una matriz entera $n \times n$ (donde $n = |V|$) con filas y columnas indexadas por los elementos del conjunto de

vértices y la (x, y)-ésima coordenada de la matriz es el número de lados que conectan x con y. Cuando consideramos grafos no dirigidos, la matriz A es simétrica. Consecuentemente, todos sus autovalores son reales. Los autovalores de A se suelen llamar los *autovalores* de Γ. Diremos que Γ es un grafo *entero* si todos sus autovalores son números enteros. El conjunto de todos los autovalores de A contados con multiplicidad se llama *espectro* de Γ y se denota por

$$Spec(\Gamma) = \{\lambda_n \leq \cdots \leq \lambda_2 \leq \lambda_1\}. \tag{5.1}$$

El *grado* de un vértice v, denotado $\deg(v)$, es el número de lados incidentes en v, donde contamos un lazo con multiplicidad 2. Con esta convención, obtenemos

$$\sum_{v \in V(\Gamma)} deg(v) = 2|E(\Gamma)|.$$

Diremos que un lado e tiene longitud 1 (salvo que sea un lazo, en este caso adoptaremos la convención de que tiene longitud 2), denotamos la longitud de e por $\ell(e)$. Para un multigrafo, una *caminata* de longitud r de x a y es una sucesión $x = v_0, v_1, \ldots, v_r = y$ con $v_i \in V$ y $e_i = (v_i, v_{i+1}) \in E$ para $i = 0, 1, \ldots, r-1$ y $\sum_{i=0}^{r} \ell(e_i) = r$. Un *camino* es una caminata que no tiene vértices repetidos. Un grafo se dice *conexo* si para cualquier par $x, y \in V$, existe un camino de x a y. Se sabe que el número de caminatas de x a y de longitud r está dado por la (x, y)-ésima entrada de A^r, donde de nuevo adoptamos la convención de contar a un lazo con multiplicidad 2. Un grafo es llamado *k-regular* si todo vértice tiene grado k. Denotaremos por

$$\Delta(\Gamma) = \max_{x \in V} \deg(x)$$

al máximo de todos los grados de Γ.

Sea v un autovector de A correspondiente a un autovalor λ. Entonces, $Av = \lambda v$. Escribimos $v = (x_1, ..., x_n)^t$ y asumimos, sin pérdida de generalidad, que $|x_1| = \max_{1 \leq i \leq n} |x_i|$. Entonces,

$$|\lambda||x_1| = |\sum_{j=1}^{n} a_{1j}x_j| \leq |x_1| \sum_{j=1}^{n} a_{1j} \leq |x_1|\Delta(\Gamma).$$

Por lo tanto tenemos lo siguiente.

Proposición 5.1.1. *Sea A la matriz de adyacencia de un grafo no dirigido Γ. Si λ es un autovalor de A, entonces $|\lambda| \leq \Delta(\Gamma)$.*

Corolario 5.1.2. *Si Γ es un grafo k-regular, entonces todos los autovalores λ de su matriz de adyacencia satisfacen $|\lambda| \leq k$.*

Ya que la matriz de adyacencia de un grafo k-regular satisface que la suma de todas sus filas son iguales a k, claramente tenemos que $\lambda_0 = k$ es un autovalor de A con autovector igual a $u = (1, 1, \ldots, 1)^t$. Más precisamente tenemos el siguiente resultado.

Teorema 5.1.3 ([38]). *Si* Γ *es un grafo* k*-regular, entonces* k *es un autovalor de* Γ *con multiplicidad igual al número de componentes conexas de* Γ.

Dado Γ un grafo k-regular, al autovalor k de Γ se le suele decir el *autovalor trivial* de Γ. El teorema anterior nos permite decir cuándo un grafo regular es conexo, solamente viendo la multiplicidad de su autovalor trivial.

Corolario 5.1.4. *Si* Γ *es un grafo* k*-regular y* k *es un autovalor de* Γ *con multiplicidad* 1*, entonces* Γ *es un grafo conexo.*

Podemos definir una métrica sobre un grafo conexo definiendo la distancia $d(x, y)$ para $x, y \in V$ como la mínima longitud de un camino desde x a y. El *diámetro* de un grafo conexo es el máximo valor de la función distancia. Para grafos k-regulares se tiene la siguiente cota del diámetro.

Teorema 5.1.5 ([7]). *Sea* Γ *un grafo* k*-regular con* n *vértices y diámetro* $\operatorname{diam}(\Gamma)$*. Si* Γ *es no-bipartito, entonces*

$$\operatorname{diam}(\Gamma) \leq \frac{\log(n-1)}{\log(k/\lambda(\Gamma))} + 1.$$

En general, si Γ es un grafo simple k-regular, ya vimos que

$$k = \text{máx}\{|\lambda| : \lambda \in Spec(\Gamma)\}.$$

Más aún, k es un autovalor de Γ con multiplicidad igual a la cantidad de componentes conexas de Γ. Si escribimos $Spec(\Gamma) = \{\lambda_n \leq \cdots \leq \lambda_1\}$ entonces

$$-k \leq \lambda_n \leq \cdots \leq \lambda_2 \leq \lambda_1 = k.$$

Además, sucede que $-k = \lambda_n$ si y sólo si Γ es bipartito (ver [38]).

Lema 5.1.6 (Alon-Boppana). *Sea* Γ *un grafo simple* k*-regular y* $Spec(\Gamma) = \{\lambda_n \leq \cdots \leq \lambda_1\}$*, entonces* $|\lambda_i| \leq 2\sqrt{k-1} - O(1)$ *para* $i = 2, \ldots, n$.

La función zeta de Ihara

Así como en teoría de números existe la función zeta de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}},$$

donde el último producto se toma en todos los números primos; en teoría de grafos se define una función zeta, llamada la función *zeta de Ihara*, donde el papel de los números primos pasa a ser el de los caminos primos en Γ.

Empecemos introduciendo el equivalente a números primos en este contexto. Sea E el conjunto de lados de un grafo simple Γ tal que $|E| = m$. Consideremos una orientación arbitraria de los lados de Γ y definamos un nuevo conjunto de lados orientados

$$E^e = \{e_1, e_2, \ldots, e_{2m}\},$$

donde e_i con $i = 1, \ldots, m$ es la i-ésima arista de E con la orientación antes dada, y $e_{i+m} = e_i^{-1}$ es el mismo lado con la orientación opuesta. Sea $c = a_1 \cdots a_s$ un camino en Γ tal que $a_i \in E^e$, adoptaremos las siguientes terminologías:

- c tiene un *retroceso*, si $a_{j+1} = a_j^{-1}$ para algún j.
- c tiene una *cola* si $a_s = a_1^{-1}$.
- Denotaremos por $\nu(c)$ a la longitud de c.
- El *producto* de dos caminos cerrados c_1 y c_2 con el mismo vértice inicial es el camino cerrado denotado por $c_1 \cdot c_2$, que consiste en recorrer primero los lados de c_1 y a continuación los de c_2.
- Un camino cerrado c es *primitivo*, si $c \neq d^f$ para todo $f \geq 2$ y todo camino d de Γ, donde d^f denota recorrer el camino cerrado d, f veces en el mismo sentido.
- Un camino cerrado c es *primo* si no tiene retrocesos ni colas y es primitivo.

De la definición de camino primo en Γ, es inmediato que los caminos cerrados sin retrocesos ni cola de Γ son primos ó potencias de un primo.

Notar que varios caminos cerrados pueden definir el mismo camino si lo vemos dibujado en el grafo. Basta con tomar un camino cerrado y hacerle permutaciones cíclicas para obtener el resto de caminos. Además, si $c = a_1 a_2 \cdots a_s$ es un primo en Γ, entonces cualquier permutación cíclica de él también va a ser un primo, por lo que vamos a definir una relación de equivalencia en la que la clase de c es

$$C = \{a_1 a_2 \ldots a_s, a_s a_1 \ldots a_{s-1}, \ldots, a_2 a_3 \ldots a_1\}.$$

A la clase de equivalencia del camino cerrado $a_s \cdots a_2 a_1$ la denotamos por C^{-1}. Si C es la clase de equivalencia de un primo, también lo será C^{-1} y viceversa, y a dichas clases denotaremos habitualmente por P y Q.

Dadas dos clases de equivalencia C y D de respectivos caminos cerrados c y d, denotaremos por $C \cdot D$ a la clase de equivalencia del camino obtenido a partir de cd eliminando los retrocesos y las colas. Los grafos cíclicos solo tienen dos primos P y P^{-1}, siendo P el primo dado por el ciclo del grafo recorrido en uno de los dos sentidos posibles.

Sea Γ un grafo conexo, finito y sin vértices de grado 1, la *función zeta de Ihara* se define por

$$\zeta(u, \Gamma) = \prod_P \frac{1}{1 - u^{\nu(P)}},$$

donde P recorre todas las clases de caminos primos del grafo Γ. Denotamos ρ_Γ al radio de convergencia de la función zeta de Γ. Esta función zeta se puede dar en términos del determinante de cierta matriz relacionada con la matriz de adyacencia del grafo y el número de generadores del grupo fundamental del grafo.

Se puede probar que el grupo fundamental del grafo Γ es un grupo libre de rango r, donde r es la cantidad de lados que no pertenecen al árbol generador de Γ. Recordemos que un árbol generador de Γ es un subgrafo de Γ que no tiene ciclos y contiene a todos los vértices de Γ.

Se tiene la siguiente fórmula llamada la *fórmula determinantal de Ihara*.

Teorema 5.1.7. *Sea Γ un grafo conexo, finito y sin vértices de grado 1. Entonces $\zeta(u, \Gamma)$ es una función racional y*

$$\zeta(u, \Gamma) = \frac{1}{(1-u^2)^{r-1} \det(I - Au + Qu^2)},$$

donde r es el rango del grupo fundamental de Γ, A es la matriz de adyacencia de Γ y Q la matriz diagonal cuya entrada i-ésima es el grado del vértice i-ésimo menos 1.

Lema 5.1.8. *Sea Γ un grafo conexo, finito y sin vértices de grado 1. Entonces*

$$\log \zeta(u, \Gamma) = \sum_{j \geq 1} \frac{N_j}{j} u^j,$$

donde N_j es el número de caminos cerrados sin retrocesos ni colas de longitud j en Γ.

Teorema 5.1.9. *Sea Γ un grafo conexo, finito y sin vértices de grado 1. Entonces*

$$\zeta(u, \Gamma)^{-1} = \det(I - W_1 u),$$

donde W_1 es la matriz de adyacencia de lados de Γ.

En teoría de números es muy importante conocer dónde se encuentran los ceros de la función zeta de Riemann y la *hipótesis de Riemann* conjetura que estos ceros se encuentran en $\Re(s) = \frac{1}{2}$. Análogamente, existe una noción de hipótesis de Riemann para la función zeta de Ihara. Dado un grafo k-regular Γ diremos que la función $\zeta((k-1)^{-s}, \Gamma)$ satisface la hipótesis de Riemann si y sólo si

$$\zeta((k-1)^{-s}, \Gamma)^{-1} = 0 \quad \Longleftrightarrow \quad \Re(s) = \tfrac{1}{2},$$

para $0 < \Re(s) < 1$. Si $u = (k-1)^{-s}$, el hecho de que $\Re(s) = \frac{1}{2}$ implica que $|u| = 1/\sqrt{k-1}$.

En la sección §5.3 veremos que existe una relación fundamental entre la función zeta de Ihara y los grafos de Ramanujan.

5.2. Grafos de Cayley y su espectro

Aquí veremos qué relación existe entre el cálculo de sumas exponenciales y el cálculo del espectro de un grafo de Cayley particular.

5.2.1. Grafos de Cayley.

Dado un grupo finito G con un subconjunto S no conteniendo al elemento neutro de G, el *grafo de Cayley*

$$\Gamma = X(G, S) = (V(\Gamma), E(\Gamma))$$

es el grafo dirigido cuyo conjunto de vértices es el grupo, i.e. $V(\Gamma) = G$, y su conjunto de lados es

$$E(\Gamma) = \{(g, h) : g^{-1}h \in S\}$$

es decir que hay una flecha de g a h si $h = gs$ con $s \in S$.

Notar que como el elemento neutro no está contenido en S, el grafo de Cayley $X(G, S)$ no tiene loops. Al conjunto S se le llama *conjunto de conexión* de Γ. El conjunto S se dice *simétrico* si

$$S = S^{-1} := \{s^{-1} : s \in S\}$$

(ó $S = -S = \{-s : s \in S\}$ si G es abeliano).

Notar que todo grafo de Cayley $\Gamma = X(G, S)$ es regular, por definición, con grado de regularidad $k = \#S$. Además, si S es un conjunto de generadores de G simétrico entonces Γ resulta un grafo simple no dirigido conexo.

Ejemplo 5.2.1 (Grafos en $\mathbb{Z}_n$)**.** (i) El ciclo de longitud n, C_n, puede ser interpretado como un grafo de Cayley, ya que si consideramos $G = \mathbb{Z}_n$ los enteros módulo n y $S = \{-1, 1\}$. Luego

$$C_n = X(G, S).$$

(ii) El grafo completo K_n es un grafo de Cayley, ya que si $G = \mathbb{Z}_n$ y $S = \mathbb{Z}_n \setminus \{0\}$, entonces

$$K_n = X(G, S).$$

(iii) El grafo *unitario* es el grafo $U_n = X(\mathbb{Z}_n, \mathbb{Z}_n^*)$, donde $\mathbb{Z}_n^*$ son las unidades de $\mathbb{Z}_n$. $\Diamond$

Ejemplo 5.2.2 (Grafos de Paley)**.** Al grafo de Cayley $X(G, S)$ donde $G = \mathbb{F}_q$ es el cuerpo finito de q elementos y S es el conjunto de conexión

$$S = \{x^2 : x \in \mathbb{F}_q^*\}$$

se lo conoce como *grafo de Payley* P_n. $\Diamond$

Espectro de $Cay(G,S)$ con G abeliano

Cuando G es un grupo abeliano finito, es posible calcular el espectro de Γ usando los caracteres de G. Si $\widehat{G}$ es el grupo de caracteres de G y $\chi \in \widehat{G}$, definimos

$$\chi(S) = \sum_{g \in S} \chi(g).$$

Lema 5.2.3. *Sea $\Gamma = X(G,S)$ un grafo de Cayley sobre un grupo abeliano finito G con conjunto de conexión S. Sea A la matriz de adyancencia de Γ. Entonces cada carácter χ de G se corresponde a un autovector de A con autovalor $\chi(S)$. En particular el espectro de Γ es el multiconjunto $\{\lambda_S = \chi(S) : \chi \in \widehat{G}\}$.*

Notar que si consideramos el grupo abeliano finito $G = (\mathbb{F}_{q^m}, +)$, entonces su grupo de caracteres $\widehat{\mathbb{F}}_{q^m}$ es cíclico generado por el carácter canónico

$$\chi(x) = \zeta_p^{\mathrm{Tr}_{q^m/p}(x)}$$

donde $\zeta_p = e^{\frac{2\pi i}{p}}$. Es decir, todo carácter χ de $\mathbb{F}_{q^m}$ es de la forma

$$\chi_\gamma(x) = \zeta_p^{\mathrm{Tr}_{q^m/p}(\gamma x)} = \chi(\gamma x), \qquad \gamma \in \mathbb{F}_{q^m}. \tag{5.2}$$

Nota. Si $\gamma = 0 \in \mathbb{F}_{q^m}$ entonces $\chi_0(x) = \chi(0) = 1$ para todo x, es decir que χ_0 es el carácter trivial.

5.2.2. Los grafos de Cayley $\Gamma_{m,\ell}$

Fijemos q una potencia de un primo y enteros $m \geq 1$, $\ell \geq 0$ y consideremos el conjunto

$$S_\ell = S_{m,\ell} = \{x^{q^\ell+1} : x \in \mathbb{F}_{q^m}^*\}. \tag{5.3}$$

Claramente, S_ℓ es un subgrupo de $\mathbb{F}_{q^m}^*$, ya que $x^{q^\ell+1}y^{q^\ell+1} = (xy)^{q^\ell+1}$. Veamos que bajo ciertas condiciones resulta simétrico.

Lema 5.2.4. *Sean $m \geq 1$, $\ell \geq 0$ enteros. Entonces S_ℓ es simétrico para todo m, ℓ si q es par y $S_{m,\ell}$ es simétrico con $\frac{m}{(m,\ell)}$ par si q es impar.*

Demostración. Claramente $S_\ell = -S_\ell$ en característica par, ya que $-x = x$ para todo $x \in \mathbb{F}_{q^m}$, independientemente de las hipótesis pedidas.

Ahora, supongamos que q es una potencia de un primo impar y sean m, ℓ enteros positivos satisfaciendo las hipótesis del lema. Notar que si existe $y \in \mathbb{F}_{q^m}^*$ satisfaciendo $y^{q^\ell} = -1$, entonces dado cualquier $x \in \mathbb{F}_{q^m}^*$ tenemos que

$$-x^{q^\ell+1} = x^{q^\ell+1}y^{q^\ell+1} = (xy)^{q^\ell+1} \in S_{m,\ell}.$$

Luego, S_ℓ es simétrico en este caso. De esta manera, sólo basta probar que existe $y \in \mathbb{F}_{q^m}^*$ tal que $y^{q^\ell+1} + 1 = 0$

Si α es un elemento primitivo de $\mathbb{F}_{q^m}$, entonces

$$S_\ell = \langle \alpha^{q^{(m,\ell)}+1} \rangle \tag{5.4}$$

dado que se tiene que $(q^m - 1, q^\ell + 1) = q^{(m,\ell)} + 1$ por el Lema 3.2.1, puesto que $v_2(m) > v_2(\ell)$ es equivalente a que $\frac{m}{(m,\ell)}$ sea par.

Luego, basta probar que existe $y \in \mathbb{F}_{q^m}^*$ tal que

$$y^{q^{(m,\ell)}+1} + 1 = 0.$$

Afirmamos que $2(q^{(m,\ell)} + 1) \mid q^m - 1$. Se tiene que $q^m - 1 = (q-1)(1 + q + q^2 + \cdots + q^{m-1})$ y como $q^{(m,\ell)} + 1$ no divide a $q - 1$ entonces $q^{(m,\ell)} + 1$ divide a $1 + q + q^2 + \cdots + q^{m-1}$. Además, como q es impar entonces $2 \mid q - 1$. Por lo tanto $2(q^{(m,\ell)} + 1) \mid q^m - 1$, como queríamos ver. Por lo tanto, existe un entero positivo t tal que

$$q^m - 1 = 2t(q^{(m,\ell)} + 1).$$

Sea $y = \alpha^t$. Notar que $y^{2(q^{(m,\ell)}+1)} = 1$, entonces

$$y^{q^{(m,\ell)}+1} = \pm 1.$$

Como α es un elemento primitivo, el orden de y es $2(q^{(m,\ell)} + 1)$. Luego, tenemos

$$y^{q^{(m,\ell)}+1} = -1.$$

Por lo tanto, $S_\ell = -S_\ell$ como queríamos demostrar. □

De este modo, el grafo de Cayley

$$\Gamma_{m,\ell} = X(\mathbb{F}_{q^m}, S_\ell), \tag{5.5}$$

donde S_ℓ es como en (5.3), resulta ser un grafo simple no dirigido. Cuando $\ell = 0$ obtenemos el grafo de Payley, más aún tenemos la siguiente caracterización de estos grafos.

Lema 5.2.5. *Sean m, ℓ enteros no negativos y denotemos $m_\ell = m/(m,\ell)$. Consideremos $\Gamma_{m,\ell}$ como en (5.5). Entonces obtenemos los siguientes dos casos:*

- *Si m_ℓ es impar, entonces $\Gamma_{m,\ell} = \Gamma_{m,0}$, es decir que es el grafo de Payley.*
- *Si m_ℓ es par, entonces $\Gamma_{m,\ell} = \Gamma_{m,(m,\ell)}$.*

Demostración. Dado que $S_\ell = \langle \alpha^{q^\ell+1} \rangle$ donde α es un elemento primitivo de $\mathbb{F}_{q^m}$. Luego S_ℓ es un subgrupo multiplicativo de $\mathbb{F}_{q^m}^*$ de orden $\frac{q^m-1}{(q^m-1,q^\ell+1)}$. Como el subgrupo generado por $\alpha^{(q^m-1,q^\ell+1)}$ tiene el mismo orden que S_ℓ y todo grupo cíclico tiene un único subgrupo por cada divisor de su orden, tenemos que

$$S_\ell = \langle \alpha^{(q^m-1,q^\ell+1)} \rangle$$

Por el Lema 3.2.1 tenemos que $(q^m-1, q^\ell+1) = 2$ si m_ℓ es impar y $(q^m-1, q^\ell+1) = q^{(m,\ell)}+1$ si m_ℓ es par. Por lo tanto

$$S_\ell = \{x^2 : x \in \mathbb{F}_{q^m}^*\}$$

si m_ℓ es impar y

$$S_\ell = \{x^{q^{(m,\ell)}+1} : x \in \mathbb{F}_{q^m}^*\}$$

si m_ℓ es par. Concluyendo así la demostración. □

Analicemos ahora el espectro de $\Gamma_{m,\ell}$. Por el Lema 5.2.3, los autovalores son de la forma

$$\chi_\gamma(S_\ell) = \sum_{y \in S_\ell} \chi_\gamma(y).$$

Para $\gamma \in \mathbb{F}_{q^m}$, por (5.2) y (5.3), tenemos

$$\chi_\gamma(S_\ell) = \tfrac{1}{q^{(m,\ell)}+1} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\mathrm{Tr}_{q^m/p}(\gamma x^{q^\ell+1})} = \tfrac{1}{q^{(m,\ell)}+1} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\mathrm{Tr}_{q/p}\mathrm{Tr}_{q^m/q}(\gamma x^{q^\ell+1})}.$$

Es decir,

$$\chi_\gamma(S_\ell) = \tfrac{1}{q^{(m,\ell)}+1} \sum_{x \in \mathbb{F}_{q^m}^*} \zeta_p^{\mathrm{Tr}_{q/p}(Q_{\gamma,\ell}(x))} \tag{5.6}$$

donde $Q_{\gamma,\ell}(x)$ es la forma cuadrática

$$Q_{\gamma,\ell}(x) = \mathrm{Tr}_{q^m/q}(xR_{\gamma,\ell}(x)) \quad \text{con} \quad R_{\gamma,\ell}(x) = \gamma x^{q^\ell}$$

con $x \in \mathbb{F}_{q^m}$. Luego, por (2.21) y teniendo en cuenta la contribución de $x = 0$, tenemos

$$\chi_\gamma(S_\ell) = \frac{T_{Q_{\gamma,\ell}} - 1}{q^{(m,\ell)} + 1} \tag{5.7}$$

donde $T_{Q_{\gamma,\ell}}$ es la suma exponencial dada en (2.21).

A partir de esto, podemos deducir el espectro del grafo $\Gamma = X(G, S)$ en característica impar, en ciertos casos.

Teorema 5.2.6. *Sea $m \geq 1, \ell \geq 0$ enteros y $\Gamma_{m,\ell} = X(\mathbb{F}_{q^m}, S_\ell)$ con S_ℓ como en (5.3). Si q es impar y $m_\ell = \frac{m}{(m,\ell)}$ es par entonces los autovalores de $\Gamma_{m,\ell}$ son*

$$k = \frac{q^m-1}{q^{(m,\ell)}+1}, \quad \frac{q^{\frac{m}{2}}-1}{q^{(m,\ell)}+1}, \quad \frac{-q^{\frac{m}{2}}-1}{q^{(m,\ell)}+1}, \quad \frac{q^{\frac{m}{2}+(m,\ell)}-1}{q^{(m,\ell)}+1}, \quad \frac{-q^{\frac{m}{2}+(m,\ell)}-1}{q^{(m,\ell)}+1} \tag{5.8}$$

donde las multiplicidades correspondientes son

$$(m_1, \ldots, m_5) = \begin{cases} 1, q^{(m,\ell)}k, 0, 0, k & \text{si } \frac{1}{2}m_\ell \text{ es par,} \\ 1, 0, q^{(m,\ell)}k, k, 0 & \text{si } \frac{1}{2}m_\ell \text{ es impar.} \end{cases}$$

Más aún, $\Gamma_{m,\ell}$ es un grafo simple, conexo y k-regular no bipartito con espectro entero.

Demostración. Sabemos que $\Gamma_{m,\ell}$ es k-regular con $k = \#S_\ell$, por ser grafo de Cayley. Por (5.4), y el comentario posterior, tenemos

$$k = \frac{q^m - 1}{q^{(m,\ell)} + 1}.$$

Además, $\Gamma_{m,\ell}$ es simple, ya que S_ℓ es simétrico por el Lema 5.2.4.

Ahora calculemos el espectro del grafo. Por (5.7), los autovalores de $\Gamma_{m,\ell}$ están dados por los distintos valores que toma $T_{Q_{\gamma,\ell}}$ en la expresión $\frac{T_{Q_{\gamma,\ell}}-1}{q^{(m,\ell)}+1}$. Si $\gamma = 0$, entonces $Q_{0,\ell} = 0$ y por (2.21) tenemos que $T_Q = q^m$, obteniendo el autovalor $\chi_0(S_\ell) = \frac{q^m-1}{q^{(m,\ell)}+1} = k$.

Para el resto de los autovalores, notemos primero que por el Teorema 2.4.2 de Klapper, como m_ℓ es par, la forma cuadrática $Q_{\gamma,\ell}$ tiene rango r par para todo γ y además

$$r \in \{m, m - 2(m,\ell)\}.$$

Recordemos que en el caso de característica impar y rango par, el tipo ϵ y $\eta(\Delta)$ coinciden (ver comentario después de Corolario 2.2.16). Luego, por (ii) del Lema 2.3.1, se tiene que $T_{Q_{\gamma,\ell}} = \epsilon q^{m-\frac{r}{2}}$ ó $T_{Q_{\gamma,\ell}} = (-1)^{\frac{r}{2}}\epsilon q^{m-\frac{r}{2}}$ según q es congruente a 1 ó a 3 módulo 4. Es decir,

$$T_{Q_{\gamma,\ell}} = \pm\epsilon q^{m-\frac{r}{2}}.$$

Teniendo en cuenta los 2 posibles valores de r y los dos signos, tenemos que los autovalores del grafo son exactamente los dados en (5.8).

Queda analizar las multiplicidades. En primer lugar, como el autovalor k se obtiene a partir de $Q_{0,\ell}(x) = 0$ y $T_{Q_{\gamma,\ell}} = \pm\epsilon q^{m-\frac{r}{2}} \neq q^m$ para $\gamma \neq 0$, se ve que la multiplicidad de k es 1. Los autovalores $\frac{\pm q^{\frac{m}{2}}-1}{q^{(m,\ell)}+1}$ se obtienen cuando $r = m$ y los autovalores $\frac{\pm q^{\frac{m}{2}-(m,\ell)}-1}{q^{(m,\ell)}+1}$ cuando $r = m - 2(m,\ell)$.

Por el Teorema 2.4.2, las multiplicidades correspondientes están dadas por

$$q^m - 1 - \#\{t \equiv 0 \pmod{q^{(m,\ell)+1}}\}, \quad 0, \quad 0, \quad \#\{t \equiv \tfrac{q^{(m,\ell)}+1}{2} \pmod{q^{(m,\ell)+1}}\},$$

cuando $\frac{1}{2}m_\ell$ es par y por

$$q^m - 1 - \#\{t \equiv 0 \pmod{q^{(m,\ell)+1}}\}, \quad 0, \quad 0, \quad \#\{t \equiv \tfrac{q^{(m,\ell)}+1}{2} \pmod{q^{(m,\ell)+1}}\}$$

cuando $\frac{1}{2}m_\ell$ es impar. Notar que, por (2.33), las multiplicidades de los autovalores toman los valores $q^m - 1 - M_1, 0, 0, M_1$ y $0, q^m - 1 - M_2, M_2, 0$, respectivamente. Por el Lema 2.4.3 tenemos que $M_1 = M_2 = k$, de donde sale que las multiplicidades de los autovalores son exactamente como en el enunciado. Luego, como la multiplicidad de k es 1, el grafo es conexo por el Corolario 5.1.4.

Finalmente, el espectro de $\Gamma_{m,\ell}$ es entero en consecuencia del Lema 3.2.3, que afirma que $q^{(m,\ell)} + 1 \mid q^{\frac{m}{2}} + (-1)^{\frac{1}{2}m_\ell+1}$ y $q^{(m,\ell)} + 1 \mid q^{\frac{m}{2}+(m,\ell)} + (-1)^{\frac{1}{2}m_\ell+1}$.

□

5.3. Grafos de Ramanujan

En esta sección vamos a introducir los grafos de Ramanujan y algunas de sus propiedades más importantes. Éstos son una clase de grafos que aparecieron durante la década del 80' para la construcción de ciertos objetos optimales muy interesantes llamados 'expanders'.

Mostraremos que los grafos de Cayley introducidos en la sección anterior pertenecen a esta clase de grafos para $q = 2$ y $q = 3$. Veremos que en el caso de $q = 2$, se pueden considerar diferentes tipos de generalizaciones, una vía formas cuadráticas y otra vía funciones especiales (APN , AB y PN), siendo la segunda la más fructifera ya que se encontrarán muchas familias diferentes de grafos de Ramanujan. Por último, veremos que en característica impar podemos encontrar otra familia de grafos de Ramanujan.

Los primeros en encontrar familias infinitas de grafos de Ramanujan de grado regular fijo fueron Lubotszky, Phillips y Sarnak ([32]). Más precisamente, encontraron familias infinitas de grafos de Ramanujan $(p + 1)$-regulares, donde p es un primo satisfaciendo $p \equiv 1 \mod 4$. Luego, Morgenstern pudo encontrar familias infinitas $(p^\ell + 1)$-regulares ([37]) con $p \equiv 1$ (mód 4). Lubotszky, Phillips y Sarnak conjeturaron que de haber familias infinitas de grafos de Ramanujan de grado de regularidad fijo k, entonces $k - 1$ tendría que ser una potencia de un primo.

En el 2008, Marcus, Spielman y Srivastava ([33]) mostraron que no estaban en lo correcto ya que pudieron probar que existen familias infinitas de grafos de Ramanujan bipartitos de grado fijo k, para todo k. Ellos hicieron uso de herramientas topológicas (2-recubrimientos) y algebraicas (familias entrelazadas) para construir dichos grafos.

Lo interesante, por lo tanto, es ver si de alguna manera uno puede encontrar familias infinitas de grafos de Ramanujan no bipartitos de un grado de regularidad fijo. En esta dirección, aquí vamos a construir muchas familias de grafos de Ramanujan no bipartitos. A futuro, sería muy bueno ver si vía herramientas topológicas (2-levantamientos) u otras herramientas, es posible usar los grafos que vamos a construir aquí para encontrar otras familias infinitas distintas a las ya conocidas.

Recordemos que el autovalor trivial de un grafo k-regular es su grado de regularidad k, y que además un grafo es bipartito si y sólo si $-k$ es un autovalor del grafo. Si Γ es k-regular bipartito, los autovalores no triviales de Γ serán todos los autovalores de Γ distintos de $\pm k$.

Dado un grafo Γ, denotaremos $\lambda(\Gamma)$ al autovalor de Γ de mayor valor absoluto no trivial, es decir

$$\lambda(\Gamma) = \text{máx}\left\{|\lambda| : \lambda \in Spec(\Gamma) \setminus \{\pm k\}\right\}. \tag{5.9}$$

Definición 5.3.1. Un grafo simple k-regular conexo Γ es *de Ramanujan* si

$$\lambda(\Gamma) \leq 2\sqrt{k-1}. \tag{5.10}$$

Veamos algunos ejemplos de grafos de Ramanujans.

Ejemplo 5.3.2. Dado n un entero positivo, consideremos K_n el grafo completo de n vértices. Se puede probar, usando la fórmula del determinante de Dedekind, que el polinomio característico de su matriz de adyacencia es

$$p(x) = (x - (n-1))(x+1)^{n-1},$$

como el grafo completo K_n es $(n-1)$-regular, por lo tanto K_n es un grafo de Ramanujan $(n-1)$-regular no bipartito.

Nota. La fórmula del determinante de Dedekind es una fórmula para calcular el determinante de ciertas matrices construidas a partir de un grupo abeliano de la manera siguiente. Sea G un grupo abeliano y sea $f : G \to \mathbb{C}$ cualquier función, consideremos A la matriz indexada por los elementos de G cuya (i,j)-ésima entrada está dada por $f(ij^{-1})$, entonces el determinante de esta matriz está dado por

$$\prod_{\chi \in \widehat{G}} \left(\sum_{g \in G} \chi(g) f(g) \right).$$

En el ejemplo anterior, basta tomar $G = \mathbb{Z}_n$, y f la función definida por $f(0) = -x$ y $f(a) = 1$ si $a \in G \setminus \{0\}$.

Notar además que el Lema 5.2.3, es una consecuencia de esta fórmula tomando como f la función indicadora del conjunto de conexión S.

Ejemplo 5.3.3. Sea r un entero positivo, consideremos el grafo bipartito completo $K_{r,r}$. De la misma manera que en el Ejemplo 5.3.2, se puede chequear que su polinomio característico es

$$p(x) = (x-r)(x+r)x^{2r-2},$$

como $K_{r,r}$ es r-regular, entonces $K_{r,r}$ es un grafo de Ramanujan r-regular bipartito.

Estos son considerados los grafos de Ramanujan triviales no-bipartito y bipartito respectivamente.

Existe una relación directa entre los grafos de Ramanujan y la función zeta de Ihara definida en la sección anterior.

Teorema 5.3.4 ([19])**.** *Sea Γ un grafo simple k-regular conexo. La función zeta de Ihara $\zeta(u, \Gamma)$ satisface la hipótesis de Riemann si y sólo si el grafo Γ es Ramanujan.*

5.3.1. Grafos de Ramanujan de tipo $\Gamma_{m,\ell}$

Veamos que los grafos de Cayley introducidos en la sección anterior son grafos de Ramanujan en características 2 y 3.

Dado que por el Teorema 5.2.6 conocemos los autovalores de $\Gamma = \Gamma_{m,\ell}$, analizaremos primero qué condiciones necesarias tienen que cumplir m, q y ℓ si los autovalores satisfacieran la desigualdad (5.10). Recordemos (de la demostracón del Teorema 5.2.3) que cuando $m/(m,\ell)$ es par entonces

$$\#S_\ell = \frac{q^m - 1}{q^{(m,\ell)} + 1} = k.$$

Por el Teorema 5.2.3, si q es impar, el autovalor no trivial de mayor valor absoluto es

$$\lambda(\Gamma) = \frac{-q^{\frac{m}{2}+(m,\ell)} - 1}{q^{(m,\ell)} + 1}.$$

Supongamos que se satisface la desigualdad (5.10) en este caso, es decir

$$\frac{q^{\frac{m}{2}+(m,\ell)} + 1}{q^{(m,\ell)} + 1} \leq 2\sqrt{\frac{q^m - 1}{q^{(m,\ell)}+1} - 1}. \tag{5.11}$$

Luego

$$\frac{q^{m+2(m,\ell)} + 2q^{\frac{m}{2}+(m,\ell)} + 1}{4(q^{(m,\ell)} + 1)} \leq q^m - q^{(m,\ell)} - 2.$$

Entonces necesariamente tenemos que

$$q^{m+2(m,\ell)} \leq 4(q^{(m,\ell)} + 1)q^m.$$

Esto es equivalente a $x^2 - 4x - 4 \leq 0$ con $x = q^{(m,\ell)}$, de donde claramente se tiene que $x \leq 4$. Como q es impar, solo se puede tener $(m, \ell) = 1$ y $q = 3$.

Luego, hemos probado lo siguiente.

Lema 5.3.5. *Sean $m, \ell \in \mathbb{N}$. Si $q \neq 3$ ó $(m, \ell) \neq 1$, entonces el grafo de Cayley $\Gamma_{m,\ell}$ sobre $\mathbb{F}_{q^m}$ no es de Ramanujan.*

Característica 3

Notar que el grafo $\Gamma_{m,\ell}$ es conexo no bipartito y $\frac{3^m-1}{4}$-regular, ya que por un lado el autovalor trivial tiene multiplicidad 1 y por otro lado $-(\frac{3^m-1}{4})$ no es un autovalor de $\Gamma_{m,\ell}$. Entonces, tenemos el siguiente resultado.

Teorema 5.3.6. *Sea $\Gamma_{m,\ell} = X(G, S_\ell)$ donde $G = \mathbb{F}_{q^m}$ y S_ℓ como en (5.3). Si m, ℓ son enteros tales que $\frac{m}{(m,\ell)}$ es par y $m \geq 4$, entonces $\Gamma_{m,\ell}$ es un grafo de Ramanujan si y sólo si $q = 3$ y $(m, \ell) = 1$. En tal caso $\Gamma_{m,\ell}$ es un grafo de Ramanujan entero no bipartito $\frac{3^m-1}{4}$-regular.*

Demostración. Por el Lema 5.3.5, sólo resta ver que las condiciones $q = 3$ y $(m, \ell) = 1$ son suficientes. Analicemos la desigualdad (5.11) en este caso:

$$\frac{3^{\frac{m}{2}+1} + 1}{4} \leq 2\sqrt{\frac{3^m - 1}{4} - 1}.$$

Esta desigualdad es equivalente a

$$3^{m+2} + 2 \cdot 3^{\frac{m}{2}+1} + 1 \leq 16(3^m - 5) = 3^{m+2} + 7 \cdot 3^m - 80,$$

que a su vez equivale a

$$81 \leq 7 \cdot 3^m - 2 \cdot 3^{\frac{m}{2}+1} = 7(3^{\frac{m}{2}} - \tfrac{3}{7})^2 - \tfrac{9}{7}.$$

Por lo tanto,

$$3^{\frac{m}{2}} \geq \frac{\sqrt{576}+3}{7} = \frac{27}{7} = 3 + \tfrac{6}{7}.$$

Esta última desigualdad es válida para $m \geq 3$, pero como m debe ser par se tiene $m \geq 4$. Por lo tanto, el grafo $\Gamma_{m,\ell}$ es un grafo de Ramanujan, como queríamos demostrar. Además, por las discusiones previas al teorema, $\Gamma_{m,\ell}$ resulta ser no bipartito y $\frac{3^m-1}{4}$-regular. □

Corolario 5.3.7. *Sea $m \geq 1, \ell \geq 0$ enteros y $\Gamma_{m,\ell} = X(\mathbb{F}_{3^m}, S_\ell)$ con S_ℓ como en (5.3). Si q es impar y $m_\ell = \frac{m}{(m,\ell)}$ es par entonces*

$$\operatorname{diam}(\Gamma_{m,\ell}) \leq \frac{\log(3^m-1)}{\log((3^m-1)/(3^{\frac{m}{2}+(m,\ell)} + (-1)^{\frac{1}{2}m_\ell}))} + 1$$

Característica par

Si consideramos el caso binario $q = 2$, no tenemos un lema sobre sumas exponenciales de formas cuadráticas en esta característica que nos permita calcular el espectro del grafo $\Gamma_{m,\ell}$ explícitamente. Sin embargo, es posible encontrar los posibles autovalores sin sus multiplicidades. En este caso, el grafo $\Gamma_{m,\ell}$ es un grafo simple, ya que $-S_\ell = S_\ell$ por estar en característica 2, y $|S|$-regular, donde $|S| = \frac{2^m-1}{2^{(m,\ell)}+1}$.

Teorema 5.3.8. *Consideremos el grafo de Cayley $\Gamma_{m,\ell} = X(\mathbb{F}_{2^m}, S_\ell)$ con conjunto de conexión $S_\ell = \{x^{2^\ell+1} : x \in \mathbb{F}_{2^m}^*\}$. Si $m \geq 4$ es par y $(m,\ell) = 1$, entonces $\Gamma_{m,\ell}$ es un grafo de Ramanujan no bipartito de orden 2^m y $\frac{2^m-1}{3}$-regular. Además, si m es multiplo de 4 y $(m,\ell) = 2$, entonces $\Gamma_{m,\ell}$ es un grafo de Ramanujan no bipartito de orden 2^m y $\frac{2^m-1}{5}$-regular.*

Demostración. Supongamos que m es par y $(m,\ell) = 1$. Consideremos el carácter de $\mathbb{F}_{2^m}$ dado por $\chi_\beta(x) = (-1)^{\operatorname{Tr}_{2^m/2}(\beta x)}$ donde $\beta \in \mathbb{F}_{2^m}$. Por el Lema 5.2.3, los autovalores de $\Gamma_{m,\ell}$ son exactamente

$$\Big\{\chi_\beta(S) = \sum_{y \in S} (-1)^{\operatorname{Tr}_{2^m/2}(\beta y)} : \beta \in \mathbb{F}_{2^m}\Big\}.$$

Cuando $\beta \neq 0$, procediendo de manera análoga al caso de característica impar, obtenemos que

$$\chi_\beta(S) = \tfrac{T_{Q_\beta}-1}{3}.$$

Por el Lema 2.3.1 se tiene que $|T_{Q_\beta}| = 0$ ó $|T_{Q_\beta}| = 2^{m-\frac{r}{2}}$, donde r es el rango de la forma cuadrática $Q_{\beta,\ell}(x) = \operatorname{Tr}_{2^m/2}(\beta x^{2^\ell+1})$. Por hipótesis, m es par y $(m,\ell) = 1$, entonces por Teorema 2.4.1 los rangos posibles de $Q_{\beta,\ell}$ son m ó $m-2$. Además, cuando $T_{Q_\beta} \neq 0$ se tiene que $T_{Q_\beta} = \epsilon 2^{m-\frac{r}{2}}$, y en tal caso los posibles autovalores no triviales de Γ son

$$\frac{-1}{3}, \quad \frac{2^{\frac{m}{2}}-1}{3}, \quad \frac{-2^{\frac{m}{2}}-1}{3}, \quad \frac{2^{\frac{m}{2}+1}-1}{3}, \quad \frac{-2^{\frac{m}{2}+1}-1}{3}. \tag{5.12}$$

Claramente, de estos autovalores posibles el de mayor valor absoluto es

$$\mu = \frac{-2^{\frac{m}{2}+1} - 1}{3}.$$

Este autovalor podría no darse, sin embargo, si la cota vale para éste, entonces vale para todos. Por lo tanto, basta probar que $|\mu| \leq 2\sqrt{|S| - 1}$. Esta desigualdad es equivalente a esta otra

$$\frac{|\mu|^2}{4} + 1 \leq |S|.$$

Como $|S| = \frac{2^m - 1}{3}$, basta probar que

$$\frac{2^{m+2} + 2^{\frac{m}{2}+2} + 1}{12} + 4 \leq 2^m.$$

Claramente,

$$\frac{2^{m+2} + 2^{\frac{m}{2}+2} + 1}{12} + 4 \leq \frac{2^{m+2} + 2^{\frac{m}{2}+2}}{8} + 5 = 2^{m-1} + 2^{\frac{m}{2}-1} + 5.$$

Sólo nos resta ver que

$$2^{m-1} + 2^{\frac{m}{2}-1} + 5 \leq 2^m,$$

pero esta última desigualdad es equivalente a

$$5 + 2^{\frac{m}{2}-1} \leq 2^{m-1},$$

la cual es cierta cuando $m \geq 4$.

Ahora veamos que $\Gamma_{m,\ell}$ es un grafo de orden 2^m y $\frac{2^m-1}{3}$-regular. Como todo grafo de Cayley $X(G, S)$ tiene orden $|G|$ y es $|S|$-regular basta ver que $|S| = \frac{2^m-1}{3}$. Sea α es un elemento primitivo de $\mathbb{F}_{2^m}$. Notar que $|S_\ell| = \langle \alpha^{2^\ell+1} \rangle$, y por lo tanto $|S_\ell|$ es exactamente el orden de $\alpha^{2^\ell+1}$. Luego

$$|S_\ell| = \tfrac{2^m-1}{(2^m-1, 2^\ell+1)}.$$

Como m es par y $(m, \ell) = 1$, el Lema 3.2.2 implica que $(2^m - 1, 2^\ell + 1) = 2^{(m,\ell)} + 1 = 3$, como queríamos ver.

Sólo resta ver que $\Gamma_{m,\ell}$ es conexo. Dado que el autovalor trivial $\frac{2^m-1}{3}$ tiene multiplicidad 1, el Corolario 5.1.4 implica que $\Gamma_{m,\ell}$ es conexo. Por lo tanto $\Gamma_{m,\ell}$ es un grafo de Ramanujan. Notar que en este caso $\Gamma_{m,\ell}$ no es bipartito ya que si $\beta \neq 0$ entonces $\chi_\beta(S) \neq -|S|$, pues los únicos valores posibles para $\chi_\beta(S)$ son los dados en (5.12).

Por lo tanto, hemos probado que $\Gamma_{m,\ell}$ es un grafo de Ramanujan no bipartito $\frac{2^m-1}{3}$-regular. De manera análoga si m es múltiplo de 4 y (m, ℓ) resulta que $\Gamma_{m,\ell}$ es un grafo de Ramanujan no bipartito $\frac{2^m-1}{5}$-regular.

□

Corolario 5.3.9. *Sea* $\Gamma_{m,\ell} = X(\mathbb{F}_{2^m}, S_\ell)$ *donde* $S_\ell = \{x^{2^\ell+1} : x \in \mathbb{F}_{2^m}^*\}$ *con* $m \geq 4$ *par y* $(m, \ell) = 1$. *Entonces*

$$diam(\Gamma_{m,\ell}) \leq \frac{\log(2^m - 1)}{\log(|S_\ell|/\lambda(\Gamma_{m,\ell}))} + 1$$

donde $diam(\Gamma_{m,\ell})$ *denota el diámetro de* $\Gamma_{m,\ell}$ *y* $\lambda(\Gamma_{m,\ell})$ *es como en* (5.9).

5.3.2. Grafos de Ramanujan y formas cuadráticas generales

La construcción del grafo de Cayley $\Gamma_{m,\ell}$ corresponde a las formas cuadráticas

$$Q_{\gamma,\ell}(x) = \mathrm{Tr}_{2^m/2}(\gamma x^{2^\ell+1}) = \mathrm{Tr}_{2^m/2}(xR_{\gamma,\ell}(x))$$

donde $R_{\gamma,\ell}(x) = \gamma x^{2^\ell}$ varía en $\mathcal{L}_\ell = \langle x^{2^\ell} \rangle$. Esta construcción se generaliza fácilmente a formas cuadráticas mas generales del tipo $\mathrm{Tr}_{2^m/2}(xR(x))$ donde $R(x)$ varía en alguna familia de polinomios 2-linealizados. Más precisamente, si tomamos

$$R^{\ell_1,\ldots,\ell_h}_{\beta_1,\ldots,\beta_h}(x) = \beta_1 x^{2^{\ell_1}} + \beta_2 x^{2^{\ell_2}} + \cdots + \beta_h x^{2^{\ell_h}} \tag{5.13}$$

con $\ell_1, \ldots, \ell_h \in \mathbb{Z}_{\geq 0}$, $\beta_1, \ldots, \beta_h \in \mathbb{F}_{2^m}$, podemos definir

$$Q(x) = Q^{\ell_1,\ldots,\ell_h}_{\beta_1,\ldots,\beta_h}(x) = \mathrm{Tr}_{2^m/2}(xR^{\ell_1,\ldots,\ell_h}_{\beta_1,\ldots,\beta_h}(x)). \tag{5.14}$$

Considerando el grupo $H = \mathbb{F}_{2^m} \times \cdots \times \mathbb{F}_{2^m}(h \text{ veces}) = \mathbb{F}_{2^m}^h$ con la suma, y definiendo

$$S_Q = \{(x^{2^{\ell_1}+1}, \ldots, x^{2^{\ell_h}+1}) : x \in \mathbb{F}_{2^m}^*\}, \tag{5.15}$$

tenemos que el grafo

$$\Gamma_Q = X(H, S_Q) \tag{5.16}$$

generaliza al grafo $\Gamma_{m,\ell}$ definido anteriormente. Una pregunta natural en este contexto es ¿cuándo Γ_Q es Ramanujan?

Supongamos que existe un ℓ_i tal que $(m, \ell_i) = 1$ y además $v_2(m) \geq v_2(\ell_i)$ para $1 \leq i \leq h$. En tal caso $|S| = \frac{2^m-1}{3}$. Notar que los caracteres de $\mathbb{F}_{2^m}^h$ son de la forma

$$\chi_{(\beta_1,\ldots,\beta_h)}(x_1, \ldots, x_h) = (-1)^{\sum_{i=1}^h \mathrm{Tr}_{2^m/2}(\beta_i x_i)}$$

donde $(\beta_1, \ldots, \beta_h) \in \mathbb{F}_{2^m}^h$. Por el Lema 5.2.3, tenemos que los autovalores de $\Gamma_Q = X(H, S_Q)$ son

$$\chi_{(\beta_1,\ldots,\beta_h)}(S_Q) = \sum_{(x_1,\ldots,x_h)\in S_Q} (-1)^{\sum_{i=1}^h \mathrm{Tr}_{2^m/2}(\beta_i x_i)}.$$

Para $(\beta_1, \ldots, \beta_h) = (0, \ldots, 0)$, tenemos que

$$\chi_{(\beta_1,\ldots,\beta_h)}(S_Q) = |S_Q|$$

y si $(\beta_1, \ldots, \beta_h) \neq (0, \ldots, 0)$ entonces

$$\chi_{(\beta_1,\ldots,\beta_h)}(S_Q) = \sum_{(x_1,\ldots,x_h)\in S_Q} (-1)^{\sum_{i=1}^h \mathrm{Tr}_{2^m/2}(\beta_i x_i)} = \frac{1}{3} \sum_{x\in\mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_{2^m/2}(\sum_{i=1}^h \beta_i x^{2^{\ell_i}+1})} = \frac{T_{Q_\beta}-1}{3}.$$

Por Lema 2.3.1 sabemos que $|T_Q| = 0$ ó $2^{m-\frac{r}{2}}$, donde r es el rango de la forma cuadrática Q. Por lo tanto, asintóticamente, los autovalores en este caso están mayorados en valor absoluto por $\mu = \frac{2^{m-\frac{r}{2}}+1}{3}$. Para que

$$\mu \leq \tfrac{2}{\sqrt{3}}\sqrt{2^m - 4}$$

tiene que suceder que $2^{2m-r} + 2^{m-\frac{r}{2}+1} + 49 \leq 2^{m+3} + 2^{m+2}$, y en tal caso $r \geq m-3$ y para $m \geq 5$ se satisface.

Por lo tanto, las formas cuadráticas $Q = Q^{\ell_1,\ldots,\ell_h}_{\beta_1,\ldots,\beta_h}$ deben tener rango $r \geq m-3$ para que Γ_Q sea Ramanujan.

Del mismo modo, supongamos ahora que $v_2(m) < v_2(\ell_i)$ para algún i, entonces en este caso $|S| = 2^m - 1$, y para $(\beta_1, \ldots, \beta_h) \neq 0$ obtenemos que

$$\chi_{(\beta_1,\ldots,\beta_h)}(S) = T_Q - 1.$$

Por lo tanto, los autovalores de Γ están mayorados en valor absoluto por $\mu = 2^{m-\frac{r}{2}} + 1$, donde r es el menor rango posible de Q cuando $(\beta_1, \ldots, \beta_h)$ varía en $\mathbb{F}_{2^m}^h \setminus \{0\}$. Para que asintóticamente $\mu \leq 2\sqrt{2^m - 2}$ tiene que suceder que $2^{2m-r} + 2^{m-\frac{r}{2}+1} + 9 \leq 2^{m+2}$, en tal caso $r > m-2$ y por lo tanto $r \geq m-1$. Entonces obtenemos lo siguiente.

Teorema 5.3.10. *Sea $\Gamma_Q = Cay(H, S_Q)$ el grafo de Cayley definido en* (5.15) – (5.16) *por la familia parametrizada de formas cuadráticas $Q = Q^{\ell_1,\ldots,\ell_h}_{\beta_1,\ldots,\beta_h}$ sobre $\mathbb{F}_{2^m}$ dadas en* (5.13) – (5.14)*. Sea m suficientemente grande tal que $(m, \ell_i) = 1$ para todo $i = 1, \ldots, h$.*

- *Si $v_2(m) \geq v_2(\ell_i)$ para todo $i = 1, \ldots, h$ entonces Γ_Q es un grafo de Ramanujan no bipartito si y sólo si el rango r de Q satisface $r \geq m-3$.*

- *Si $v_2(m) < v_2(\ell_i)$ para algún $1 \leq i \leq h$ entonces Γ es un grafo de Ramanujan no bipartito si y sólo si el rango r de Q satisface $r \geq m-1$.*

Ejemplo 5.3.11. Consideremos la forma cuadrática Q_R en m variables sobre $\mathbb{F}_q$ donde

$$R(x) = \beta_1 x^{2^\ell} + \beta_2 x^{2^{3\ell}}.$$

Cuando m_ℓ es impar, entonces el rango de la forma cuadrática es m si $R \neq 0$ (ver [26]). Por la segunda parte del Teorema anterior Γ_Q es un grafo de Ramanujan $(2^m - 1)$-regular no bipartito. $\Diamond$

5.4. Grafos de Ramanujan vía funciones especiales

En esta sección construiremos grafos de Ramanujan vía funciones especiales de cuerpos finitos. Más precisamente, en la sección 5.4.1 las construcciones darán grafos de Ramanujans en característica par y en la sección 5.4.2 en característica impar. Usaremos funciones Booleanas, es decir $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, especiales como APN, AB, PN, en este caso. Mientras que en la sección 5.4.2 haremos una construcción en característica impar usando la clase de funciones planares PN.

5.4.1. Construcciones en característica par

Recordemos que en Capítulo 4 probamos que si $(m, \ell) = 1$, el dual del código $\mathcal{C}_{\ell,1}$ es optimal en el sentido que su distancia es lo más grande posible entre una cierta familia de códigos cíclicos binarios.

La optimalidad de este código implica que la función $F(x) = x^{2^\ell+1}$ usada para construir el cero $\alpha^{-(2^\ell+1)}$ es especial, como lo notó Charpin en [6].

Esta función cae en una clase especial de funciones Booleanas, las llamadas APN (*almost perfect nonlinear*), que definimos abajo. Más aún, cuando m es impar esta función resulta ser una función AB, por *almost bent* (ver Definición 5.4.6). También haremos uso de funciones PN (*perfect nonlinear*).

Comenzamos definiendo distintos tipos de funciones Booleanas.

Definición 5.4.1. Una función $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^r}$ con $1 \leq r \leq m$ se dice (m, r)-*Booleana*. F es m-*Booleana* si $r = m$ y *Booleana* si $r = 1$.

Ahora seguimos con las funciones *casi perfectas no-lineales*.

Definición 5.4.2. Una función m-Booleana $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ se dice APN (*almost perfect nonlinear*) sobre $\mathbb{F}_{2^m}$ si para todo $a, b \in \mathbb{F}_{2^m}$, $a \neq 0$, la ecuación

$$F(x + a) + F(x) = b \tag{5.17}$$

tiene a lo sumo 2 soluciones.

En el caso binario, podemos generalizar la construcción del grafo $\Gamma_{m,\ell} = X(\mathbb{F}_{2^m}, S_\ell)$ donde S_ℓ como en (5.3) para cualquier función APN. Dada F una función APN, definimos el grafo de Cayley

$$\Gamma_F = X(\mathbb{F}_{2^m}, S_F) \qquad \text{con} \qquad S_F = \{F(x) : x \in \mathbb{F}_{2^m}^*\}. \tag{5.18}$$

Notar que si $F(x) = x^{2^l+1}$ entonces $\Gamma_F = \Gamma_\ell$

Una inquietud natural que surge en este contexto es la siguiente

Pregunta. ¿Cuándo el grafo de Cayley $\Gamma_F = X(\mathbb{F}_{2^m}, S_F)$ es Ramanujan?

Funciones APN monomiales

Para empezar, es importante notar que la función F en (5.18) debe cumplir $F(x) \neq 0$ para todo $x \in \mathbb{F}_{2^m}^*$, ya que de otro modo el grafo Γ_F tendría lazos y no sería simple. Un ejemplo de funciones APN satisfaciendo esta condición, son las funciones APN monomiales de la forma

$$F(x) = x^h.$$

En este caso, escribimos S_{x^h} en lugar de S_F. Notar que $S_\ell = S_{x^{q^\ell+1}}$, con $q = 2$. Por ejemplo, tenemos $S_1 = S_{x^3}$.

Estas funciones satisfacen la siguiente propiedad (ver [36]).

Proposición 5.4.3. *Sea $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ una función APN de la forma $F(x) = x^h$. Luego,*

- *Si m es par, entonces $(h, 2^m - 1) = 3$.*
- *Si m es impar, entonces $(h, 2^m - 1) = 1$.*

Esta proposición implica que si m es impar, entonces Γ_F es el grafo completo para toda función APN monomial F, ya que en este caso $S_F = \mathbb{F}_{q^m}^*$ y por lo tanto todos los vértices son vecinos en Γ_F, y es bien sabido que el grafo completo es un grafo de Ramanujan (trivial). Sin embargo, si m es par, el grafo Γ_F es un grafo $\frac{2^m-1}{3}$-regular.

En este punto parecería que tenemos muchas elecciones de funciones APN tal que Γ_F es un grafo de Ramanujan, sin embargo resulta que todas dan lugar a un único grafo, como veremos a continuación.

Proposición 5.4.4. *Sea $m \geq 4$ par y $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ una función APN monomial. Entonces, los grafos de Cayley $\Gamma_F = X(\mathbb{F}_{2^m}, S_F)$, $\Gamma_{x^3} = X(\mathbb{F}_{2^m}, S_{x^3})$ y $\Gamma_{m,1} = X(\mathbb{F}_{2^m}, S_1)$ coinciden. Por lo tanto, Γ_F es un grafo de Ramanujan.*

Demostración. Sea $m \geq 4$ par y $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ una función APN monomial, digamos $F(x) = x^h$ con $h \in \mathbb{N}$.

Notar que $S_F = \{x^h : x \in \mathbb{F}_{2^m}^*\} = \langle \alpha^h \rangle$, donde α es un generador de $\mathbb{F}_{2^m}^*$. Por lo tanto S_F es un subgrupo del grupo cíclico $\mathbb{F}_{2^m}^*$ de orden $\frac{2^m-1}{3}$. Como todo grupo cíclico tiene un único subgrupo por cada divisor de su orden, resulta que $S_F = \langle \alpha^3 \rangle$.

Por lo dicho previamente, el grafo de Cayley $\Gamma_F = X(\mathbb{F}_{2^m}, S_F)$ es igual a $\Gamma_{x^3} = X(\mathbb{F}_{2^m}, S_{x^3})$, donde $S_{x^3} = \{x^3 : x \in \mathbb{F}_{2^m}^*\}$, el cual a la vez coincide con $\Gamma_{m,1} = Cay(\mathbb{F}_{2^m}, S_1)$. Por el Teorema 5.3.8, este último resulta de Ramanujan. Luego, Γ_F es un grafo de Ramanujan no bipartito $\frac{2^m-1}{3}$-regular. □

Funciones AB

Comencemos definiendo la clase de funciones AB con las que construiremos nuevos grafos de Ramanujan.

Definición 5.4.5. Las *funciones componentes* de una función (m, r)-Booleana F son las funciones $f_\beta : \mathbb{F}_{2^m} \to \mathbb{F}_2$ dadas por

$$f_\beta(x) = \mathrm{Tr}_{2^r/2}(\beta F(x))$$

para cada $\beta \in \mathbb{F}_{2^r}$. La *transformada de Walsh* de F es

$$\mathcal{L}_F(\beta, \gamma) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f_\beta(x) + \mathrm{Tr}_{2^m/2}(\gamma x)} \in \mathbb{Z} \tag{5.19}$$

para $\beta \in \mathbb{F}_{2^r}$, $\gamma \in \mathbb{F}_{2^m}$.

Notar que $\mathcal{L}_F(\beta, \gamma)$ es un entero por ser suma de ± 1's.

Definición 5.4.6. Una función m-Booleana F se dice AB (*almost bent*) si su transformada de Walsh sólo puede tomar los valores 0 y $\pm 2^{\frac{m+1}{2}}$, es decir

$$\mathcal{L}_F(\beta, \gamma) \in \{0, \pm 2^{\frac{m+1}{2}}\}$$

para todo $\beta, \gamma \in \mathbb{F}_{2^m}$.

Notar que este tipo de funciones sólo están definidas cuando m es impar. Además, toda función AB es una función APN (ver [36]). Sin embargo, hay funciones APN que no son AB, por ejemplo, $F(x) = x^{-1}$ en F_{2^m} con m impar.

Primera construcción. Al igual que antes, uno puede considerar el grafo Γ_F con F función AB monomial, pero no ganaríamos mucho ya que toda función AB es una función APN, y ya vimos que si m es impar toda función APN monomial induce el grafo completo. Sin embargo, para funciones AB es posible considerar otro grafo muy similar a Γ_F.

Tomemos el grupo abeliano $G = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Sus caracteres son de la forma

$$\chi_{\beta,\gamma}(x, y) = (-1)^{\mathrm{Tr}_{2^m/2}(\beta x + \gamma y)} \tag{5.20}$$

donde $\beta, \gamma \in \mathbb{F}_{2^m}$.

Dada $F(x)$ una función AB sobre $\mathbb{F}_{2^m}$, podemos considerar el grafo de Cayley

$$\Gamma_F^* = X(\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}, R_F) \quad \text{donde} \quad R_F = \{(x, F(x)) : x \in \mathbb{F}_{2^m}^*\}. \tag{5.21}$$

Notar que, en este caso, R_F es el gráfico de la función sin considerar el punto $(0, F(0))$. Además $|R_F| = 2^m - 1$, ya que la cantidad de pares ordenados en R_F está determinado por la primer variable. Por lo tanto, Γ_F^* es un grafo $(2^m - 1)$-regular. Como todos los caracteres de G son como en en (5.20), por Lema 5.2.3 sus autovalores de Γ_F^* están dados por las sumas

$$\chi_{\gamma,\beta}(R_F) = \sum_{(x,y) \in R_F} \chi_{\gamma,\beta}(x, y) = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{f_\beta(x) + \mathrm{Tr}_{2^m/2}(\gamma x)}$$

con $\beta, \gamma \in \mathbb{F}_{2^m}$, y donde $f_\beta(x)$ son las funciones componentes de F si $\beta \neq 0$, y 0 si $\beta = 0$. Luego,

$$\chi_{\gamma,\beta}(R_F) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f_\beta(x)+\mathrm{Tr}_{2^m/2}(\gamma x)} - (-1)^{f_\beta(0)} \tag{5.22}$$

Como F es una función AB tenemos que

$$\chi_{\gamma,\beta}(R_F) \in \{\pm 1,\ 2^{\frac{m+1}{2}} \pm 1,\ -2^{\frac{m+1}{2}} \pm 1\},$$

cuando $(\gamma, \beta) \neq (0, 0)$. Por otro lado, si $(\gamma, \beta) = (0, 0)$ entonces $\chi_{\gamma,\beta}(R_F) = 2^m - 1$. Luego, los posibles autovalores de Γ_F^* son

$$\pm 1, \quad 2^{\frac{m+1}{2}} \pm 1, \quad -2^{\frac{m+1}{2}} \pm 1, \quad 2^m - 1.$$

Notar que la multiplicidad del autovalor trivial del grafo Γ_F^* (el grado de regularidad $2^m - 1$) en este caso es 1. Por Corolario 5.1.4 el grafo Γ_F^* tiene una única componente conexa y por lo tanto es conexo.

Por otra parte, se puede probar al igual que antes que para $m \geq 5$ se satisface la desigualdad

$$\lambda(\Gamma_F^*) \leq 2\sqrt{|R_F| - 1}.$$

Por lo tanto obtenemos el siguiente resultado.

Teorema 5.4.7. *Sea $m \geq 5$ impar y $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ una función AB. Entonces Γ_F^* como en* (5.21) *es un grafo de Ramanujan entero $(2^m - 1)$-regular no bipartito.*

Este último teorema se aplica no solamente para funciones AB monomiales sino que para cualquier función AB. Notar además que si $F(0) \neq 0$ es posible considerar el grafo de Cayley

$$\widehat{\Gamma}_F = X(G, R'_F). \tag{5.23}$$

donde $G = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ y

$$R'_F = \{(x, F(x)) : x \in \mathbb{F}_{2^m}\}.$$

En este caso $|R'_F| = 2^m$ y, razonando de la misma manera que antes, obtenemos que los autovalores de $\widehat{\Gamma}_F$ son

$$0, \quad 2^{\frac{m+1}{2}}, \quad -2^{\frac{m+1}{2}}, \quad 2^m.$$

Claramente, los autovalores no triviales de $\widehat{\Gamma}_F$ satisfacen la desigualdad

$$\lambda(G) \leq 2\sqrt{2^m - 1}.$$

Notar que al igual que Γ_F (con $F(0) \neq 0$), este grafo tiene su espectro simétrico si no tenemos en cuenta su autovalor trivial.

Teorema 5.4.8. *Sea $m \geq 5$ impar y $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ una función AB tal que $F(0) \neq 0$. Entonces $\widehat{\Gamma}_F$ como en* (5.23) *es un grafo de Ramanujan entero 2^m-regular no bipartito.*

Demostración. Sólo queda probar que $\widehat{\Gamma}_F$ es un grafo conexo. Notar que si $F(0) = \omega \neq 0$, entonces $G(x) = F(x) + \omega$ es una función AB tal que $G(0) = 0$. En efecto, si $g_\beta(x)$ son las funciones componentes de $G(x)$, entonces

$$g_\beta(x) = \mathrm{Tr}_{2^m/2}(\beta G(x)) = \mathrm{Tr}_{2^m/2}(\beta F(x)) + \mathrm{Tr}_{2^m/2}(\beta\omega) = f_\beta(x) + C_{\beta,\omega},$$

donde $f_\beta(x)$ son las funciones componentes de $F(x)$ y $C_{\beta,\omega} = \mathrm{Tr}_{2^m/2}(\beta\omega)$. Entonces, la transformada de Walsh de $G(x)$ satisface

$$\mathcal{L}_G(\beta,\gamma) = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{g_\beta(x)+\mathrm{Tr}_{2^m/2}(\gamma x)} = (-1)^{C_{\beta,\omega}}\mathcal{L}_F(\beta,\gamma).$$

De este modo $\mathcal{L}_G(\beta,\gamma) \in \{0, \pm 2^{\frac{m+1}{2}}\}$, por lo tanto G es una función AB y por construcción $G(0) = 0$.

Por Teorema 5.4.7, Γ_G^* es un grafo de Ramanujan y en particular es un grafo conexo. Sea $(z_1, z_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \setminus \{(0,0)\}$, para probar que $\widehat{\Gamma}_F$ es conexo, basta probar que existe un camino de $(0,0)$ a (z_1, z_2). Como Γ_G^* es conexo, existen $x_1, \ldots, x_m \in \mathbb{F}_{2^m}$ tales que

$$x_1 + \cdots + x_m = z_1 \quad \text{y} \quad G(x_1) + \cdots + G(x_m) = z_2.$$

Por definición de G tenemos que

$$F(x_1) + \cdots + F(x_m) + m\omega = z_2.$$

Dado que estamos en característica 2, resulta que $m\omega$ es 0 si m es par y ω si m es impar. Por lo tanto, si m es par obtenemos el camino que buscábamos. Ahora, supongamos que m es impar, entonces

$$F(x_1) + \cdots + F(x_m) + \omega = z_2.$$

Como $F(0) = \omega$, obtenemos que

$$x_1 + \cdots + x_m + 0 = z_1 \quad \text{y} \quad F(x_1) + \cdots + F(x_m) + F(0) = z_2.$$

Luego $\widehat{\Gamma}_F$ es un grafo conexo y, por lo visto en la discusión previa al teorema, $\widehat{\Gamma}_F$ es un grafo de Ramanujan no bipartito 2^m-regular. □

Segunda construcción. Veamos que es posible definir otros grafos de Ramanujan con una función AB. Supongamos que m es un entero positivo impar, y sea $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ una función AB. Para cada $s \mid m$, consideremos el mapeo traza $\mathrm{Tr}_{2^m/2^s}(x)$ y definamos

$$F_s(x) = \mathrm{Tr}_{2^m/2^s}(F(x)).$$

Llamaremos Γ_s al grafo de Cayley

$$\Gamma_s = X(\mathbb{F}_{2^m} \times \mathbb{F}_{2^s}, S_{F_s}), \tag{5.24}$$

donde

$$S_{F_s} = \{(x, F_s(x)) : x \in \mathbb{F}_{2^m}^*\}.$$

En este caso los caracteres del grupo $\mathbb{F}_{2^m} \times \mathbb{F}_{2^s}$ son de la forma

$$\chi_{a,b}(x) = (-1)^{\mathrm{Tr}_{2^m/2}(ax)+\mathrm{Tr}_{2^s/2}(bx)}$$

donde $a \in \mathbb{F}_{2^m}$ y $b \in \mathbb{F}_{2^s}$. Por lo tanto los autovalores del grafo Γ_s son sumas exponenciales del tipo

$$\sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_{2^m/2}(ax)+\mathrm{Tr}_{2^s/2}(bF_s(x))}.$$

Usando la $\mathbb{F}_{2^s}$-linealidad de la función traza $\mathrm{Tr}_{2^m/2^s}$ y que además

$$\mathrm{Tr}_{2^m/2}(x) = (\mathrm{Tr}_{2^s/2} \circ \mathrm{Tr}_{2^m/2^s})(x)$$

se tiene que

$$\mathrm{Tr}_{2^s/2}(bF_s(x)) = \mathrm{Tr}_{2^m/2}(bF(x)).$$

Por lo tanto, los autovalores de Γ_s están dados por las sumas

$$\sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_{2^m/2}(ax)+\mathrm{Tr}_{2^m/2}(bF(x))} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(ax)+\mathrm{Tr}_{2^m/2}(bF(x))} - (-1)^{\mathrm{Tr}_{2^m/2}(bF(0))}.$$

Como la función es AB, al igual que antes los posibles autovalores del grafo son

$$\pm 1, \quad 2^{\frac{m+1}{2}} \pm 1, \quad -2^{\frac{m+1}{2}} \pm 1, \quad 2^m - 1.$$

Para mostrar que Γ_s es conexo, basta ver que dado cualquier vértice (z_1, z_2) distinto del $(0,0)$ en Γ_s existe un camino de $(0,0)$ a (z_1, z_2). Por definición de Γ_s, dicho camino existe si y sólo si existen $x_1, \ldots, x_m \in \mathbb{F}_{2^m}$ tales que

$$x_1 + \cdots + x_m = z_1 \quad \text{y} \quad F_s(x_1) + \cdots + F_s(x_m) = z_2.$$

Como la función traza es sobre existe $z_2' \in \mathbb{F}_{2^m}$ tal que $\mathrm{Tr}_{2^m/2^s}(z_2') = z_2$. Como Γ_F^* es conexo, existen $x_1, \ldots, x_m \in \mathbb{F}_{2^m}$ tal que

$$x_1 + \cdots + x_m = z_1 \quad \text{y} \quad F(x_1) + \cdots + F(x_m) = z_2'.$$

Podemos tomar traza en la segunda ecuación, por linealidad de la función traza obtenemos que

$$F_s(x_1) + \cdots + F_s(x_m) = z_2.$$

Por lo tanto Γ_s es un grafo conexo. En consecuencia, al igual que antes, Γ_s resulta un grafo de Ramanujan no bipartito para cada $s \mid m$.

Teorema 5.4.9. *Sea $m \geq 5$ impar y $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ una función AB. Entonces Γ_s es un grafo de Ramanujan entero $(2^m - 1)$-regular no bipartito para cada $s \mid m$.*

De igual manera que antes, si $F_s(0) \neq 0$ es posible considerar el grafo de Cayley $\Gamma_s' = X(\mathbb{F}_{2^m} \times \mathbb{F}_{2^s}, R_{F_s})$ donde

$$R_{F_s} = \{(x, F_s(x)) : x \in \mathbb{F}_{2^m}\}$$

y así obtener un grafo de Ramanujan 2^m-regular.

Teorema 5.4.10. *Sean $m \geq 5$ impar, s un entero positivo tal que $s \mid m$ y $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ una función AB tal que $F_s(0) \neq 0$. Entonces Γ'_s es un grafo de Ramanujan entero 2^m-regular no bipartito.*

Es natural preguntarse si es posible definir grafos a partir del gráfico de funciones APN para m par. Notar que si consideramos, por ejemplo, la función $F(x) = x^3$, en este caso la transformada de Walsh de $F(x)$ toma los valores $\{0, \pm 2^{\frac{m}{2}}, \pm 2^{\frac{m+2}{2}}\}$. En tal caso se puede verificar que el grafo Γ^*_F no satisface la desigualdad $\lambda(\Gamma^*_F) \leq 2\sqrt{|S_F| - 1}$ y por lo tanto no es Ramanujan. Por lo tanto, cuando m es par Γ^*_F no necesariamente es Ramanujan si F es una función APN.

Cuando m es impar es posible encontrar funciones APN que no son AB, pero los valores de su transformada de Walsh implican que Γ^*_F es un grafo de Ramanujan.

Existen otra clases de funciones Booleanas especiales cuyos valores de la transformada de Walsh permiten encontrar grafos de Ramanujan como veremos a continuación.

Definición 5.4.11. Una (m, r)-función Booleana F es una función PN (perfect nonlinear) si satisface que

$$\mathcal{L}_F(\beta, \gamma) \in \{\pm 2^{\frac{m}{2}}\}$$

para todo $\beta \in \mathbb{F}_{2^r}, \gamma \in \mathbb{F}_{2^m}$.

Tenemos el siguiente resultado debido a K. Nyberg ([39]).

Lema 5.4.12. *Si F es una (m, r)-función Booleana PN, entonces m es par y $r \leq m/2$.*

Dada F una (m, r)-función PN, para cada $s \mid r$ podemos considerar el grafo Γ_s. De la misma manera que sucedía con las funciones AB, estos resultan ser Ramanujan, ya que en este caso los autovalores del grafo son

$$2^{\frac{m}{2}} \pm 1, \quad -2^{\frac{m}{2}} \pm 1, \quad 2^m - 1.$$

Al igual que antes $2^m - 1$ es un autovalor con multiplicidad 1.

Teorema 5.4.13. *Sea $m \geq 4$ par y $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^r}$ una (m, r)-función PN. Entonces Γ_s es un grafo de Ramanujan entero $(2^m - 1)$-regular no bipartito para cada $s \mid r$.*

5.4.2. Construcciones en característica impar

En esta sección, varemos que podemos hacer construcciones de grafos de Ramanujan similares a las de la sección anterior pero en característica impar. Veamos las definiciones básicas que nos harán falta.

Sea f una función de $\mathbb{F}_{p^m}$ a $\mathbb{F}_p$. Recordemos que $\zeta_p = e^{\frac{2\pi i}{p}}$ y denotemos por χ_f a la función *signo* de f definida por

$$\chi_f(x) = \zeta_p^{f(x)}$$

para todo $x \in \mathbb{F}_{p^m}$. La transforma de Fourier $\widehat{\chi}_f$ de la función χ_f está definida por

$$\widehat{\chi}_f(b) = \sum_{x \in \mathbb{F}_{p^m}} \chi_f(x)\, \zeta_p^{-b \cdot x}.$$

A $\widehat{\chi}_f(b)$ se la llama la *transformada de Walsh* de f en b, donde $\cdot$ es cualquier producto escalar en $\mathbb{F}_{p^m}$. Como la noción de una transformada de Walsh refiere a un producto escalar, es conveniente elegir el isomorfismo tal que el producto escalar en $\mathbb{F}_{p^m}$ coincida con el producto escalar canónico en $\mathbb{F}_{p^m}$, que es la traza del producto

$$b \cdot x := \mathrm{Tr}_{p^m/p}(bx).$$

Por lo tanto la transformada de f en b está definida por

$$S_f(b) = \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{f(x) - \mathrm{Tr}_{p^m/p}(bx)}.$$

Podemos recuperar a la función f vía la fórmula de inversión

$$\zeta_p^{f(x)} = \tfrac{1}{p^m} \sum_{b \in \mathbb{F}_{p^m}} S_f(b)\, \zeta_p^{\mathrm{Tr}_{p^m/p}(bx)}.$$

Evaluando en $x = 0$, se tiene que para todo función f de $\mathbb{F}_{p^m}$ a $\mathbb{F}_p$

$$\sum_{b \in \mathbb{F}_{p^m}} S_f(b) = p^m \chi_f(f(0)).$$

Además, se tiene la *Identidad de Parseval*

$$\sum_{b \in \mathbb{F}_{p^m}} |S_f(b)|^2 = p^{2m}.$$

Definición 5.4.14. Una función f se dice *bent p-aria* si todos sus coeficientes de Walsh satisfacen $|S_f(b)|^2 = p^m$. Una función bent se dice *regular* si para todo $b \in \mathbb{F}_{p^m}$,

$$p^{-\frac{m}{2}} S_f(b) = \zeta_p^{f^\star(b)}$$

para alguna función $f^\star : \mathbb{F}_{p^m} \to \mathbb{F}_p$. Esta función $f^\star$ es llamada la *función dual* de f.

Para construir los grafos nos van a interesar funciones F de $\mathbb{F}_{p^m}$ en sí mismo, tal que sus funciones componentes $f_a(x) = \mathrm{Tr}_{p^m/p}(aF(x))$ sean funciones bent p-arias.

Definición 5.4.15. Sea $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$, se dice que F es una función planar o PN (perfect nonlinear) si para cualquier $a \in \mathbb{F}_{p^m}^*$ el mapeo $x \mapsto F(x+a) - F(x)$ es biyectivo.

Veamos algunos ejemplos de este tipo de funciones.

Ejemplo 5.4.16. Sea $F(x) = x^{\frac{3^\ell+1}{2}}$ la función definida sobre $\mathbb{F}_{3^m}$ tal que $(m, \ell) = 1$ y ℓ impar. Esta función fue estudiada por Coulter-Mathews y probó que es una función es planar.

Ejemplo 5.4.17. Sea $F(x) = x^{p^\ell+1}$ la función definida sobre $\mathbb{F}_{p^m}$ tal que p es impar y $m/(m,\ell)$ también es impar. Esta función es planar y es llamada función de Dembowsky-Östrom.

Notar que ambas funciones de los ejemplos son funciones pares.

La siguiente proposición es la clave para unir la nociones de función planar y funciones bent ([5]).

Proposición 5.4.18. *Sea $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$. Entonces F es una función planar si y sólo si para todo $a \in \mathbb{F}_{p^m}^*$ las funciones componentes $\mathrm{Tr}_{p^m/p}(aF(x))$ de F son funciones bent p-arias.*

Lema 5.4.19. *Sea F función planar sobre $\mathbb{F}_{p^m}$ con p un primo impar y $F(0) = 0$. Si $S_F = \{(x, F(x)) : x \in \mathbb{F}_{p^m}^*\}$, entonces $-S_F \cap S_F = \varnothing$.*

Demostración. Supongamos que $-S_F \cap S_F \neq \varnothing$, entonces existen x e y en $\mathbb{F}_{p^m}^*$ tal que

$$(x, F(x)) = -(y, F(y)),$$

entonces $x = -y$ con $F(x) = -F(y)$, es decir que F satisface $F(-y) = -F(y)$.

Como $y \neq 0$, consideremos la función $\Delta_y(t) = F(t-y) - F(t)$. Luego, como $F(0) = 0$ obtenemos que

$$\Delta_y(0) = F(0-y) - F(0) = F(-y) = -F(y).$$

Además, evaluando en y tenemos que

$$\Delta_y(y) = -F(y).$$

Como F es una función planar, Δ_y es una función biyectiva y, por lo tanto $y = 0$, llegando así a un absurdo de la suposición que x, y eran distintos de 0. Por lo tanto

$$-S_F \cap S_F = \varnothing$$

como queríamos demostrar. □

Dada F una función planar par con $F(0) = 0$, consideremos

$$T_F = -S_F \cup S_F.$$

Luego, T_F es simétrico en el sentido que $-T_F = T_F$ y además el lema anterior implica que

$$|T_F| = |S_F| + |-S_F| = 2|S_F| = 2(p^m - 1).$$

Entonces el grafo de Cayley $\Gamma_{F,p} = X(G, T_F)$, donde $G = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, es un grafo simple $(2p^m - 2)$-regular. Vamos a probar que este grafo es Ramanujan.

Teorema 5.4.20. *Sea p un primo impar y $m \geq 4$. Sea F una función planar sobre $\mathbb{F}_{p^m}$ con $F(0) = 0$. Consideremos $G = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ y $T_F = -S_F \cup S_F$, donde S_F es el conjunto*

$$S_F = \{(x, F(x)) : x \in \mathbb{F}_{p^m}^*\}.$$

Entonces, el grafo de Cayley $\Gamma_{F,p} = X(G, T_F)$ es un grafo de Ramanujan $(2p^m - 2)$-regular no bipartito.

Demostración. Los autovalores de $\Gamma_{F,p}$ estan dados por

$$\chi_{a,b}(T_F) = \sum_{(x,y)\in T_F} \chi_{a,b}(x, y) = \sum_{(x,y)\in S_F} \chi_{a,b}(x, y) + \sum_{(x,y)\in -S_F} \chi_{a,b}(x, y)$$

donde $\chi_{a,b}(x, y) = \zeta_p^{\mathrm{Tr}_{p^m/p}(ax+by)}$. Por definición de S_F tenemos que

$$\begin{aligned} \chi_{a,b}(T_F) &= \sum_{x\in\mathbb{F}_{p^m}^*} \zeta_p^{\mathrm{Tr}_{p^m/p}(ax+bF(x))} + \sum_{x\in\mathbb{F}_{p^m}^*} \zeta_p^{\mathrm{Tr}_{p^m/p}(-ax+bF(-x))} \\ &= \sum_{x\in\mathbb{F}_{p^m}^*} \zeta_p^{f_b(x)+\mathrm{Tr}_{p^m/p}(ax)} + \sum_{x\in\mathbb{F}_{p^m}^*} \zeta_p^{f_b(x)-\mathrm{Tr}_{p^m/p}(ax)} \end{aligned}$$

donde $f_b(x) = \mathrm{Tr}_{p^m/p}(bF(x))$ es la función componente de F.

Como F es una función planar con $F(0) = 0$, sus funciones componentes $f_b(x)$ son funciones bent p-arias para $b \neq 0$. Luego,

$$|\chi_{a,b}(T_F)| \leq 2p^{\frac{m}{2}} + 2.$$

Por lo tanto, basta probar que

$$2p^{\frac{m}{2}} + 2 \leq 2\sqrt{2p^m - 3}.$$

Esta última desigualdad es equivalente a esta otra

$$(p^{\frac{m}{2}} + 1)^2 \leq 2p^m - 3,$$

que a su vez es equivalente a

$$2p^{\frac{m}{2}} + 4 \leq p^m.$$

Luego, se tiene que

$$5 \leq (p^{\frac{m}{2}} - 1)^2.$$

Evidentemente esta última desigualdad es válida para $m \geq 4$.

Si $b = 0$ y $a \neq 0$, entonces por las propiedades de ortogonalidad de los caracteres del cuerpo finito $\mathbb{F}_{p^m}$ tenemos que $\chi_{a,b}(T_F) = -2$, que trivialmente satisface la desigualdad $|\chi_{a,b}(T_F)| \leq 2\sqrt{|T_F| - 1}$.

Por último, notemos que el autovalor trivial $|T_F|$ se alcanza sólo cuando $a = b = 0$ y entonces tiene multiplicidad 1 implicando que $\Gamma_{F,p}$ es un grafo conexo no bipartito. Por lo tanto $\Gamma_{F,p}$ resulta ser un grafo de Ramanujan. □

Bibliografía

[1] T.P. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbb{F}_2^n$. *IEEE Trans. on Inform. Theory* **52:9** (2006), 4160–4170.

[2] L.D. Baumert, R.J. MacEliece. Weights of irreducible cyclic codes. *Inform. Contr.* **20** (1972), 158–175.

[3] B. Berndt, R.J. Evans, K. Williams. Gauss and Jacobi sums *New York: Wiley* 1998.

[4] C. Carlet, P. Charpin, V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography* **15:2** (1998), 125–156.

[5] C. Carlet, S. Dubuc. On generalized bent and q-ary perfect nonlinear functions. *Fifth International Conference Finite Fields and Applications*, 81–94, 2001.

[6] P. Charpin. Open problems on cyclic codes. *Handbook of coding theory*, vol. 1, 963–1063, 1998.

[7] F.R.K. Chung. Diameters and eigenvalues. *Journal of the American math. Society*, vol. 2, 187-196, 1989.

[8] P. Delsarte. On subeld subcodes of modied Reed-Solomon codes. *IEEE Trans. Inform. Theory* **21:5** (1975), 575–576.

[9] C. Ding, T. Helleseth, T. Klove, X. Wang. A general construction of authentication codes. *IEEE Trans. Inform. Theory* **53:6** (2007), 2229–2235.

[10] C. Ding, X. Wang. A coding theory construction of new systematic authentication codes. *Theoret. Comput. Sci.* **330:1**, (2005), 81–99.

[11] H.Q. Dinh, C. Li, Q. Yue. Recent progress on weight distributions of cyclic codes over finite fields. *J. Algebra Comb. Discrete Appl.* **2:1** (2014), 39–63.

[12] S. Draper, X. Hou. Explicit Evaluation of Certain Exponential Sums of Quadratic Functions over $\mathbb{F}_{p^n}$, p Odd. *arXiv preprint arXiv:0708.3619*, 2007.

[13] K. Feng, J. Luo. Value distributions of exponential sums from perfect nonlinear functions. *IEEE Trans. Inform. Theory* **53:9** (2007), 3035–3041.

[14] K. Feng, J. Luo. Weight distribution of some reducible cyclic codes. *Finite fields Appl.* **14** (2008), 390–409.

[15] K. Feng, J. Luo. On the weight distribution of two classes. *IEEE Trans. Inform. Theory* **54:12** (2008), 5332–5344.

[16] K. Feng, J. Luo. Cyclic codes from generalized Coulter-Matthews functions. *IEEE Trans. Inform. Theory* **54:12** (2008), 5345–5353.

[17] T. Helleseth, A. Kholosha. Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Trans. Inform. Theory* **52:5** (2006) 2018–2032.

[18] W. C. Huffman, V. Pless. Fundamentals of error correcting codes. *Cambridge University Press* (2003).

[19] Y. Ihara On discrete subgroup of the two by two projective linear group over p-adic field. *J. Math. Soc. Japan* **18** (1966), 219–235.

[20] S. Li, S. Hu, T. Feng, G. Ge. The weight distribution of a class of cyclic codes related to Hermitian forms graphs. *IEEE Trans. Inform. Theory* **59:5** (2013), 3064–3067.

[21] R. Lidl, H. Niederreiter. Finite fields. *Reading, MA: Addison-Wesley, vol. 20* (1983).

[22] J. Luo, Y. Tang, H. Wang. Cyclic codes and sequences: the generalized Kasami case. *IEEE Trans. Inform. Theory* **56:5** (2010), 2130–2142.

[23] H. Janwa, R.M. Wilson. Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in char. 2 and some applications to cyclic codes. *Springer Verlag, New York/Berlin* **673** (1993), 180–194.

[24] H. Janwa, G. McGuire, R.M. Wilson. Double-error-correcting codes and absolutely irreductible polynomials over $GF(2)$. *Journal of Algebra* **178** (1995), 665–676.

[25] T. Kasami. Weight distributions of Bose-Chaudhuri-Hocquenghem Codes. *Combinatorial Math. and Applications* **Ch. 20** (1969).

[26] T. Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Info. and Control* **18** (1971) 369–394.

[27] A. Klapper. Cross-relations of geometric sequences in characteristic two. *Des. Codes Cryptogr.* **3:4** (1993), 347–377.

[28] A. Klapper. Cross-relations of quadratic forms sequences in odd characteristic. *Des. Codes Cryptogr.* **3:4** (1997), 289–305.

[29] T. Klove Codes for error detection. *Signapore: World scientific* 2007.

[30] G. Lachaud. Distribution of the weights of the dual of the Melas code. *Discrete Mathematics* **79** (1989), 103–106.

[31] X. Liu, J. Luo. The weight distributions of some cyclic codes with three or four nonzeros over $\mathbb{F}_3$. *Designs, codes and cryptography* **73(3)** (2014), 747–768.

[32] A. Lubotzky, R. Phillips, P. Sarnak. Ramanujan graphs. *Combinatorica*, **8:3** (1988), 261–277.

[33] A. Marcus, D.A. Spielman, N. Srivastava. Interlacing families I: Bipartite Ramanujan graphs of all degrees. *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium*, 529–537.

[34] C. Moreno. Algebraic curves over finite fields. *Cambridge University Press* (1991).

[35] F.J. MacWilliams, N.J.A. Sloane. The theory of error correcting codes. *North-Holland Publishing Company* (1977).

[36] G. L. Mullen, D. Panario. Handbook of finite fields. *CRC Press*, 2013.

[37] M. Morgenstern. Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q. *Journal of Combinatorial Theory*, Series B **62:1** (1994), 44–62.

[38] R. Murty. Ramanujan Graphs. *J. Ramanujan Math. Soc.*, **18** No. 1 (2003), 1–20.

[39] K. Nyberg. Perfect non-linear S-boxes. *In Proceedings of* Eurocrypt *'91, Lecture Notes in Computer Science* **547**, 378–386, 1992.

[40] V. Pless. Power moment identities on weight distributions in error correcting codes. *Information and Control* **6**, 2, (1963), 147–152.

[41] S. Roman. Coding and information theory, *Springer Verlag* (1992).

[42] R. Schoof, M. Van der Vlugt. Hecke operators and the weight distribution of certain codes. *Journal of Comb. Theory* Series A **57** (1991), 163–186.

[43] G. Van der Geer, M. Van der Vlugt. Reed Muller codes and supersingular curves I. *Compositio Math.* **84** (1992), 333–367.

[44] G. Van der Geer, M. Van der Vlugt. Weight distributions for a certain class of codes and maximal curves . *Discrete Mathematics* **106/107** (1992), 209–218.

[45] G. van Lint, R.M. Wilson. On the minimum distance of cyclic codes. *IEEE Trans. on Information Theory* **32:1** (1986), 23–40.

[46] G. van Lint, R.M. Wilson. Binary cyclic codes generated by $m_1 m_7$. *IEEE Trans. on Information Theory* **32:2** (1986), 283.

[47] J. Wolfmann. The weights of the dual code of the Melas code over $GF(3)$. *Discrete Mathematics* **74:3** (1989), 327–329.

[48] J. Wolfmann, G. Lachaud. Kloosterman sums, elliptic curves and cyclic codes in characteristic 2. *Comptes rendus de l'academie des sciences serie I-mathematique* **305:20** (1987), 881–883.

[49] X. Zeng, L. Hu, W. Jiang, Q. Yue, X. Cao. The weight distribution of a class of p-ary cyclic codes. *Finite Fields Appl.* **16** (2010), 56–73.

[50] D. Zheng, X. Wang, X. Zeng, L. Hu. The weight distribution of two classes of p-ary cyclic codes. *Finite Fields Appl.* **29** (2014), 202–224.

[51] D. Zheng, X. Wang, X. Zeng, L. Hu. The weight distribution of a family of p-ary cyclic codes. *Des. Codes Cryptogr.* Doi: 10.1007/s10623-013-9908-2 (2013).

[52] Z. Zhou, C. Ding. A class of three-weight cyclic codes. *Finite Fields Appl.* **25** (2014), 79–93.

[53] Z. Zhou, C. Ding, J. Luo, A. Zhang. A family of five-weight cyclic codes and their weight enumerators. *IEEE Trans. Inform. Theory* **59:10** (2013), 6674–6682.

[54] Z. Zhou, A. Zhang, C. Ding, M. Xiong. The weight enumerator of three families of cyclic codes. *IEEE Trans. Inform. Theory* **59:9** (2013), 6002–6009.